

Basic Review Of Wireless Networks

Shreya Jain¹, Sukhwinder Singh²

Student, Electronics and Electrical Communication Department, PEC University of Technology, Chandigarh, India¹

Mentor, Assistant Professor, Electronics and Electrical Communication Department, PEC University of Technology, Chandigarh, India²

Abstract: With the arrival of wireless technology the human efforts for accessing data at various locations has reduced by replacing wired infrastructure with wireless infrastructure and also providing access to devices having mobility. In the past, some believed wired networks were faster and more secure than wireless networks. But continual enhancements in wireless networking standards and technologies have eroded those speed and security differences. Since bandwidth has to be constrained, some of the key challenges in wireless networks are Signal fading, mobility, data rate enhancements, minimizing size and cost, user security and (Quality of service) QoS. This paper is intended to provide the reader with an overview of the Wireless networking and Challenges in wireless networks.

Keywords: Wireless Local Area Networks (WLANs), Wireless Personal Area Networks(WPANs), IEEE 802.11, Quality of Service (QoS), Wired Equivalent Privacy (WEP), Virtual Private Network (VPN)

I. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. The explosive growth in wireless networks over the last few years resembles the rapid growth of the internet within the last decade. Wireless communication continues to enjoy exponential growth in the cellular telephony, wireless internet and wireless home networking arenas. With advent of Wireless LAN (WLAN) technology, computer networks could achieve connectivity with a useable amount of bandwidth without being networked via a wall socket. Wireless personal area networks (WPANs) are also there used to interconnect devices within a relatively small area, that is generally within a person's reach. For example, both Bluetooth radio and invisible infrared light provides a WPAN for interconnecting a headset to a laptop.

New generations of handheld devices allowed users access to stored data even when they travel. Users could set their laptops down anywhere and instantly be granted access to all networking resources. This was, and is, the vision of wireless networks, and what they are capable of delivering. Today, while wireless networks have seen widespread adoption in the home user markets, widely reported and easily exploited holes in the standard security system have stunted wireless deployment rate in enterprise environments. Over time, it became apparent that some form of security was required prevent outsiders from exploiting the connected resources.

We believe that the current wireless access points present a larger security problem than the early Internet connections. As more wireless technology is wireless technology, this will be a good stepping-stone for providing a good secure solution to any wireless solution. In the rest of this paper we present something more about wireless network, its benefits and a brief overview about Challenges and Issues of Wireless Networks. Finally conclusion of the whole paper is presented.

II. MORE ABOUT WIRELESS NETWORKS

A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications. The distinguishing feature of wireless networks is that packets (segments) are transmitted with the presence of wireless links. A device can send messages in a wireless network via the wireless medium, air, to another device provided that the receiver is within the transmission range of the sender. Examples of wireless networks include cell phone networks, Wi-Fi local networks and terrestrial microwave networks.

A. Terrestrial microwave

Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low-gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.

B. Communication satellite

Satellites communicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 mi) above the equator. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals.

C. Cellular and PCS systems

They use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area.

D. Radio and spread spectrum technologies

Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. IEEE 802.11 defines common

flavor of open-standards wireless radio-wave technology known as Wi-Fi.

E. Free-space optical communication

It uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices.[7]

III. BENEFITS OF WIRELESS NETWORK

A. Convenience

We can access network resources from any location within wireless network's coverage area or from any Wi-Fi hotspot.

B. Mobility

You are no longer tied to your desk as you were with a wired connection you and your employees can go online in conference room meetings, for example.

C. Productivity

Wireless access to the Internet and to your company's key applications and resources helps your staff get the job done and encourages collaboration.

D. Easy setup

You don't have to string cables, so installation can be quick and cost-effective.

E. Expandable

You can easily expand wireless networks with existing equipment, while a wired network might require additional wiring.

F. Security

Advances in wireless networks provide robust security protections.

G. Cost

Because wireless networks eliminate or reduce wiring costs, they can cost less to operate than wired networks.[8]

IV. CHALLENGES OF WIRELESS NETWORK

Since wireless devices need to be small and wireless networks are bandwidth limited, some of the key challenges in wireless networks are data rate enhancements, minimizing size, cost, low power networking, user security and Quality of Service (QoS).[1]

A. Signal Fading

Unlike wired media, signals transmitted over a wireless medium may be distorted or weakened because they are propagated over an open, unprotected, and ever changing medium with irregular boundary. Besides, the same signal may disperse and travel on different paths due to reflection, diffraction, and scattering caused by obstacles before it arrives at the receiver. The dispersed signals on different paths may take different times to reach the destination. Thus, the resultant signal after summing up all dispersed signals may have been significantly distorted and attenuated when compared with the transmitted signal. The receiver may not recognize the signal and hence the transmitted data cannot be received. This unreliable nature of the wireless medium causes a substantial number of packet losses.

B. Mobility

Without the constraints imposed by the wired connections among devices, all devices in a wireless network are free to move. To support mobility, an ongoing connection should be kept alive as a user roams around. In an infrastructure network, a handoff occurs when a mobile host moves from the coverage of a base station or access point to that of another one. A protocol is therefore required to ensure seamless transition during a handoff. This includes deciding when a handoff should occur and how data is routed during the handoff process. In some occasions, packets are lost during a handoff.

C. Power and Energy

A mobile device is generally handy, small in size, and dedicated to perform a certain set of functions; its power source may not be able to deliver power as much as the one installed in a fixed device. When a device is allowed to move freely, it would generally be hard to receive a continuous supply of power. To conserve energy, a mobile device should be able to operate in an effective and efficient manner.

D. Data Rate

Improving the current data rates to support future high speed applications is essential, especially, if multimedia service are to be provided. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control, and the data transfer protocol. Data compression plays a major role when multimedia applications such as video conferencing are to be supported by a wireless network. Currently, compression standards such as MPEG-4 produce compression ratios of the order of 75 to 100. The challenge now is to improve these data compression algorithms to produce high quality audio and video even at these compression rates. Unfortunately, high compressed multimedia data is more sensitive to network errors and interference and this necessitates the use of algorithms to protect sensitive data from being corrupted, be to employ intelligent data transfer protocols that adapt to the time varying network and traffic characteristics. Efficient error control algorithms with low overhead must be explored.

E. Security

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications.[6] Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users. The IEEE 801.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point. In large enterprises, an IP network level security[4] solution could ensure that the corporate network and proprietary data are safe. Virtual private network (VPN) is an option to make access to fixed access

networks reliable. Wireless security features must be updated constantly.

F. Quality of Service(QoS)

Quality of Service is a measure of network performance that reflects the network's transmission quality and service availability. For each flow of network traffic, QoS can be characterized by four parameters: Reliability, Delay, Jitter, and Bandwidth. Several important wireless network characteristics include handoff, dynamic connections, and actuating transport QoS[2]. In a wireless environment, connections may temporarily break during a process termed handoff[3]. Unlikely that handoff can take place without at least a short connection interruption. Applications running in a wireless environment must be able to recover from temporary interruptions, and should specify the maximum connection interruption time that they can tolerate. [1]

V. CONCLUSION

This paper identifies and describes various things related to wireless network. In conclusion, wireless networks are rapidly becoming popular, and user demand for useful wireless applications is increasing as there are many benefits of wireless networks like convenience, mobility, productivity, security. It is easy to set and has less cost. Still, there is a comprehensive list of research issues and challenges of the wireless network like signal fading problem, mobility problem, power and energy, data rate enhancement, security and the quality of service issues. By successfully addressing the issues presented in this paper, end users will not be disappointed.

ACKNOWLEDGEMENT

I take this opportunity to sincerely thank my teacher Mr. Sukhwinder Singh whose inspiring guidance, help and motivation allowed me to develop a keen interest in the topic. This work would not have been possible without the support of my parents who have always been a source of inspiration. Last but not the least I wish to thank all my friends.

REFERENCES

- [1] Raj Kumar Singh "Research issues in wireless networks" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012
- [2] Paulo Salvador, Ant'onio Nogueira, Rui Valadas —Predicting QoS Characteristics on Wireless Network 25 June 2007.
- [3] Jim Kurose —Open issues and challenges in providing quality of service in high-speed networks Computer Communication Review, 23(1):6-15, January 1993.
- [4] Sandra Kay Miller —Facing the Challenge of Wireless Security July 2001
- [5] V.O.K. Li and X. Qiu, —Personal Communication Systems (PCS), Proc. IEEE, vol. 83, no. 9, Sept. 1995.
- [6] Chip Craig J. Mathias Principal, Farpoint Group COMNET 2003 —Wireless Security: Critical Issues and Solutions 29 January 2003
- [7] http://en.wikipedia.org/wiki/Wireless_network
- [8] http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/work_from_anywhere/what_is_a_wireless_network/index.html.