WIRELESS TECHNOLOGY IN NETWORKS

Surabhi Surendra Tambe

EXTC branch, Electrical Engineering Department, Veermata Jijabai Technical Institute(VJTI),Mumbai, India

Abstract- The following research paper presents an overview regarding the emerging technology of Wireless Brodband networks. It focuses on the history,tools,standards and implementation of Wi-Fi networks.However the main purpose of this research paper is to understand the various problems associated with the implementation of these WLANs and propose recommendation and measures to solve these problems and mitigate potential risk factors.

Index Terms- QoS, Security, WLANS, Wi-Fi

I. INTRODUCTION

Telecommunication has become an integral part of our daily lives and has been contributing widely to the advancement in various fields. One of the emerging mode is Wireless broadband technology which transmits multiplexed information on a wide band of frequencies. The deployment of Wireless broadband services is done by weighing the geographical population density against the bandwidth limitation. Wireless technologies are designed to reduce the time and different types of obstacles created by cables and more convenient than wired networking. In 1997,'Wireless fidelity-popularly known as Wi-Fi technology was developed by IEEE 802.11 standards which provided users the liberty to connect to the internet from any place.But this service was pretty expensive till 2002 ,however the new 802.11g standards in 2003 has lead to creation of Wifi enabled devices to the masses as a result today a Wi-Fi router has become a household commodity in most modern homes in India.

Since its inception, the Wi-Fi technology has a come a long way in providing quicker wireless access to Internet applications an data across a radio network thereby making the access process faster than conventional modem. Radio bands such as 2.4GHz and 5GHz depend on wireless hardware such as Ethernet protocol and CSMA for the Wi-Fi Technology to work .Like every communication network, this method also involves transmitter(Wireless Router/Hotspot) and receiver which can be any Wifi enabled device like laptop,mobile,tablet etc.

Many organizations and users have found that wireless communications and devices are convenient, flexible, and easy to use. Users of wireless local area network (WLAN) devices have flexibility to move their laptop computers from one place to another within their offices while maintaining connectivity with the network. Wireless personal networks allow users to share data and applications with network systems and other users with compatible devices, without being tied to printer cables and other peripheral device connections. Users of handheld devices such as personal digital assistants (PDAs) and cell phones can synchronize data between PDAs and personal computers and can use network services such as wireless email, web browsing, and Internet access. Further, wireless communications can help organizations cut their wiring costs.

A. WIFI – SOFTWARE TOOLS

Windowusers:KNSGEM2,NetStumbler,OmniPeek,Stumbverter, WiFi Hopper,APTools.

Unix users:Aircrack,Aircrack-ptw,AirSnort,CoWPatty,Karma

Mac users:Macstumble,KisMac,Kismet.

(Users may select a Wi-Fi software tool that is compatible with their computer or else it should be builtin)

B.FOR CONNECTING TO A WI-FI

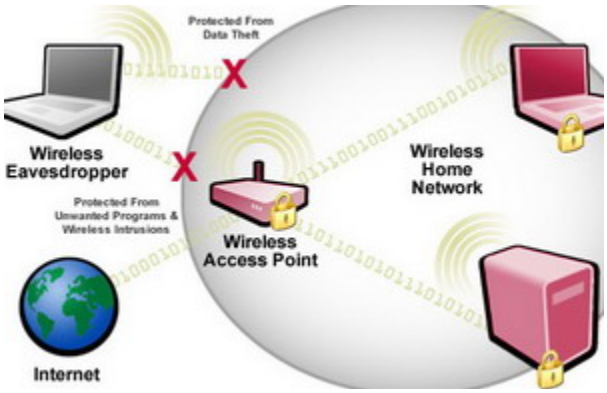
A wireless adapter card is essential .

The SSID infrastructure, and data encryption are also required.

The Wi-Fi security methods include-MAC ID filtering,Static IP addressing and WEP encryption.

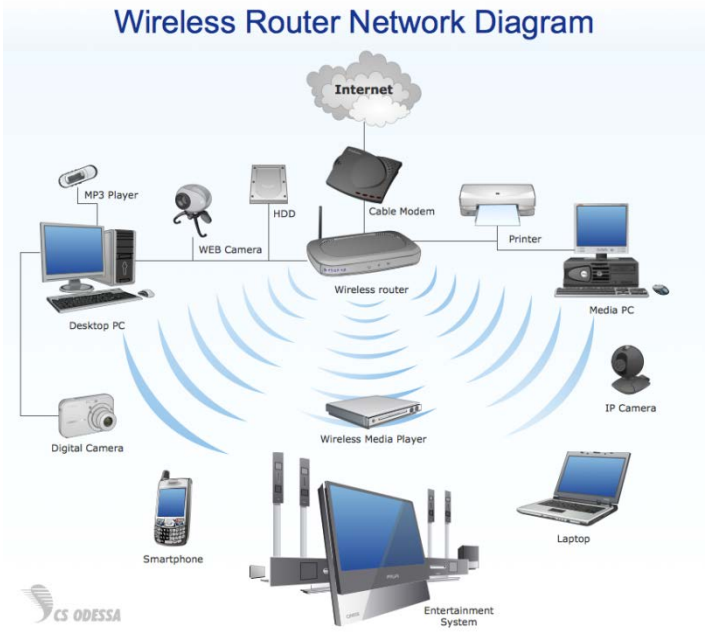
C.The Wi-Fi network technology is based on IEEE 802.11 protocol.Following are the various Wi-Fi Standards:

1)802.11a technology has a range of 5.725 GHz to 5.850GHz with a data rate of 54Mbps.
2)802.11b with a data rate of 11Mbps at 2.4GHz
3)802.11e addresses Qos issues and is excellent for streaming quality of video,audio and voice channels.
4)802.11f addresses multivendor interoperability
5)802.11g deals with higher data rate extension to 54Mbps in the 2.4GHz.
6)802.11h deals with dynamic frequency selection and transmit power control for operation of 5GHz products.
7)802.11i addresses enhanced security issues.
8)802.11j addresses channelization in Japan's 4.9GHz band.
9)802.11k enables medium and network resources more efficiently.
10)802.11 deals with Wireless Network Management which is still in progress.



II. EXISTING TECHNOLOGIES AND PROBLEMS

The basic existing technology for implementation of Wireless networks(WLAN) in residential and enterprise setups can be understood simply from these explanatory diagrams.



However our major concern in this research paper is that there are several issues associated with the deployment and management of WLAN. These include scalability,provisioning,real-time and non-real time data flow,accessibility range,power management interference from other systems operating in the same spectrum such as Bluetooth. Major problems that we need to address are-

1.Security Management

2.QoS(Quality of Service) and centralized Management of WLANs.

The Risk Environment

While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Wireless networks transmit data through radio frequencies, and are open to intruders unless protected. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users. Another risk is the theft of the small and portable devices themselves.

Wireless networks and handheld devices are vulnerable to many of the same threats as conventional wired networks. Intruders who gain access to information systems via wireless communications can bypass firewall protection. Once they have accessed systems, intruders can launch denial of service attacks, steal identities, violate the privacy of legitimate users, insert viruses or malicious code, and disable operations. Sensitive information that is transmitted between two wireless devices can be intercepted and disclosed if not protected by strong encryption. Handheld devices, which are easily stolen, can reveal sensitive information

III. SOLUTIONS BASED ON RESEARCH

Recommendations for Secure Wireless Networks

- Maintain a full understanding of the topology of the wireless network.
- Label and keep inventories of the fielded wireless and handheld devices.
- Create backups of data frequently.
- Perform periodic security testing,audits and assessment of the wireless network.
- Perform a risk assessment, develop a security policy, and determine security requirements before purchasing wireless technologies.
- Apply security management practices and controls to maintain and operate secure wireless networks after careful installation

- The information system security policy should directly address the use of 802.11, Bluetooth, and other wireless technologies.

- Configuration/change control and management practices should ensure that all equipment has the latest software release, including security feature enhancements and patches for discovered vulnerabilities.
- Standardized configurations should be employed to reflect the security policy, and to ensure change of default values and consistency of operations.
- Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies.
- Robust cryptography is essential to protect data transmitted over the radio channel, and theft of equipment is a major concern

- Enable, use, and routinely test the inherent security features, such as authentication and encryption methods that are available in wireless technologies.
- Firewalls and other appropriate protection mechanisms should also be employed

IV. RESULTS

THE RESEARCH FINDINGS SUGGEST THE RESULT THAT A SECURE ENVIRONMENT CAN BE CREATED FOR WIRELESS NETWORKS BY UNDERTAKING CERTAIN MEASURES WHICH WOULD ENABLE US TO GAIN ACCESS TO THESE WLANS BY MITIGATING POTENTIAL RISKS.

V. CONCLUSION

Organizations and individuals benefit when wireless networks and devices are protected. After assessing the risks associated with wireless technologies, organizations can reduce the risks by applying countermeasures to address specific threats and vulnerabilities. These countermeasures include management, operational, and technical controls which will not prevent all penetrations and adverse events, they can be effective in reducing many of the common risks associated with wireless technology.

ACKNOWLEDGMENT

I would sincerely thank CETTM, MTNL-Mumbai for providing useful resources and material for my research and would also like to thank my peers for the constant encouragement and critical review of my manuscript.

REFERENCES

[1] 3GPP:Standards organization associated with ITU.

[2] Gast,Matthew,802.11 Wireless Networks:The Definitive Guide,2nd Edition,O'Reilly Media,Inc.,2005

[3] Ni,Qiang,Romdhani,Lamia,and Turletti,Thierry,"A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN",Journal of Wireless Communication and Mobile computing,Vol.4,No.5,2004,pp547-566

[4] Mani Subramanium,Network Management-Principles and Practices,2nd Edition,Pearson,2013.

AUTHOR

First Author – Surabhi.S.Tambe

Final year Btech EXTC student,
Electrical Engineering Department,
Veermata Jijabai Technical Institute(VJTI)
Mumbai,India.

Email id- surabhitambe149@gmail.com