# Issues and the Advantages of Wireless Network

[1]N. Poorinma, [2]S.Gowri, [3]r.Abinaya

[1]Assistant Professor, [2]B.E Student, [3]B.E Student

[1]Valliammai Engineering College, Chennai, India, [2]Valliammai Engineering College, Chennai, India, [3]Valliammai Engineering College, Chennai, India

***Abstract*—Wireless networking has many advantages and it also discuss about the various security or challenges that are present in this technology. This paper is majorly deals with the concept of troubleshooting the problems along with the solutions and it also gives an information about why we have to prefer the wireless networking technologies. Wireless technologies have many different kind of procedures in various kinds of OS that is mainly used for troubleshooting the problems that are occurred based on this wireless network. Thus many effective solutions are also discussed for countering the threats**

***IndexTerms*— Wireless network, Wireless security, Troubleshooting**

## 1. INTRODUCTION

Wireless Internet Access technology[1] is being increasingly deployed in both office and public environment as well as by the Internet users at home. A wireless local areanetwork is a flexible data communication system implemented as an extension to,or as an alternative for a wired LAN. Wireless technologies, in the simplest sense enable one or more devices to communicate with physical connection without requiring network or peripheral cabling. Wireless network serve as the transport mechanism between devices and they are frequently classified[2] into three groups:(1)WWAN-Wireless Wide Area Network which includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPC), Global System for Mobile Communication(GSM) and Mobitex. (2)WLAN- Wireless Local Area Network representing Wireless LAN includes 802.11,Hiper LAN and several others.(3)WPAN-Wireless Personal Area Network represents Wireless Personal Area Network technologies such as Bluetooth and IR. The purpose of this paper is to give an overview of the wireless network technologies and also it deals with some of the issues and security or challenges of this technology.

## 2. WHY DO WE PREFER WIRELESS NETWORK?

A wireless network is any type of computer network[3] that uses wireless data connections for connecting network nodes.

| SNO | PARAMETER | USES |
|---|---|---|
| 1. | Increased mobility and collaboration | • roam without losing your connection<br>• work together more effectively |
| 2. | Improved responsiveness | • connect to the information when you need it<br>• gives us better customer services |
| 3. | Better access to information | • processes are improved<br>• hard-to-reach areas can be connected |
| 4. | Easier network expansion | • it quickly add the users<br>• grow your network cost effectively |
| 5. | Enhanced guest access | • give secure connections<br>• value-added services are offered |
| 6. | Shannon's theorm | • provides maximum data rate of any single wireless links are related to bandwidth in hertz and the noise on the channel |
| 7. | Safety | • radio frequency exposure from wifi are likely to be lower than those from mobile phones . |
| 8. | Scalability | • It increases its total output under an increased load when resources are added. |
| 9. | Productivity | • It used to produce the measure of total efficiency of the production process. |

## 3.TROUBLESHOOTING PROBLEMS IN WIRELESS NETWORK:

There are certain problems may occur while connecting to the wireless network. They may be like not proper connectivity or any tower problems and many technical problems also present like [4] IP address assignment,effect of loopback interfaces on AP's, no image in AP flash, booting issues with the AP, power issues with the AP, use of nonoverlapping channels, IOS upgrade etc.

*3.1.Possible categories of attacks in wireless networks:*

Wireless networks have become ubiquitous as a means of connecting to a network and this has some common attacks which can be performed aganist this networks.

*3.2AaccessCcontrol Attacks:*

In this there are many kinds of attacks such as War driving( which is used for listening the beacons or sending probe requests),[5]AdHoc associations(connecting directly to unsecured stations), MAC Spoofing(attacker's MAC address are reconfigured to pose an authorized AP).

*3.3. Confidentiality Attacks:*

These attacks are try to attempt to intercept the private information sent over wireless asscociations and it also has many types such as WEP key cracking(capturing data to recover WEP key using passive or active methods),Evil twin AP(masquerading as an authorized AP by beaconing the WLAN's service set identifier to lure users).Wired Equivalent Privacy (WEP) is relatively trivial to defeat and numerous attacks exist which can either decrypt WEP protected packets or recover the WEP key. WEP has been broken for more than 10 years and should not be used to secure a wireless network.

*3.4. Integrity Attacks:*

802.11 Frame Injection which is used for crafting and sending forged 802.11 frames and 802.11 data replay for capturing modified replay are used in the integrity attacks.

Enterprise network authentication is secure and not vulnerable to a man-in-the-middle attack, many clients are incorrectly configured, leaving them susceptible to an attack. The vulnerability arises from the use of a certificate to verify the RADIUS server.[6] Many clients will configure their device so that it does not reject certificates provided by the RADIUS server. These may be signed by the wrong certificate authority and/or have the wrong common name. To ensure they are not vulnerable when authenticating to their wireless network, clients should only accept certificates from the correct.

certificate authority with the correct common name. By accepting any certificate, a malicious AP can use either a selfsigned certificate or a certificate signed by the correct certificate authority (if a public certificate authority is used) to intercept credentials.

*3.5. Authentication Attacks:*

Shared key guessing which is attempting authentication with guessed vendor default or cracked WEP keys .A wireless network can be attacked is to try to flood the Access Point (AP) with authentication and association frames. To association flood, the attacking device will spoof its wireless MAC address then, rapidly and repeatedly, try associating to the AP. At each attempt the attacker will change its MAC address, mimicking the existence of many clients. This has the affect of consuming the AP's memory and processing ability, denying service to legitimate clients.

PSK cracking which is recovering WAP/WAP2 PSK from captured key handshake frames using dictionary attack tools. Wi-Fi Protected Access (WPA) [7] and WPA2 make the protocol secure there is a weak point in the system: the passphrase. Users configuring WPA/WPA2 passphrases often choose short, dictionary based passphrases leaving them susceptible to attack. Attackers can capture packets during the key exchange phase of a client joining a wireless network then perform an offline dictionary attack to obtain the WPA/WPA2 passphrase.

*3.6. Security Issues or Challenges in Wireless Network*

The security of any network is an important issue. No one likes the idea that the possibility exists that someone could be intercepting the internet traffic, reading their mail, ordering items with their credit cards or sending inappropriate messages to their head in their name. Security of wired networks is often a primary objective of system administrators.

There are two main issues that wireless security solutions tend to address. First since all the wireless packets are available to anyone who listens,security is needed to prevent eavesdropping. Since it is impossible to keep the people away from the WAP's short of erecting a fence around your building, solutions tend to rely on encryption in form or another.

*3.7. Security Problems:*

- Security features in Wireless products are frequently not enabled.
- Use of static WEP keys (keys are in use for a very long time). WEP does not provide key management.
- Cryptographic keys are short.
- No user authentication occurs – only devices are authenticated. A stolen device can access the network.
- Identity based systems are vulnerable.
- Packet integrity is poor.

*4. Major Security Problems and Solutions to Overcome these Issues Eavesdropping and Authentication:*

The security of any network is an important issue, No one likes the role that the possibility of some reaching your e-mail, ordering items. Security of wired networks is always a primary objective. When considering a wireless network new security concerns come into play. Because wireless network is broadcast in nature. Anyone within the wireless network range can interrupt the packets sent out. Because of this wireless network are more concentrated than the wired networks.

The problem in this that there are two main issues:

1. Since all the wireless packets are available to anyone who listens, security is needed to prevent eavesdropping. It is impossible to physically keep people away from the wireless network.
2. Second issue is authentication that in wired network, a system administrator might determine who generated certain traffic. In wired network, many user can access the same point making it more difficult to map from where the traffic was generated.

The solutions to the above two problems are as follows:

1. It can rely on encryption in one form or another. Depending upon what is implemented.

2. When considering the security solution for any wireless network, it is important to keep those issues in mind, however for various reasons. It is not always possible to get a total solution for your network

### *4.1. Wep and the Small Network:*

The wireless network are more appealing to home and small office userseveryday. In terms of security, these ad-hoc networks provide consist access to outsiders.

The main problem in this is the cost of security. The large company with large number of people can afford to purchase appropriate security equipments. On the other hand, a small company or a house rely on inexpensive security measures.

The solution to the above problem is to use an encrypted key before using that network. The use of WEP can have a significant impact on your throughput.

### *4.2. Larger Wireless Environments:*

WEP is not suitable for larger environments. Most of the system administrator prefer authentication larger wireless environment such as internet cafe, airport, universities provide wireless networks.

They have no way of tracking someone enjoying in illegal activities of their networks. Some organisations use static addressing for their security. Users are assigned a static IP by a central authority. It is easy to change the IP so the central authority uses MAC addresses of user’s wireless cards. A similar concept of DHCP is also used .the use of both these methods is generally not viewed as acceptable methods of authentication.

Another method of wireless authentication is Archipelago wireless, it provides authentication before you connect. If authentication is successful their traffic is allowed to pass through to the rest of the network.

### *4.3. War Driving and War Cholking:*

As wireless networking becomes increasingly popular, more and more people are looking for places they can pick up wireless Internet access.wireless owners started a trend known as “war driving”, the ongoing search for vulnerable access points where they might plug in and access unsecured networks.

War driving is the similar to ‘war dialing’. War driving primarily involves driving around with suitable antennae and software and looking for vulnerable access points.War dialers who wish to leave tracks for those who follow can learn about something called “war chalking”. This information usually includes the SSID of the network, the security status of the network, and signal strength. Not only are vulnerable WAP’s frequently logged on web sites for anyone to find, but anyone who knows what the marks mean is instantly informed of an access point without even having to turn their wireless devices on.

As the number of wireless networks increases, the need for security increases. At present, several encryption solutions ask users to sacrifice throughput for security. Many agree that the concept of a security gateway between your base stations and the rest of your network is the best way to go.

## V. Conclusion

A clear brief idea about the issues of wireless network is discussed in this paper and where this networks are used why we have to prefer wireless networks and an appropriate answer is given. Every system has its own disadvantage, likewise some of the disadvantages are present in this wireless network too, that was briefly explained in the troubleshooting the problem like technical problems that are discussed and also tower problems that leads to interrupt in the connectivity.

At present, there is no perfect security solution. The only environment that can be confidently secured is one where all machines are nearly identical.Then there is the issue of cost. Many ad-hoc wireless networks are set up instead of having a wired network to avoid the cost of wiring the building or buildings where the network will be used. The price of purchasing additional hardware and software for security puts many solutions out of reach. The free solutions, which frequently implement WEP, are inadequate and give a false sense of security.

REFERENCES:

[1]wireless network technologies www.searchnetworks.com/index.html

[2]Major classification of wireless network Wireless Network Security 802.11, Bluetooth and Handheld Devices 802.11, Tom Karygiannis,Les Owens

[3]wireless networks www.sevenforums.com

[4]Troubleshooting connection for wireless network www.cisco.com

[5] Wireless attacks www.sans.edu en.m.Wikipedia.org/wiki/wireless_security

[6] Attacks in wireless network www.imss caltech.edu

[7]wireless sample networks technology problems www.techtarget.com

[8] wireless security attacks www.searchsecurity.techtarget.com

www.sans.edu

www.sersc.org
[9]security www.esecurityplanet.com
www.infosecinstitute.com
www.windowsecurity.com
[10] wireless security attacks
www.sans.org
www.ciscopress.com
[11]attacks
www.Interscience.in
www.omnisecu.com
www.scmagazine.com