"WIRELESS TECHNOLOGY: AN OVERVIEW"

Tanvi Grover
Department of Electronics & IT, S.D.College, Ambala Cantt

Abstract: **Wireless Technology has become a boon in each and every field now a days. Wireless LANs are everyplace recently from home to massive enterprise company networks because of the benefit of installation, worker convenience, avoiding wiring price and constant quality support. However, the larger convenience of wireless LANs means that redoubled danger from attacks and redoubled challenges to a corporation, IT workers and IT security professionals. This paper represents an overview of Wireless networking. Which configuration and protocol it follows for communication. The vulnerabilities and threats it possess while transmitting the information between users.**

Keyword: **WLAN, Wireless, Security, WPA, Attack etc.computer**

I.INTRODUCTION

A Wireless Local Area Network (WLAN) is a kind of local area network (LAN) that uses high frequency radio waves rather than cables to communicate between network-enabled devices. A WLAN connects computers by make use of radio technology using standard protocols, but without the use of wires. A WLAN can be set up as the sole network in a school or building as well as can also be used to extend an existing network to the areas where wiring would be too expensive or too difficult to implement, or to the areas located distant from the main network or building. The major difference between wired and wireless networks is the use of different form of cables to associate computers together. A wireless network does not require any physical connection (cabling) between computers. Wireless networks can be implementing to provide the same network functionality as wired networks, ranging from simple point-to-point configurations to large-scale infrastructures accommodating large amount of users.

II. WIRELESS NETWORK COMPONENTS:

These components are the basic requirements of WLAN technology:

A). This network requires a network interface card (NIC) that can be added to our desktop computer or laptop. Sometimes it is already built-in (already added into the system).

These plug-in cards are of two types :
1) **PCI** which is inserted into one of the internal slots in a desktop computer**.**
2). **PCMCIA** which is inserted into the relevant slot in the side of a laptop and. Wireless NICs contains an in-built antenna to connect with the network. *f*

B). Wireless Network has an "Access Point" that works in a same manner as that of Switch used in Wired Network. It either receives the signal from surroundings or broadcast it to surroundings through this Network Interface Card (NIC).

III. DIFFERENT CONFIGURATION OF WIRELESS NETWORK:

The different configurations of Wireless Network as follows-

A). ACCESS POINT :
Access Point is basically a hardware device that helps in communication of the devices like Mobile, PDA (Personal Digital Assistance) and Computers through Wireless network.

Basically, an Access Point with the help of a wired network gets connected and then facilitates a bridge for communication between wired and wireless devices.

B). AD-HOC MODE
This mode is one of the famous networking topology used in the 802.11 standard. This mode consists of minimum of two wireless stations where no access point is required in communication. This mode is also known as "Peer-to-peer" mode. Ad-hoc mode WLANs are not very costly to use because they don't require any access point for their communication. However, this topology cannot used for larger networks due to lack of some security features like access control and MAC (Multiple Access Control) filtering.

C). INFRASTRUCTURE MODE
This mode is another networking topology also used in the 802.11 standard. This mode consists of a number of access points and wireless stations. The access points are basically connected to a larger wired network. This network topology can be used for large-scale networks with huge coverage and complexities.

IV.DIFFERENT WLAN TECHNOLOGIES

Wireless Technology has become more popular with the time. Some of the l Wireless LAN technologies are as follows-

A). Narrow Band(UHF)
B). Spread spectrum
C). Frequency hopping spread spectrum(FHSS)
D). Direct sequence spread spectrum(DSSS)

A) Narrowband(UHF):
This technology uses a specific radio frequency between range 300-3400 Hz for data transmission. It transfers the radio frequency in a narrow bandwidth. So, it is named as Narrow Band or Ultra High Frequency.

B) Spread spectrum:
Initially produced for military utilize, spread range innovation takes into account more noteworthy data transfer capacity by consistently changing the recurrence of the transmitted flag, subsequently spreading the transmission over different frequencies. Spread range utilizes more data transfer capacity than narrowband; however the transmission is more secure, dependable, and simpler to distinguish.

C) Frequency hopping spread spectrum(fhss):
Frequency hopping spread spectrum (FHSS) innovation synchronizes the changing recurrence of both the transmitter and recipient (utilizing a narrowband bearer) to, in actuality, create a solitary transmission flag. This recurrence "bouncing" can happen as frequently as a few times each second; it is continually changing starting with one recurrence then onto the next, transmitting information for a specific timeframe before changing recurrence once more. Like spread range innovation, FHSS innovation expends extra transmission capacity, be that as it may, this is through the span of various bearer frequencies.

D) Direct Sequence Spread Spectrum(DSSS):
Direct sequence spread spectrum (DSSS) technology separates the transmitted stream of information into little pieces over a recurrence channel. An excess piece design (known as a chipping code) is created for each piece transmitted. For the most part, the more extended the chipping code, the more probable it is that the first transmitted information will be appropriately gotten. DSSS innovation utilizes more data transfer capacity than FHSS; however DSSS is viewed as more solid and opposes impedance. As a result of the chipping code, information can in any case be recouped without retransmission of the flag, even on account of harmed information bits. U.S. Mechanical autonomy remote systems administration items use DSSS innovation.

V.PRIVACY POLICY OF WIRELESS TECHNOLOGY

Wi-Fi Protected Access (WPA) is a remote security convention intended to address and settle the known security issues in WEP. WPA gives clients a larger amount of affirmation that their information will stay ensured by utilizing Temporal Key Integrity Protocol (TKIP) for information encryption. 802.1 x validations has been acquainted in this convention with enhance client confirmation.

Wi-Fi Protected Access 2 (WPA2), in view of IEEE 802.11i, is another remote security convention in which just approved clients can get to a remote gadget, with components supporting more grounded cryptography (e.g. Propelled Encryption Standard or AES), more grounded validation control (e.g. Extensible Authentication Protocol or EAP), key administration, replay assault assurance and information respectability.

VI.SECURITY THREATS AND RISKS

The outline imperfections in the security instruments of the 802.11 standard likewise offer ascent to various potential assaults, both inactive and dynamic. These assaults empower interlopers to spy on, or mess with, remote transmissions.

A) PARKING LOT ATTACK:
Access points emit radio signals in a circular pattern, and the signals almost always extend beyond the physical boundaries of the area they intend to cover. An attacker may also fool legitimate wireless clients into connecting to the attacker's own network by placing an authorised access point with a stronger signal in close proximity to wireless clients. The aim is to capture end-user passwords or other sensitive data when users attempt to log on these rogue servers.

B) SHARED KEY AUTHENTICATION FLAW:
Shared Key Authentication (SKA) is a procedure by which a PC can access a remote system that uses the Wired Equivalent Privacy (WEP) convention. With SKA, a PC outfitted with a remote modem can completely get to any WEP system and trade encoded or decoded information.

WEP uses the RC4 stream cipher as its encoding algorithmic program. A stream cipher works by generating a key stream, i.e. a sequence of pseudo-random bits, supported the shared secret key, along with the formatting vector (IV). The key stream is then XORed against the plaintext to provide the cipher text. A very important property of a stream cipher is that if each the plain text and also cipher text are best-known, the key stream are often recovered by merely XORing the plaintext and

therefore the cipher text along, during this case the challenge and also the response. The recovered key stream will then be employed by the attacker to encode any resultant challenge text generated by the access purpose to provide a legitimate authentication response by XORing the two values along. As a result, the attackers are often authenticated to the access purpose.

C) SERVICE SET IDENTIFIER FLAW

Access points go with default SSIDs. If the default SSID isn't modified, it's relatively attract a lot of attacks from attackers since these units ar considered poorly designed devices. Besides, SSIDs ar embedded in management frames that may be broadcasted in clear text regardless access purpose is designed to disable SSID broadcasting or enabled cryptography. By conducting analysis on the captured network traffic from the air, assailant is ready to get the network SSID and performs more attacks.

D) *ATTACK ON TEMPORAL KEY INTEGRITY PROTOCOL (TKIP):*

The TKIP attack uses a mechanism the same as the WEP attack that making an attempt to decrypt one byte at a time by exploitation multiple replays and perceptive the response over the air. Exploitation this mechanism, an attacker will decrypt little packets like ARP(Address Resolution Protocol) frames in concerning Fifteen Minutes. If Quality of Service (QoS) is enabled within the network, attacker will additional inject up to fifteen randomly frames for each decrypted packet. Potential attacks contain ARP poisoning, DNS manipulation and denial of services.

Although this can be not a key recovery attack and it doesn't cause compromise of TKIP keys or decoding of all succeeding frames, it's still a significant attack and poses risks to any or all TKIP implementations on each WPA and WPA2 network.

VII. THE VULNERABILITY OF WIRED EQUIVALENT PRIVACY PROTOCOL

Data passing through a wireless computer network with WEP disabled (which is that the default setting for many products) is prone to eavesdropping & information modification attacks. However, even once WEP is enabled, the confidentiality and integrity of wireless traffic remains in danger as a result of variety of flaws in WEP are unconcealed, that seriously undetermine its claims to security. Specifically, the sub sequent attacks on WEP are possible:

A). Passive attacks to decode traffic supported better-known plaintext and chosen cipher text attacks.
B).Passive attacks to decode traffic supported statistical analysis on ciphertexts;
C). Active attacks to inject new traffic from unauthorised mobile stations;
D).Active attacks to change data; or
7.5 Active attacks to decode traffic, supported tricking the access purpose into redirecting wireless traffic to associate attacker's machine.

VIII. ADVANTAGE & DISADVANTAGES OF WIRELESS NETWORK

A). ADVANTAGES:

1). WI-FI HOT SPOTS

It has become a necessity for several individuals to stay connected to the net whenever they're awake. Wireless network could be a boon to such individuals. Several public places have Wi-Fi hot spots accessible to that you'll be able to connect your laptops. You'll be able to try this by providing the actual Wi-Fi password. This facility is accessible in hotels, railway stations etc. So, you would like to not worry once you are fa raway from home or workplace.

2) BETTER MOBILITY

Mobility can be an advantage offered by wireless networks particularly for businesses. It permits you to access the server from anyplace within the workplace. you'll additionally attend conferences where you're, whether or not within the meeting space or outside. Some businesses permit you to attach to that remotely if you're removed from workplace.

3) COST EFFECTIVE

Compared to wired network, wireless network are cost effective as a result of it needs no cables and alternative accessories to attach. additionally to the cost of the cables, wired networks ought to pay plenty on the labor to put in the connections throughout the building. though wireless could value to a small degree at first, it needs terribly less for its maintenance since there's no wiring concerned.

4) VOIP FACILITY

VOIP (Voice Over net Protocol) facility is obtainable with wireless networks. it's a telephone service exploitation the web that is incredibly affordable in comparison to ancient phone service. you'll do VOIP calls to anywhere if you have got a web connection. creating international calls also are the bottom with VOIP.

5) SCALABILITY

Expanding a wired network may be expensive and troublesome with adding new cables and rerouting the prevailing ones. However enlargement with wireless is pretty simple. a brand new user are often added by

supplying a positive identification and updating it within the server.

B) DISADVANTAGES OF WIRELESS NETWORKS

1) LESSER RANGE

Normally, the range of a medium-range wireless network is up to around a hundred meters. this could be appropriate for a home or alittle workplace, however inadequate for larger structures. to extend the range, extra access points or repeaters are needed. this can be an additional charge that will increase the price.

2) SECURITY ISSUES

Security could be a major concern in any kind of communication. Wireless networks involve the chance of modification and eavesdropping. in order that they build use of sure encoding techniques for security. There also are authentication mechanisms in situ for identical. However it's been found that a number of the encoding techniques may be simply compromised.

3). RELIABILITY

Since wireless networks work with electromagnetic radiation communication, the signal is suffering from a lot of interference. it's additionally subjected to bound propagation effects. The movement of the user additionally creates instability within the signals. These disturbances to the signal could become tough to handle for the network administrator.

4). LESS SPEED

The maximum speed of 802.11n normal network is 600Mbps. this is often solely virtually half the speed of a wired network. Same is that the case with all the wireless networks. in comparison to wired, they're terribly slow. The speed additional decreases in an exceedingly busy network.computer.

IX.CONCLUSION

Wireless Technology has change the life of an individual. Anyone can communicate with others at any time. So it makes life more flexible. But everything has some disadvantages with advantages. But the major issue with the Wireless Networking is it’s security concern. Thus, true WLAN security is often about to be a game of equalization acceptable risk and therefore the step to mitigate those risks provide higher security solutions.

REFERENCES

[1] www.wikiipedia.com
[2] “Wireless Network Security and Interworking”, the Proceedings of IEEE on Cryptography and Security 2005
[3] Peter Rysavy, "Secure Wireless Networking Using SSL VPNs," Rysavy Research
[4] John R. Vacca, The Essential Guide To Storage Area Networks, Prentice Hall, 2002.computer