IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 67-75
www.iosrjournals.org

WLAN Security Issues and Solutions

Deepika Dhiman[1]

[1]*(Central University of Punjab, Bathinda, India)*

Abstract: *Wireless network is widely used in many sectors due to ease of installation, flexibility, mobility, reduced cost-of-ownership, and scalability. Wi- Fi network can be accessed with laptops, mobile phones, cameras, game consoles and many other increasing numbers of consumer electronic gadgets. Wireless Local Area Network (WLAN) technology has changed the way people communicate and share information by eliminating the boundaries of distance and location. However, WLAN have some security threats- Denial of Service, Spoofing, Eavesdropping, Man-In-The-Middle etc. In this report, we will discuss about the various WLAN (IEEE 802.11) security standards – WEP, WPA, WPA2 (IEEE 802.11i – 802.1x, PPP and EAP). The solutions /products to prevent wireless networks from the described threats have also been brought to limelight for current and future WLAN security.*

Keywords: *IEEE 802.11, IEEE 802.1x, Wireless LAN, WEP,WPA, SSID, MAC.*

I. INTRODUCTION

A wireless local area network is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, IEEE 802.11 was implemented as the first WLAN standard based on radio technology [7].Till date, following WLAN standards have been developed:

TABLE 1: WLAN standards

Standard	Data rate	Frequency	Modulation	Range	Date of release
802.11a	54 Mbps	5GHz	OFDM	35-120 m	Sep 1999
802.11b	11 Mbps	2.4 GHz	DSSS	35-140 m	Sep 1999
802.11g	54 Mbps	2.4GHz	OFDM,DSSS	38-140 m	June 2003
802.11n	150 Mbps	2.4-5 GHz	OFDM	70-250 m	Oct 2009
802.11ac	867 Mbps	5 GHz	OFDM	------	Dec 2012

802.11 ad is supposed to be implemented by February 2014."Wi-Fi" is being misunderstood as a short term for "wireless fidelity." However, Wi-Fi is simply a trademarked term meaning IEEE 802.11x. The Wi-Fi alliance, the organization that owns the Wi-Fi (registered trade mark) term specifically defines Wi-Fi as "any wireless local area network (WLAN) products that are based on the IEEE 802.11 standards." [19].

1.1. WLAN Components

There are two basic components of WLAN [6][7]:

- Access points

The hub of wireless local area network (AP) helps in exchange of information with other wireless devices by the means of antenna. It uses 802.11 standard specified modulation techniques working within specific frequency spectrum.

- Network Interface Cards/client adapters

The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client.

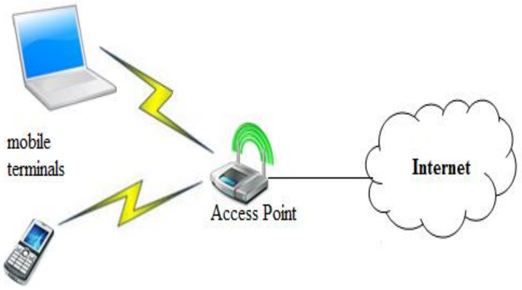

Fig.1. Components of WLAN

II. WLAN SECURITY THREATS

Despite the productivity, convenience and cost advantage that WLAN offers, the radio waves used in wireless networks create a risk where the network can be hacked. Reconnaissance is the first thing hackers do before attacking the WLAN. There are many security threats and attacks that damage the security of WLANs such as [1]:

2.1. Attack on Service Set Identifier

Service Set Identifier (SSID) is the name given to a certain WLAN by AP to identify a network as a way to distinguish between different networks can have up to 32 characters [25]. If the SSID provided by the user and provided by the AP's SSID is inconsistent, then the AP refuse to directly access it through a wireless service area. Hence, SSID provide the password authentication mechanism shielding the access of illegal users to ensure the security of wireless local area network. It works in two modes [13]-

- In the open mode, the SSID of the AP is broadcast to the world. A client may also send a probe request frame to find an AP with a particular SSID. Network beacon sniffers such as NetStumbler3 can be used to find such networks.
- In the closed mode, SSID remains hidden. Closed mode WLANs do not respond to messages unless they contain the correct SSID in the message headers. All devices connecting to a particular WLAN must be configured with the same SSID.

Another default configuration in APs is that Dynamic Host Configuration Protocol is ON so users can obtain IP addresses automatically and hence access the WLAN easily. SSID broadcasting is usually out by the AP. Taking into account security, we can ban AP broadcast SSID number, but that the wireless base station must take the initiative to send the correct SSID number to associate with the AP [1].

2.2. MAC spoofing and session hijacking

Each wireless card has a unique MAC address- physical address used to prevent unauthorized users access. Adding Access Control (Access Control List) based on the physical address to the AP, to ensure that only the physical address of the registered card to enter the network. So we can manually maintain the AP through a group of the physical address access list to achieve physical address filtering [6]. The approach is used to deny access to the wireless network if the MAC address of an authenticating client doesn't match with the list of authorized MAC addresses. This makes it harder for a hacker to access your network with a random MAC Address. However, the physical address of IP packets can be forged, so this is less secure authorization certification. Physical address filtering solution is hardware certification rather than user authentication [6] [22]. But it has some shortcomings- it requires a physical address in the list of AP to update and is manual. MAC addresses are sent in clear when a communication between STAs and AP takes place. This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. Once the address information is gathered, it can easily be spoofed by manually inputting another MAC address in the network settings [25]. This happens because 802.11 networks do not authenticate the source address, which is MAC address of the frames. Attackers may therefore spoof MAC addresses and hijack the session [7]. Moreover, 802.11 doesnot require an Access Point to prove it is actually an AP. This facilitates attackers who may masquerade as AP's. Even network addresses can easily be captured from legitimate wireless traffic using packet monitoring tools such as Ethereal or Kismet to generate a database of legitimate wireless stations and MAC addresses [1].

2.3. Information Disclosure (Attack on WEP)

Wired Equivalent Privacy (WEP) is a security protocol based on encryption algorithm called "RC4" which generates a key which is XORed with the plaintext to form cipher text [1][6]. At the same time, the key stream are sent out with the initial vector start RC4 IV. Receiver can obtain the original plaintext data through the XOR operation between the received data and key. This approach has certain security vulnerabilities. Plaintext can be inferred by intercepting multiple sets of data. The two cipher text XOR operation can be launched to do the XOR of two clear results.

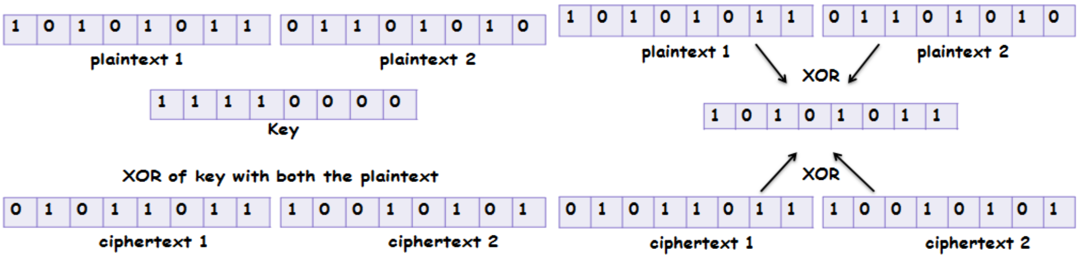

Fig.2. XOR operation for WEP cracking

Hence, after a period of monitoring, according to the monitoring results can be constructed one dictionary, which contains the IV, key stream, so that all the intercepted data can be parsed out.Tools like Airsnarf, WEPCrack, AirCrack, AirSnort are used in conjunction with software like Void11 to cause “auth” and “deauth” flood attacks. This WEP is easily vulnerable to attacks due to this usage of XOR operation, small IV and short RC4 encryption key.

2.4. Signal interference

Wireless LAN radio frequency radio waves have a fixed frequency usually 2.4GHZ. When the wireless router is next to such a device is operating, a wireless user communications may be affected, as wireless AP and the base station over the same channel may be a signal for the confusion. In addition, if there is bulky obstacle between the wireless base station and AP, it can lead to reduced access rate or disconnected. On the same floor, when there are multiple wireless routers working simultaneously in the same frequency transmit the signal, then also it causes interference [6].

2.5. Eavesdropping

This involves attack against the confidentiality of the data that is being transmitted across the network. Wireless LANs radiate network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. Hence, eavesdropping by the third parties enables the attacker to intercept the transmission over the air from a distance [7].

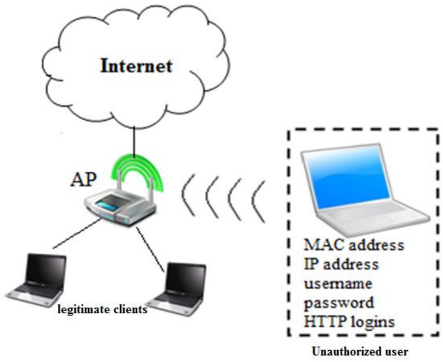

Fig.3. Eavesdropping in WLAN

2.6. Senior attack

Once the attacker penetrated the wireless LAN, wireless LAN will serve as a springboard for further invasion of other network. General network is equipped with Secure Shell but the internal of the shell is very fragile. Wireless networks can be easily involved in the core network through a simple configuration once the wireless local area network is compromised; the entire network is equivalent to exposure in front of the attacker. As wireless LAN are less secure, more vulnerable to attack. Therefore, companies often put the wireless LAN outside the security shell of the core network. So even if the wireless LAN was attacked, the core network can be made more secure [6].

2.7. Man-In-The-Middle attack

An illicit STA intercepts the communication between the legitimate STA and AP. The illegal STA fools the AP and pretends to be legitimate STA. On the other hand, it also fools the other end STA and pretends to be trusted AP. Hence, the fake AP turns into an “Evil Twin”. Once the unknowing user has been connected to an evil twin, hacker can intercept transmitted data. Users just log into evil twin with bogus log-in prompts, hence passing sensitive data like username and password or unknowingly installing viruses, worms and keyloggers. The best example of this attack is of an IT Conference when Spencer Parker, a director of technical solutions at AirDefense whose computer was infected by MITM [14].

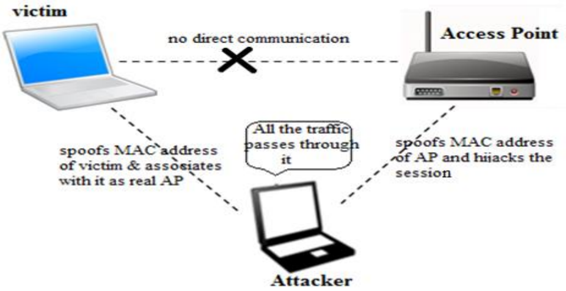
victim
no direct communication
Access Point
All the traffic passes through it
spoofs MAC address of victim & associates with it as real AP
spoofs MAC address of AP and hiiacks the session
Attacker

Fig.4. Man-in-the middle attack

2.8. Denial of service

Denial of service result in the inability of users or systems to access needed resources. They are launched specifically against WLAN networks at Layer 1/Physical layer and Layer 2/Data Link Layer [23].

Layer 1 or Physical layer attack or RF jamming attack:

When the intentional radiators put out the RF energy at the power levels they support, it drowns out the RF energy being transmitted by valid STAs on the WLAN. Since the device (called a signal generator) puts out a signal that drowns out the signals of the WLAN, it effectively causes a DoS scenario.

Layer 2 attack:

Itis launched by exploiting the processes used for frame management and network communications in a WLAN. For example, an attacker may spoof a deauthentication frame. This means that the attacker generates a frame on the WM that uses (spoofs) the MAC address of the AP, and the frame generated is a deauthentication or disassociation frame. These frames are management frames and, more specifically, notification frames. They cannot be ignored by the client STAs so the client stations will be denied access to the WLAN as long as the attacker continues to transmit the spoofed disassociation or deauthentication frames.

DoS attack at layer2 scenario [23]:

a) The attacker starts his own AP through software running on his computer.
b) The attacker configures his AP to use the same SSID as the WLAN to which the victim is currently associated.
c) The attacker sends a deauthentication frame (or turns on a high−powered RF signal generator causing interference that results in the victim needing to re-associate) forcing the victim to look for a new AP with which to associate.
d) Since the attacker's AP is closer and provides a stronger signal, the victim associates with the attacker's AP. The user of the machine doesn’t even realize that he is no longer associated with the valid AP.

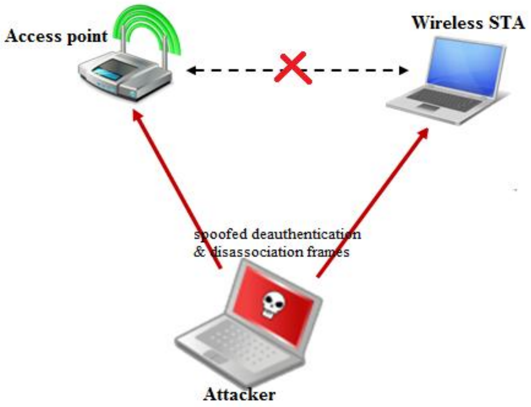

Fig.5. DoS scenario at layer 2

2.9. ROGUE ACCESS POINTS

In normal situations, AP authenticates STAs to grant access to the WLAN. The AP is never asked for authentication, this raises a security concern, what if the AP is installed without IT center's awareness? These APs are called "Rogue APs" and they form a security hole in the network. An attacker can install a Rogue AP with security features disabled causing a mass security threat [1]. Technologies like IEEE802.1x can be used to overcome this problem. Network security administrators can discover Rogue APs by using wireless analyzing tools to search and audit the network.

2.10. AP's coverage

The signals broadcasted by the AP can propagate outside the perimeter of a room or a building, where an AP is placed, allowing users who are not physically in the building to gain access to the network. Attackers use special equipments and sniffing tools to find available WLANs and eavesdrop live communications while driving a car or roaming around CBD areas. Because RF signals obey no boundaries, attackers outside a building can receive such signals and launch attacks on the WLAN. This kind of attack is called "war driving"[1]. NetStumbler is a publicly available tool used for war driving.

Hobbyists also chalk buildings to indicate that signals are broadcasted from the building so that WLAN in it can be easily accessed. This marking is called "war chalking" [1]. The information about the speed of the connection and whether the authentication scheme used is open or shared keys are mentioned in the form of special codes agreed upon between war-chalkers.

2.11. Physical placement of APs

The installation location of APs is another security issue because placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs.

III. STANDARDS FOR WLAN SECURITY

In order to prevent and protect against these attacks, several security techniques and protocols have been introduced.

3.1. Wired Equivalent Privacy

Wired equivalent privacy, developed in 1997, is a user authentication and data encryption which uses a pre-established shared secret key called the base key, the RC4 stream cipher encryption algorithm and the CRC-32 checksum as its building blocks [1].

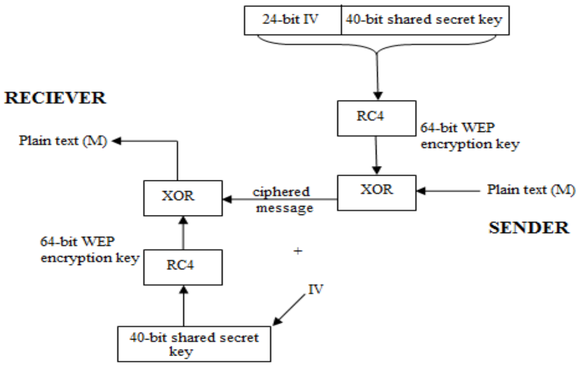

Fig.6. Schematics of WEP protocol

WEP failed theoretically and practically because of following reasons -

- The input key of RC4 is composed of 24bit IV and 40 bit WEP key. The IV is used to guarantee that the same plaintext will never generate the same cipher text. But many wireless cards reset the IV to 0, each time a card is initialized, and increment the IV by 1 with each packet. Because of the invariance of WEP key the data will be encrypted with the same key stream. The IV is also sent in plain text which allows an attacker to create a WEP key combination database or dictionary that can then be used to either inject or decode packets [25].
- The cipher text (C) is generated from a simple XOR operation between the WEP encryption key (K) and the plain text message (M). The result of XORing two cipher text messages is equal to the result obtained by XORing two plain text messages. If one of the plain text messages is known, or at least parts of it, finding the WEP encryption key will becomes trivial [1].
- Since, the IV is only 24 bits, it only provides 224 combinations and offers the possibility of having duplicate IV's in a relatively short time. We can easily finger out that how much time will generate one repeat IV (Ye & Yue, 2010). For example- An AP sends 1500 byte packets at 11 Mbps, and the time is about 1500*8/(11*10^6)*2^24=18000 seconds, which is about 5 hours.
- In 802.11, the use of WEP is optional as it has to be manually configured. WEP enables the AP to confirm the identity of the mobile client. However, the mobile client does not confirm the identity of the AP. An attacker could use this one-way authentication process to their advantage by masquerading as the AP, authenticating clients and redirecting traffic destined for the AP [13].
- RC4, a stream key algorithm to encrypt the plaintext or decrypt the cipher text, is composed of key schedule algorithm and pseudo-random generation algorithm. In KSA process, the WEP key is changed to a state array‘s’ with hundreds of plus and swap operation. The process of PRGA generates a pseudo-random stream. RC4 algorithm is vulnerable in the aspect that every 256 keys or less produce one weak key. This is called “invariance weakness” [25]. These weak keys will result in the pseudo-random having the specific and recognizant prefix. Their relativity with the key will become low, hence the data encrypted with these weak keys will become breakable.
- WEP's implementation of the Cyclic Redundancy Check algorithm also contributes in compromising data integrity. The checksum created is a non-cryptographic value referred as known attacks such as side-channel attacks [18].

WEPCrack, AirSnort, AirCrack etc. are some of the tools working on above mentioned flaws used for breaking the WEP key. To overcome these flaws in WEP, IEEE 802.11 Task group 1 introduces WPA security structure in 2003.

3.2. Wi-Fi Protected Access

WPA security protocol operates in two modes [19] - personal mode and enterprise mode. Personal mode makes use of pre-shared key (PSK) for authentication but provides less security than enterprise mode which works on IEEE 802.1x protocol and EAP for mutual authentication. PSK mode uses "Temporal Key Integrity Protocol"(an encryption method) which is a WEP patch with three new elements: message integrity code (MIC) named Michael, packet sequencing procedure and per packet key mixing function [13].

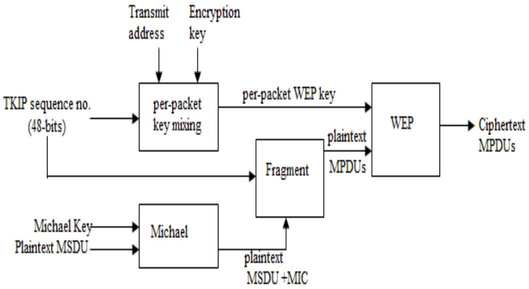

Fig.7. Flow of TKIP processing

For mutual authentication and efficient key exchange mechanism between clients and servers,a port-based network access control protocol "IEEE 802.1x" [7] is used. It is based on three network elements [2][13]:

a) Supplicant is the wireless station which tries to access the network or the client that requires authentication onto the network. e.g.- mobile node.
b) Authenticatoris a mediating device between the client and the network that provides network access. It is a network access node which allows STAs to access the network. e.g. - network accesses server, access point.
c) Authentication serveridentifies the supplicant, checks its credentials, and defines privileges and restrictions and allows or denies its access to the network and services. e.g. - RADIUS, DIAMETER.

In addition to these, "Port Access Entity" is the protocol entity associated with a port supporting the functionality of Authenticator, Supplicant or both.

IEEE802.1x uses Extensible Authentication Protocol (EAP) messages to handle authentication requests and replies. EAP messages travelling between supplicants and the authenticator in wired or wireless LAN environment are encapsulated in an encapsulation technique called EAP over LAN or EAPoL[7].

Weakness of WPA

- WPA is based on RC4 encryption which is weak [1], hence is vulnerable to denial of service attack.
- WPA affects the overall network performance due to heavy cryptographic computations per packet, hence causing larger overheads [22].
- The biggest issue is being incompatibility with legacy hardware and older operating systems such as Windows 95.
- MIC value and EAPoL message are sent in plaintext form, hence the attacker focuses on MIC hash value [13].
- TKIP used in WPA is a short term solution [6] as it is achieved by hardware shipped with current APs and wireless interface cards.

Hence, for better security new protocol was designed- WPA2 or IEEE 802.11i.

3.3. WPA2/IEEE 802.11i

To solve the roots of the problems in WEP and TKIP, IEEE specified a new standard WPA2/IEEE 802.11i in July 2004 that provides enhanced security as well as support to legacy protocols for backward compatibility. RSN IEEE802.11i defines the concept of Robust Security Network (RSN). According to IEEE802.11i, RSN is the description of the network that can establish an RSN Association (RSNA) between its entities [1]. RSNA equipments use pre-RSNA security framework which includes authentication and encryption protocols like shared key authentication and WEP encryption protocol to communicate with pre-RSNA equipment. RSNA equipments use RSNA security framework which includes two encryption protocols, Counter mode with CBC-MAC protocol (CCMP) and TKIP as well as enhanced authentication protocol based on IEEE802.1x and advanced key management algorithm called the 4-way handshake when it communicates with RSNA equipment [2].

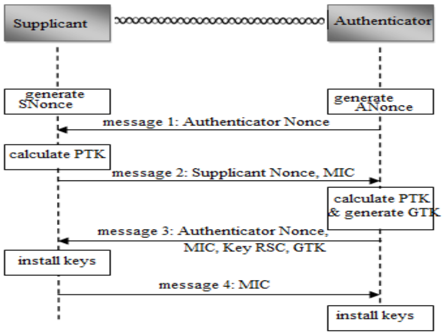
Supplicant
Authenticator
generate SNonce
generate ANonce
message 1: Authenticator Nonce
calculate PTK
message 2: Supplicant Nonce, MIC
calculate PTK & generate GTK
message 3: Authenticator Nonce, MIC, Key RSC, GTK
install keys
message 4: MIC
install keys

Fig.8. 4-way Handshake mechanism

WPA2 vulnerabilities:

- "Hole196" is a vulnerability in the WPA2 security protocol exposing WPA2-secured Wi-Fi networks to insider attacks [9]. Central to this vulnerability is the group temporal key (GTK) that is shared among all authorized clients in a WPA2 network. In the standard behavior, only an AP is supposed to transmit group-addressed data traffic encrypted using the GTK and clients are supposed to decrypt that traffic using the GTK. However, nothing in the standard stops a malicious authorized client from injecting spoofed GTK-encrypted packets. Exploiting the vulnerability, an insider can sniff, decrypt data from other authorized users and scan their Wi-Fi devices for vulnerabilities, install malware and compromise those devices.
- CCMP protocol in WPA2 is vulnerable to Time Memory Trade Off pre-computation attack [9]. The adversary computes a large database, and then uses this database for potentially capturing different secret keys. This attack does not require any knowledge of the plaintext during the pre-computation stage.

Measures are being carried out to solve these flaws in WPA2, hence it is still being considered in improving (upgrading) stage.

IV. Practical Solutions To Wlan Security

- Changing Default SSID

  As SSID is the only security mechanism that the access point requires toenable association in the absence of activating optional security features. Not changing the default SSID is one of the most common security mistakes made by WLAN administrators. So, in order to protect WLAN from malicious threats, SSID should never be set to default [6][18].
- Utilize VPN

  A VPN authenticates users coming from an untrusted space and encrypts their communication so that someone listening cannot intercept it. A secure method of implementing a wireless AP is to place it behind a VPN server [18] which provides high security for the wireless network implementation without adding significant overhead to the users. If there is more than one wireless AP in the organization, it is recommended to run them all into a common switch, then connecting the VPN server to the same switch. Then, the desktop users will not need to have multiple VPN dial-up connections configured on their desktops. They will always be authenticating to the same VPN server no matter which wireless AP they have associated with [7].

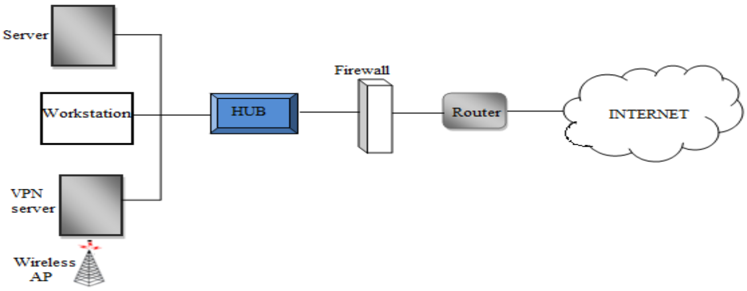

Fig.9. Securing a wireless AP

- Utilize Static IP

  By default, most wireless LANs utilize Dynamic Host Configuration Protocol [18] to more efficiently assign IP addresses automatically to user devices. But, DHCP does not differentiate a legitimate user from a hacker. With a proper SSID, anyone implementing DHCP will obtain an IP address automatically and become a genuine node on the network. But, by disabling DHCP and assigning static IP addresses to all wireless users, the possibility of the hacker to obtain a valid IP address can be minimized. On the other hand, 802.11packet analyzer can be used to sniff the exchange of frames over the network for knowing IP addresses in use [7]. Thus, the use of static IP addresses is not fool proof, but at least it is a deterrent.

- Access Point Placement
  WLAN access points should be placed outside the firewall to protect intruders from accessing corporate network resources. Firewall can be configured to enable access only by legitimate users based on MAC and IP addresses [6]. Though this is not a final or perfect solution because MAC and IP addresses can be spoofed.
- Minimize radio wave propagation in non-user areas
  Try orienting antennas to avoid covering areas outside the physically controlled boundaries of the facility[7]. By steering clear of public areas such as parking lots, lobbies etc. the ability for an intruder to participate on the wireless LAN can be significantly reduced. This will also minimize the impact of someone disabling the wireless LAN with jamming techniques.
- Set and Enforce WLAN Policies
  WLAN policies should begin with the basics of forbidding unauthorized access points, ad hoc networks and reconfiguration of access points/WLAN cards. The policies that limit WLAN traffic to operate on set channels, at connection speeds of 5.5Mbit/sec and 11Mbit/sec, and only during select hours should be implemented to have a check on suspicious activities [10]. Such policy enforcement requires 24/7 monitoring of a WLAN also.
- Intrusion detection and protection
  Only WLAN-focused IDS should be implemented to protect the network by continuous monitoring of all WLAN attack signatures, protocol analysis, statistical anomaly and policy violations [10].

V. Tools For Protecting Wlan

Following products can minimize the security threats of WLAN such as [7]:

- AirDefense
  A commercial wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a WLAN from intruders and attacks.
- Isomair Wireless Sentry
  It monitors the air space of the enterprise to identify insecure access points, security threats and wireless network problems using unique and sophisticated analysis technology.
- Wireless Security Auditor (WSA)
  An IBM research prototype of 802.11 WLAN security auditor running on Linux helps network administrators to close any vulnerability by automatically auditing a wireless network for proper security configuration.
- Freeware tools
  NetStumbler, MacStumbler, WaveStumbler etc. are a freeware AP discovery tools for passively monitoring beacons and probe response frames.

VI. Conclusion

As wireless networks have become more prolific and complex, security vulnerabilities and issues have to be met with well thought-out solutions to maintain security. There are many protocols or technologies for wireless network security but every protocol has some demerits. Although the security concerns of WLAN can't be completely eliminated by a single absolute security technology, we can mitigate them by a proper management and integration of standards, technologies, policies and service environments. In other words, enough security knowledge, proper implementation and continued maintenance is the need of hour for preserving the security of wireless networks.

References

[1] Al Naamany, A. M., Shidhani, A., &H. Bourdoucen, IEEE 802.11 wireless LAN security overview. *International Journal of Computer Science and Network Security, 6(5B)*, 2006,138-186.

[2] S. K. Asagodu, *Wireless LAN Security and IEEE 802.11* Department of Computer Science Engineering: Vishveshwaraiah Technological University- S.D.M College of Engineering and Technology, 2009-10.

[3] H. Boland&H. Mousavi, Security issues of the IEEE 802.11b wireless LAN.*Canadian Conference on Electrical and Computer Engineering*, 2004.

[4] V.Chandramouli, *A detailed study on wireless LAN technologies*, "http://crystal. uta. edu/~ kumar/cse6392/termpapers/Vijay_paper.pdf#search='A%20Detailed%20Study%20on%20Wireless% 20LAN% 20Technologies," 2002.

[5] R.T. Chinta, T.F. Wong &J.M. Shea, Energy-efficient jamming attack in IEEE 802.11 MAC,*Military Communications Conference(MILCOM)*, 2009.

[6] P. Feng,Wireless LAN security issues and solutions,*IEEE Symposium on the Robotics and Applications (ISRA)*, 2012.

[7] R.A. Hamid, *Wireless LAN: Security Issues and Solutions* [Press release], 2003.

[8] M. Ihonen, A. Salo &T. Timonen, *802.11 security protocols*, Lappeenranta University of Technology, 2009.

[9] M. Junaid, M. Mufti, &M.U.Ilyas, *Vulnerabilities of IEEE 802.11i wireless LAN CCMP protocol*, "http://whitepapers. techrepublic.com/whitepaper. aspx," 2006.

[10] A. Khatod, *Five Steps To WLAN Security - A Layered Approach*, "http://www.computerworld.com/s/article/97178/Five_Steps_To_WLAN_Security_A_Layered_Approach," 2004.

[11] V. Kumar, S. Chakraborty, F.A. Barbhuiya, &S. Nandi, Detection of stealth Man-in-the-Middle attack in wireless LAN.*2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC)*, 2012.

[12] C. Liu &J. Yu, Rogue access point based dos attacks against 802.11 WLAN.*4th Advanced International Conference on Telecommunications (AICT'08)*, 2008.

[13] M. Mathews &R. Hunt, Evolution of wireless LAN security architecture to IEEE 802.11i (WPA2), *4th Asian Conference on Communication Systems and Networks Asia Proc.* , 2007.

[14] G. A. Mendez, L. C. D. Silva &A. Punchihewa, *Review of Present IEEE 802.11 "Wi-Fi" Security Issues and of Other Possible Vulnerabilities*, Institute of Information Sciences & Technology, Massey University, New Zealand.

[15] E, Misel, *Advantages/Disadvantages: WEP/WPA Network Security*,"http://www.brighthub.com/computing/smb-security/articles/78216.aspx".

[16] C. H. J. C. Mitchell, Security Analysis and Improvements for IEEE 802.11i,*12th Annual Network and Distributed System Security Symposium (NDSS'05)*, Stanford University, Stanford, 2005.

[17] V. Nagarajan, V. Arasan&D. Huang, Using power hopping to counter MAC spoof attacks in WLAN,*7th IEEE Consumer Communications and Networking Conference (CCNC)*, 2010.

[18] J.S.Park &D. Dicoi, WLAN security: current and future. *IEEE Internet Computing, 7(5)*, 2003,60-65.

[19] Promila & Chhillar, Review of WI-FI Security techniques,*International Journal of Modern Engineering Research (IJMER), 2(5)*, 2012, 3479-3481.

[20] V. Ramachandran,*BackTrack5:Advanced WLAN Attacks*, "http://www.packtpub.com/article/backtrack5-advanced-wlan-attacks," 2011.

[21] E. Sithirasenan, V. Muthukkumarasamy &D. Powell, IEEE 802.11i WLAN security protocol-a software engineer's model, *4th Asia Pacific Information Technology Security Conference (AusCERT'05) Proc.*, 2005.

[22] *What's New in Security: WPA (Wi-Fi Protected Access)*, "http://kb.netgear.com/app/answers/detail/a_id/1105."

[23] *Wireless Vulnerabilities and Attack Methods*, "http://www.unix-edu.se/student/wlan/Chapter_9.pdf."

[24] C. Xu&H. Wang,Heterogeneous wireless LAN-based wireless network attack analysis and research, *International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE)*, 2011.

[25] P. Ye &G. Yue, Security Research on WEP of WLAN,*2nd International Symposium on Networking and Network Security (ISNNS'10) Proc.*, Jinggangshan, PR China, 2010.