Wireless Communication Networks and Technical Challenges

Ritika Tandon
Assistant Professor, EC Depatment
MIT, Moradbad, Uttar Pradesh, India
ritikatandon15@gmail.com

Alpana Singh
Assistant Professor, EC Depatment
MIT, Moradbad, Uttar Pradesh, India
aalps_646@rediffmail.com

Saurbh Khanna
Assistant Professor, EC Depatment
NIT, Meerut, Uttar Pradesh, India
Saurabh.khanna33@gmail.com

Pragati Gupta
Assistant Professor, EC Depatment
MIT, Moradabad, Uttar Pradesh, India
guptapragati30@gmail.com

Abstract:

This paper presents an overview of wireless networks, with emphasis on the most popular standards: IEEE802.11. 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.

Keywords— Wireless Local Area Networks (WLANs), IEEE 802.11.

I. INTRODUCTION

The wireless arena has been experiencing exponential growth in the past decade. The advances in network infrastructures, growing availability of wireless applications, and the emergence of omnipresent wireless device such as portable or handheld computers, cell phones are all getting more powerful in their capabilities. A wireless network is an infrastructure to communicate 'through the airwaves', in other words, no cables are needed to connect from one point to another. These connections can be used for speech, e-mail, surfing on the Web and to transmit audio and video. The most widespread use is mobile telephony. Wireless networks are also used to communicate between computers. The primary attraction is its ability to cross long distances without installing fixed lines and cables**.** These devices are now playing an ever increasingly important role in lives. Recently, industry has made significant progress in resolving some constraints to the widespread adoption of wireless technologies. Some of the constraints have included disparate standards, low bandwidth, and high infrastructure and service cost. Wireless technologies can both support the institution mission and provide cost effective solutions. Wireless is being adopted for many new applications: to connect computers, to allow remote monitoring and data acquisition, to provide access control and security, and to provide a solution for environments where wires may not be the best solution.

This paper is organized to survey the state of wireless networking as follows; firstly we present the evolution of wireless networks and giving the brief discussion of development in wireless communication in second section. We then provide a discussion of IEEE 802.11 in third section and then we discuss some advantages and disadvantages of Wireless Networks in section fourth section. And finally the section fifth gives the conclusion of the whole paper.

II. EVOLUTION OF WIRELESS NETWORK

In February 1896, Guglielmo Marconi journeyed from Italy to England in order to show the British telegraph authorities what he had developed in the way of an operational wireless telegraph apparatus. His first British patent application was filling on June 2 of that year. Through the cooperation of Mr W.H. Preece, who was at that time the chief electrical engineers of the British Post-office Telegraphs, signals were sent in July 1896 over a distance of one-and-three-fourths miles on Salisbury Plain.

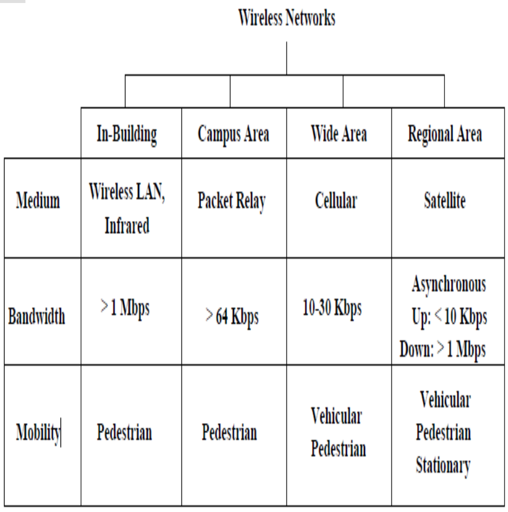
Table1. A simple timeline in Wireless Technologies evolution

1896	Guglielmo Marconi develops the first wireless telegraph system
1927	First commercial radiotelephone service

	operated between Britain and the US
1946	First car-based mobile telephone set up in St. Louis, using 'push-to-talk' technology
1948	Claude Shannon publishes two benchmark papers on Information Theory, containing the basis for data compression (source encoding) and error detection and correction (channel encoding)
1950	TD-2, the first terrestrial microwave telecommunication system, installed to support2400 telephone circuits
1960	Early in the decade, the Improved Mobile Telephone System (IMTS) developed with simultaneous transmit and receive, more channels, and greater Power
1962	The first communication satellite, Telstar, launched into orbit
1964	The International Telecommunications Satellite Consortium (INTELSAT) established, and in 1965launches the Early Bird geostationary satellite
1968	Defence Advanced Research Projects Agency – US(DARPA) selected BBN to develop the Advanced Research Projects Agency Network (ARPANET), the father of the modern Internet
1970s	Packet switching emerges as an efficient means of data communications, with the X.25 standard emerging late in the decade
1977	The Advanced Mobile Phone System (AMPS),invented by Bell Labs, first installed in the US with geographic regions divided into 'cells' (i.e. cellular telephone)
1983	January 1, TCP/IP selected as the official protocol for the ARPANET, leading to rapid growth
1990	Motorola files FCC application for permission to launch 77 (revised down to 66) low earth orbit communication satellites, known as the Iridium System (element 77 is Iridium)
1992	One-millionth host connected to the Internet, with the size now approximately doubling every year
1993	Internet Protocol version 4 (IPv4) established for reliable transmission over the Internet in conjunction with the Transport Control Protocol (TCP)
1994-5	FCC licenses the Personal Communication Services (PCS) spectrum (1.7 to 2.3 GHz) for $7.7 billion
1998	Ericsson, IBM, Intel, Nokia, and Toshiba announce they will join to develop Bluetooth for wireless data exchange between handheld computers or cellular phones and stationary computers
2000	802.11(b)-based networks are in popular demand
2000-1	Wired Equivalent Privacy (WEP) Security is broken. The search for greater security for 802.11(x)-based networks increases

III. TYPES OF WIRELESS NETWORK

Wireless network gives user information access regardless of their location. Keeping this in mind the wireless network can be classifies as given below



	In-Building	Campus Area	Wide Area	Regional Area
Medium	Wireless LAN, Infrared	Packet Relay	Cellular	Satellite
Bandwidth	>1 Mbps	>64 Kbps	10-30 Kbps	Asynchronous Up: <10 Kbps Down: >1 Mbps
Mobility	Pedestrian	Pedestrian	Vehicular Pedestrian	Vehicular Pedestrian Stationary

According to network formation and architecture the wireless network can be divided into two broad categories:

(i)**Infrastructure based network-** A network with reconstructed infrastructure that is made of fixed and wired network node and gateways with typically network services delivered via these preconfigured infrastructure.

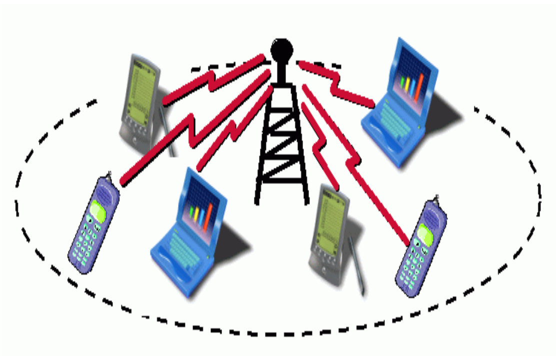


Fig. 1 Infrastructure wireless network

(ii)Infrastructure less (ad hoc) network- in this case a network is formed dynamically through the cooperation of an arbitrary set of independent nodes. There is no prearrangement regarding the specific role each node should assume. Instead, each node makes its decision independently, based on the network situation, without using a preexisting network infrastructure.

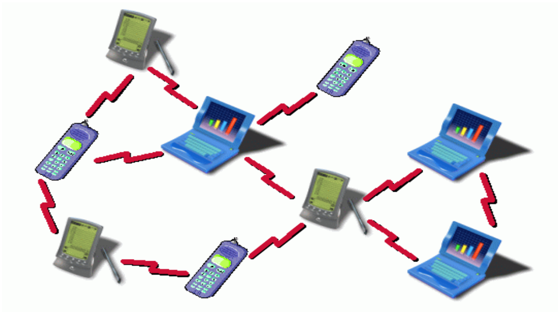


Fig. 2 Ad Hoc wireless network

IV. DEVELOPMENT OF WIRELESS TECHNOLOGY

The wireless communication landscape has been changing dramatically, driven by the rapid advances in wireless technologies and the greater collection of new wireless services and applications. The emerging third generation cellular networks have greatly improved data transmission speed, which enables a variety of higher-speed mobile data services. Meanwhile, new standards for short range radio such as Bluetooth, 802.11, Hipper LAN, and infrared transmission are helping to create a wide range of new applications for enterprise and home networking, enable wireless broadband multimedia and data communication in office and home.

The use of wireless networks in developing areas is promising. Since ground cables are only economic in high-density environments, a wireless network is much cheaper when long distances need to be crossed to rural areas.The strengths of wireless networks are their easy installation, low costs, high capacity, and no transmission costs. Since there are no cables to be destroyed, they are also physically robust. Weaknesses include their sensitive equipment and the need for 'line of sight' (LOS) and specialized expertise. Capacity is also lower than for fibercables. On the opportunity side, they can be used in almost any social or economic activity that needs to connect many people, especially in rural or remote areas.

V. IEEE Wireless Networking Specifications

The IEEE (Institute of Electrical and Electronic Engineers) released the 802.11 specifications in June 1999. The initial specification, known as 802.11, used the 2.4 GHz frequency and supported a maximum data rate of 1 to 2 Mbps. In late 1999, two new addenda were released. The 802.11b specification increased the performance to 11 Mbps in the 2.4 GHz range while the 802.11a specification utilized the 5 GHz range and supported up to 54 Mbps.

Unfortunately, the two new specifications were incompatible because they used different frequencies. This means that 802.11a network interface cards (NICs) and access points cannot communicate with 802.11b NICs and access points. This incompatibility forced the creation of the new draft standard known as 802.11g. 802.11g supports up to 54 Mbps and is interoperable with 802.11b products on the market today. The concern is that the 802.11g specification is currently in development and products will not be available until a later date.

A wireless LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Base Service Set or BSS*) is controlled by a Base station(called Access point or AP). Wireless LAN standards that are currently being explored inthe field of communications technology are:

1.IEEE 802.11.

a) 802.11a

b) 802.11b

c) 802.11g

d) 802.11h

e) 802.11i

2.Hipper LAN/2.

3.Bluetooth.

4.HomeRF.

- **802.11 Specifications**

The 802.11 specifications were developed specifically for Wireless Local Area Networks (WLANs) by the IEEE and include four subsets of Ethernet-based protocol standards: 802.11, 802.11a, 802.11b, and 802.11g.

i)**802.11**

802.11 operated in the 2.4 GHz range and was the original specification of the 802.11 IEEE standard. This specification delivered 1 to 2 Mbps using a technology known as phase-shift keying (PSK) modulation. This specification is no longer used and has largely been replaced by other forms of the 802.11 standard.

a) 802.11a

802.11a operates in the 5 - 6 GHz range with data rates commonly in the 6 Mbps, 12 Mbps, or 24 Mbps range. Because 802.11a uses the orthogonal frequency division multiplexing (OFDM) standard, data transfer rates can be as high as 54 Mbps. OFDM breaks up fast serial information signals into several slower sub-signals that are transferred at the same time via different frequencies, providing more resistance to radio frequency interference. The 802.11a specification is also known as Wi-Fi, and though regionally deployed, it is not a global standard like 802.11b.

b)802.11b

The 802.11b standard (also known as Wi-Fi) operates in the 2.4 GHz range with up to 11 Mbps data rates and is backward compatible with the 802.11 standard. 802.11b uses a technology known as complementary code keying (CCK) modulation, which allows for higher data rates with less chance of multi-path propagation interference (duplicate signals bouncing off walls).

U.S. Robotics 22 Mbps 802.11b

Recent developments to 802.11b have seen numerous improvements to this well-established and widely-deployed wireless standard. New U.S. Robotics 22 Mbps products are designed to support Packet Binary Convolution Coding (PBCC) in addition to CCK modulation. This not only increases performance but also maintains complete 802.11b compatibility with both 11 Mbps and 22 Mbps products.

The overall benefits include:

• Up to twice the data rate of conventional

11 Mbps 802.11b standard products

• Greater WLAN coverage: up to 70% greater than standard 11 Mbps 802.11b products

• Full interoperability with all 802.11b products: works with 802.11b 11 Mbps, 802.11b 22 Mbps, and upcoming 802.11g products

• Improved security over standard 802.11b: 256-bit WEP encryption and MAC address authentication*

c)802.11g

802.11g is the most recent IEEE 802.11 draft standard and operates in the 2.4 GHz range with data rates as high as 54 Mbps over a limited distance. It is also backward compatible with 802.11b and will work with both 11 and 22 Mbps U.S. Robotics wireless networking products.

802.11g offers the best features of both 802.11a and 802.11b, but as of the publication date of this document, this standard has not yet been certified, and therefore is unavailable.

d)802.11h

This standard is supplementary to the MAC layer to comply with European regulations for 5 GHz WLANs. radio regulations for the 5 GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the farthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.

e)**802.11i**

It will apply to 802.11 physical standards a, b, and g. It provides an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1X forms a key part of 802.11i.

2. HipperLAN 1/2

European Telecommunications Standards Institute, ETSI, ratified in 1996 with High Performance Radio LAN (Hipper LAN 1) [4] standard to provide highspeed communications (20Mbps) between portable devices in the 5GHz range. Similarly to IEEE802.11, Hipper LAN/1 adopts carrier sense multiple access protocol to connect end user devices together. On top of that, Hipper LAN/1 supports isochronous traffic fordifferent type of data such as video, voice, text, etc. Later, ETSI, rolled out in June 2000, a flexible Radio LAN standard called Hipper LAN 2, designed to provide high speed access (up to 54 Mbps at PHY layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks, and also for private use as a wireless LAN system.

3. Bluetooth

Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices with its functional specification released out in 1999 by Bluetooth Special Interest Group [6]. Bluetooth communicates on a frequency of **2.45 gigahertz**, which has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM). One of the ways Bluetooth devices avoid interfering with other systems is by sending out very weak signals of 1 mill watt. The low power limits the range of a Bluetooth device to about **10 meters**, cutting the chances of interference between a computer system and a portable telephone or television. Bluetooth makes use of a technique called spread-spectrum frequency hopping. In this technique, a device will use 79 individual, randomly chosen frequencies within a designated range, changing from one to another on a regular basis. Bluetooth devices essentially come in two classes, both using point to-point communication to speak. Class 3 devices operate at 0 dBm ranges and are capable of transmitting 30 feet, through walls or other objects and the other class are termed as class 1 product. These devices operate at 20 dBm, which allows for the signal to travel about 300 feet through walls or other solid objects. Both Bluetooth classes are rated at traveling at about 1 Mbps, with next generation products allowing anywhere from 2 to 12 Mbps, to be determined at a later date.

4. Home RF

HomeRF is an open industry specification developed by Home Radio Frequency Working Group [2] that defines how electronic devices such as PCs, cordless phones and other peripherals share and communicate voice, data and streaming media in and around the home. Home RF-compliant products operate in the license-free 2.4 GHz frequency band and utilize frequency-hopping spread spectrum RF technology for secure and robust wireless communications with data rates of up to 1 Mbps (Home RF 1). Unlike Wi-Fi, Home RF already has quality-of-service support for streaming media and is the only wireless LAN to integrate voice. Home RF may become the worldwide standard for cordless phones. In the year 2001, the Working group unveiled Home RF 2.0 that supports 10 Mbps (Home RF 2.0) or more.

VI. TECHNICAL ISSUES IN WIRELESS NETWORKS

Wireless networks have recently emerged as a premier research topic. They have great long term economic potential, ability to transform our lives, and pose many new system building challenges. Wireless networks also pose a number of new conceptual and optimization problems. Some, such as location, deployment, and tracking, are fundamental issues, in that many applications rely on them for needed information.

[1]Coverage problem-One of the fundamental issues that arises in wireless networks, in addition to location calculation, tracking, and deployment, is coverage. Due to the large variety of wireless network and applications, coverage is subject to a wide range of interpretations. In general, coverage can be considered as the measure of *quality of service* of a sensor network. For example, in the previous fire detection sensor networks example, one may ask how well the network can observe a given area and what the chances are that a fire starting in a specific location will be detected in a given time frame. Furthermore, coverage formulations can try to find weak points in a network field and suggest future deployment or reconfiguration schemes for improving the overall quality of service

[2]Scheduling Problem-In wireless networks the problem of allocating transmission rights to subsets of network users at each time and under different channel qualities is known as the scheduling problem. It arises in wireless environments because of three main reasons related to the fundamental properties of the wireless medium.

Specifically, scheduling is mandatory since in wireless environments (i) communication resources are shared amongst geographically separated users, (ii) transmissions interfere with each other, and (iii) transmissions undergo impairments, such as fading, attenuation, etc.

[3]Hidden Terminal problem- Hidden nodes in a wireless network refer to nodes that are out of range of other nodes or a collection of nodes[5]. Take a physical star topology with an access point with many nodes surrounding it in a circular fashion: Each node is within communication ion range of the AP, but the nodes cannot communicate with each other, as they do not have a physical connection to each other. In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as **A**, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, **B**. These nodes are known as hidden .The problem is when nodes **A** and **B** start to send packets simultaneously to the access point. Since node **A** and **B** cannot sense the carrier, Carrier sense multiple access with collision avoidance (CSMA/CA) does not work, and collisions occur, scrambling data.

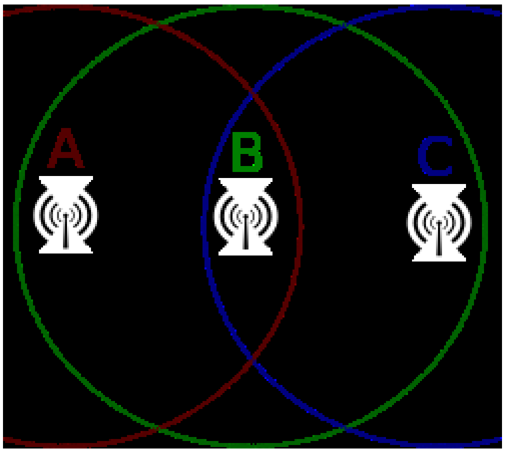


Fig 3: Hidden Terminal Problem

[4]Security-Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications. 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 802.11 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 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.

[5]Quality of Service- Next generation wireless communications will have to meet the demands of multimedia applications such as steaming video, IP telephony, teleconferencing, interactive games, distance learning etc. and it would be challenging due to constraints and heterogeneities such as power constraint, bandwidth limitation, different protocols and standards, fading effects and stringent quality of service (QoS) requirements. Provisioning of QoS is a key problem in next generation wireless communication systems. Provisioning of end-to-end QoS would be challenging due to major difficulties of IP based multimedia communication in mobile networks. QoS refers to the set of those quantitative and qualitative characteristics which are necessary in order to achieve the desired functionality/ performance of an application or service. From a user’s perspective, it is the perceived quality such as picture quality of a video, or the quality of a voice conversation. For cellular data networks, QoS mechanisms have been proposed in the literature in the form of medium access control (MAC) enhancement, scheduling and admission control schemes. However, the emerging broadband networks (e.g. wireless LAN and mesh networks) bring newer challenges and have attracted much attention recently. There are many future issues in QoS in various layers as network layer, MAC layer and in cross layer design. In network layer, major challenge is to satisfy QoS requirements for dynamic networks and to provide end-to-end QoS. Another important issue for ad hoc networks is QoS based routing as link failure happens because of fading and mobility. In MAC layer challenge is the designing of MAC protocol with QoS mechanisms and to devise scheduling and admission control schemes. The challenge also lies in designing mechanisms which can adapt to emerging applications as network gaming, wireless teleconferencing etc. Further, separate design for network QoS and MAC layer QoS is inefficient and hence, an important issue is jointly optimal design of both layers i.e. cross layer design. It is challenging because of the too many variables that exists in optimization.

[6]Fading- Multipath fading has a distinct impact on the fragility of wireless links. It is considered a small-scale phenomenon in the sense that the level of attenuation of the signal changes substantially if the position of the receiver or the transmitter is varied by about half a wavelength. One of the most common features of wireless sensor networks is the fact that the nodes are usually static; static multipath fading is therefore of particular interest. Another physical phenomenon of interest is shadowing; it is considered a large scale effect, as it corresponds to substantial deviations of the RF signal from its mean due to large obstacles, which create shadow zones that cause deep fades if a receiver happens to enter them. Although the impact of multipath fading is particularly strong in rich scattering environments such as offices and other indoor locales, outdoor deployments of wireless sensing nodes are not immune to it. Radio waves still get reflected off buildings and other landscape features. Multipath fading and shadowing contribute to the volatility of wireless links and must be accounted for when modeling the wireless channel. When the analysis of a higher-layer scheme (typically medium access and routing algorithms) is carried out, realistic assumptions must be made about the physical layer.

VII. ADVANTAGES OF WIRELESS NETWORK

i) It is very flexible within the reception area.

ii) Ad-hoc networks arepossible without previous planning.

iii) There is no difficulty of wiring. E.g.historic buildings, firewalls.

iv) More robust against disasters. E.g., earthquakes, fire - or users pulling a plug

v)Economical networking infrastructures possible.

vi) Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls.

vii) Wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.

viii) Wireless networks can survive disasters, if the wireless devices survive people can still communicate.

VIII. DRAWBACKS

i) Very low bandwidth compared to wire networks 1-10 Mbit/s and error rates of about 10-4 instead of 10-12.

ii) Many proprietary solutions, especially for higher bit-rates.

• Standards take their time, e.g., IEEE 802.11

iii) Products have to follow many national restrictions if working wireless

iv) It takes a very long time to establish global solutions like, e.g., IMT-2000

v) Lack of security, “open” air interface, War driving.

vi)WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission (1-10 Mbit/s) and higher error rates due to interference.

vii) Safety and security: using radio waves for data transmission might interfere with other high-tech equipment.

IX. CONCLUSION

This paper identifies and describes the various standards used for wireless networks. In this paper we first presented an overview of the evolution of the wireless network and then we have discussed the various wireless standard specifications eg. IEEE 802.11. The brief details about the advantages and disadvantages of wireless network have been discussed also.

In conclusion, wireless networks are rapidly become popular and user demand for useful wireless applications is increasing. This can be achieved by successful implementation of the standards mentioned in this paper. By successfully addressing the standards presented in this paper, end users will not be disappointed

X. REFERENCES

[1] Vijay Chandramouli, “A Detailed Study on Wireless LAN Technologies” Department of Computer Science and Engineering, vmouli@uta.edu

[2] 802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard. White Paper, 2002, www.proxim.com

[3] IEEE 802.11Working Group. http://grouper.ieee.org/groups/802/11/index.html.

[4] A History of Wireless Technologies, on Wikipedia.com

[5] “The Evolution of Personal Communications,” IEEE Commun. Magazine, vol. 1, No. 2 1994.

[6] Atul M. Gonsai, Nilesh N. Soni, “WIRELESS NETWORK: STANDARDS AND ITS APPLICATIONS”

[7] “Certified Wireless Network Administrator Official Study Guide” by Planet3 Wireless, Inc., pp.3-8

[8] IEEE 802.11, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Nov. 1997.

[9] Wave Access Wireless Communications, "Jaguar PC132 – Wireless LAN Adapter" 1997

[10] Paulo Salvador, Antonio Nigeria, Rui Valadas ―Predicting QoS Characteristics on Wireless Networks‖ 25 June 2007.

[11] 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.

[12] 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.

[13] "Mobile Communications", Jochen Schiller, chapter 7 "Wireless LAN", Addison Wensley 2000.

[14] Ramiro Jordan and Chaouki T. Abdullah, "Wireless Communications and Networking: An Overview" Electrical & Computer Engineering Department, the University of New Mexico.

[15] Seapahn Meguerdichian, Farinaz Koushanfar, Miodrag Potkonjak, Mani B. Srivastava, "Coverage Problems in Wireless Ad-hoc Sensor Networks".

[16] L. Tassiulas and A. Ephremides. Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks. IEEE Transactions on Automatic Control, 37(12), December 1992.

[17] S. Kompella, J. E. Wieselthier, and A. Ephremides. Revisiting the optimal scheduling problem. In Proceedings of Conference on Information Sciences and Systems (CISS), March 2008.

[18] A. Pantelidou and A. Ephremides. Optimal rate control policies for proportional fairness in wireless networks. In Proceedings of Conference on Information Sciences and Systems (CISS), March 2008.

[19] RappaportT.S, "Wireless Communication principle and practice, 2nd EditionPrentice Hall (1996).

[20] Ms. Ritu Patidar, Prof. Dinesh Chandra Jain, "Solving the Hidden Terminal problems Using Directional-Antenna Based MAC Protocol for Wireless Ad hoc Networks".

[21] C.R. Buffler and P.O. Risman, "Compatibility Issues between Bluetooth and High Power Systems in the ISM Band," Microwave Journal, pp. 126131, July 2000.

[22] G. M. Koien, "An introduction to access security in UMTS," IEEE Wireless Communications, vol. 11, pp. 8–18, 2004.

[23] Joseph Mitola and Gerald Q. Maguire Jr., "Cognitive radios: making software radios more personal," IEEE Personal Communications, vol. 6, no. 4, pp. 13-18, August 1999.

[24] Y. C. Hu, A. Perrig, and D. B. Johnson, "A secure on-demand routing protocol for ad hoc networks," In Proc. of MobiCom, 2002.

[25] Kapila C. Wavegedara, Gaurav Bansal, Praveen Kaligineedi, Majid Kabbazian, Ashok K. Karomokar, Mamunur Rashid, Hugues Mercier and Vijay K. Bhargava, "Wireless Communications: Trends and Challenges".

[26] Daniele Puccinelli and Martin Haenggi, "Multipath Fading in Wireless Sensor Networks: Measurements and Interpretation".

[27] G. Zhou, T. He, S. Krishnamurthy, and J. Stankovic. Impact of Radio Irregularity on Wireless Sensor Networks. In The Second International Conference on Mobile Systems, Applications, and Services (MobiSys'04), Boston, MA, June 2004.

[28] R. Kohno, R. Median, and L. B. Milstein. Spread Spectrum Access Methods for Wireless Communications. IEEE Communications Magazine, 33(1):58–67, 1995.