SECURITY ON UNGUIDED MEDIA: A REVIEW PAPER

Ch.Shravika[1], B.Varshitha[2], B.Spandana[3], G.Durga Bhavani[4].

[1,2,3&4]Student(B.Tech.),Department of Computer Science and Engineering, Vivekananda Institute of Technology and Science, Karimnagar, Telangana.

[1]email: shravikachittampally@gmail.com

[2]email: varshithabilla@gmail.com

[3]email: bspandana55@gmail.com

[4]email: durgabhavani.gajula26@gmail.com

ABSTRACT

In our current generation, unguided media (wireless communication) has a major role. Based on that communication, we can access the information anywhere. Wireless network provides flexibility and freedom that wired network lacks. The broadcast nature of wireless networks makes it easy for everyone to attack the network, if not secured. So, we have to provide security for such connections. Hackers are capable to decrypt the data on wireless links. This can be protected by using built-in WEP encryption. Providing security is vital because information is prone to several flaws like packet sniffing, password theft, Bluetooth attacks, Man-in-the-middle attacks. This paper includes overflow of existing standards, literary research on security. It includes wireless communicating methods, assessments and audits to identify security vulnerability.

KEYWORDS

Availability, Confidentiality, Integrity, Security attacks, Encryption, Authentication, Threats.

INTRODUCTION

Telecommunication links can be broadly be classified into two categories, namely, guided media(wired) and unguided media(wireless).Both media are used for short distance (LAN,MAN) and long distance(WAN) communications.

There is a physical interaction between two devices in guided media, where as in unguided media there is no physical interaction. In unguided media electromagnetic signals are broadcasted through air or sometimes water. Unguided media is also called as wireless communication, unbounded media. Unguided media is categorized into radio waves, micro waves, Infrared waves.

Radio waves: radio waves are generated easily. These are low frequency signals and can travel a long distance. This waves can penetrate through buildings.

Micro waves: the distance covered by the micro wave signals depend on the height of the two antenna. It has a frequency higher than the radio wave. They are used for telephone communication, mobile phones, television distribution etc..

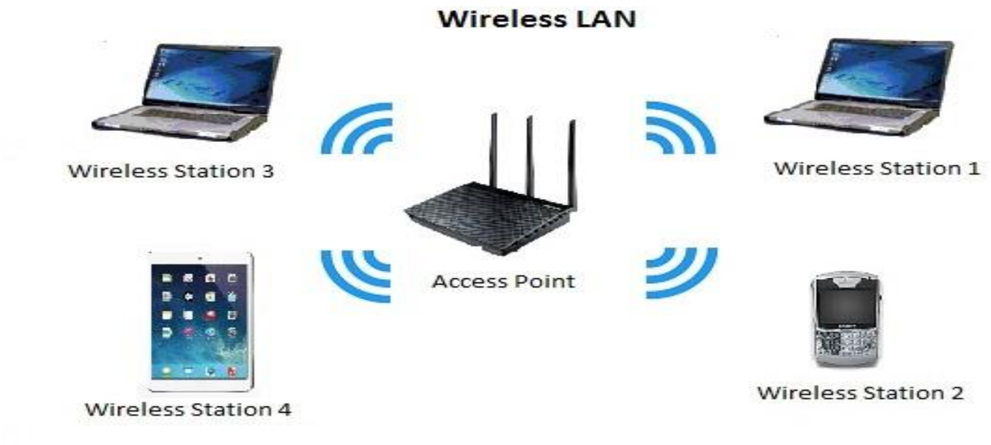
Infrared waves: Infrared waves are used for short range communication like , the remote control for TV's, VCR's(Video Cassette Recorder) etc..

Wireless networks have spread between home users and companies in an increasing fashion. The main reason behind the fast adaptation is due to the nature of wireless networks where it provides the flexibility and freedom that wired networks lacks. Increasing of band width capabilities has inspired people to think seriously about replacing wired networks. Especially in places where it is hard or expensive to have wired networks. One of the main places that can benefit from these ideas or rural areas, where wired networks infrastructure is either difficult or impossible to create due to physical obstacles.

The main standards in the wireless world are: 802.11, which describes the WLAN architecture, and 802.16 which describes the WMAN architecture. These two wireless networks are usually known by two acronyms: WIFI [wireless fidelity] to be a symbol of WLAN and WiMAX [Worldwide Interoperability for Microwave Access] to describe WMAN.

Wireless LAN [WLAN]:

WLAN's increasingly popular and homes, offices, cafes, libraries, airports, zoos and other public places are being outfitted with them to connect computers, PDA's and small places to the internet.



WLANs can also be used to let two or more nearby computers communicate without using internet. Most modern WLANs are based on IEEE 802.11 standards.802.11 networks can be used in two modes. The most popular mode is to connect clients, such as laptops and mobiles to another network, such as a company internet or the intranet. Each client is associated with AP (Access Point) that is in turn connected to another network. The client sends and receives its packets via the AP. Several access points may be connected together typically by a wired network called a distribution system, to form an extended 802.11 network.

The other mode is an ad hoc network. This mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point. Since internet access is the killer application for wireless, ad hoc networks are not very popular.

Wireless MAN [WMAN]:

Idea behind The using WMAN is to offer a broadband Internet service using wireless infrastructure. The idea is very similar to a TV broadcast network. The theoretical speed of WMAN is 75Mbps extended to several miles, which offer a replacement to cable and DSL connections in the future.

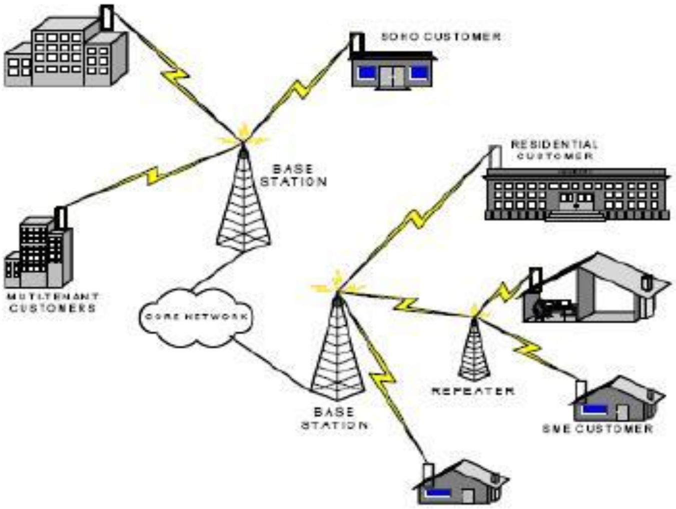


fig : WMAN

WMAN is also called BWA (Broadband Wireless Access) as a formal title along with the industry icon acronym WiMAX. The main target of implementing WiMAX technologies is provide a convenient solution to the “last mile access”, where the fast data backbone traffic is to be distributed among consumers. This also helps expand the Internet covered areas especially in rural areas.

Most of the WMANs are based on 802.16. Base stations connect directly to the providers backbone network, which is in turn connected to the internet. Base stations communicate with stations over the wireless air interface.

INTRODUCTION TO SECURITY:

Security in computer world determines the ability of systems to manage, protect and distribute sensitive information data security was found many years before the advent of wireless communication due to the mankind’s need to send information (in war or in peace time) without exposing its content to others. “ Protect information from unauthorized users, access, discloser, destruction, modification for in order to confidentiality, integrity, availability is known as security”.

Three primary goals of security are;

- Confidentiality
- Integrity
- Availability

Security attacks:

The information which is not secured can be accessed by unauthorized person, due to the absence of physical barriers where the range of wireless transmission ranges from 300ft to half a mile.

Most common attack types and threats are listed under the following categories:

Packet sniffing: When information is sent back and forth over a network, it is sent in what we call packets. Since wireless traffic is sent over the air, it's very easy to capture.

Quite a lot of traffic (FTP, HTTP,SNMP, etc.) is sent in the clear, meaning that there is no encryption and files are in plain text for anyone to read. So using a tool like Wireshark allows you to read data transfers in plain text. This can lead to stolen passwords or leaks of sensitive information quite easily. Encrypted data can be captured as well, but it's obviously much harder for an attacker to decipher the encrypted data packets.

Password theft: When communicating over wireless networks, think of how often you long into a website. You send passwords out over the network, and if the site doesn't use SSL or TLS, that password is sitting in plain text for an attack to read.

Bluetooth attacks: There are a variety of Bluetooth exploits out there. These range from annoying pop up messages, to full control over the victims Bluetooth enabled device.

Man in the middle attack: In this attack, the hacker gets the packets before the intended receiver does. This allows her to check the content of the message. One of the most known subset of this attack is called ARP (Address Resolution Protocol) attacks, Where the hacker redirects network traffic to pass through her device.

Wireless security:

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

WEP is a security algorithm for IEEE 802.11 wireless networks. Introduced as the part of the original 802.11 standard ratified in 1997, its intension was to provide data confidentiality comparable to that of a traditional wired network. The encryption process is only between the client and AP, meaning that packet transfers after the AP are unencrypted. WEP uses RC4 for the encryption process.

WEP WEAKNESS: One of the major reasons behind WEP weaknesses is its key length. WEP has a 40 bit key, which can be broken in less than 5hours using parallel attacks with the help of normal computer machines.

WPA (Wi-Fi Protected Access) :

WPA is a security standard for users of computing devices equipped with wireless internet connections, or Wi-Fi. The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA provides more sophisticated data encryption then WEP, and it also provides user authentication. The WPA protocol implements much of the IEEE 802.11i standard.

802.11i: This standard is supposed to be the final solution to wireless security issue. It improves authentication, integrity and data transfer. Since the market needs require more standardized WEP, WPA was released as a substitute to it on April 2003. After the final release of 802.11i the vendors implemented the full specifications under the name WPA2.

WPA2:

The security standard that superseded it in 2004.WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).it is based on the obligatory Advanced Encryption Standard Algorithm, which provides message authenticity and integrity verification, and it is much stronger and more reliable than the original TKIP protocol for WPA.

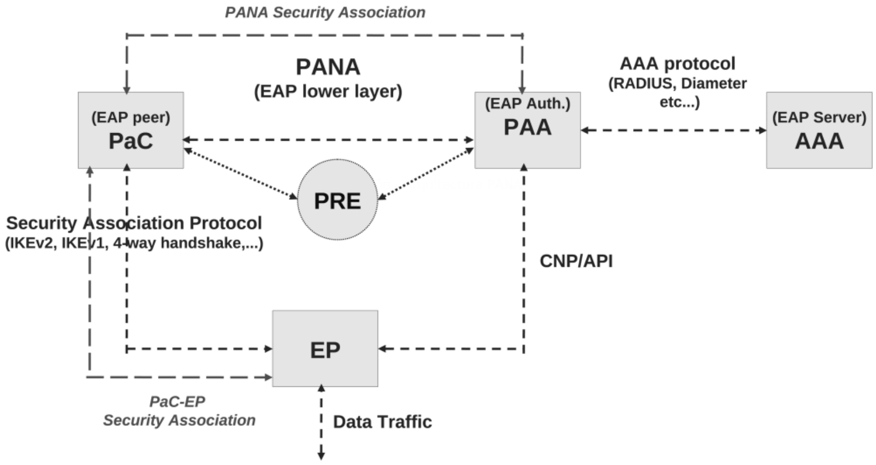
As we go deep in to the concept of WPA2, there is occurrence of drawbacks therefore the IP based protocol PANA was introduced.

RECENT PROPOSALS:

PANA:

One of the recent proposal is PANA (Protocol for Carrying Authentication for Network Access). PANA target is to improve the authorization between WLAN clients and AAA (Authentication Authorization Accounting) servers. It is an IP based protocol that allows a device to authenticate itself with a network to be granted access. PANA will not define any new authentication protocol, key distribution, key agreement or key derivation protocols. For these purposes the Extensible Authentication Protocol (EAP) will be used, and will carry the EAP payload. PANA allows dynamic server provider selection supports varies authentication methods, is suitable for roaming users, and is independent from the link layer mechanisms.

PaC (PANA Client) is the client part of the protocol. This element is located in the node that wants to reach the access network. Once the client is authenticated, PANA SA (Security Association) is created in both PAA and PaC. Furthermore, information filters are installed on the EP(Enforcement Point). Even after the client is authenticated, there might be other authentication messages exchanged between PaC and PAA during the connection session.



ARGUMENTS AGAINST PANA

- Terminal should authenticate before obtaining and IP address.
- PANA is architecturally wrong.

WPA3:

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. The new standard uses 192 bit security suit for protecting Wi-Fi user's with higher security requirements, such as government, defence and industrial organisations.WPA3 protocol strengthens user privacy in open networks through individualized data encryption. WPA3 protocol will also protect against brute-force dictionary attacks, preventing hackers from making multiple login attempts by using commonly used passwords.

CONCLUSION:

In this paper we have acquired the information and reviewed about the security. In wireless data networks that has evaluated form past years. The comparision between the wired, wireless network and the different data transfer mediums was conversed which are used. These networks play major role in giving view about the possible attacks that are going to be faced by the systems. Avoidance of security treat will always be around by maintaining various wired and wireless security policies by using standards. 802.11i standard proves that it is efficient in solving many of the security issues found in its predecessor WEP. Since the 802.11i standard is currently introduced the chance of testing it thoroughly impossible.

Further modulations of the developed standards view the result about the wireless network security. As we mentioned some of the paths provided to overcome the security holds in unguided media with the proper utilization can increase security levels.

PANA is an IP based protocol that allows a device to authenticate itself with a network to be granted access. WPA3, is an advanced version that is used as a substitute for PANA in order to rectify the disadvantages of PANA

REFERENCES

[1] "wireless security's future,". Security & Privacy Magazine.

[2] "Wireless LAN, " http://cncenter.future.co.kr/hot-topic/wlan.html".

[3] "PANA", http://pepole.nokia.net/~patil/IETF56/PANA/PANA.

[4] Andrew S.Tanenbaum, David J.Wetherall "Computer networks".