STM JOURNALS

Recent Trends in
Sensor Research & Technology

ISSN: 2393-8765
Volume 8, Issue 1, 2021
DOI (Journal): 10.37591/RTSRT

http://engineeringjournals.stmjournals.in/index.php/RTSRT/index

Review Article RTSRT

Wireless Technology in Network Application

Anand Singh[1,*], Rishita Pandey[2], Ankur Shukla[3]

Abstract

This research paper represents an overview regarding the Wireless Broadband network technology. This is focus on the history, tools, standards and implementation of Wi-Fi network. The wireless term refers to the transmission of the information over a medium without requiring wire. In present days, wireless technology has become an essential part of various type of wireless device. This research paper is used to understand the problem associated with the implementation of theses WLAN's and purpose recommendation and measures to solve these problem and risk factor.

Keywords: Wi-Fi, Security, QoS, WLAN's.

INTRODUCTION

In our daily lives telecommunication has been contributing widely advancement in various fields. A computer network that uses wireless data connection between networks nodes is called as a wireless network. Wireless broadband technology is used to transmit multiplexed information on a wide band of frequencies. The wireless broadband service is deployed by weighing the geographical population density against the limitation of bandwidth [1]. Wireless network are rapidly renderinga wide range pf personalized communicationservice as portable as cellular phones. There are many new wireless technologies involves Wireless Local Area Networks (WLAN's), which is enable a wide range of communication devices to stay connected to more conventional wired network without requiring users to be physically connected. The WLAN's allows users to move from one point to another without having to disconnect a network wire or cable from one jack and reconnect it to another jack. It was only few years ago that the thoughts of calling over 75 percent of the world from a hand-held wireless phone was inconceivable but nowadays it is normal. However, the change in wireless technology in just five years, it is reasonable to predict that wireless networks will replace all wired networks within the next few years.

This technology is designed to reduce different types of obstacles created by cable and it is also reducing the time which is convenient than wired networking. Wi-Fi technology is known as 'Wireless fidelity-popularly' in 1997 which was developed by IEEE standards which is used to provide users liberty to connect to the internet from any location. But this was quite expensive till 2002, until the new 802.11g standard in 2003 has leads to creation of Wi-Fi enabled devices to masses as a result nowadays Wi-Fi router has become a household commodity of the modern homes in India.

Since the inception of wireless technology, wireless technology has a come in a long way for providing quicker wireless access to internet application and data across a radio network thereby making the access process faster than conventional modem .Many organization and users have found

***Author for Correspondence**
Anand Singh

[1]Assistant Professor, Electronics & Communication Engineering, Bansal Institute of Engineering and Technology Lucknow, India
[2]Student, Electronics & Communication Engineering, Bansal Institute of Engineering and Technology Lucknow, India
[3]Assistant Professor, Electronics & Communication Engineering, Bansal Institute of Engineering and Technology Lucknow, India

Received Date: June,2,2021
Accepted Date: June,10,2021
Published Date: June,15,2021

Citation: Anand Singh, Rishita Pandey, Ankur Shukla. Wireless Technology in Network Application. Recent Trends in Sensor Research & Technology. 2021; 8(1): 1–5p.

that wireless communication and devices are convenient, flexible, and easy to use. Users of Wireless local area network (WLAN) devices have flexibility to move their laptop computer from one place to the within their offices while maintaining connectivity with the network [2]. Wireless personal network allows users to share data and compatible devices, without being tied to printer cables and other peripheral device connections. Users of handheld devices such as personal digital assistant 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 communication can help organization cut their wiring costs.

WIFI-SOFTWARE TOOLS

Windowusers: KNSGEM2, Netstumbler, Omnipeek, Stumbverter, Wifi Hopper, APTools.
Unix users: Aircrack, Aircrack-ptw, CoWPatty
Mac users: Macstumble, KisMac, Kismet.
(Users may select a WiFi software tool that is compatible with their computer or else it should be built-in).

For Connecting to a Wi-Fi

A wireless adapter card is essential. The SSID infrastructure and the data encryption are also required [3]. The Wi-Fi security methods include – MAC ID filtering, Static IP addressing and WEP encryption (Figure 1).

The Wi-Fi network is based on IEEE 802.11 protocols

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

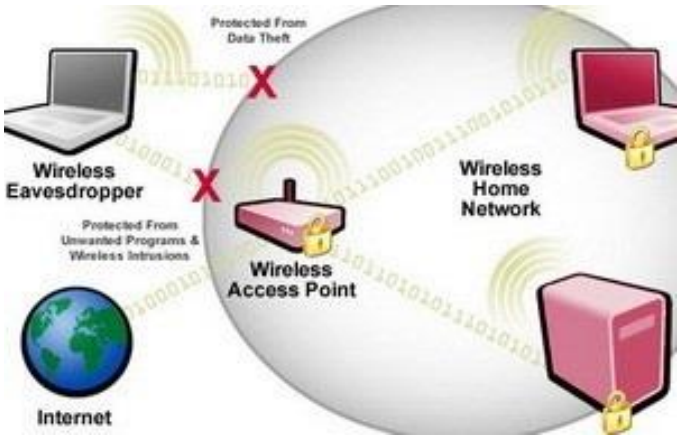

Figure 1. WiFi network using IEEE standard.

EXISTING TECHNOLOGIES AND PROBLEMS

The basic existing technology for implementation of Wireless Network in residential and enterprise setups can be understood simply.

However our major concern in this research paper is that there are several issues associated with the deployment and management of WLAN [4].

Figure 2. Wireless router Network Diagram.

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 in Figure 2 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 various of the same risks as wired networks, they are vulnerable to additional risks as well.

Wireless networks transmit data through the radio frequencies, and are to open to intruders unless protected. Intruders have exploited this openness to access systems, destroy or steal the data, and launch attacks that tie up network bandwidth and deny service to authorized users. Another risk is the theft of small and portable devices themselves [5, 7]. Wireless networks and handheld devices are vulnerable to several 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 and disables the operations. Handheld devices, which are easily stolen, can reveal sensitive information.

TYPES OF WIRELESS COMMUNICATION

The different types of wireless communication mainly include IR wireless communications, satellite communications, broadcast radio, Microwave radio, Bluetooth, Zigbee etc.

Satellite Communication

Satellite communication is one type of self contained wireless communication technology; it is widely spread all over the world to allow users to stay connected almost anywhere on the earth. When the signal is sent near the satellite then, satellite amplifies the signal and sent it back to the antenna receiver which is located on the surface of the earth call earth station (Figure 3). Satellite communication contains two main components: the space segment and the ground segment. The ground segment consists of fixed or mobile transmission, reception and ancillary equipment and the space segment, which mainly is the satellite itself.

Figure 3. Satellite Communication.

Infrared Communication

Infrared wireless communication communicates information in a device or systems through IR radiation. IR is an electromagnetic energy at a wavelength that is longer than that of red light wavelength. It is used for security control, TV remote control and short range communications. In the electromagnetic spectrum, IR radiation lies between microwave and visible light range. So, they can be used as a source of communication for a successful infrared communication, a photo LED transmitter and a photo diode receptor are required [9].

Figure 4. Infrared Communication.

The LED transmitter transmits the IR signal in the form of non visible light that is captured and saved by the photoreceptor. So the information between the source and the target is transferred in the way shown in Figure 4. The source and destination can be mobile phones, TVs, security systems, laptops etc supports wireless communication.

Broadcast Radio

The first wireless communication technology is the open radio communication to seek out widespread use, and it is still serving a purpose nowadays. Handy multichannel radios permit a user to speak over short distances, whereas citizen's band and maritime radios offer communication services for sailors. Ham radio enthusiasts share data and function emergency communication aids throughout disasters with their powerful broadcasting gear, and can even communicate digital information over the radio frequency spectrum [9].

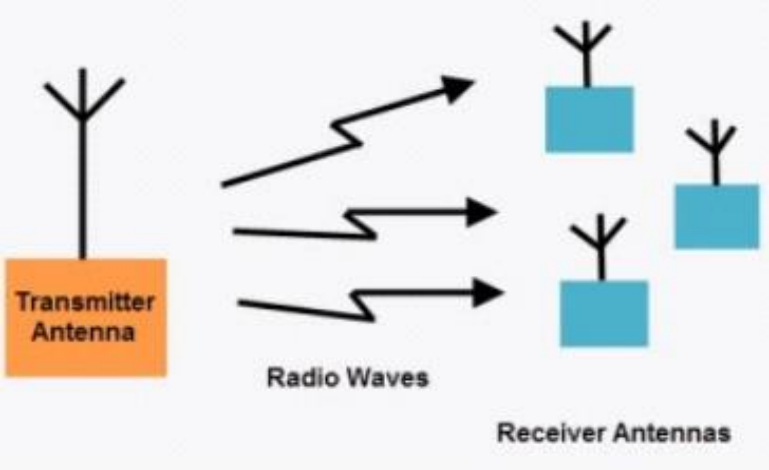

Figure 5. Broadcast Radio.

Mostly an audio broadcasting service, radio broadcasts sound through the air as radio waves. Radio uses a transmitter which is used to transmit the data in the form of radio waves to a receiving antenna (Different Types of Antennas). To broadcast common programming, stations are associated with the radio N/W's. The broadcast happens either in simulcast or syndication or both. Radio broadcasting may be done via cable FM, the net and satellites. A broadcast sends information over long distances at up to two megabits/Sec (AM/FM Radio) Figure 5.

Radios waves are electromagnetic signals that are transmitted by an antenna. These waves have completely different frequency segments, and you will be ready to obtain an audio signal by changing into a frequency segment.

SOLUTION BASED ON RESEARCH

Recommendation for secure Wireless Networks

- Maintain a full understanding of the topology of the wireless network [8].
- Label and keep inventories of the fielded wireless and handheld devices.
- Create backups of data frequently.
- Perform periodic security testing, audits and assessments of the wireless network.
- Perform a risk assessment, develop a security policy, and determine security requirements before purchasing wireless technologies [7].
- 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 features enhancement and patches for discovered vulnerabilities.
- Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies [6].
- Robust cryptography is essential to protect data transmitted over a 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 mechanism should also be employed.

CONCLUSION

Organizations and individual benefits when wireless networks and devices are protected. After assessing the risks associated with the wireless technologies, organization 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.

REFERENCES

1. Gast, Matthew, “802.11 Wireless Networks: The Definitive Guide”, 2nd Edition, O’Reilly Media, Inc.,2005
2. 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
3. Mani Subramanium, “Network Management-Principles and Practices”, 2nd Edition, Pearson, 2013.
4. P. E. Rybski, S. E. Stoeter, M. Gini, D. F. Hougen, and N. P. Papanikolopoulos,"Performance of a distributed robotic system using shared communications channels," IEEE Trans. Robot. Autom., vol.18, no. 5, pp. 713-727, Oct. 2004
5. V. K. Kongezos and C. R. Allen, "Wireless communication between A.G.V.'s (autonomous guided vehicle) and the industrial network C.A.N. (controller area network)," in Proc. IEEE Int. Conf. Robotics and Automation, 2002, pp. 434-437
6. J.-D. Decotignie and P. Pleineveaux, "Asurvey on industrial communication networks," Ann. Telecomm., vol. 48, no. 9, p. 435ff, 1993.
7. F. Hernandez-Campos, M. Karaliopoulos, M. Papadopouli, and H. Shen, "Spatio-temporal modeling of traffic workload in a campus WLAN," In Second Annual International Wireless Internet Conference, Boston, USA, 2006, pp. 265-272.
8. Andrew Miceli, “Wireless Technician’s Handbook, Second Edition”, Artech House, 2003.
9. Dr.M.Sengaliappan , Dr.K.Kumaravel, “Analysis Study of Wireless Technology and its Communication Standards Using IEEE 802.11”, IJARSET Vol. 4, Issue 6 , June 2017.

