Volume 2, Issue 2, April 2015 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Challenges in Wireless Networks

Pooja Ahirwar
Research Scholar
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email:pooja.adina@gmail.com @gmail.com

Namrata Mishra
Research Scholar
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email: namrita.adina@gmail.com

Rajneesh Pachouri
Assistant Professor
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]
Email: rajneeshrocks92@gmail.com

Swati Jain
Head of The Department
Department of Computer Science & Engineering
Adina Institute of Science and Technology
Sagar (M.P.), [INDIA]

Abstract

The advantages of wireless technology with wireless infrastructure by replacing the wired infrastructure for accessing data at different locations and also to provide access to mobility devices being decreased in human endeavors. For bandwidth constrained wireless devices need to be small and, since some of the key challenges in wireless network signal size and cost, user safety and (Quality of Service) QoS to reduce the data rate enhancements, fading mobility have been. This paper is intended to provide the reader with an overview of the Challenges in wireless networks.

Keywords:*—GDS, BPR, electronic commerce, information technology, OIS.*

I. Introduction

The explosive growth of wireless networks in recent years is similar to the rapid growth of the Internet in the last decade. Wireless communication continues to enjoy exponential growth of mobile telephony, wireless Internet and wireless home networking arenas. With the advent of wireless LAN technology (WLAN), computer networks could achieve connectivity with a useful amount of bandwidth without being networked through an outlet. The new generation of handheld devices allows users to access stored data even when traveling. Users could configure their laptops anywhere and instantly be granted access to all network resources. This was, and is, the vision of wireless networks, which are able to deliver. Today, while wireless networks[1] have seen widespread adoption in the market of home users, widely and easily exploited holes in the standard security system has atrophied rate wireless deployment in enterprise environments. Over time, it became clear that some sort of security is needed to prevent outsiders from exploiting the resources online. We believe that current wireless access points have a bigger security problem than internet early connections. As the wireless technology is wireless, this will be a good stepping stone to provide a good secure solution for any wireless solution.

The rest of this article is organized as follows; first taxonomy of wireless networks and giving presents discussion of the two operating modes of the IEEE 802.11 in the second section. Here is a brief review of research on the challenges and issues of wireless networks in the third section and finally, the fourth section gives the conclusion of the whole paper.

2. Taxonomy of Wireless Networks

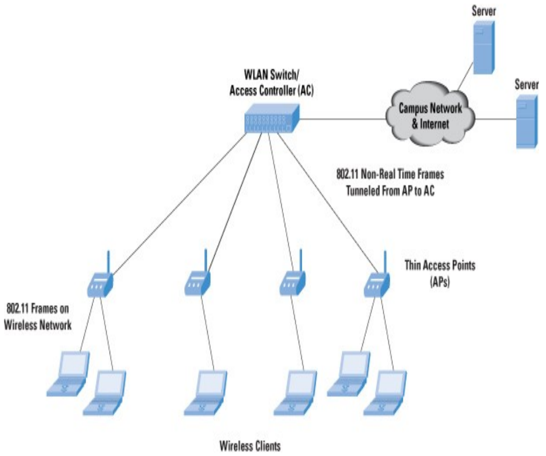

Figure 1: Taxonomy of Wireless Networks

The distinguishing feature of the wireless network packet (s) with the presence of the wireless link is transmitted. A device receiver is within transmission range of the sender, subject to another device, the wireless medium, through the air in a wireless network can send messages. It has set up a wireless network is structured and how the flexibility to say. In addition, the device supports mobility.

IEEE 802.11

IEEE 802.11 wireless local area network (WLAN) communication is a basic standard. IEEE 802.11 wireless local area connectivity standard before it envisioned for the home and office environments, was started in 1997 and broadcast technologies, ie Infrared (IR), frequency spectrum (FHSS Hopping Spread) was to support three types of Direct Sequence Spread Spectrum (DSSS). In 1999 two other transmission technologies including Orthogonal Frequency Division Multiplexing (OFDM) and a high rate Direct Sequence Spread Spectrum (Acar-DSSS). The second OFDM modulation scheme was introduced in 2001 for higher data rates.[2] standard wireless networks, namely, infrastructure networks and ad hoc networks, the introduction of two operating modes.

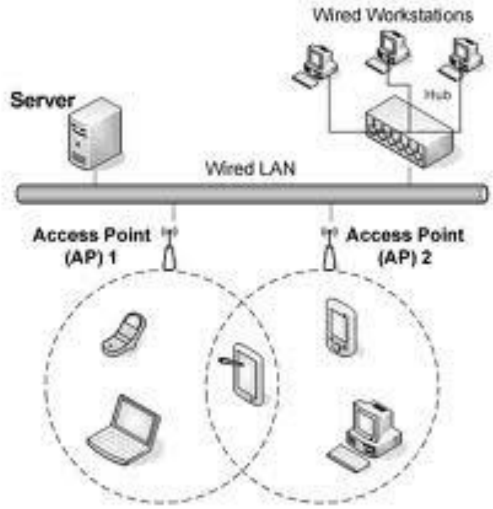

Figure 2: Wireless Local Area Network

A. Infrastructured Networks

The infrastructure operating mode (Figure 1) all STAs to access the network must be connected to the AP, which an Access Point (AP) with a network. AP STAs communicate with each other through. The infrastructure is planned, with permanent network device installations. It is host to a base station or a wireless access point, known as a fixed point, which can connect via a fixed topology, can be installed with. After often connected to each other via a link, is connected to the backbone network. Cellular Network[3] and most of Wireless Local Area Network (WLANs) [4] as a stable network infrastructure to operate. Broadcast coverage of the base station within the wireless hosts to connect to it and spinal cord to communicate with the network can use it. This introduced a wireless host or hosts all communications destined connects directly to the base station through which to pass the means. Also, a basic structured network topology with a semi-static or a dynamic being installed. [5] A satellite network belongs to this category. It is a space segment and a ground segment. The space segment includes the satellites. Ground segment through long-haul satellite links through which all communications take place entrance stations (GSS), known as a large number of base stations. Base station, or access point, communication is an important element.

B. Ad Hoc Networks

No access points in the network (APS) are the second operating mode, free mode or ad hoc mode (Figure 2) is used. In this mode, stations (STAs) with each other directly, as an ad hoc network. An ad-hoc network, such as a packet radio network, a certain topology is without. Whenever a wireless receiver directly into the host broadcast coverage independently and can communicate with the host. The host is not in a wireless coverage area that you want to send messages to another host, the first time in their transmission range will relay them to the host. As a relay on its way to the destination host functions to forward messages. The major advantage is the flexibility of configuration. An ad hoc network any predetermined fixed infrastructure can be easily created without the need. In addition, an ad-hoc network to maintain connectivity to the network device does not have any significant as compared to an infrastructure network is generally more robust. In other words, it failed all wireless communication between the base station and blocking connecting host, to host an ad hoc wireless network will be divided because of failure, but a failure of a base station network infrastructure division is not likely to be the other host in the network. However, there are some drawbacks to the ad hoc network. First, it hosted the dynamics of constant changes in network topology due to perform ad-hoc network routing is more difficult and complex.

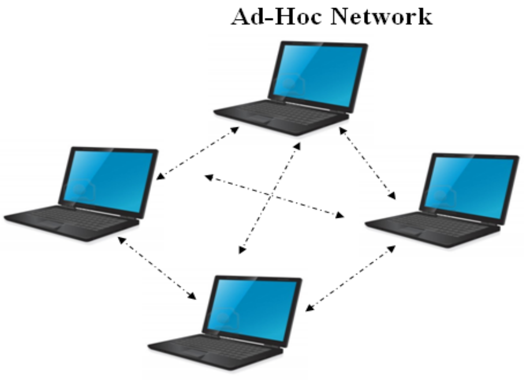

Figure 3: Ad Hoc Wireless Network

Second, it is more difficult to control or coordinate proper operation of an ad hoc network, since each wireless host may have its own algorithms to perform activities such as time synchronization, power management, and packet scheduling. In an infra structured network, these algorithms are often implemented in and thus harmonized by the base stations or access points.

3. RESEARCH CHALLENGES OF WIRELESS NETWORKS

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).

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. In an ad hoc network, the topology changes when a mobile host moves. This means that, for an ongoing data communication, the transmission route may need to be recomputed to, cater for the topological changes. Since an ad hoc network may consist of a large number of mobile hosts, this imposes a significant challenge on the design of an effective and efficient routing protocol that can work well in an environment with frequent topological changes.

C. Power and Energy

Figure 4: 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. To be specific, it should be able to transmit and receive in an intelligent manner so as to minimize the number of transmissions and receptions for certain communication operations [7].

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. Therefore, it is imperative that manufacturers implement a well thought out design that considers these factors in order to achieve higher data rates. 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, highly 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. Efficient error control algorithms with low overhead must be explored. Another way to enhance the data rates would be to employ intelligent data transfer protocols that adapt to the time-varying network and traffic characteristics.

E. Security

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications [8]. 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[2] 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[9] 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. Since hackers are getting smarter, it is imperative that wireless security features must be updated constantly [10].

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.

There are several important issues related to QoS in wireless networks that do not get addressed in the wired-line environment. These issues arise because wireless networks are inherently different from wired-line networks. Several important wireless network characteristics include handoff, dynamic connections, and actuating transport QoS [11]. The traffic QoS parameters (throughput, delay and loss rate) are not sufficient in a wireless environment. In a wired-line environment, the application layer can normally be assured that once a connection is established it will continue to exist until it is closed. In a wireless environment, connections may temporarily break during a process termed handoff [12]. It is 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. The application could specify such a time via a large loss rate; however, this would overload the meaning of loss rate. Loss rate should only reflect losses due to buffer overflow or transmission errors. A maximum frequency of connection interruption is another performance parameter that would be valuable in a wireless network. Some applications may request a low interruption frequency so that the QoS perceived by the user remains satisfactory. For example, an application may wish to guarantee that a voice connection will not be broken more than once per minute. A low interruption frequency implies that handoffs do not occur too often. Applications may accept a larger maximum connection interruption time in exchange for a low interruption frequency. For example, it may be more desirable to have infrequent long breaks in a video connection, rather than frequent smaller breaks.

4. CONCLUSION

This paper identifies various research issues and challenges in the wireless domain describes. We presented an overview of the classification of the fist wireless network. Signal problems, mobility problems, power and energy, increase data rate, security and in addition, the popularity of wireless network problems in the quality of service issues is fading as we research the issues and challenges of wireless networks with a broad list overview of wireless networks is growing at an exponential rate, data rate enhancements, QoS issues necessary to achieve the size, cost, low-power networking, user safety and minimize the need for good and becomes more challenging.

Finally, wireless networks are becoming increasingly popular, and useful user demand for wireless applications is increasing. By successfully addressing the issues presented in this paper, end users will not be disappointed.

REFRENCES:

[1] http://en.wikipedia.org/wiki/Wireless_network

[2] IEEE 802.11-1999, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 12, 1999.

[3] V.O.K. Li and X. Qiu, ―Personal Communication Systems (PCS),‖ *Proc. IEEE*, vol. 83, no. 9, Sept. 1995,

[4] J.H. Schiller, *Mobile Communications, 2nd ed.*, Addison-Wesley, 2003.

[5] Y. Hu and V.O.K. Li, ―Satellite-Based Internet: A Tutorial, *IEEE Common. Mag.*, vol. 39, no. 3, Mar. 2001, pp. 154–62.

[6] A. Gupta, I. Wormsbecker, and C. Williamson, Experimental Evaluation of TCP Performance in Multi-Hop Wireless Ad Hoc Networks, *Proc. IEEE MASCOTS 2004*, Volendam, The Netherlands, 4–8 Oct. 2004, pp. 3–11.

[7] H. Singh and S. Singh, ―Energy Consumption of TCP Reno, Newreno, and SACK in Multi-Hop Wireless Networks, *ACM SIGMETRICS Perf. Evaluation Rev.*, vol. 30, no. 1, June 2002, pp. 206-216.

[8] Chip Craig J. Mathias Principal, Far point Group COMNET 2003 ―Wireless Security: Critical Issues and Solutions‖ 29 January 2003.

* * * * *