VOL 2 (2018) NO 4

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

WLAN Security: Threats and Countermeasures

Suroto #

Department of Information System, Faculty of Engineering, Batam University
E-mail: suroto@univbatam.ac.id

***Abstract*— A wireless local area Network (WLAN) is being widely recognized as a viable cost effective general purpose solution in providing high speed real time access to information. With a WLAN, users can gain access to shared information without being bound to fixed plug-in-point. WLAN transmit and receive data over the air and thus collectively combine data connectivity with ease of mobility. WLAN provides wireless access to multi location enterprises, small and medium enterprises. It can replace wired LAN or simply be used as extension of wired infrastructure. Besides all these advantages WLAN are also facing major problems of security. So security is the aspect where most of the researchers are working. Following are the major objective of our study : i) To study the various Vulnerabilities and attacks on WLAN and their solutions. ii) To study the some of the exiting security methods used for securing WLAN and explore the possibility of improvements in the same. Our conclusion that WLAN security is not easy, and it is constantly changing. They expose the network to a new group of hackers. All businesses need to determine their security requirements based on the application using the WLAN. Goal so that a WLAN is as protected as Wired LAN.**

***Keywords*— WLAN Security, Wireless Security, Wireless Countermeasure, Wireless Threats.**

I. INTRODUCTION

Currently, Wireless LAN (WLAN) is more famous for its cheap price, easy to spread anytime and anywhere. WLAN allows clients to be able to send large files, access the internet and large bandwidth without the need for cables. Fig. 1 shows a example of WLAN.

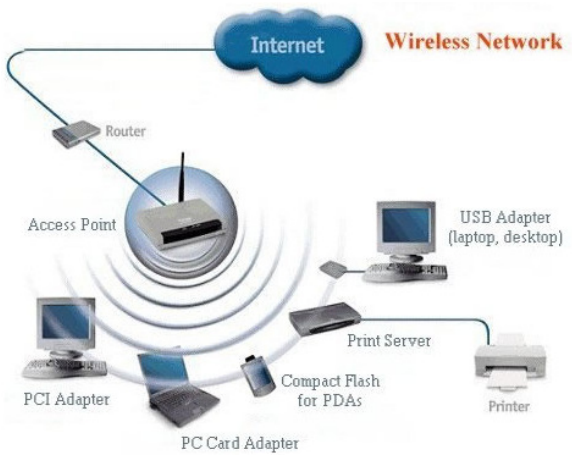

Fig. 1 A Sample of WLAN

Radio Frequency (RF) is used for transmitting data through air. This is the very characteristic in the Wi-Fi technology. Access Point (AP) is considered as very significant feature in the Wi-Fi network technology. Access Point (AP) has a radio transmitter and also a radio receiver. This directly gets linked with the wired network or to the internet network [1].

In addition to all these advantages, WLAN faces security issues, resulting in various WLAN technology standards. In 1997, the IEEE (Institute of Electrical & Electronic Engineer) created the first WLAN standard. This standard is called IEEE 802.11 [2]. The 802.11 standard only supports 2 Mbps bandwidth. The IEEE settled on the shortened "WiFi", in order more companies and consumers interested in the wireless technology. It would be adopted across the board as the universal term to describe a wireless LAN network that multiple users can transmit data to and from simultaneously.

Then in July 1999, IEEE released the 802.11b specification, which supports bandwidth up to 11 Mbps on the 2.4 GHz frequency, comparable to traditional Ethernet. While 802.11b is in development, IEEE creates a second extension to the original 802.11 standard, called 802.11a. The 802.11a standar support bandwidth up to 54 Mbps and the signal in the frequency spectrum is set to around 5 GHz.

This frequency is higher than 802.11b shortening the 802.11a network range.

In 2003, IEEE released the 802.11g specification that supports bandwidth up to 54 Mbps, with a frequency of 2.4 GHz. In 2009, 802.11n was released with support bandwidth uo to 300 Mbps.

In 2009, the IEEE ratified 802.11n with a specification that provides up to 300 Mbps network bandwidth. The 802.11n standard (also sometimes known as "N Wireless") is designed to fix 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas (called MIMO technology) instead of one. In wireless the term "MIMO" referred to the use of multiple antennas at the transmitter and the receiver.

In 2014, the latest generation, 802.11ac, offers bandwidth up to 1300 Mbps on the 5 GHz spectrum and 450 Mbps bands on the 2.4 GHz spectrum.

II. Related Work

Much research has been done in exploring threats, vulnerabilities, attacks and various steps to overcome them. A study of security issue on Wifi was performed by Akshika Aneja [1]. Aneja found that every security protocol has its demerits, until now there is no security protocol which can provide security 100% or near about it. The attack on WLAN was introduced by S.D.Kanawat and P.S. Parihar [9]. Their paper show that network integration model provides workable framework for wireless security concerns and for challenges in the realization of open wireless architecture. The study about a Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX was performed by G. Lackner [4]. Reference [4] conclusions that recent developments in wireless network security are pointing in the right direction. Standards become more and more robust and secure allowing the implementation of critical applications based wireless technologies.

The study of Wireless Security Using Wi-Fi Protected Access 2 (WAP2) was performed by Prastavana and S. Praveen [8]. A. Sari and M. Karay [7] have done a study about Comparative Analysis of Wireless Security Protocols: WEP vs WPA. Reference [7] found out that the WPA2 is more secured in data transmission compared to the preceding protocols, although they all have their shortcomings. D. Bilolikar and S.Y. Gaikwad [6] have perform a study about Spoofing Attackers Using Cluster Analysis in Wireless Network. The security study of the WEP algorithm was performed by Vilas Deotare [10]. Wang, S., Wang, J., Feng, C., & Pan have perform analyzing the vulnerabilities and types of attacks on IEEE 802.11 WLAN[14]. IEEE 802.11 is a wireless network which uses radio to transfer data and hence is most susceptible to the security issues such as WPE/WPA/WPA2 cracking, Denial of Service (DoS), and rouge access points[14].

The organization of this paper is as follows: The way WIFI works in section 3, Security Protocol & Attacks on WLAN in Section 4, How to Work Attack in section 5, Countermeasures are discussed in Section 6, finally Section 7 is their respective conclusions and references.

III. How To Works Wifi

Reference [11] show that the WiFi client goes through five stages to connect to a wireless network: scanning, joining, authentication, Association and Re-association. Scanning is the process of finding a WiFi network that is around. Classical wired networks use cables for the interconnection. In the wireless network, the first thing we need to do is to to identify the appropriate network. The first thing that WiFi clients do is to identify the appropriate network by scanning. After scanning, clients can choose to join one of the available wireless networks (access point).

There are two basic types of wireless networks: BSS (Basic Service Set) and ESS (Extended Service Set). BSS is a wireless network with only one access point. ESS is a larger network made of access points that are connected to the wired network device, such as: a router.

Joining does not guarantee the network access. It is only the first step for the client to be connected to the WLAN network. After joining, the client also needs to pass the authentication and associate stage. In a wireless network, we do not need physical access to the network. The client just needs to be within reach.

The client can connect to the BSS in two ways:

- Manually
- Automatically

In the manual joining the client chooses the BSS manually. In the automatic joining wireless client picks the best access point according to a power level and signal strength. In the both cases, parameters configured on wireless client and access point, need to match.

Wireless authentication is a method of security on a wireless network. In this phase the station is authenticated with the authentication server. The station and the AP have to authenticate mutually in order for the station to escape false access points and for the access points to escape false stations. 802.1x standard uses EAP for different authentication mechanisms. Fig. 2 show a process of client authentication.

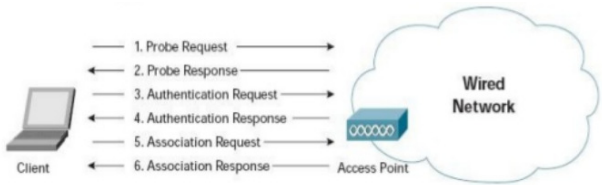

Fig. 2 Client Authentication Process

If the authentication is successful then the client can connect to the destination access point, so that he gets access to wireless network. The security protocol will be explained in the next paragraph. The 802.1x authentication has several advantages [17]:

- Administrators can define users' responsibilities in the network, they do not have to pair manually users' names with MAC addresses,and can easily find mistakes and supervise the network.
- Administrators allow access to the network according to the manufacturer standards.
- An authorized port cannot be compromised by a non-802.1x client.

Association is the process that enables the client the actual access to the WLAN network. It is the same like plugging the cable into the wired network. It is not possible to be associated in more than one access point. Associations can occur only in ESS wireless networks. The client, in this case, associates to another Access Point (AP) in the same ESS. This is triggered when the client detects that the other AP has a strong wireless signal.

The Reassociation can occur only in the ESS wireless network. The client, in this case, associates to the other access point in the same ESS. It is triggered when the client detects that the other access point have a stronger wireless signal.

IV. Security Protocol & Attacks Type On WLAN

Various wireless security protocols were developed to protect our wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own strengths — and weaknesses. In addition to preventing uninvited guests from connecting to our wireless network, wireless security protocols encrypt our private data as it is being transmitted over the airwaves.

Following are descriptions of the WEP, WPA, and WPA2 wireless security protocols:

A. WEP

WEP (Wired Equivalent Privacy) first appeared in 1999. The WEP standard specification supports a 40-bit key length while the non-standard specification provides a 128 and 256-bit key length in data encryption. The secret key used in WEP algorithm is 40-bit long with a 24-bit Initialization Vector (IV) that is concatenated to it for acting as the encryption/decryption key.

WEP2 is a enhancement to WEP was present in some of the early 802.11i drafts. It was implement able on some (not all) hardware not able to handle WPA or WPA2, and extended both the Initialization Vector (IV) and the key values to 128 bits. It was hoped to eliminate the duplicate Initialization Vector (IV) deficiency as well as stop brute force key attacks. After it became clear that the overall WEP algorithm was deficient however (and not just the IV and key sizes) and would require even more fixes, both the WEP2 name and original algorithm were dropped. The two extended key lengths remained in what eventually became WPA's TKIP.

The WEP protocol has some security weakness such as:

- WEP does not prevent forgery of packets.
- WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired and they will be accepted as legitimate.
- WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.
- WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.
- WEP allows an attacker to undetectably modify a message without knowing the encryption key.
- Key management is lack and updating is poor.
- Problem in the RC-4 algorithm.
- Easy forging of authentication messages.

B. WPA

The WPA protocol was introduced in 2003 by the Wi-Fi alliance to try and eliminate or overcome the laps that's in WEP. The main reason for the WPA is to address the cryptography issues in WEP. The WPA provided some good security feature such as WPA Encryption Process, WPA Authentication Mechanisms which includes; WPA-Personal or WPA-PSK, WPA-Enterprise [1]. Most current WPA implementations use a preshared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

WPA has two variants: AES and TKIP. AES (Advanced Encryption Standards) is a stronger encryption scheme than RC4, the encryption scheme in WEP. TKIP makes use of the RC4 algorithm for encryption and hence is backward compatible with the WEP hardware. WPA2 made further changes to WPA by making AES encryption mandatory and using CCMP in place of MIC for integrity check [15].

WPA Pre-Shared key is static and it is used in initiating communication between two users. The static key is a Pairwise Master Key (PMK) in TKIP must be ready before an association can be set. In the WPA-PSK, an authentication server is not required because it is most suitable for small office or home networks. A 256-bit key is used for authentication of devices and a 64-bit MIC key and a 128-bit key is created from the pre-shared key for data encryption.

The WPA-Enterprise: This is basically designed for enterprise networks, where the EAP provides a stronger authentication method. The Remote Authentication Dial in User Service (RADIUS) is essential for providing excellent security for wireless network. The RADIUS server checks that the information is correct using the authentication scheme Extensible Authentication Protocol (EAP) to process the information. RADIUS is the de facto standard for authentication and other protocols are rarely used. A RADIUS server can be used for different internet connections other than dial-up [15].

C. WPA2.

WEP was officially replaced by WPA in 2004, which in turn was later replaced by WPA2. WPA2 replaces the original WPA technology since 2006 and becomes the technology standard for current data encryption [4]. WPA2 uses AES algorithm for encryption which is stronger than TKIP. AES in combination with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) provide high level security to WLAN. The CCMP algorithm creates message integrity code (MIC) to protect data integrity. WPA2 supports both Enterprise mode and Personal mode. WPA2 Personal uses a set of password. WPA2 Enterprise uses EAP and a RADIUS server for centralized client authentication using multiple authentication methods such as token cards, Kerberos, and certificates [16].

Attacks can be classified into four broad categories, namely snooping, modification, masquerading, and denial of

service[12]. In practice, attacks can use some of these approaches.

A. Snooping

Snooping is accessing personal information. This information can be used for a profit, such as getting company secrets to help our own business. Snooping is also known as "foot-printing" or "information gathering".

Foot-printing activity is able to doing by a tool, such as nmap, google dork, maltego, etc. They is powerful tool can be used to glean infrastructural and personal information about a target. Examples of infrastructural information that it accesses are DNS records, DNS to IP mappings, WhoIS records, name servers etc. As for personal information, it's able to harvest email addresses, social profiles, websites, telephone numbers and display relationships between them.

B. Modification

After an attacker has read data from a target, the next step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. For example, an attacker modifies e-mails with malicious content or alters numbers in an electronic bank transfer. Another example, if we can intercept the wireless transmission and change the destination address field of the message, we may cause the message to be forwarded to we, not to the intended recipient.

C. Masquerading

Masquerading is a term used when a network device attack mimics a valid device. If the device can successfully deceive the target network until it validates as a legitimate device, the attacker gets all the permissions and is not detected.

The intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

D. Denial of Service

DoS attacks are attacks to prevent network operation. This attack is done by sending a large number of packets to the target server. For example, DoS attacks are distributed against multiple websites. Attacks blocked access to the site for hours. This attack comes from thousands of computers that are controlled remotely around the world. The attackers use these "zombie" computers to generate large amounts of traffic directed to their victims, preventing them from serving valid requests. There are several types of DoS attack which are described below:

Radio frequency (RF) Jamming: An 802.11 network operates in the unlicensed 2.4 GHz and 5 GHz frequency band. In this type of attack, the attacker jams the WLAN frequency with a strong radio signal which renders access points useless. As a result, legitimate users cannot access the WLAN.

802.11 Associate/Authentication Flood: In this type DoS attack, an attacker sends thousands of authentication/association packets from MAC addresses in order to fill up the target AP's association table. This makes it harder for a legitimate user to gain access in the network.

802.11 De-authentication & Disassociation: The attacker pretends to be a client or AP and sends unauthorized management frames by flooding thousands of deauthentication messages or disassociation messages to the legitimate target. This forces them to exit the authentication state or to exit the association state.

V. How to Work Attack

As explained above, there are several categories of attack types that can be done on WLAN. The author will discuss the case separately: first, the attack on the network without a key, and second, the attack to reveal the key itself [5].

A. Attack Without Keys

The first thing an attacker does is Snooping. Attackers have Wi-Fi cards designed to intercept data. It usually involves Ethernet capture software. There are a number of freely available software that can be used e.g. Netstumbler, Kismet etc.

First of all, the attacker will be able to see and read all the information coming from an Access Point. Therefore, the attacker knows the name of the network (or SSID). Attackers can identify the manufacturer of Access Point by looking at the MAC address, and may even know the model number. If the model has a hidden weakness, then it is information that may be useful.

Attackers can also see the data bits that go to and from the access point. Attackers can also calculate how many wireless devices are connected to each access point. In this case, the attacker uses a technique called *Traffic Analysis*. Traffic analysis is the study of external messages, for example, frequency of communication and size. The attacker should be able to identify the protocol they are using by checking the length of the packet. For example, certain TCP/IP messages, such as acknowledgment frames that have a fixed length. Thus, the overall network activity has been acquired by the traffic analysis attack

This information is combined with other information obtained from other methods or sources. One of them is the combination of snooping and modification. Modification can be done with an attack, known as *Man-in-the-Middle Attack*. Suppose two people are communicating. We call Sandra and John. Sandra received a message from John and John received from Sandra. Suppose there is an attacker can intercept and cut off communication. Suppose an attacker can imitate John when sending to Sandra and imitating Sandra when sending to John.

B. Attacks On Keys

Most access points use a single key or password that is shared with all connecting devices on the wireless LANs. A brute force attack can be applied on sniffing packets captured by the attacker in order to obtain the key. The simplest way to get a key is to see someone as he enters the password. One solution is to keep the key inside the computer. The problem with this approach is that, if the computer is stolen, the key is inside and the thief can gain access by masquerading as a user. The problem for the attacker is that the data is encrypted. What to do next? First,

let's look at some assumptions about what the attacker knows. To do this, we need to recognize some common terms:

- **Plain-text:** The data before this encryption is what we want to protect.
- **Cipher-text**: An encrypted version that enemies can see through radio links.
- **Key:** The secret value used to encrypt / decrypt a message.
- **Cipher**: Algorithms and rules used to perform encryption and decryption.

To summarize, cipher-text is made by plain-text processing with cipher suite using the button, as shown in Fig. 2. We assume that the attacker has a copy of the cipher-text because it taps directly and does not know the key. Here, the attacker must know the algorithm (cipher) used for encryption Most the attack methods are finding the weakness of the algorithm.

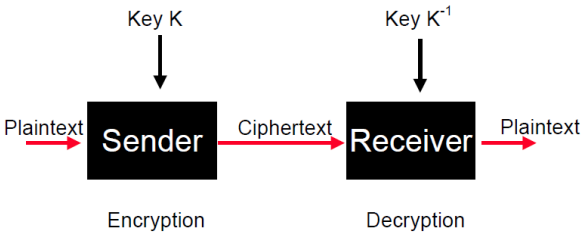

Fig. 3 Diagram of Encryption and Decryption Process

After the attacker knows the cipher-text and the cipher, the next attempt is to convert it into a plain-text form for the message to be read (decrypt it). Many websites offer decrypt services on-line. But if through the on-line web can not be done, then the other way is to get the key. There are several ways for an attacker to get a sample of plain-text.

The first way has been mentioned: the protocol header. In IEEE 802.11, the MAC header is not encrypted. If we are using protocols such as TCP/IP, this means that the header section of TCP/IP message is part of the plain-text that is converted to cipher-text. The danger is that headers always happen in the same place (at the beginning of the package) and that some fields have a fixed value.

The second way, if someone accesses the website, and the attacker can guess which website, he can get plain-text just by going to the same site. Homepage is downloaded and sends encryption via wireless link. If an attacker can guess correctly which frame has plain-text and cipher-text.

The final way to get plain-text is by sending an e-mail. Attackers have the opportunity to identify when long messages are read. Or, an e-mail that persuades a user to click a link to a web page from an attacker's website.

As soon as the attacker has all three, cipher-text, plain-text, and cipher. they can start attacks on keys. Some methods of attack on this key, namely Brute Force, Dictionary Attacks and Algorithmic Attacks.

1) *Brute Force:* The brute force method means that an attacker tries every possible key until attacker find a match. The attacker will sooner or later find the right key, as he tries all possible key combinations. The time taken for a brute force attack depends on the size of the key. For example, authentication method of IEEE 802.11 WEP uses a 40-bit key. To break the 40-bit key using brute force, we should try 2^39 times, (550 billion different keys). That's a huge amount, but it's not impossible. A supercomputer that can perform one test per microsecond, can crack keys in about a week. Because 40-bit keys can be solved, many security systems use larger keys. Some manufacturers of IEEE 802.11 WLAN systems use a 104-bit key. The key length is finally adopted as the official standard.

2) *Dictionary Attack:* Attackers try only a few keys that users tend to use. For example, an attacker can assume that the key consists of only letters. This approach reduces the number of keys. This idea calls Dictionary Attacks [3]. In Dictionary Attacks, an attacker uses a large dictionary, or database, which contains all possible passwords. This will certainly include every word in English and may contain other languages as well. Creation of such a database may seem like a tough task. Little by little hackers add data to the dictionary. Of course, eventually there will be millions of entries in the dictionary. However this work can be done with the help of password generator program. The availability of the dictionary attacks explains why security managers want users to specify passwords that use both uppercase and lowercase letters and to include numbers or other strange characters.

3) *Algorithmic Attacks:* If the enemy can not do brute force or dictionary attack, another approach is to try to solve the algorithm. Attackers try to find defects in the way of encryption. It is difficult to describe algorithmic attacks because they are heavily dependent on the algorithm and understand its weakness. This method is usually done by a cryptographer.

VI. Countermeasures Against Threats

The nature of wireless communication creates three basic threats: Interception, Alteration and Disruption. Here are some security solutions to deal with security attacks mentioned above.

A. Securing Wireless Network

Here are some ideas for securing a wireless network.

1) *Use of firewall technology:* A firewall checks the data packet and then decides to reject, accept or forward. A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

2) *Use of encryption and decryption technology:* Most wireless devices have built-in encryption and decryption mechanisms. Turn on WPA2 encryption on our wireless access point (WAP). In this technique, plain text is encrypted using encryption technology and again decrypts at the destination (receiver), so a message can be sent safely from source to destination.

3) *Disable SSID broadcast:* Many wireless devices have a mechanism called a broadcast ID. This mechanism allows an AP to transmit a signal to each device around it. In order to intercept the wireless transmission, first, the attacker

identifies and finds the wireless network. So make sure that the broadcast ID is turned off.

4) *Do not access public hot spots:* Many cafes, hotels, airports and other public places offer us access to its wireless network. However there are some networks to hack our system and access the information we send.

5) *Reduces AP signal strength:* The AP Signal be reduced but it still provides the required coverage. minimizing the opportunity for outsiders to access WLAN. Physically locate the AP in an area that limits its radio emanations.

B. Prevent Changes from Caught Communications

Interception and changes in wireless transmission is a form of attack in the middle man. Strong encryption and strong authentication on devices and users can reduce those risks.

C. Protecting Confidentiality

This action is an attempt to reduce the risk of 'eavesdropping' wireless transmission. A method to make it more difficult to find and intercept the wireless signal.

D. Securing Access Point

The actions to secure the wireless access point are as follows:

1) Authentication: Using the authentication methods available to authenticate all connected devices. Create a really long wireless network password (Pre-Shared Key). In conjunction with creating a strong network name that isn't on the list of the most common SSIDs, we should choose a strong password for our pre-shared key.

A shorter length password is more likely to be cracked than a longer one. Longer passwords are better because the Rainbow Tables that are used to crack passwords aren't practical after we exceed a certain length of password due to storage limitations.

Consider setting our wireless network's password to a length of 16 or more characters. We have plenty of room to get creative with our Pre-shared Key as the maximum password length for WPA2-PSK is 64 characters. Moreover, larger organisations should consider using certificate-based authentication mechanism or RADIUS, allowing the users to access their own managed credentials in order to protect their network from sharing.

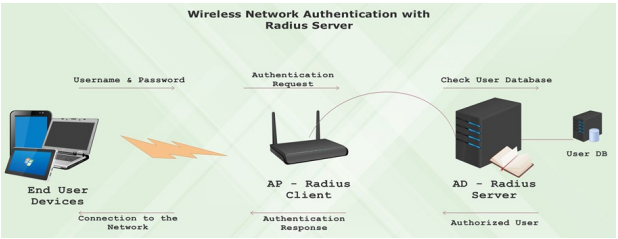

Fig. 4 Wireless Network Authentication with RADIUS Server

2) Secure configuration of Access Point: Secure configuration of AP is ensuring that all wireless APs are configured securely. All default settings need to be changed. Here are some configurations that can be changed:

First, MAC Address Filtering is Enabled. Every device that connects to a network has a unique hardware address called a MAC address (Media Access Control). We can identify our wireless clients by their unique MAC address. So, by creating a list of unique MAC addresses we can restrict what PCs can connect to the AP. This is called MAC address filtering. If a PC with an unknown MAC address tries to connect, it will not be able to associate with the AP and thus will not be allowed to connect.

Second, change the AP's Default Admin Password. Create a strong password for Admin account. Password combination letter, numerics, special character.

Third, Disable DHCP. Instead, assign static IP addresses for every wireless client.

E. Reduce The Risk Of Denial-Of-Service Attacks

Some steps to reduce the risk of Denial Of Service (DoS) attacks, that is:

First, Doing routine audits. Routine audit on wireless network activity and performance can identify problems. Penetration test using a tool, such as: Aircrack-ng, Airsnort, etc.

Second, create a demilitarized zone (DMZ) subnet. A De-Militarized Zone (DMZ) is a special local network configuration designed to improve security by segregating computers on each side of a firewall.

A DMZ divides splits such a network into two parts by taking one or more devices inside the firewall and moving them to the outside. This configuration better protects the inside devices from possible attacks by the outside (and vice versa). By placing a DMZ on the network between the router and the external firewall, it can protect the LAN.

Virtual Local Area Networks (VLAN) are another technology that can be used in corporate wireless network to enforce a security policy. VLANs work by tagging LAN frames assigned to different workgroups. Those tags actually decide where incoming frames can and cannot go within the corporate network. For example, if a business provides guest and consultant access, all traffic coming from that wireless LAN will be tagged so that traffic is limited to the public internet thus, keeping them away from corporate data and services.

Finally, Installing an Intrusion Detection System (IDS). An Intrusion detection system (IDS) is software and/or hardware deliberate to detect surplus attempts at accessing, manipulating, and/or disabling of computer largely throughout a network, such as the Internet. An intrusion detection system is created to become aware of quite a few types of malicious behaviours that can negotiate the safety and faith of a computer system. This includes network attacks alongside susceptible services, data driven attacks on applications [19].

An Intrusion Detection System monitors the network traffic and monitors for suspicious activity and alerts the System Administrator. In some cases, the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in

different ways [13]. Thus intrusion prevention systems should be there to prevent subsequent failures due to intrusion.

VII. CONCLUSIONS

A Wireless network are different from wired network. Communication over the air leaves them vulnerable to various attacks. WLAN security is not straightforward or easy, and keeps changing. They expose the network to a new group of hackers because the WLAN is working on Over The Air (OTA). Given the security flaws of the 802.11 standard, all businesses need to define their security requirements based on applications using WLAN. In this case we have covered all the security issues and solutions to issues so that WLAN is protected like Wired LAN. This paper gives an analyses on threats and countermeasures for their prevention. This paper will inspire the next generation researcher to overcome the problems with the existing architecture.

ACKNOWLEDGMENT

The author would like to thank Faculty of Technology, Batam University for permits to use Laboratory of Computer and Internet connection when write this paper.

REFERENCES

[1] A. Aneja, G. Sodhi, "A Study of Security Issues Related With Wireless Fidelity (WI-FI)", *International Journal of Computer Science Trends and Technology (IJCST),* vol. 4 Issue 2, pp. 346-350, April 2016.

[2] C. Beard and W. Stallings. *Wireless Communication Networks and Systems.* London, England: Pearson, 2016.

[3] D.D. Coleman, D.A. Westcott and B.E. Harkins. *CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205*, 2nd Edition. New Jersey, US: Wiley Publishing, 2016.

[4] G. Lackner, "A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX", *International Journal of Network Security*, Vol.15, No.6, pp.420-436, November 2013.

[5] J. Edney and W.A. Arbaugh. *Real 802.11 Security*. Massachusets, USA: Addison Wesley, 2004.

[6] D. Bilolikar and S.Y. Gaikwad, "Spoofing Attackers Using Cluster Analysis in Wireless Network", *International Journal of Innovative Research in Computer and Communication Engineering,* Vol. 3, Issue 4, April 2015.

[7] A. Sari, and M. Karay. "Comparative Analysis of Wireless Security Protocols: WEP vs WPA". *International Journal Communications, Network and System Sciences,* Vol.08 No.12, pp. 483-491, December 2015.

[8] M. Prastavana and S. Praveen. "Wireless Security Using Wi-Fi Protected Access 2 (WPA2)". *International Journal of Scientific Engineering and Applied Science (IJSEAS)* ,Vol 2, Issue-1, pp. 374-382, January 2016.

[9] S.D.Kanawat and P.S. Parihar, "Attacks in Wireless Networks", *International Journal of Smart Sensors and Adhoc Networks (IJSSAN)*, vol. 1 Issue 1, pp. 113-116, May 2011.

[10] V. Deotare, S. Wani and S. Shelke. "Wired Equivalent Security Algorithm for Wireless LAN", *International Journal of Emerging Technology and Advanced Engineering.* Vol. 4 Issue 3, pp. 66-69, March 2014

[11] I. Bartolic (2017) on thebestwirelessinternet.com, [Online]. Available:http://thebestwirelessinternet.com/how-wlan-works.html

[12] (2017) the etutorials website. [Online]. Available:http://etutorial.org.

[13] B. Tony (2018). on Lifewire. [Online]. Available:https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799.

[14] Wang, S., Wang, J., Feng, C., & Pan, Z.. "Wireless Network Penetration Testing and Security Auditing", 2016, *ITM Web of Conferences*, 7, 03001

[15] Bhatia V. et al. "Security And Vulnerability Analysis Of Wireless Networks". *International Journal of Neural Networks,* Vol. 2, Issue 1, pp. 10-13, November 2012

[16] A. I. Angela, "Evaluation of Enhanced Security Solutions in 802.11-Based Networks", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.4, pp. 29-42, July 2014

[17] S. Malgaonkar, et al, "Research on Wi-Fi Security Protocols", *International Journal of Computer Applications (0975 – 8887),* Vol.164, No 3, pp. 30-36, April 2017

[18] Md. Waliullah, Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", *International Journal of Advanced Computer Science and Applications*, Vol. 5, No. 1, pp.176-13, 2014

[19] T. Habib Sardar, Z. Ansari, A. Khan, "A Methodology for Wireless Intrusion Detection System ", *International Journal of Computer Applications* (0975 – 8887), pp. 12-15, 2014