Volume 2, Issue 4, April 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Research Issues in Wireless Networks

Raj Kumar Singh[1]
M.Tech. (2nd yr)
Department of Instrumentation & Control
Dr. B.R. Ambedkar National Institute of Technology
Jalandhar, Punjab (India)
rajmtechnit@gmail.com

Dr.A.K.Jain[2]
Professor & Head
Department of Instrumentation & Control
Dr. B.R. Ambedkar National Institute of Technology
Jalandhar, Punjab (India)
jainak@nitj.ac.in

Abstract— **The arrival of wireless technology has reduced the human efforts for accessing data at various locations by replacing wired infrastructure with wireless infrastructure and also providing access to devices having mobility.Since wireless devices need to be small and bandwidth 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 Research Issues and Challenges in wireless networks.**

Keywords— **Wireless Local Area Networks (WLANs), IEEE 802.11, Quality of Service (QoS).**

I. INTRODUCTION

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. 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 [1] 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 to prevent outsiders from exploiting the connected resources. We believe that the current wireless access points present a larger security problem than the early lntemet 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.

The rest of this paper is organized as follows; firstly we present the taxonomy of wireless networks and giving the discussion of the two operating modes of the IEEE 802.11 in second section. We then provide a brief overview about Research Challenges and Issues of Wireless Networks in section third. And finally the section fourth gives the conclusion of the whole paper.

II. TAXONOMY OF WIRELESS NETWORKS

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. This adds flexibility to how a wireless network is formed and structured. Besides, it supports device mobility.

IEEE 802.11

IEEE 802.11 is a basic standard for Wireless Local Area Network (WLAN) communication. IEEE 802.11 standard was first introduced in 1997. It was envisioned for home and office environments for wireless local area connectivity and supports three types of transmission technologies namely i) Infrared (IR), ii) Frequency Hopping Spread Spectrum (FHSS), iii) Direct Sequence Spread Spectrum (DSSS). In 1999 two other transmission technologies were included Orthogonal Frequency Division Multiplexing (OFDM) and High Rate Direct Sequence Spread Spectrum (HR-DSSS). The second OFDM modulation scheme was introduced in 2001 for high data rates [2]. The standard introduces two operating modes of wireless networks, namely, the infrastructure networks and the ad hoc networks.

A. Infrastructured Networks

The infrastructure operating mode (Fig 1) is a network with an Access Point (AP), in which all STAs must be associated

with an AP to access the network. STAs communicate with each other through the AP. An infrastructured one with planned, permanent network device installations. It can be set up with a fixed topology, to which a wireless host can connect via a fixed point, known as a base station or an access point. The latter is connected to the backbone network, often via a wired link. Cellular networks [3] and most of the wireless local area networks (WLANs) [4] operate as the static infrastructured networks. All wireless hosts within the transmission coverage of the base station can connect to it and use it to communicate with the backbone network. This means that all communications initiated from or destined to a wireless host have to pass through the base station to which the host connects directly. In addition, an infra-structured network is also be established with a quasi-static or a dynamic topology. A satellite network [5] belongs to this category. It has a space segment and a ground segment. The space segment comprises of satellites. The ground segment has a number of base stations, also known as gateway stations (GSs), through which all communications via long-haul satellite links take place. The base station, or access point, is a critical element for communication.

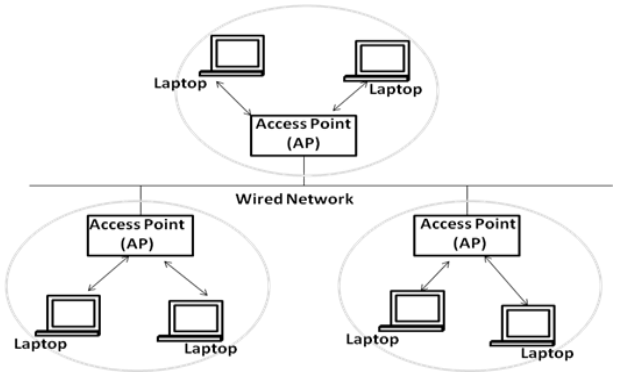

Fig. 1 Infrastructure wireless network

To maintain an ongoing connection when a mobile host moves away from the coverage of its base station, a terminal handoff occurs such that a mobile host hands over its proxy for communication from one base station to another one. Whenever the coverages of several neighboring base stations overlap with each other, a mobile host may connect to one of the reachable base stations based on certain criteria.

B. Ad Hoc Networks

The second operating mode, the independent mode or the ad hoc mode (Fig 2) is used if there are no Access Points (APs) in the network. In this mode, Stations (STAs) form an Ad hoc network directly with each other.An ad hoc network, such as a packet radio network, is one without a fixed topology. A wireless host can freely communicate with another host directly whenever the receiver is in its transmission coverage. If a wireless host would like to send messages to another host which is not in the coverage region, it will first relay them to a host in its transmission range. The host functions as a relay to forward the messages on its way to the destination. The major advantage of this configuration is flexibility. An ad- hoc network can be built easily, without the need of any preset, fixed infrastructure. In addition, an ad hoc network is generally more robust than an infrastructured network as it does not have any critical device to maintain the network connectivity. In other words, it is unlikely an ad hoc network will be partitioned due to the failure of a wireless host, but the malfunction of a base station may partition an infrastructure network, blocking the communication between all wireless hosts connecting to the failed base station and all other hosts in the network. However, there are some drawbacks for ad hoc networks. First, it is much more difficult and complex to perform routing in ad hoc networks because of frequent changes in the network topology due to host mobility.

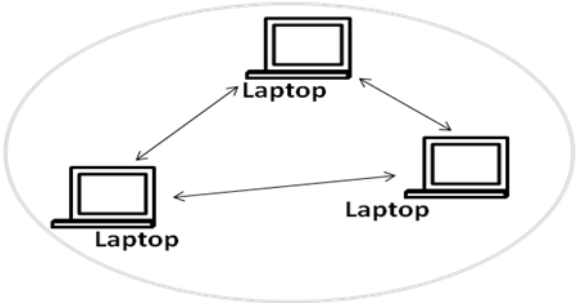

Fig. 2 Ad Hoc wireless network

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.

III.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 infrastructured 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

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 wireline environment. These issues arise because wireless networks are inherently different from wireline 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 wireline 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.

IV. CONCLUSION

This paper identifies and describes the various research issues and challenges available in the wireless domain. We fist presented an overview of the taxonomy of wireless network. We presented an overview of 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 problems of the wireless networks .In addition the popularity of wireless networks growing at a exponential rate, the data rate enhancements, minimizing size, cost, low power networking, user security and the best requirement to obtain the required QoS problems becomes more challenging.

In conclusion, wireless networks are rapidly becoming popular, and user demand for useful 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 Commun. 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, Farpoint Group COMNET 2003 "Wireless Security: Critical Issues and Solutions" 29 January 2003

[9] Sandra Kay Miller "Facing the Challenge of Wireless Security" July 2001

[10] T. Karygiannis and L. Owens. Wireless Network Security:802.11, Bluetooth and Handheld Devices. In *NIST Special Publication 800-48*, November 2002.

[11] Paulo Salvador, Ant´onio Nogueira, Rui Valadas "Predicting QoS Characteristics on Wireless Networks" 25 June 2007.

[12] Jim Kurose "Open issues and challenges in providing quality of service in high-speed networks" Computer Communication Review, 23(1):6-15, January 1993.

AUTHOR BIOGRAPHIES

Raj Kumar Singh was born at Bareilly, Uttar Pradesh, India on 24th October, 1989. Currently, He is pursuing his M.Tech degree in Instrumentation and Control Engineering from NIT Jalandhar. He did his B.Tech in Electronics and Communication Engineering from M.J.P. Rohilkhand University Bareilly Uttar Pradesh India in 2009. He has published several papers in national conferences and international journals on wireless and robotics. His area of research interest includes modelling and simulation of wireless networks, robotics, brain computer interfacing and biomedical applications.

A.K.Jain received his B.E and M.E both from IIT, Roorkee, (erstwhile University of Roorkee, Roorkee) India in 1981 and 1987 respectively and received his Ph.D. degree on Quality of Service in High Speed Networks from the Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India in 2009.He has published over twenty-five research papers in national and international journals/conferences. He is presently working as Professor and Head in the Department of Instrumentation and Control Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India. He is guiding Ph.D and M.Tech students in the area of Wireless Networks. Before joining N.I.T, Jalandhar, he has served at TIET Patiala, IET Lucknow, and NIT Hamirpur (Erstwhile REC Hamirpur) in various capacities. His research interests include quality of service in wireless networks, medium access protocols for mobile computing, and mesh networks. Dr. Jain is life member of ISTE India.