Implementation and Analysis of Wireless Local Area Networks for High-Mobility Telematics

Farhan Muhammad Aziz

Thesis submitted to the Faculty of Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Master of Science

in

Electrical Engineering

Dr. Brian D. Woerner (Chair)

Dr. William H. Tranter

Dr. R. Michael Buehrer

Mr. Ashwin E. Amanna

May 30, 2003

Blacksburg, Virginia

Keywords: Networks, Wireless LAN, Mobile Communication, IEEE Standards, Communication System Performance, Throughput

Implementation and Analysis of Wireless Local Area Networks for High-Mobility Telematics

by

Farhan Muhammad Aziz
Committee Chair: Prof. Dr. Brian D. Woerner
Bradley Department of Electrical and Computer Engineering

Abstract

Wireless networks provide communications to fixed, portable and mobile users and offer substantial flexibility to both end-users and service providers. Current cellular/PCS networks do not offer cost effective high data rate services for applications, such as, telematics, traffic surveillance and rescue operations. This research studies the feasibility and behavior of outdoor implementation of low-cost wireless LANs used for high mobility telematics and traffic surveillance. A multi-hop experimental wireless data network is designed and tested for this purpose. Outdoor field measurements show the wireless coverage and throughput patterns for static and mobile users. The results suggest that multi-hop wireless LANs can be used for high mobility applications if some protocols are improved.

In the name of ALLAH, the Beneficent, the Merciful

dedicated to

my parents,

Abdul-Aziz Khan and Sabra Begum

Acknowledgements

I am very grateful to my Lord Almighty ALLAH who helped and guided me throughout my life and made it possible. I could never have done it by myself!

I am very thankful to my parents Abdul-Aziz Khan and Sabra Begum for their continuous support, encouragement, prayers and having trust in me. My family especially my brothers, my sister Sumbul and my wife Fauzia deserve special thanks for their moral support and encouragement. Fauzia also deserves very special thanks for providing me big help in taking field measurements and editing this thesis.

My advisor, Prof. Dr. Brian D. Woerner, has a tremendous contribution in achievement of this important milestone in my life. He has not only been my academic advisor but also a mentor throughout my studies at Virginia Tech. I feel lucky that I will be doing my doctoral studies under his supervision. I am also thankful to my committee members Dr. William H. Tranter, Dr. R. Michael Buehrer, and Mr. Ashwin E. Amanna for their valuable time and feedback.

Special thanks to Mobile and Portable Radio Research Group (MPRG) and Virginia Tech Transportation Institute (VTTI) for providing me with research opportunities. Dr. Woerner and Mr. Amanna also deserve special thanks for bringing in research funds and facilities for this project. I am grateful to VTTI personnel especially Dr. Aaron Schroeder, Leonore C. Nadler, and Sean Hughes for their cooperation. I am also thankful to my fellow MPRG students and staff for providing me help and cooperation whenever needed.

I would also like to thank Samir Al-Ghadhban and Saajed Ali for helping me in planning the network deployment and data collection during the initial phase of this research. My friend Sajid Aafaque also deserves special thanks for helping me voluntarily during two-user mobile tests.

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

This thesis discusses the design, implementation, and analysis of a wireless local area network for high mobility telematics applications. Although the network is designed for high data rate telematics applications, its guiding principles and results can be used for any generalized form of wireless data networks. The proposed audience of this document is the research community interested in examining the performance of current wireless LANs under mobility. This chapter discusses the rationale, research problem and the scope of our investigation and presents a brief description of the content discussed in the next chapters.

1.1 Rationale

Wireless networks can provide communications to both fixed, and mobile users without any need of using data cables and can provide substantial flexibility to both end-user and service provider. The use of current cellular/PCS high data rate services for data networking is not economically feasible due to high usage costs. Wireless local area networks have been designed and used for mostly indoor applications. The possible use of these wireless LANs for high mobility outdoor applications, such as, telemetry, traffic surveillance, rescue operations, and outdoor data networking can provide reasonably high data rates at minimal operational costs. These attractions led us to investigate the feasibility and operational characteristics of current wireless LAN standards in high mobility outdoor environments.

1.2 Research Problem

The basic issue addressed in this research is to study the feasibility and characteristics of wireless local area networks used for high mobility outdoor applications. The success of current wireless LANs under these conditions will lead us to use them as high rate outdoor wireless data networks.

1.3 Research Scope

This study focuses on the *IEEE 802.11b* [802.11b] standard, which is one of the most commonly deployed and commercially available wireless LANs around the world. The success of *802.11b*

[802.11b] lies in the use of license-free 2.4 GHz band, reasonably high available data rates (up to 11 Mbps), and commercially available products around the world. The investigation enables us to study the throughput and delay performance of an experimental multi-hop outdoor wireless network with increasing number of hops and speed. The experimental wireless network designed for this study consists of wireless backbone along with a wireless access network along *Virginia's Smart Road* [Smart Road]. Based on the network performance results obtained by measurements, recommendations are made for its feasibility for high mobility outdoor environments.

1.4 Organization of the Thesis

This document is divided into six chapters. The first chapter briefly discusses rationale, research problem and scope of the study. The second chapter discusses the background of wireless LANs, with a brief description of *IEEE 802.11b* standard. The third chapter presents site details of the experimental network. The fourth and fifth chapters discuss and analyze the performance results, and the last chapter presents the summary of the findings and suggestions for future work.

Chapter 2: Wireless LANs and IEEE 802.11b

This chapter discusses the need and use of wireless local area networks with special reference to the *IEEE 802.11* [802.11] standard. The experimental wireless network used in this study is 802.11b [802.11b] compliant. The chapter also briefly discusses *IEEE 802.11* family of standards, current research trends, and some key definitions used in this thesis.

2.1 Introduction to Wireless LANs

This section presents a brief description of wireless local area networks (WLANs). Some of the material in this section are inspired by [Gas02], [Gei02], and [Lar02].

2.1.1 Advantages of Wireless Networks

Wireless LANs are usually designed to operate in license-free bands making their operation and maintenance costs less than contemporary cellular and PCS networks (for details on cellular and PCS networks see [Rap01]). The use of license-free spectrum, however, increases the risk of network security and in-band interference. The key advantages of wireless networks as opposed to wired networks are mobility, flexibility, ease of installation and maintenance, and reduced cost (for details on wireless networks, see [Gei02], and for wired networks, see [Pet00]). Some of them are discussed below.

Mobility

The most significant advantage of wireless networks is mobility and portability. They allow wireless network users to connect to existing networks and roam freely. A wired network user, in contrast, cannot roam freely or move while connected to the network [Gas02].

Flexibility

Flexibility is an important feature of wireless networks and has been very attractive for wireless service providers. The wireless service providers can add new users only by authorizing their

usage provided the network infrastructure is already built. The same infrastructure can be used to spread network coverage over a larger area than wired networks and the service providers do not need to run any cables or install network ports in order to increase the coverage. Thus this kind of flexibility is convenient to both the service provider and the end-user.

Ease of Installation

Wireless networks offer substantial ease of installation and cost savings as compared to wired networks. The required network infrastructure including base station equipment (routers, bridges etc) and antennas can be installed at any convenient place even at those places where wired networks are impossible to install or cost too much such as rivers, freeways etc.

Cost Savings

Wireless networks lead to both deployment and operational cost savings. The substitute for cabling allows companies to spend less on installation and maintenance of the network. In addition, compared to wired networks, flexibility allows them to scale their networks easily.

2.1.2 Radio Spectrum

All wireless devices are constrained to operate in certain frequency bands. The use of radio spectrum is rigorously controlled by regulatory authorities through licensing procedures. In the United States, the *Federal Communications Commission (FCC)* [FCC] regulates the frequency bands for commercial systems, whereas in Europe, CEPT's [CEPT] newly established *Electronic Communications Committee (ECC)* is now responsible for spectrum allocation. Also, the *International Telecommunications Union (ITU)* [ITU] performs allocation work in other countries around the world. Frequency bands used in different countries can be found in many texts including [Gas02].

The ISM Bands

In the United States, there are three *Industrial, Scientific, and Medical (ISM)* bands, which are set aside for equipment that, broadly speaking, is related to industrial or scientific purposes or is used by medical equipment. ISM bands are license-free if the devices operate at low power. A

microwave oven (2.4 GHz ISM band) is said to be the most familiar ISM band device. Many wireless LANs, such as IEEE 802.11 [802.11] networks, also operate in ISM bands, which make them less costly and hence attractive for both service providers and end-users. The ISM bands used in the United States are tabulated in Table 2.1.

Table 2. 1: United States ISM Bands

Band	Frequency Range
UHF ISM	902 – 928 MHz
S-Band ISM	2.4 – 2.483 GHz
C-Band ISM	5.725 – 5.875 GHz

2.1.3 Brief History of WLANs

ALOHANET is said to be the first wireless local area network realized in 1971 at the University of Hawaii. It was stretched over four islands and enabled computer sites at seven different campuses to communicate bi-directionally via a star topology. In the 1980s, amateur radio hobbyists, *hams*, built "Terminal Node Controllers (TNCs)" to interface their computers through ham radio equipment within North America. Also the *American Radio Relay League (ARRL)* and *Canadian Radio Relay League (CRRL)* started to sponsor the Computer Networking Conferences since the early 1980s to provide a forum for the development of wireless LANs. In 1985, the *FCC* allowed the public use of *ISM bands* (between 902 MHz and 5.85 GHz), which was founded to be very attractive to wireless network vendors. In the late 1980s, *the Institute of Electrical and Electronic Engineers (IEEE)* [IEEE] Working Group 802 started working on standardizing wireless LANs in the 2.4 GHz and 5.7 GHz ISM bands. In the meantime companies began shipping proprietary wireless LAN radio cards and access points operating in 902 MHz ISM band. The *IEEE 802.11 Working Group* developed the specifications for Wireless LAN *Medium Access Control (MAC)* and *Physical Layer (PHY)* [802.11]. The *IEEE* standards board approved the standard on June 26, 1997 which was published by the *IEEE* on November 18, 1997. In December 1999, the IEEE released the supplements ([802.11a] and [802.11b]) to the *IEEE 802.11* [802.11] standard in order to increase the speed of PHYs (up to 11 Mbps in 2.4 GHz ISM band and 54 Mbps in 5.7 GHz ISM band).

2.1.4 Current WLAN Technologies

There are four common wireless LAN standards, namely, *IEEE 802.11, HiperLAN, HomeRF SWAP,* and *Bluetooth.* A brief description of each of them is given below.

IEEE 802.11

In June 1997, the *IEEE* finalized the initial standard for wireless LANs: *IEEE 802.11* [802.11]. This standard specifies a 2.4 GHz operating frequency with data rates of 1 Mbps and 2 Mbps. In the late 1999, the *IEEE* released two supplements to *IEEE 802.11* (1997) standard: *IEEE 802.11a* [802.11a] and *IEEE 802.11b* [802.11b]. The initial 802.11 standard mainly uses two types of physical layers *802.11* FHSS (frequency hopping – spread spectrum) and *802.11* DSSS (direct sequence – spread spectrum). *802.11b* is a data rate extension of initial *802.11* DSSS providing data rates up to 11 Mbps in 2.4 GHz ISM band and *802.11a* defines a new physical layer operating up to 54 Mbps in 5.7 GHz ISM band using *Orthogonal Frequency Division Multiplexing (OFDM)* (for more information see [Ter01]). The *IEEE 802 Working Group* is still in the process of extending the data rates up to 54 Mbps in the 2.4 GHz band, and the standard will be called *IEEE 802.11g*.

HiperLAN

European Telecommunications Standards Institute's (ETSI) [ETSI] *Broadband Radio Access Network (BRAN)* standardized *HiperLAN* (High Performance Radio Local Area Networks) in Europe in 1996. *HiperLAN/1* operates in the 5 GHz radio band at rates up to 24 Mbps and shares access to the wireless LAN medium via a connectionless protocol similar to *Ethernet* (for more information on *Ethernet,* see [Pet00]). It also provides quality of service (QoS) support for various data, video, voice and image traffic. *ETSI* is currently engaged in developing the *HiperLAN/2* standard under the organization *HiperLAN/2 Global Forum (H2GF)* [H2GF]. It is supposed to operate in the 5 GHz band up to data rates of 54 Mbps using a connection-oriented sharing access control protocol. It will also include QoS support and be able to carry *Ethernet* frames, *ATM* cells and *IP* packets (see [Pet00] for more information on *Ethernet* frames, *ATM* cells, and *IP* packets).

HomeRF SWAP

The *SWAP* specification defines a common wireless interface supporting voice and data services at 1 Mbps and 2 Mbps using frequency hopping spread spectrum modulation in the 2.4 GHz ISM band. In March 1998, *HomeRF Working Group (HRFWG)* [HomeRF] standardized an open industry specifications, *Shared Wireless Access Protocol (SWAP),* for wireless digital communication between personal computers and consumer electronic devices within a home. *HRFWG* is currently developing a 10 Mbps version of *SWAP*.

Bluetooth

Bluetooth is a specification published by the *Bluetooth Special Interest Group (SIG)* [Bluetooth]. It is a wireless personal area network (WPAN) which operates at 1 Mbps with relatively low power over short ranges using frequency hopping spread spectrum technique in the 2.4 GHz ISM band.

2.1.5 Classification of Wireless Data Networks

The current wireless data networks can be conveniently classified by distance. A *Wireless Personal Area Network (WPAN)* is a short-range wireless network with communication distances of 10 meters or less. A *WLAN* usually handles distances of several hundred meters or less and typically links devices within a building or campus. A *Wireless Metropolitan Area Network (WMAN)* generally provides broadband wireless access for small regional areas such as cities or metropolitan areas. Cellular networks cover large regional and global areas. The following is a summary of current wireless networks classified according to distance.

Table 2. 2: Classification of Wireless Data Networks

WPANs	WLANs	WMANs	Cellular Networks
IEEE 802.15	IEEE 802.11	IEEE 802.16	2.5 G (EDGE, IS-95)
Bluetooth	HomeRF	LMDS	3 G (WCDMA, cdma2000)
IrDA	HiperLAN	MMDS	SMS
UWB	OpenAir	HiperMAN	CDPD

2.1.6 Limits of Wireless Networking

The main purpose of using wireless LANs is to take advantage of mobility and flexibility. They do not replace fixed networks. The network servers and other data center equipment need to be fixed. Besides the many benefits of wireless LANs as discussed in section 2.1.1, there are also few issues with wireless LANs. A brief discussion of some of these issues is given below.

Multipath Propagation

A multipath propagation is a phenomenon where the receiver may receive multiple copies of the same transmitted signal due to reflections from physical objects such as office furniture or hills etc. This phenomenon can cause signal corruption or interference. The amount of delay experienced by the reflected signals compared to the primary signal is reflected in a quantity termed as "delay spread". As the delay spread increases, the signal at the receiver becomes more distorted and possibly undetectable. This problem, however, is more pronounced in indoor case despite the fact that the delay spread is smaller in indoor systems. As the data rate goes up delay spread becomes more of an issue. Communications engineers often use signal-processing techniques such as RAKE receivers, equalization, or antenna diversity in order to mitigate this problem (for further details see [Rap01]).

Path Loss

The signal path loss between transmitter and receiver depends on the transmitter frequency and site details and it grows exponentially as the distance increases between the transmitter and receiver. For typical indoor applications the path loss increases approximately 20 dB/100 feet (see [Rap01] for more information).

Radio Signal Interference

Most of the wireless local area networks operate in the ISM bands. The ISM bands are publicly accessed, and are affected from interference from other systems operating in the same or neighboring frequency bands. Similarly wireless LANs cause interference to other devices working in the same or neighboring bands. For example, microwave ovens and Bluetooth networks are the two most common sources of interference for IEEE 802.11b devices. Also a

second 802.11b system working in the same frequency band can cause interference to the first 802.11b system. This interference degrades the performance of wireless networks. Active research is in progress in interference cancellation and rejection.

Limited Battery Life

Many of the wireless devices are equipped with batteries for portability and mobility. They all suffer from limited battery lives. This problem can be addressed by power management schemes and using low power devices.

System Interoperability

Interoperability of different wireless LAN technologies is almost impossible. Even with same wireless LAN technology, interoperability cannot be assumed in all situations. In order to ensure interoperability with wireless LANs it is recommended to use equipment from the same vendor. An organization *Wireless Ethernet Compatibility Alliance (WECA)* [WECA] ensures compliance among *IEEE 802.11b* wireless LANs through its *Wi-Fi™ (Wireless Fidelity)* tests. *IEEE 802.11 Working Group* is working on this issue in order to ensure interoperability of multi-vendor equipment.

Network Security

Network security, broadly speaking, refers to protection of information and resources from loss, corruption and improper use. Due to radio wave propagation the wireless network boundaries cannot be well defined or restricted which may allow unauthorized persons to access or connect to the network.

Application Connectivity Problems

The use of traditional wire-based protocols over wireless networks introduces problems with maintaining connections between user's appliance and the applications residing on a server. Generally, response time of wireless networks is much higher than wired networks and wireless networks often need to request retransmission due to data loss or corruption. These problems

make a wireless network less reliable as compared to wired networks. In addition, the mobile nature of wireless end-users can cause addressing problems.

2.2 An Overview of The IEEE 802.11 Family of Standards

This section briefly discusses the *IEEE 802.11* standard with special focus on *IEEE 802.11b*, which is one of the most widely deployed wireless LAN standards around the world and is used in our experimental network. It is to be noted here that *802.11b* (1999) is an extension of its precursor *802.11*, which was published in 1997. Detailed information about these standards can be found in [802.11], and [802.11b].

2.2.1 Structure of IEEE 802.11 Working Group

The *IEEE Working Group 802.11* is a part of *IEEE 802 LAN/MAN Standards Committee*. The *Group 802.11 (IEEE WLAN Working Group)* is responsible for standardizing wireless LANs that support devices in a fixed location, as well as support portability and mobility. A brief description of the Task and Study Groups within *802.11 Working Group* can be found in [Lar02]. *802.11 Task Groups* are mentioned in Table 2.3. The task groups 802.11, 802.11a, 802.11b, 802.11c, and 802.11d have completed their specifications. Others are currently active or part of other task groups.

Table 2. 3: The *802.11* Task Groups

Task Group	Task
802.11	Wireless LAN PHY and MAC specifications (infrared and 2.4 GHz radio)
802.11a	Wireless LAN PHY and MAC specifications for 5 GHz radio band
802.11b	Higher-Speed (5.5 Mbps and 11 Mbps) Wireless LAN PHY and MAC specifications for 2.4 GHz radio
802.11c	Bridge operation with IEEE 802.11 MACs (incorporated into 802.1d)
802.11d	Extensions to 802.11 for operation in additional regulatory domains
802.11e	802.11 MAC Quality of Service (QoS) for advanced applications
802.11f	Multivendor access point interoperability across distribution systems: IAPP
802.11g	Higher-Rate extensions in the 2.4 GHz radio band
802.11h	Enhancements for dynamic channel selection and transmit power control
802.11i	Enhancements for security and authentication

2.2.2 2.4-GHz Spectrum Regulations

As discussed earlier, devices in 2.4 GHz band are subject to regulation by the *FCC* in the United States, by the *ECC* in Europe and by the *ITU* across the globe. The actual *ISM band* specified by the *FCC* ranges from 2.4 to 2.4835 GHz. The *FCC* regulates emissions, output power, spectrum management techniques in this band, which have a direct affect on the design and implementation of the *IEEE 802.11 PHY* layer. Moreover, the *FCC* requires every 2.4 GHz device to use spread spectrum transmission and modulation techniques. Different spread spectrum modulation techniques are the key differences between *IEEE 802.11, IEEE 802.11a, IEEE 802.11b* and *IEEE 802.11g* devices. Frequency range and maximum transmit power in the ISM bands are regulated by different agencies around the globe (see [Pet95] for detailed information on spread spectrum techniques). The maximum transmit power regulations in the 2.4 GHz ISM band around the world are summarized in Table 2.4.

Table 2. 4: Maximum Transmit Power in 2.4 GHz ISM Band

Frequency Band	***Maximum Transmit Power***
North America: 2.4 – 2.4835 GHz	1,000 mW
Europe: 2.4 – 2.4835 GHz	100 mW
Japan: 2.471 – 2.497 GHz	10 mW/MHz
Spain: 2.445 – 2.475 GHz	100 mW
France: 2.4465 – 2.4835 GHz	100 mW

2.2.3Brief History of IEEE 802.11 Development

The *Institute of Electrical and Electronic Engineers (IEEE)* [IEEE] *802.11 Working Group* was given charter, in the late 1980s, to develop standards for wireless LANs. It developed the wireless LAN Medium Access Control (MAC) and Physical (PHY) layer specifications, initially in infrared and 2.4 GHz radio bands. The standard was approved and published by IEEE on June 26 and November 18, 1997 respectively and is named as *"IEEE 802.11"* [802.11]. This standard finalized 1 Mbps and 2 Mbps wireless LANs based on an infrared, 2.4 GHz frequency hopping spread spectrum (FHSS) and 2.4 GHz direct sequence spread spectrum (DSSS) physical layers. Later on, in December 1999, *IEEE* released the supplements to *802.11* standard (*802.11a* and *802.11b*) in order to increase the performance of wireless LANs. The *IEEE 802.11a* [802.11a] is based on 5 GHz Orthogonal Frequency Division Multiplexing (OFDM) physical layer and can

operate up to data rates of 54 Mbps. Whereas *IEEE 802.11b* [802.11b] is based on 2.4 GHz high rate direct sequence spread spectrum (HR/DSSS) physical layer and can operate up to 11 Mbps. *ISO/IEC* adopted these standards in 1999 as *ISO/IEC 8802*-11 [8802-11]. Further, in 2001, *IEEE* released a third amendment to the original *802.*11 standard in order to operate it in additional regulatory domains. This amendment is known as *IEEE 802.11d* [802.11d] standard. Also, *IEEE* released a corrigendum to *802.11b* standard in 2001 and can be found in [802.11b Cor 1]. Work is in progress by *IEEE 802.11g* Task Group in order to standardize a possible 2.4 GHz OFDM based physical layer capable of supporting data rates up to 54 Mbps [Gei02]. This physical layer specification will be different from those specified in *802.11a.*

2.2.4 Scope and Purpose of the Standard

The *ISO/IEC 8802-11* [8802-11] states the scope of the wireless LAN standard as follows:

"The scope of this standard is to develop a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area". [8802-11]

Further, [8802-11] defines the purpose of standard as follows:

"The purpose of this standard is to provide wireless connectivity to automatic machinery, equipment, or stations that require rapid deployment, which may be portable or hand-held, or which may be mounted on moving vehicles within a local area…." [8802-11]

2.2.5 Physical Components of 802.11 LANs

802.11 networks consist of four major physical components, namely, distribution system, access points, wireless medium, and stations [Gas02]. They are briefly discussed below.

Distribution System (DS)

"A system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS)." [8802-11]

Access Points (APs)

"Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations." [8802-11]

Wireless Medium

"The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities of a wireless local area network (LAN)." [8802-11]

Stations

"Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM)." [8802-11]

2.2.6 IEEE 802.11 Network Topologies

The basic building block of an *802.11* network is called the *basic service set (BSS),* which consists of a group of stations that communicate with each other.

[8802-11] defines the *basic service set (BSS)* as: *"A set of stations controlled by a single coordination function."* [8802-11] (for definition of *coordination function*, see [8802-11]).

Communications among different stations take place within a fuzzy wireless area called the *basic service area*, defined by the propagation characteristics of wireless medium. A station is free to move within the basic service area, but it can no longer communicate directly with other members of *BSS* if it leaves the area.

According to [8802-11], *basic service area (BSA)* is defined as: *"The conceptual area within which members of a basic service set (BSS) may communicate."* [8802-11].

The *802.11* networks can be classified into two major categories based on two different flavors of *BSSs* as follows.

Independent BSS (IBSS) Networks

The *Independent Basic Service Set (IBSS)* is a standalone BSS with no backbone infrastructure, consisting of at least two wireless stations. Stations in an *IBSS* communicate directly with each other and thus must be within direct communication range. This type of network is often referred to as an *ad-hoc network* or *ad-hoc BSS* because it can be constructed quickly without much planning. These networks are mostly short lived.

[8802-11] defines *independent basic service set (IBSS)* as follows:

"A BSS that forms a self-contained network, and in which no access to a distribution system (DS) is available." [8802-11]

Infrastructure Networks

[8802-11] defines *infrastructure* as follows:

"The infrastructure includes the distribution system medium (DSM), access point (AP), and portal entities. It is also the logical location of distribution and integration service functions of an extended service set (ESS). An infrastructure contains one or more APs and zero or more portals in addition to the distribution system (DS)." [8802-11]

Infrastructure BSS (never called IBSS) networks are distinguished by the use of an access point. Access points are used for all communications in infrastructure networks, including communications between mobile nodes in the same service area. With all communications relayed through an access point, the basic service area corresponding to an infrastructure BSS is defined by the points in which transmissions from the access point can be received.

For requirements exceeding the range limitations of an infrastructure BSS, *802.11* defines an *Extended Service Set* (ESS) LAN by linking BSSs together by a *backbone network*. This type of configuration satisfies the needs of large coverage networks of arbitrary size and complexity.

[8802-11] defines an *extended service set (ESS)* as: *"A set of one or more interconnected basic service sets (BSSs) and integrated local area networks (LANs) that appears as a single BSS to the logical link control layer at any station associated with one of those BSSs."* [8802-11]

802.11 does not specify a particular backbone technology, it only requires that the backbone provide a specified set of services.

Examples of *IBSS, infrastructure BSS* and *ESS* networks are given in Figure 2.1.

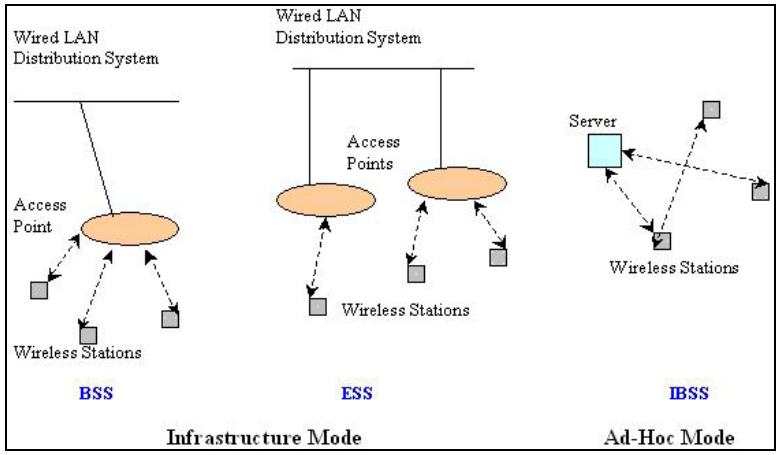

Figure 2. 1: Types of IEEE 802.11 Networks

2.2.7 IEEE 802.11 Logical Architecture

The logical architecture defines a network's operation. The logical architecture of 802.11 standard that applies to each station consists of a single MAC and one of multiple PHYs defined in the standard. It can be further clarified from Figure 2.2.

As mentioned earlier, *802.11* only standardizes MAC and PHY layers. The objective of the MAC layer is to provide access control functions, such as, addressing, access coordination, frame check generation and checking, *LLC PDU* delimiting etc for shared-medium PHYs in support of the LLC layer. It is to be noted here that *IEEE 802.2* standardized the *Logical Link Control (LLC)* layer. The *802.11* standard uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), whereas *802.3* (e.g. *Ethernet*) uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection). Since it is impossible to transmit and receive on the same channel at the same time, therefore, *802.11* can take measures only to avoid collisions, and not detect them.

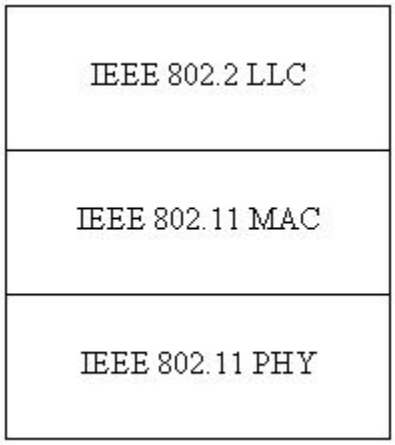

Figure 2. 2: IEEE 802.11 Logical Architecture

2.2.8 Network Boundaries

The *802.11* networks have fuzzy boundaries because o the nature of wireless medium. Often some degree of fuzziness is desirable in wireless networks. Allowing basic service areas to overlap, increases the probability of successful transitions between them and offers higher level of network coverage. Different types of 802.11 networks may also overlap. For example, independent BSSs can be created within coverage range of an access point.

2.2.9 Mobility Support

As discussed earlier, mobility is the major motivation for building wireless networks. The standards allow wireless stations to transmit and receive frames while in motion and can move while connected. The *802.11* standard (and its supplements) recognizes three different types of transitions due to mobility as discussed below.

No Transition

This type of mobility refers to stations that do not move and those that move within a local BSS. In this case *no transition* is necessary.

BSS Transition

This type of mobility refers to stations that move from one BSS in one ESS to another BSS within the same ESS. It requires the cooperation of access points. Stations continuously monitor the signal strength and quality from all access points. The *802.11* provides MAC layer mobility within an extended service area. The stations attached to the distribution system can send out frames addressed to the MAC address of a mobile station and let the access point handle the final hop to the mobile station. Distribution system stations do not need to be aware of a mobile station's location as long as it is within the same extended service area. *802.11* does not specify the details of communications between access points during BSS transitions. Since inter-access point communications are not standardized yet (*802.11f Task Group* is working on it), mobility between access points supplied by different vendors is not guaranteed.

It is to be noted here that MAC layer mobility can only be guaranteed if the two BSSs partially overlap or are physically co-located. 802.11 does not specify a limit to the distance between BSSs. Hence in situations when extended service area does not provide contiguous coverage, *BSS transition* can not be guaranteed.

ESS Transition

This type of mobility refers to stations that move from a BSS in one ESS to another BSS in a different ESS. *802.11* does not guarantee MAC layer mobility when making an *ESS transition*. The standard allows stations to associate with an access point in the second ESS once it leaves the first and support from higher-level protocols may be employed to maintain seamless transitions. For example, in case of *TCP/IP*, *Mobile IP* (its details can be found in [Pet00]) may be used to support seamless *ESS transition*.

2.2.10 Network Services

The *802.11* provides nine services, only three of them are used for moving data; the remaining six are management operations that allow the network to keep track of the mobile nodes and deliver frames accordingly. Below is a brief description of *IEEE 802.11*'s architectural services.

Authentication

[8802-11] defines *authentication* as: *"The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station".*

802.11 [8802-11] defines two types of authentication services:

- Open System Authentication
- Shared Key Authentication:

Association

According to [8802-11], *association* is defined as: *"The service used to establish access point/station (AP/STA) mapping and enable STA invocation of the distribution system services (DSSs)".*

Deauthentication

[8802-11] defines *deauthentication* as:"*The service that voids an existing authentication relationship".*

Disassociation

[8802-11] defines *disassociation* as: *"The service that removes an existing association".*

Distribution

[8802-11] defines *distribution* as: *"The service that, by using association information, delivers medium access control (MAC) service data units (MSDUs) within the distribution system (DS)".*

Integration

[8802-11] defines *integration* as: *"The service that enables delivery of medium access control (MAC) service data units (MSDUs) between the distribution system (DS) and an existing non-IEEE 802.11 local area network (via a portal)".* (for definition of *portal,* see [8802-11]).

Privacy

According to [8802-11], *privacy* is: *"The service used to prevent the content of messages from being read by other than the intended recipients"*.

To offer similar level of privacy, *802.11* provides an optional privacy service called *Wired Equivalent Privacy (WEP)*. [8802-11] defines *wired equivalent privacy (WEP)* as: *"The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy"*.

Reassociation

[8802-11] defines *reassociation* as:"*The service that enables an established association [between access point (AP) and station (STA)] to be transferred from one AP to another (or the same) AP"*.

MSDU Delivery:

Stations provide the *MAC Service Data Unit (MSDU)* delivery service, which is responsible for getting the data to the actual endpoint.

These services can be classified based on whether they are provided by an *802.11* station or distribution system. [8802-11] defines *distribution system service (DSS)* as: *"The set of services provided by the distribution system (DS) that enable the medium access control (MAC) to transport MAC service data units (MSDUs) between stations that are not in direct communication with each other over a single instance of the wireless medium (WM)…"*, and *station service (SS)* as: *"The set of services that support transport of medium access control (MAC) service data units (MSDUs) between stations within a basic service set (BSS)."* [8802-11] (for definition of *MSDU,* see [8802-11]). Table 2.5 classifies them into above-mentioned groups.

Table 2. 5: Types of *802.11* Architectural Services

Service	**Type**
Association	DSS
Disassociation	DSS
Distribution	DSS
Integration	DSS
Reassociation	DSS
Authentication	SS
Deauthentication	SS
Privacy	SS
MSDU Delivery	SS

2.2.11 IEEE 802.2 LLC Overview

The *Logical Link Control (LLC)* is the highest layer of the *IEEE 802 Reference Model* and corresponds to *Data Link* layer of *OSI model* (details about OSI model can be found in several texts including [Pet00]). *ISO/IEC 8802-2* (*ANSI/IEEE Standard 802.2*) dated May 7, 1998, specifies the *LLC*. The basic purpose of the LLC is to exchange data between end users across a LAN using an *802-based* MAC controlled link. The LLC provides addressing and data link control, and is independent of the topology, transmission medium, and medium access control technique used.

Higher layers such as *TCP/IP*, pass user data down to the LLC expecting error-free transmission across the network. The LLC in turn appends a control header, creating an LLC protocol data unit (PDU). The LLC uses the control information in the operation of the LLC protocol. Before transmission, the LLC PDU is handed down through the MAC service access point (SAP) to the MAC layer, which appends control information at the beginning and end of the packet, forming a MAC frame. The control information in the frame is needed for the operation of the MAC protocol. The LLC provides following three services for a Network Layer protocol. [Gei02]

- Unacknowledged connectionless service
- Connection-oriented service and
- Acknowledged connectionless service.

2.2.12 The 802.11 MAC Layer Operations

Each station and access point on an *802.11* wireless LAN implements the MAC layer service, which provides the capability for peer LLC entities to exchange MAC service data units (MSDUs) between MAC service access points (SAPs). The MSDUs carry LLC-based frames that facilitate functions of the Logical Link Control (LLC) layer. Overall, MAC services encompass the transmission of MSDUs by sharing a wireless radio wave or infrared light medium. The MAC layer provides following primary operations:

- Accessing the wireless medium
- Joining a network and
- Providing authentication and privacy.

Further details can be found in [802.11].

2.2.13 The IEEE 802.11 Physical Layers (PHY)

This section briefly discusses the parameters and characteristics of physical layers used by *802.11*.

Physical Layer Architecture

The architecture of all physical layers used by *802.11* consists of three major components as shown in Figure 2.6 [Gei02].

Physical Layer Management

Physical layer management works in conjunction with MAC layer management and performs functions for the Physical layer.

Physical Layer Convergence Procedure (PLCP) Sublayer

The MAC layer communicates with PLCP via primitives through the Physical layer service access point (PHY SAP). When the MAC layer instructs, the PLCP prepares MAC protocol data units (MPDUs) for transmission. The PLCP also delivers incoming frames from the wireless medium to the MAC layer.

The PLCP appends fields to the MPDU that contain information needed by the Physical layer transmitters and receivers. The 802.11 standard refers to this composite frame as a PLCP protocol data unit (PPDU). The frame structure of a PPDU provides for asynchronous transfer of MPDUs between stations. The physical layer of the receiving station, as a result, synchronizes its circuitry to each individual incoming frame.

Different PLCPs have been defined for each specific Physical layer including FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) and IR (Infrared) Physical layers.

Physical Medium Dependent (PMD) Sublayer

Under the direction of the PLCP, the PMD provides actual transmission and reception of Physical layer entities between two stations via the wireless medium. To provide this service, the PMD interfaces directly with the wireless medium and provides modulation and demodulation of the frame transmissions. The PLCP and PMD communicate via primitives to govern transmission and reception function through the PMD service access point (PMD SAP).

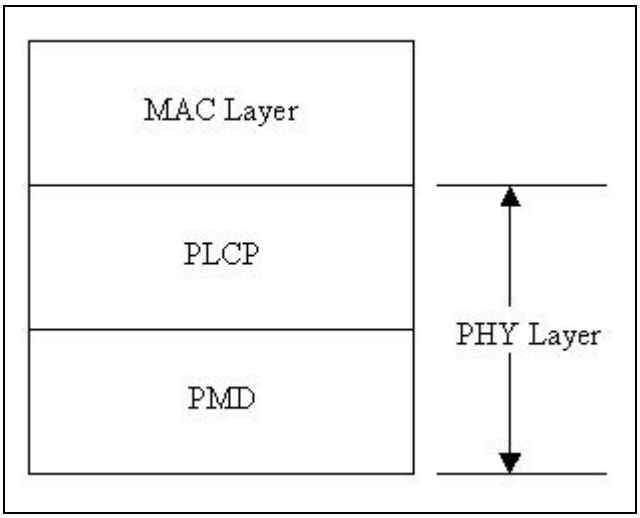

Figure 2. 3: IEEE 802.11 PHY Architecture

Physical Layer Operations

The general operation of the individual Physical layers is very similar. To perform PLCP functions, the *802.11* standard specifies to the use of state machines. Each state machine performs one of the following functions [Gei02].

- *Carrier Sense:* To determine the state of the medium.
- *Transmit:* To send individual bytes of the data frame.
- *Receive:* To receive individual bytes of the data frame.

More detail can be found in [802.11] and later supplements [802.11a], and [802.11b].

The 802.11 DSSSS PHY

Direct-sequence modulation has been the most widely deployed modulation technique used in *802.*11 (details of direct-sequence modulation can be found in many texts including [Pet95]). The initial *802.11* specification standardized a low-rate, direct-sequence spread-spectrum (DSSS or DS PHY) physical layer. As compared to frequency-hopping techniques, direct-sequence transmission requires more power in order to achieve the same throughput [Pet95], but it can be readily scaled to much higher data rates.

The *802.11* specification uses an *11-bit Barker word* for spreading. Using 11-bit spreading code [Pet95] allows *802.11* to meet regulatory requirements of 10-dB processing gain with some safety margin. Although longer spreading codes allow higher processing gains, they require wider frequency bands. The DSSS PHY has 14 channels, each with 5-Mhz bandwidth, in the 2.4-GHz ISM band. Table 2.6 shows the available DSSS channels allowed in each country [Gas02]. Channel 10 is available throughout North America and Europe; most products use channel 10 as the default operating channel.

Most of the signal energy in *802.11* DSSS systems is spread across a 22-MHz band. Due to the use of 11-MHz clock, energy is spreads out from the channel center in multiples of 11-MHz. In order to prevent interference to the adjacent channels, the first side lobe is filtered 30 dB below the power at the channel center. Additional side lobes are filtered 50 dB below the power at the channel center. In order to prevent interference from networks operating on adjacent channels, *802.11 DSSS* equipment must be separated by a frequency band of at least 22 MHz, which corresponds to a separation of five channels, each with 5 MHz spacing.

Table 2. 6: 802.11 DSSS Available Channels in Different Countries

Country	Allowed Channels	Total # of Channels
US & Canada	1 to 11 (2.412 – 2.462 GHz)	11
Europe (excluding France and Spain)	1 to 13 (2.412 – 2.472 GHz)	13
France	10 to 13 (2.457 – 2.472 GHz)	4
Spain	10 to 11 (2.457 – 2.462 GHz)	2
Japan	14 (2.484 GHz)	1

All *802.11 DSSS* systems use *Differential Phase Shift Keying (DPSK)* modulation schemes. DBPSK (Differential Binary Phase Shift Keying) is used for transmissions at 1 Mbps, whereas DQPSK (Differential Quadrature Phase Shift Keying) is employed for transmissions at 2 Mbps (for further details about *DPSK*, see [Pro01]).

The 802.11b: HR/DSSS PHY

In 1999, the *802.11 Working Group* released its second extension to the basic *802.11* specification, known as *802.11b*. It uses the same MAC layer as defined by *802.11,* and is based on direct-sequence, spread-spectrum modulation. *802.11b* enables data rate up to 11 Mbps. The *802.11b* PHY is also known as the high-rate, direct-sequence, spread-spectrum PHY, abbreviated as HR/DSSS or HR/DS. Even though the modulation is different, the operating channels are exactly the same as used by the *802.11* low-rate direct sequence layer discussed above.

802.11b HR/DSSS PHY, in contrast to *802.11 DSSS,* uses a different encoding method called *Complementary Code Keying (CCK)*. *CCK* [Pro01] in *802.11b* divides the, 11 million chips per second, chip stream into a series of 8-bit code symbols, resulting in underlying series of 1.375 million code symbols per second transmission. Based on mathematical transforms that allow the use of a few 8-bit sequences to encode 4 or even 8 bits per code word, it allows data throughputs of 5.5 Mbps or 11 Mbps, respectively. Barker spreading, as used in the low-rate, direct-sequence layers, uses a static code to spread the signal over the available frequency band. CCK, on the other hand, uses the code word to carry information, as well as simply to spread the signal. Several phase angles are used to prepare a complex code word of eight bits. Further information about *802.11b CCK* can be found in many texts including [Gas02] and [Gei02].

In order to ensure backward compatibility with the *802.11 DSSS PHY*, the *HR/DSSS PHY* is designed to transmit and receive at *1 Mbps* or *2 Mbps*. Slower transmissions are supported in the same manner as the low-rate, direct-sequence layers described above. Higher-rate transmission is accomplished by building on the DQPSK-based phase shift keying techniques. DQPSK transmits two bits per symbol period, encoded as one of four different phase shifts. By using CCK, the symbol words themselves carry additional information. *5.5-Mbps* transmission encodes four data bits into a symbol. Two are carried using conventional DQPSK, and the other two are carried through the content of the code words. To move to a full *11 Mbps*, 8 bits must be encoded with each symbol. As with other techniques, the first two bits are encoded by the phase shift of the transmitted symbol relative to the previous symbol. Six bits are encoded using CCK.

802.11b includes two optional physical-layer features including *Packet Binary Convolution Coding (PBCC)* and *channel agility*. *PBCC* is an optional coding method that has not been widely implemented. To avoid interfering with existing *802.11* networks based on frequency-hopping technology, *802.11b* includes the channel agility option. When employing the channel agility option, *802.11b* networks periodically hop to a different channel. Three direct-sequence channels are used for nonoverlapping networks; the hop sequences and dwell times are designed to avoid interfering with a frequency-hopping network deployed in the same area. *802.11b HR/DSSS* PHY allows a maximum MAC frame size of 4,095 bytes, and its slot time is equal to 20 µs. [Gas02]

2.3 Issues with *802.11* Networks

The 802.11 technology is facing a number of problems and challenges. Here we will discuss only few of them, which are most important.

2.3.1 Network Security

For both wired LANs and wireless LANs, several categories of security issues violate the three basic functions of security – *authentication, integrity,* and *confidentiality*. The optional *WEP* standard does not provide adequate protection against security threats, such as, virus infection, attacks by unauthorized persons, and misuse by authorized personnel [Lar02].

The common techniques used to overcome the shortfalls of *WEP* are use of *Virtual Private Networks (VPN), SSH,* and *IPSec* (for details on these protocols, see [Pet00]). Current

authentication protocols are designed for a known, static group of users. The wireless networks are expected to cover hard-to-reach spots. Their use at public places raises the issue of authentication; who is allowed to use the network, how to authenticate users, and most importantly, how to protect users from each other. Better authentication methodologies are needed in order to address these problems.

IEEE 802.11i Task Group, responsible for improving security on *802.11* networks, proposed and adopted the *802.11x* framework in June 2001. It includes a new authentication protocol – the *Extensible Authentication Protocol (EAP).* *EAP* is an encapsulation protocol, and used to authenticate between the client and the access point. *WEP* keys can be dynamically generated and distributed by the use of *EAP.* Currently, *EAP* supports only *WEP,* but the *Advanced Encryption Standard (AES)* is also being considered. *AES* uses a block cipher algorithm as compared to linear cipher (RC4) used in *WEP.* [Lar02]

It is to be expected that recent advances in network authentication and security algorithms will lead us to more secure and private wireless networks as desired.

2.3.2 Roaming

A critical function in a multiple-cell wireless LAN i.e. ESS, is *roaming*, which enables wireless users to move from cell to cell seamlessly. As the *802.11* standard does not provide specification for roaming, it is up to the radio LAN vendors to define roaming protocols on their own. Companies that manufacture radio LAN access points have their own flavor of roaming. The *Wireless Ethernet Compatibility Alliance (WECA)* includes interoperable roaming as a requirement to receiving Wi-Fi™ certification. The *IAPP (Inter-Access Point Protocol)* specification builds upon the capabilities of the IEEE 802.11 standard, using the distribution system interfaces of access point that 802.11 provides. IAPP operates between access points, using the *User Datagram Protocol (UDP)* and the *Internet Protocol (IP)* as a basis for communications. *UDP* is a transport-layer protocol that provides connectionless and unacknowledged end-to-end data transfers (further details about *UDP/IP* can be seen in [Pet00]).

If the network protocol is *IP*, *IETF*'s [IETF] RFC 2002 known as *Mobile IP* (an enhancement to the standard *IP* protocol) can be implemented. The *Mobile IP* can be used if users need to roam to parts of the network associated with a different *IP address* than what's loaded in the appliance.

The main goal of *Mobile IP* is to enable mobile stations to roam transparently throughout networks, automatically maintaining proper *IP-based* connections to their home networks. This avoids the impracticality of changing the *IP address* in the appliance when operating in a different area of the network. The need for *Mobile IP* arises most often in wireless systems. For instance, when users roam from an access point located on one subnet of a network to another access point on a different subnet. *Mobile IP* uses an address-forwarding mechanism similar to postal mail forwarding service, to continue the delivery of packets to a mobile station as it moves from network to network. A positive feature of *Mobile IP* is that its implementation does not require changes to routers or the *Domain Name Servers (DNS)* (for more information, see [Pet00]). To implement *Mobile IP*, one only needs to include few software elements, such as, *Mobile Node, Home Agent*, and *Foreign Agent*. When the user moves to a different subnet, the user notifies the home subnet of his or her current location. The *home subnet* intercepts traffic intended for delivery to the mobile user and forwards it to a special node in the network known as the *foreign agent*. The *foreign agent* then forwards the messages to the roaming user. Messages sent by roaming user do not have to use this mechanism. These messages can travel directly to the recipient resulting in a triangular pattern of conversation. [Gei02]

2.3.3 Issues with TCP/IP over Wireless LANs

Currently, most of the wireless LANs implement *TCP/IP* as communication protocols. *TCP/IP*-based protocols provide an excellent platform for high-speed wired LANs with constant connections; however, the use of *TCP/IP* protocols over wireless LANs poses significant problems. Some of them are discussed below [Gei02].

- *High overhead:* Because of *TCP*'s connection-oriented protocol, it often sends packets that only perform negotiations or acknowledgements and that do not contain real data. This additional overhead consumes a relatively large amount of the limited wireless bandwidth, deteriorating the performance over the wireless LAN.
- *Incapability to adjust under marginal conditions: TCP* is fairly rigid when posed with changes in wireless coverage. With *TCP*, a marginal connection between the wireless appliance and an access point can cause *TCP/IP* protocol to terminate the connection, requiring the application or user to re-establish a connection.
- *Difficulty in dealing with mobile node addresses:* Traditional *IP addressing* assumes that the network device will always permanently connect to the network from within the same network domain. Problems arise when an appliance associated with an *IP address* roams

to an access point located within a different network domain, separated from the original network domain by a router. This may confuse the router and possibly other devices located within the new network domain. The result is a network that cannot route the packets to the destination of the mobile stations; unless device's IP address is changed physically according to new domain. However, this is not feasible in most of the cases.

If the wireless system consists of a larger number of appliances (usually greater than 10) per access point, service providers may contemplate the use of wireless *middleware* to deal with the limited bandwidth and need to operate in marginal conditions. Middleware products provide communication over the wireless network using a lightweight *non-TCP/IP* protocol between the appliances and middleware software residing on a server or separate PC. The gateway then communicates to the devices on the higher-speed wired network using standard *TCP/IP-based* protocols.

2.3.4 Mobility

The *802.11* offers only link-layer mobility which is possible only when all the access points can communicate with each other in order to keep track of mobile stations. Standardization of the *IAPP* by *Task Group F* should make it easier to deploy networks by facilitating interoperability between multiple vendors, and merge distinct wireless networks into each other. It, however, requires a lot of planning if a wireless LAN has to be deployed with a substantial coverage area, especially if seamless mobility throughout the entire coverage area is required. *Mobile IP* has been standardized to a reasonable degree, but an open source *Mobile IP* implementation of choice is yet to emerge. [Gas02]

2.3.5 Radio Resources

At present, wireless networks tend to have relatively few users, and the networks themselves are physically relatively far apart. However, when their usage will become more common, system designers and planners may need to consider many issues like their performance under stress, or in densely populated areas crowded with co-located networks. Right now, we don't really have the answers to these questions. As wireless networks will become more common, we'll be forced to answer them. It is clear, though, that there are resource constraints. Current technologies will suffer from overcrowding within the unlicensed bands. [Gas02]

2.3.6 Deployment

One of the major problems faced by the architects of the public-access wireless networks is that the service is quite generic. In the absence of any constraints, anybody can put up an antenna and offer Internet access via *802.11* equipment. Mobile telephony coped with this problem by licensing the spectrum. A similar solution, however, is not possible with *802.11* because it explicitly uses the unlicensed bands. Competition between network providers therefore shifts to the "*political layer of OSI model"*. [Gas02]

2.4 Recent Research Trends

In this section we will present a brief survey of recent research work that has been done in related areas to our work. However due to richness of research materials and tremendous activity in research community we would not be able to do an exhaustive search in this area. But we hope that this section will give the reader some idea about recent research trends and future perspectives.

With the approval of *IEEE 802.11b* [802.11b] standard in 1999, many researchers tried to measure and predict its performance over different network conditions. [Hop99] presented field trial results of a unique *802.11* compliant micro-cellular wireless network aimed at providing high bandwidth mobile communications. [Hop99] claimed that *802.11* compliant wireless LAN equipment, when modified can provide a total cellular coverage of 1 Km in free space and suggested supplementary work to achieve desired coverage using alternate antenna designs and configurations. [Bin99] reported practical performance of two *802.11* compliant wireless LANs and concluded that frame buffering and fragmentation are two crucial factors affecting performance of a wireless LAN. [Bin99] also suggested that length of a data frame and wireless bit rate also affect the transmission capabilities of a wireless LAN, and performance of an *802.11* compliant wireless LAN is generally unaffected by the type of frame addressing and use of reservation frames. [Lin99] presented a prototype implementation of an *802.11* compliant multihop wireless LAN with base-driven multihop bridging protocol running on access points and mobile stations to enable multihop routing and roaming.

Many researchers analyzed the performance of various transport layer protocols over wireless LANs. [Xyl99] presented measurement results performed over an *802.11b* compliant wireless

LAN and analyzed performance of *TCP* and *UDP* over it. [Pen01] presents a simulation analysis of *TCP* performance over *802.11* compliant wireless LANs. [Pen01] considered dual node and multi-node scenarios and concluded that the *IEEE 802.11 MAC* protocol has hidden the packet discard of lower layer and buffer overflow affects the *TCP* performance in dual node case. [Pen01] also claims that due to MAC retransmissions the throughput does not improve much, however the queue delay improves a lot in dual node case. [Pen01] also shows that throughput and delay characters of RTS/CTS enabled DCF are better than that with RTS/CTS disabled DCF in multi-node case. [Arr01] in 2001 characterized the behavior of *UDP* transport protocol in terms of throughput and delay over an *802.11b* compliant experimental wireless LAN. [Arr01] showed that the fragmentation procedure in hostile wireless environments is important except when using the lowest bit rate of 1 Mbps, and an additional error correction scheme is required at the highest bit rate in order to ensure an appropriate *IP* loss rate. [Rui03] presented a study of interactions between *TCP* and *802.11b MAC* protocols and their parameters that affect performance in multihop wireless networks, based on simulations and analysis. [Rui03] showed that the fundamental cause of performance degradation of multihop wireless networks is the occurrence of false link failures at the MAC layer and using a lower value of maximum *TCP* congestion window improves performance. [Rui03] also suggested that the optimal value for the number of retransmission attempts for failed packets is a function of traffic load as well as mobility and for a static topology or low mobility environments, using a higher value improves system performance significantly, whereas for highly mobile environments a high value results in increased delay in link failure detection. [Rui03] also discussed the effect of *TCP* packet size on overall throughput and suggested that there is a trade-off involved and determined threshold packet size for *TCP* connections beyond which throughput starts to degrade with increase in packet size. [Rui03] suggested that this threshold depends on the path length as interference increases with number of hops. Similarly, [Xyl01] in 2001 discussed the performance of *TCP/IP* protocol suite over wireless links when used for providing Internet connectivity.

With the spread of *802.11* compliant wireless LANs, many researchers analyzed the performance of different voice and data applications over them. [Suz99] evaluated the performance of *802.11 MAC* protocol for integrated *H.263* video and data transmission in a single basic service area of an infrastructure network using simulations. [Suz99] showed that if *CFP* repetition interval is set too long, the video delay performance deteriorates drastically and the capacity of *CP* becomes slightly larger. [Suz99] also studied the affect of *CFP* maximum duration on system performance. [Pra99] presented a qualitative comparison of four voice transmission schemes (Distributed

Coordination Function, Point Coordination Function, Priority Queuing, and Blackburst) over *802.11* wireless LANs. [Pra99] suggested that there is a trade-off between delivered QoS and implementation difficulty and Blackburst outperforms all other schemes in terms of delay as number of users increase, but its implementation is difficult and not totally compatible with the *802.11* standard. [Zah00] calculated a lower bound on the capacity of wireless LANs with voice and data services using *UDP/IP* and *TCP/IP* respectively. [Zah00] assigned the *UDP* protocol for voice and *TCP* for data communications in order to accommodate delay requirements for an acceptable quality of service. Also [Zah00] calculated maximum number of voce users under different conditions for maximum allowable voice packet time delay, channel bandwidth, and specified data traffic. [Fre01] presented a design and implementation of *Kinesis*, an object oriented architecture for transmission of real-time *H.263+* video on 802.11 ad-hoc networks with multicasting support. [Fre01] further suggested that new protocol supports needs to be provided to guarantee reliable video communication in multicast wireless networks. [Vee01] presented a design and analysis of a system that uses polling mode for interactive voice traffic in *802.11* networks. [Vee01] demonstrated that the PCF mode of *802.11 MAC* protocol can be used to carry telephony traffic, and using a connection admission control algorithm to control the number of voice calls admitted to polling list, network can provide delay guarantees. [Vee01] further showed that voice packets can be expected to suffer a high packet error rate in *802.11* networks. [Rag02] presented an analysis of associated issues with real-time video streaming over an *802.11b* compliant wireless LAN test bed at University of New Mexico. [Ban02] proposed ad-hoc, cluster-based, multihop network architecture for video communications using *802.11 FHSS*. [Ban02] observed that selecting a higher throughput rate (2 Mbps) of FHSS is advantageous for video communications, but it will require deployment of 4GFSK modulation, which is inefficient in terms of RF range for multihop communications. [Ban02], therefore, considered a combination of diversity and non-coherent Viterbi based receiver design techniques in order to improve its performance. [Ban02] also considered a bi-stream splitting technique together with packet-based error protection strategy to combat packet drops for video transmissions under multipath fading scenarios. [Oht02] presented an implementation of wireless *MPEG2* transmission system using *802.11b PHY*. [Oht02] proposed a new approach for Hybrid ARQ, in which retransmission control is performed by using data frames and claimed that the proposed protocol performs much better than packet based retransmission protocol.

Throughout the years, many researchers were trying to propose techniques for wireless LAN system deployment and planning. [Wu01] proposed an analytical model based on Markov chains

to compute the saturated throughput of *802.11* distributed coordination function (DCF). [Ala01] described a wireless LAN system architecture that combines the WLAN radio access technology with mobile operators' SIM-based subscriber management functions and roaming infrastructure (*GSM/GPRS*). [Ala01] claimed that this solution supports roaming between cellular and WLAN access networks and was the first step toward an *all-IP* network architecture. [Hil01] describes techniques to design a large-scale wireless LAN. [Cla02] discusses the feasibility of designing an outdoor cellular network based on *802.11b* standard and evaluated the performance of radio link for outdoor applications. [Kam02] discussed different approaches to coverage planning to WLAN systems and proposed a new optimization scheme for obtaining a close-to-optimal positioning of wireless LAN access points. [Kam02] also evaluated their performance in a typical downtown or campus environment. Similarly, [Leu02] studied the feasibility of designing an outdoor cellular network based on *802.11* specification. [Par02] presented an analysis on radio interference between channels of *802.11b* wireless LANs. [Sin02] assessed the performance of *802.11b* compliant wireless LAN in different vehicular mobility, peer-distance and driving environment scenarios.

New trends are emerging in indoor applications and usage of local area networking. [PLLAN] discusses a new indoor LAN concept known as *"Power Line Local Area Networks"*. The main attraction provided by wireless networks is flexibility and mobility, which cannot be easily achieved by wired networks. [Pro02] proposes a new approach for wireless LAN design. [Hun02] discusses some new perspectives and problems related with use of the *802.11* compliant multi-hop wireless networks.

So far not much work has been done on practical implementations of *802.11* based multi-hop wireless networks, used for high mobility roaming. This document presents one of the early applications of the *IEEE 802.11b* networks to high mobility outdoor environments.

2.5 Definitions of Key Terms

Definitions of some keywords used in this document are presented here.

Access Point: An entity that has station functionality and provides access to the destination services, via the wireless medium for associated stations. [8802-11]

Ad hoc Network: A network composed solely of stations within mutual communication range of each other via the wireless medium. [8802-11]

Bandwidth: Literally speaking, it is a measure of the width of a frequency band. Bandwidth of a communication link, generally speaking, is a measure of the capacity of a link or connection, usually given in units of bits per second. [Pet00]

Bridge: A device that forwards link-level frames from one physical network to another, sometimes called a LAN switch. [Pet00]

Channel: An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume pf space, with other instances of medium use (on other channels) by other instances of the same physical layer (PHY), with an acceptably low frame error ratio due to mutual interference. [8802-11]

Client: The requester of a service in a distributed system. [Pet00]

Congestion: A state resulting from too many packets contending for limited resources, which may force the router (switch) to discard packets. [Pet00]

Congestion Control: Any network resource management strategy that has, as its goal, the alleviation or avoidance of congestion. [Pet00]

Connectionless Protocol: A protocol in which data may be sent without any advance setup. [Pet00]

CSMA/CD: Carrier Sense Multiple Access with Collision Detect. CSMA/CD is a functionality of network hardware. “Carrier sense multiple access” means that multiple stations can listen to

the link and detect when it is in use or idle; "collision detect" indicates that if two or more stations are transmitting on the link simultaneously, they will detect the collision of their signals. [Pet00]

Ethernet: A popular local area network technology that uses CSMA/CD and has a bandwidth of 10 Mbps. [Pet00]

Hidden Node Problem: Situation that occurs on a wireless network where two nodes are sending to a common destination, but are unaware that the other exists. [Pet00]

Host: A computer attached to one or more networks that supports users and runs application programs. [Pet00]

internet: A collection of (possibly heterogeneous) packet-switching networks interconnected by routers. Also called an internetwork. [Pet00]

Internet: The global internet based on the Internet (*TCP/IP*) architecture, connecting millions of hosts worldwide. [Pet00]

Interoperability: The ability of heterogeneous hardware and multivendor software to communicate by correctly exchanging messages. [Pet00]

IP: Internet Protocol. A network layer protocol that provides a connectionless, best-effort delivery service of Datagrams across the Internet. [Pet00]

Latency: A measure of how long it takes a single bit to propagate from one end of a link or channel to the other. Latency is measured strictly in terms of time. [Pet00]

Link: A physical connection between two nodes of a network. [Pet00]

MAC: Medium Access Control. Algorithms used to control access to shared-media networks. [Pet00]

Measured Time: *Chariot* defines the parameter "Measured Time" as the time elapsed between the start of the data transmission by the source host and the very moment after receiving an acknowledgement from the destination host. [NetIQ]

Mobile Station: A type of station that uses network communications while in motion. [8802-11]

MPEG: Moving Picture Experts Group. Typically used to refer to an algorithm for compressing video streams developed by the MPEG. [Pet00]

Node: A generic term used for individual computers that make up a network. Nodes include general-purpose computers, switches, and routers. [Pet00]

OSI: Open System Interconnection. The seven-layer network reference model developed by the ISO. [Pet00]

Portable Station: A type of station that may be moved from location to location, but that only uses network communications while at a fixed location. [8802-11]

Protocol: A specification of an interface between modules running on different machines, as well as the communication service that those modules implement. The term is also used to refer to an implementation of the module that meets this specification. [Pet00]

Response Time: *Chariot* calculates the "Response Time" as follows.

$$\text{Response Time} = (\text{Measured Time})/(\text{Transaction Count})$$

Where the parameter "Transaction Count" refers to the transactions made between the source and destination hosts. [NetIQ]

Router: A network node connected to two or more networks that forwards packets from one network to another. [Pet00]

RTT: Round-trip time. The time it takes for a bit of information to propagate from one end of a link or channel to the other and back again; in other words, double the latency of the channel. [Pet00]

Server: The provider of a service in a client/server distributed system. [Pet00]

Station: Any device that contains an *IEEE 802.11* conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium. [8802-11]

Streaming Throughput: *Chariot* calculates the "Streaming Throughput" as follows. [NetIQ]

Streaming Throughput = (Bytes Received By Destination Host)/(Measured Time)

Switch: A network node that forwards packets from inputs to outputs based on header information in each packet. Differs from a router mainly in that it typically does not interconnect networks of different types. [Pet00]

TCP: Transmission Control Protocol. Connection-oriented transport-layer protocol of the Internet architecture. TCP provides a reliable, byte-stream delivery service. [Pet00]

Throughput: The observed rate at which data is sent through a channel. It is calculated as

Throughput = TransferSize/TransferTime

Where TransferTime includes not only the elements of one-way Latency, but also any additional time spent requesting or setting up the transfer. [Pet00]

Chariot calculates the "Throughput" as follows. [NetIQ]

Throughput = (Bytes Sent By Source Host + Bytes Received By Source Host)/(Throughput Units)/(Measured Time)

UDP: User Datagram Protocol. Transport-layer protocol of the Internet architecture that provides a connectionless Datagram service to application-level processes. [Pet00]

2.6 Summary

In this chapter we briefly discussed the features and limitations of wireless networks emphasizing on IEEE 802.11 standard. Our experimental network as to be discussed in next chapter is built using 802.11b equipment, which is probably the most widely deployed wireless LAN around the world. The main reasons for 802.11b success are commercial availability of its equipment, low cost and use of license-free ISM band. Current research trends have also been discussed from which we could see ongoing problems and future of 802.11 wireless LANs.

Chapter 3: Experimental Wireless Data Network

We designed and deployed an *802.11b* compliant experimental wireless network on *Virginia's Smart Road* [Smart Road]. This chapter discusses the experimental network design and architecture, and describes site details including link budget calculations and network components.

3.1 Network Design

Virginia's Smart Road [Smart Road] serves as a research and development facility for new transportation technologies including safety and human factors research, vehicle dynamics, road-to-vehicle communications, ITS product evaluation, and automated vehicle control. Its rich testing and monitoring facilities require a high-speed wireless connection with data storage and processing facilities at the *Virginia Tech Transportation Institute (VTTI)* [VTTI] building located by the road entrance. The nature of telematics applications at the *Smart Road* requires an asymmetric wireless network with more *bandwidth* (for details, see [Pet00]) in the *reverse link* (from stations on road to *VTTI* building) direction.

Considering the specific requirements at the *Smart Road*, we designed an *Infrastructure based (ESS) 802.11b* compliant asymmetric experimental wireless network. Today, *802.11b* is one of the most widely deployed wireless LAN standards around the world, mostly due to its commercial viability, low deployment and operational costs, and use of license-free ISM bands. Although, the network has been designed for the *Smart Road,* its deign principles and results can be applied to any wireless LAN.

3.2 Network Architecture

Our designed network features a multi-hop *wireless backbone* with a *linear topology*, and four different nodes stretched over the road length (approximately 2.2 miles). The network is based on IEEE 802.11b wireless LAN standard [802.11b], and is equipped with four *Wireless Access Points (WAPs)*, and four *backbone routers.*

Our designed network is built on four distinct nodes. The nodes are numbered as 1, 2, 3, and 4 starting from the road entrance and moving towards the East. Each node consists of a *backbone router* and an *access point* with the exception at the first node, where both *ROR-1* (first backbone router) and *AP-1* (first access point) share the processing power and hardware of single router *ROR-1000* simultaneously. Each router and access point has the capability to handle two *Wi-Fi Clients* simultaneously; hence each device can have two different links at two different frequency channels. All *backbone routers* are connected to one another via wireless links in a point-to-point fashion forming a *linear backbone*. The *access points* along the road provide *access network* coverage.

As discussed in Chapter 2, eleven *802.11b* frequency channels can be used in the United States. While assigning frequency channels, maximum separation between the neighboring cells is considered in order to maximize radio link performance. It is to be noted here that the *access network* and the *backbone* are fairly non-interfering with each other due to use of narrow beam backbone antennas, and access network deployment at a lower altitude. Therefore, we can treat these two networks separately. Their interference, however, cannot be totally neglected due to co-location in the same area.

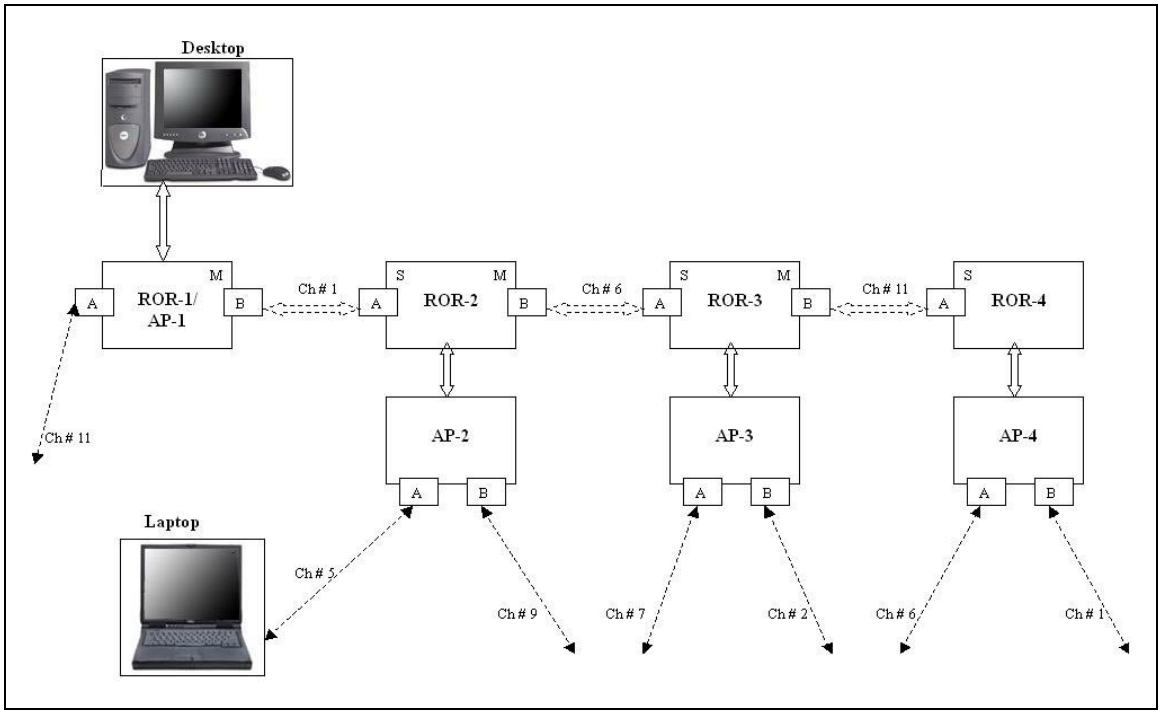

Figure 3. 1: Network Architecture

Figure 3.1 shows the network architecture and frequency channel assignments. The *linear backbone network* is built by connecting outdoor routers in a point-to-point fashion. Each outdoor router and access point has two wireless interfaces, which are represented by letters 'A', and 'B' in Figure 3.1. The channel number used by each of the wireless links is clearly marked in Figure 3.1. Backbone routers communicate with each other in a *Master/Slave* manner (The Master device is shown by letter 'M', and the Slave device by letter 'S' in Figure 3.1), and *Access Points (APs)* are connected to *Remote Outdoor Routers (RORs)* by straight *Ethernet* cable. Solid arrows denote *Ethernet* connections, and *dotted arrows* in *Figure 3.*1 represent wireless links. We used a fixed computer (will be referred as *Desktop*) and a (sometimes two) mobile computer (will be referred as *Laptop*) for taking measurements on the road as shown in Figure 3.1. The fixed computer is connected to first router *ROR-1* via crossover *Ethernet* cable, whereas the laptop is connected to the wireless network by a wireless link.

3.3 Site Details

The experimental network deployed on *Virginia's Smart Road* [Smart Road] is located in southwest Virginia in a fairly rural locality. The road is still under development by the *Virginia Department of Transportation (VDOT)* [VDOT] and is administered by *VTTI* [VTTI]. Currently its two-lane version is in use for research and development purposes only [Smart Road], which is approximately 2.2 miles long. This version is equipped with a variety of test equipment and structures [Smart Road] and is widely used for research in the areas of ITS, traffic engineering, human factors and vehicular research. The experimental network was built with the help of *VTTI* [VTTI] and the research was conducted under the supervision of both *VTTI* [VTTI] and *The Mobile and Portable Radio Research Group at Virginia Tech (MPRG)* [MPRG]. The basic purpose of this research is to design and analyze the performance of a wireless network capable of sending high data rate telematics data back to the *VTTI building* and transmitting control signal and information to fixed and mobile wireless stations on the road.

3.3.1 Smart Road Pictures

This section presents some pictures to describe site details clearly. These pictures help us to understand coverage pattern and network performance. Figure 3.2 shows an aerial view of the *Smart Road.*

Figure 3. 2: An Aerial View of *The Smart Road*

Figure 3.2 shows the curvature and location of surrounding hills and the difference in elevation levels at different locations. The *Smart Road* has loops on its both ends for research purposes.

Figure 3.3 shows aerial view from another angle with some more surroundings details. The rural nature of the road location can be seen from it. The *VTTI building* is also visible in Figure 3.3 on left hand side of the first loop. The network's first router *ROR-1* and fixed computer *Desktop* are installed in this building.

These two figures give us an idea about the surrounding hills and terrain. The road is also equipped with weather stations [Smart Road] in the middle section where third router *ROR-3* and access point *AP-3* are installed. Figure 3.4 shows a section of it with a vehicle moving in rain poured by these weather stations. Besides rain, these weather stations are also capable of simulating real snow with variable lighting. This section of *Smart Road* is crowded with metallic poles used for weather and lighting simulations. These poles may cause a source of reflection and obstruction for radio waves. A hill is also present besides these poles, which might also reflect the radio signals.

Figure 3. 3: Another Aerial View of *The Smart Road* with More Surroundings Details

Figure 3. 4: A View of Weather Section at *The Smart Road*

Figure 3.5 shows the road curvature and locations of different wireless network nodes along the road. It is to be noted here that the road continues after the fourth node location (first from the left hand side) in a straight line for about 950 meters and is not shown in Figure 3.5. As explained

earlier, the first routing and access node is located on the roof of *Control Room* at *VTTI building*, which is located by the side of road entrance. As discussed earlier the road is built with two loops at both ends in order to accommodate long-run tests [Smart Road]. The first of these loops, located at the entrance is shown in Figure 3.5. The other loop is omitted from it because we didn't include that small part in our measurements.

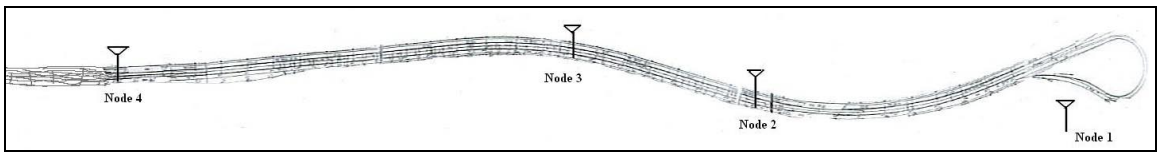

Figure 3. 5: Smart Road Map

The *VTTI building* serves as Node 1 location and is located close to the road entrance as shown in Figure 3.5. Its view from the road is shown in Figure 3.6.

Figure 3. 6: A View of VTTI Building from The Smart Road

The ground views from different wireless nodes help us in understanding site details further. These ground views are presented below in Figures 3.7 to 3.10 taken from each wireless node in the direction of movement. It is to be noted here that we always move on the eastbound lane of the road while taking measurements.

Figure 3. 7: A View from Road Entrance

Figure 3. 8: A View from Second Wireless Node along The Road

Figure 3. 9: A View from Third Wireless Node among Road's Weather Section

Figure 3. 10: A View from Last Wireless Node on The Road

A plot of elevation levels along the road is given in Figure 3.11 below. This figure gives us an idea of changes in elevation level along the road. However, Figure 3.11 does not show the

elevation changes along the complete road. It only covers the starting 2.8 Km section of the road, whereas the complete road spans over approximately 3.5 Km.

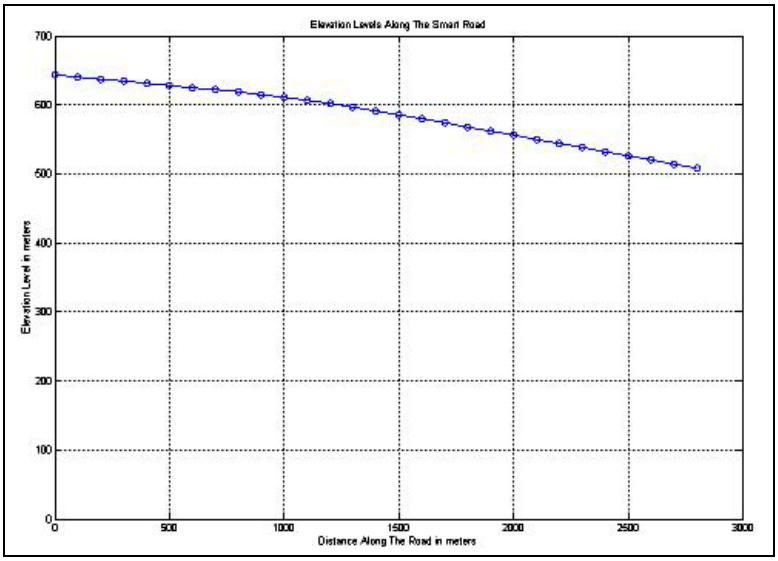

Figure 3. 11: Elevation Levels Along The Road for The First 2.8 Km Section

After the first 2.8 Km section presented above, there is a dip on the road, which can be seen in Figure 3.12. This dip is located on the last bridge on the road [Smart Road] and causes abnormal coverage patterns discussed in the Chapter 4.

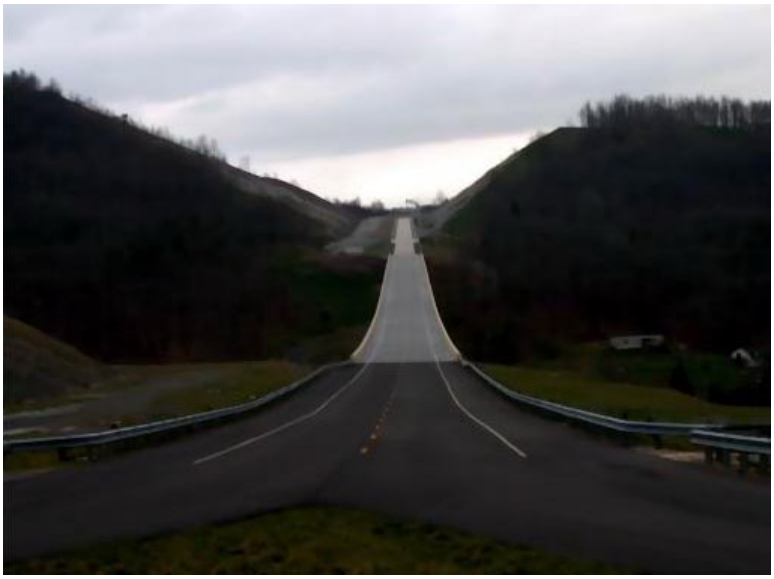

Figure 3. 12: A View of The Smart Road from The Road End

The network's backbone routers are equipped with 13.5 dBi Yagi antennas installed on light poles along the road. A view of them is shown in Figure 3.12. The access points are equipped with 12 dBi-sectored antennas mounted on the same light poles as backbone antennas. A view of these antennas is shown in Figure 3.13.

Figure 3. 13: A View of Backbone Yagi Antennas

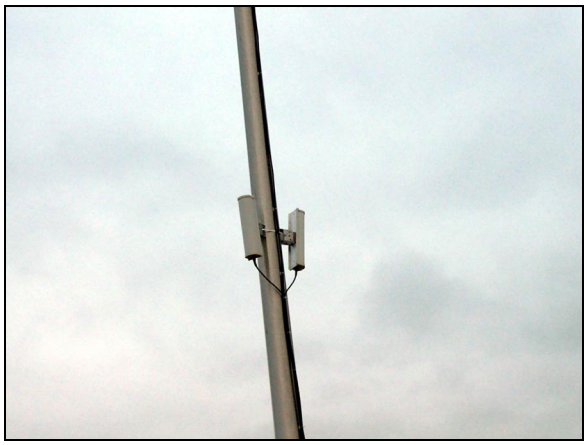

Figure 3. 14: A View of Access Points' 12 dBi Sectored Antennas

3.3.2 Distances & Elevations

As explained earlier, the experimental network consists of four wireless nodes with a backbone router and an access point at each location. With the exception of the first node, which is located at *the Control Room*, all nodes are located along the road. As shown in Figure 3.5, *the VTTI*

building is located near the road entrance (the loop). Location of the other wireless nodes and road curvature is also visible in Figure 3.5. In Table 3.1, approximate aerial distances among different wireless nodes and road ends are given.

Table 3. 1: Aerial Distances Between Different Locations on The Smart Road

Distance (m)	Node 1	Road Entrance	Node 2	Node 3	Node 4	Road End
Node 1	-	200 m	500 m	1200 m	2100 m	3200 m
Road Entrance	200 m	-	700 m	1400 m	2300 m	3400 m
Node 2	500 m	700 m	-	700 m	1600 m	2700 m
Node 3	1200 m	1400 m	700 m	-	900 m	2000 m
Node 4	2100 m	2300 m	1600 m	900 m	-	1100 m
Road End	3200 m	3400 m	2700 m	2000 m	1100 m	-

There is a variation in elevation levels all along the road. These elevation levels (approximate) are recorded in Table 3.2 below.

Table 3. 2: Elevation Levels at Different Locations on The Smart Road

Location	Node 1	Road Entrance	Node 2	Node 3	Node 4	Road End
Elevation (m)	651 m	632 m	629 m	593 m	590 m	500 m

Due to road curvature, the ground distances vary from aerial distances. These ground distances between different locations on the road are given in Table 3.3.

Table 3. 3: Ground Distances Between Different Locations on The Smart Road

Distance (m)	Road Entrance	Node 2	Node 3	Node 4	Road End
Road Entrance	-	874 m	1581 m	2476 m	3426 m
Node 2	874 m	-	707 m	1602 m	2552 m
Node 3	1581 m	707 m	-	895 m	1845 m
Node 4	2476 m	1602 m	895 m	-	950 m
Road End	3426 m	2552 m	1845 m	950 m	-

3.4 Network Equipment

The network interfaces one access point and one router at each wireless node along the road. All routers are connected with each other via wireless links forming a three-hop wireless backbone. Each router node is equipped with an *ORiNOCO* [ORiNOCO] outdoor router *ROR-1000, Silver PC Cards,* and *Telex Wireless* [Telex] 3.5 dBi Yagi antennas (with 30° half-power beamwidth). The access points are connected to routing nodes via straight *Ethernet* cables. However, the first router (*ROR 1*) and access point (*AP 1*) share the hardware and processing power of the same router *ROR-1000* simultaneously. Each access point is equipped with *ORiNOCO* access point *AP-1000*, *Silver PC Cards,* and *Telex Wireless* [Telex] 12 dBi 120° sector antennas. All *backbone antennas* are installed at an approximate height of 40 feet (12.2 meters), whereas most of the *access network antennas* are installed at an approximate height of 30 feet (9.1 meters) from ground level. The *backbone router* and *wireless access points* are installed in underground bunkers, approximately 6 feet below ground level along the road. It is to be noted here that each *ROR-1000* and *AP-1000* has two slots for *PC cards*. Hence each *ROR-1000* is configured to have two distinct wireless links in different directions with two different frequency channels. Similarly, each *AP-1000* is configured to have two distinct access points in different directions with two different channels. However, *ROR-1/AP-1* is an exception here because they both use the same router equipment *ROR-1000* and can have only one link each. A computer is connected to first router using cross over Ethernet cable. One and sometimes two laptops are used for taking network performance measurements using *ORiNOCO Client Manager* and *NetIQ Chariot* software tools.

3.4.1 ORiNOCO™

Remote Outdoor Routers (*ROR-1000)*

As mentioned earlier, we used *ORiNOCO* [ORiNOCO] outdoor routers *ROR-1000* for the *backbone network*. These support point-to-point and point-to-multipoint links in 2.4 GHz ISM band. They are also equipped with a *10/100 Base-T Ethernet (IEEE 802.3)* interface. Its dual slot architecture allows us to create *WiFi* cells in conjunction with outdoor connection as we used it at first node. It is this dual slot architecture of outdoor router, which allows us to use two *ORiNOCO PC Cards* in single hardware. Thus two different frequency channels can be used on each router

supporting two different wireless links. It is to be noted here that these routers use the Turbocell communication protocol in order to support large distance wireless links [ORiNOCO].

Wireless Access Points

We used *ORiNOCO* [ORiNOCO] wireless access points *AP-1000* in our network. Similar to *ROR-1000*, it has dual slot architecture, which allows us to use two different *PC Cards* in single *AP-1000* hardware. This accounts for two different frequency channels used on each access point (except first node as explained earlier). Similar to network router it is also equipped with *10/100 Base-T Ethernet (IEEE 802.3)* interface.

WiFi™ Client

We used *ORiNOCO* [ORiNOCO] *Silver PC Cards* as wireless client in our laptops and network infrastructure including backbone routers and access points. The same card can be used as *WiFi* wireless client for both backbone and access point applications and delivers data rates up to 11 Mbps.

Client Manager™

The *Client Manager* software tool enables us to measure and record wireless link SNR, signal and noise levels and number of messages received at different data rates over the link. We used this software tool extensively to measure wireless link signal-to-noise ratio (SNR).

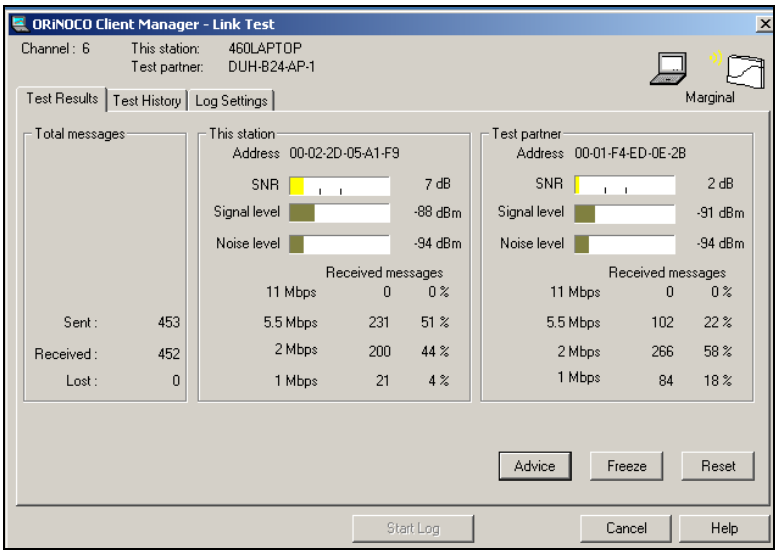

Figure 3. 15: The Link Test Window of ORiNOCO Client Manager

OR Manager™

ORiNOCO OR Manager is used to configure and troubleshoot outdoor routers and access points. We used this software tool to set up our network routers and access points and debug configuration errors.

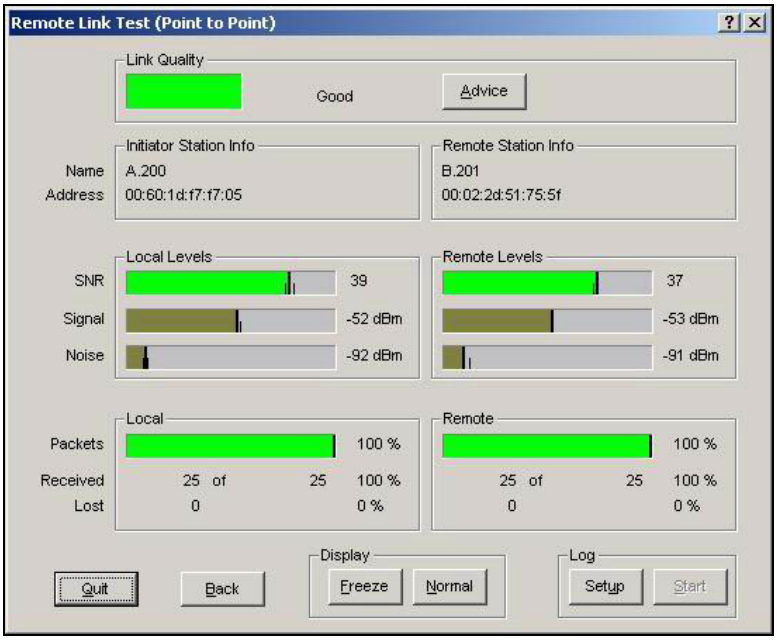

Figure 3. 16: OR Manager Link Test Window

3.4.2 NetIQ®

Chariot™

The *NetIQ* [NetIQ] *Chariot* software tool was used to measure our network performance. This tool allows us to test system performance including *throughput, response time, streaming tests* etc. with various network layer, and transport layer protocols such as *IP, Mobile IP, IPSec, TCP, UDP, RTP* etc. The tool has several application scripts including *MPEG Video, FTP, File Transfer* and many others. These applications can be used to test network performance under specific conditions.

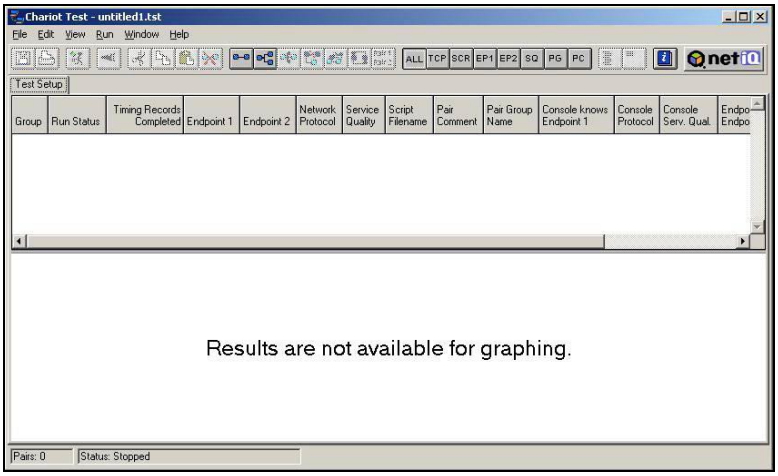

Figure 3. 17: Chariot Test Window

3.4.3 HyperGain® Antennas

We used following 2.4 GHz, 3 dBi Magnetic Vehicle Mount Omnidirectional antenna from *Hyperlink Technologies Inc.* [HyperLink].

3.4.4 Telex Wireless Antennas

Following antennas, manufactured by *Telex Wireless* [Telex] were used.

- 2.4 GHz 13.5 dBi WLAN Yagi antennas were used for *backbone* links.

- 2.4 GHz 12 dBi 120° Sectored antennas were used for *access network*.

3.4.5 5-dBi Mobile Antenna

5-dBi magnetic vehicle mount omnidirectional antenna was mainly used for static and mobile measurements. This antenna was manufactured by *Fleeman Anderson & Bird Inc., USA* [Fleeman].

3.4.6 Fixed Computer

We connected a computer with an *AMD 850 MHz* processor to the first network router using approximately 100 feet crossover Ethernet cable. The computer is equipped with 256 MB RAM and *Microsoft* [Microsoft] *Windows 2000 Server* operating system. In future references, this computer will be referred as *Desktop* as compared to two laptops, which were used for performance measurement purposes.

3.4.7 Laptops

We used two laptops for our network performance measurement purposes. The first laptop is equipped with *Intel* [Intel] *Pentium III Mobile* 800 MHz CPU, 128 MB RAM and *Microsoft* [Microsoft] *Windows 2000* operating system. This laptop is installed with *NetIQ* [NetIQ] *Chariot* and *ORiNOCO* [ORiNOCO] *Client Manager* [Client Manager] software tools, which were used to measure network performance. This laptop is used throughout to measure network performance.

For two-user measurements another laptop is used which is equipped with 700 MHz *Intel Pentium III* CPU, 256 MB RAM and *Microsoft Windows 2000* operating system.

We refer these two laptops as *Laptop 1* and *Laptop 2* in future references. *ORiNOCO* WLAN *PC Cards* are used for communicating with access points in both of these laptops. All of these computers are loaded with static IP addresses.

3.5 Link Budget Calculations

A *Wideband PCS Microcell Model* [Rap01] is used for link budget calculations. This model was developed using path loss, outage and delay spread measurements taken with a 20 MHz pulsed transmitter at 1900 MHz in typical microcellular environments. Various base station antenna heights (3.7 m, 8.5 m and 13.3 m) are considered separately whereas the mobile receiver is assumed to have an antenna at a height of 1.7 m. This model predicts that a 2-ray ground reflection model [Rap01] model is a good estimate for path loss in line-of-sight environments whereas a simple log-distance path loss model [Rap01] holds well for obstructed microcell environments. This model gives us a good estimate for our link budget calculations.

For flat earth ground reflection model, first Fersnel zone clearance d_f (the distance at which first Fersnel zone just becomes obstructed by the ground) is given by

$$d_f = \frac{1}{\lambda}\sqrt{16h_t^2 h_r^2 - \lambda^2\left(h_t^2 + h_r^2\right) + \frac{\lambda^4}{16}} \quad , \tag{3.1}$$

where

$d_f =$ First Fersnel Zone Clearance

$\lambda =$ Wavelength

$h_t =$ Transmitter Antenna Height

$h_r =$ Receiver Antenna Height

The backbone antennas are installed at an approximate height of 13.3 meters (43.64 feet) whereas access point antennas are mounted approximately at 8.5 meters (27.88 feet) above the ground level. Hence we can calculate two d_f values for our network.

Thus for backbone we have,

$\lambda =$ 0.125 m @ 2.4 GHz

$h_t = h_r =$ 13.3 m

Hence,

$d_f\,|_{Backbone}$ = 5660.45 meters

Similarly for access point we have,

λ = 0.125 m @ 2.4 GHz

h_t = 8.5 m and

h_r = 1.7 m (mounted on top of vehicle)

Hence,

$d_f\,|_{WAP}$ = 462.32 meters

For the line-of-sight case, the double regression path loss model is used and average path loss is calculated from

$$\overline{PL}(d) = \begin{cases} 10n_1 \log_{10}(d) + p_1, & for\ 1 \langle d \langle d_f \\ 10n_2 \log_{10}(\frac{d}{d_f}) + 10n_1 \log_{10}(d_f) + p_1, & for\ d \rangle d_f \end{cases} \quad (3.2)$$

where,

$p_1 = \overline{PL}(d_0)$ is the path loss in dBs at the close-in reference distance of 1 m, and

n_1, n_2 are path loss exponents as functions of transmitter height and are tabulated in [Rap01].

The p_1 can be calculated from free space model with unity gain antennas [Rap01] as below

$$p_1 = \overline{PL}(d_0 = 1m) = -20\log_{10}(\frac{\lambda}{4\pi}) = 40.046dB$$

The following values of path loss exponent were used from [Rap01] in order to calculate average path loss for the backbone and access point network components.

For backbone (Tx Antenna Height = 13.3 m),

$n_1 = 2.07$ and $n_2 = 4.16$

whereas for access points (Tx Antenna Height = 8.5 m),

$n_1 = 2.17$ and $n_2 = 3.36$

For path loss calculations the following result from [Rap01] are used,

$$\overline{PL}(d)[dB] = P_t[dBm] + G_t[dBi] + G_r[dBi] - P_r[dBm] - L[dB] \quad (3.3)$$

where

$\overline{PL}(d)$ indicates average path loss as a function of Tx-Rx distance

P_t indicates power transmitted by transmitter

$G_t and G_r$ indicate transmit and receive antenna gains

P_r indicates receiver sensitivity and

L indicates system loss

The following transceiver data is obtained from *ORiNOCO PC Card* [ORiNOCO] specifications

- Transmitter Nominal Output Power: 15 dBm
- Receiver Sensitivity @ 11 Mbps: -82 dBm
- Receiver Sensitivity @ 5.5 Mbps: -87 dBm
- Receiver Sensitivity @ 2 Mbps: -91 dBm
- Receiver Sensitivity @ 1 Mbps: -94 dBm
- Max. Tolerable Delay Spread (at FER < 1%) @ 11 Mbps: 65 ns
- Max. Tolerable Delay Spread (at FER < 1%) @ 5.5 Mbps: 225 ns
- Max. Tolerable Delay Spread (at FER < 1%) @ 2 Mbps: 400 ns
- Max. Tolerable Delay Spread (at FER < 1%) @ 1 Mbps: 500 ns
- Bit Error Rate (BER): Better than 10^{-5}

As discussed earlier, 13.5 dBi Yagi antennas are used at both ends of backbone whereas 12 dBi sectored and 5 dBi omnidirectional antennas are used for access point network. Moreover, a

system loss of 10 dB is assumed for these calculations. The resulting link budget distances are tabulated below. These results are based on the *PC Card* receiver sensitivity values discussed above.

Table 3. 4: Maximum Possible Coverage Range of The Experimental Network

Network Type/Data Rate	11 Mbps	5.5 Mbps	2 Mbps	1 Mbps
Backbone	3738 m	6077 m	7582 m	8952 m
Access Network	704 m	991 m	1303 m	1601 m

Based on the above link budget calculations, the antenna locations can be predicted along the road. However, it should be kept in mind that these calculations are based on line-of-sight environment as our observation shows that obstructed environment results in a very poor performance of wireless link.

3.6 Summary

In this chapter the *Smart Road Experimental Wireless Network* and site details are discussed, which help the reader in understanding the coverage patterns and throughput results discussed in succeeding chapters. This chapter also describes the hardware/software equipment and tools used for network design, implementation, performance measurement and analysis purposes. Link budget calculations are also discussed in this chapter in order to estimate network coverage and usability.

Chapter 4: Network Performance Results & Analysis – Static

This chapter discusses results of static performance of the network, signal-to-noise ratio (SNR), response time and throughput values parameters. These parameters estimate the behavior and characteristics of the network. The two transport layer protocols, *TCP* and *UDP* are used in these measurements with IP as network layer protocol. The measurements are taken with the help of *ORiNOCO Client Manager* and *NetIQ Chariot* tools.

4.1 Backbone SNR

As discussed in Chapter 3, the experimental network consists of an *802.11b* compliant wireless backbone with three hops. The backbone is implemented by connecting *ORiNOCO* outdoor routers *ROR-1000* with *Telex Wireless Yagi* antennas in a linear fashion. This backbone serves the purpose of *distribution system (DS)*, and transfers data among various nodes statically. Following is a summary of average SNR of backbone links.

Table 4. 1: Average SNR of Backbone Links

Link No.	Channel No.	Average SNR
1	1	51 dB
2	6	48 dB
3	11	29 dB

These measurements are taken with the help of *ORiNOCO OR Manager*. The backbone SNR values give us an insight into network performance. The better the SNR the better the network performance may be. It is to be noted here that the link between ROR-3 and ROR-4 (third link) has comparatively low SNR due to presence of metallic weather poles and surrounding hills between them. But this SNR is enough to support network communications as will be shown in the next section.

4.2 End-user Wireless Link SNR and Coverage

This section discusses network coverage and SNR for stationary users in the last section of the road (from AP-3 to the road end) and only AP-3 is used to provide network access. Hence, in this configuration, the network has only one active access point i.e. AP-3. This section of the road is relatively straight but with significant changes in the elevation at various sections on the road. All of these measurements are taken by *ORiNOCO Client Manager,* which can record end-user SNR and the data rate. The end-user wireless link is defined as the link between the wireless access point and the laptop. All of the following results are based on averages taken over multiple readings at a particular place.

4.2.1 5-dBi Omnidirectional Antenna

We use 5-dBi magnetic vehicle mount antenna during these tests with the *Laptop* 1. There is only one active access point (AP-3) in the network. The measurements are taken at static locations along the road moving on the eastbound lane. The access point (AP-3) and *Laptop*'s SNR plot with distance is shown in Figure 4.1. The SNR curves represent average SNR values measured at every 200 feet starting from location of AP-3.

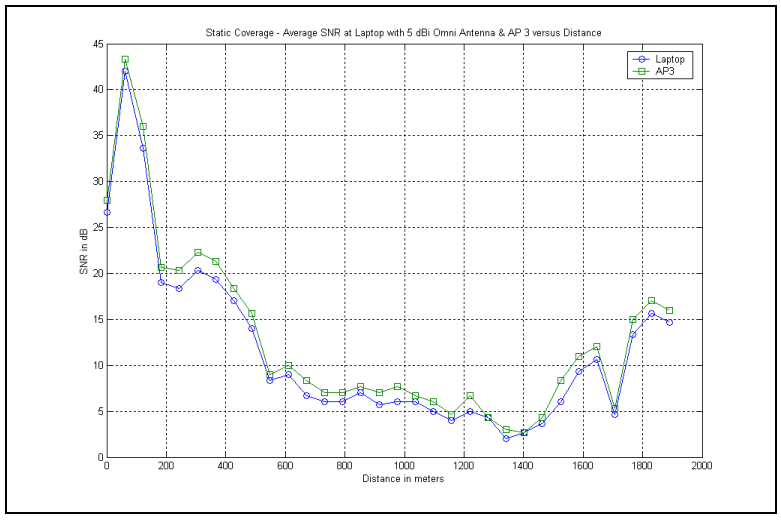

Figure 4. 1: Average SNR at AP-3 and *Laptop* with 5-dBi Antenna

The typical shape of these SNR curves is a result of elevation changes along the road. It is to be noted here that both access point and *Laptop* SNR are almost the same throughout the tests.

Figure 4.2 shows *Laptop*'s average received power and noise level variation with distance.

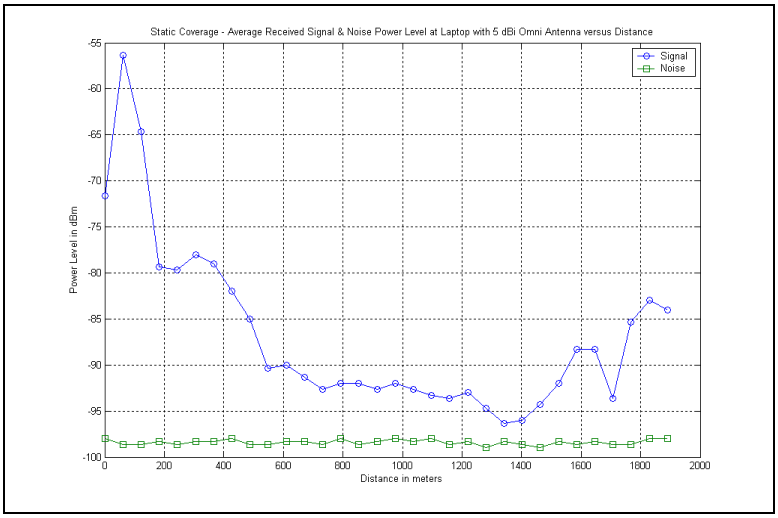

Figure 4. 2: *Laptop*'s Average Received Signal and Noise Power Level with 5-dBi Antenna

Figure 4.2 shows that the average noise level almost remains the same throughout the region with a mean value of *–98.43 dBm.* Received signal power, however, varies with the distance in a typical fashion as shown in Figure 4.1. The access point shows similar behavior, but the results are not reported here for the sake of brevity.

Figure 4.3 shows a graph of *Laptop*'s average data rate as measured by *Client Manager.* However, this parameter here does not show network throughput rather it shows the end-user wireless link (between *Laptop* and AP-3) average data rate. It is calculated by averaging the number of test messages received at different rates recorded by *Client Manager.* It is to be noted here that at a particular static location, test messages may not be received at a constant rate due to random nature of SNR and subsequent power and data rate adoption of access point. Based on Figures 4.1, 4.2, and 4.3, it may be predicted that the end-user wireless link data rate depends on SNR values, and at least 15-dB SNR may guarantee data rate of 11 Mbps between the *Laptop* and access point. However, these values merely show a reflection of our observations while taking measurements and may not be true in general.

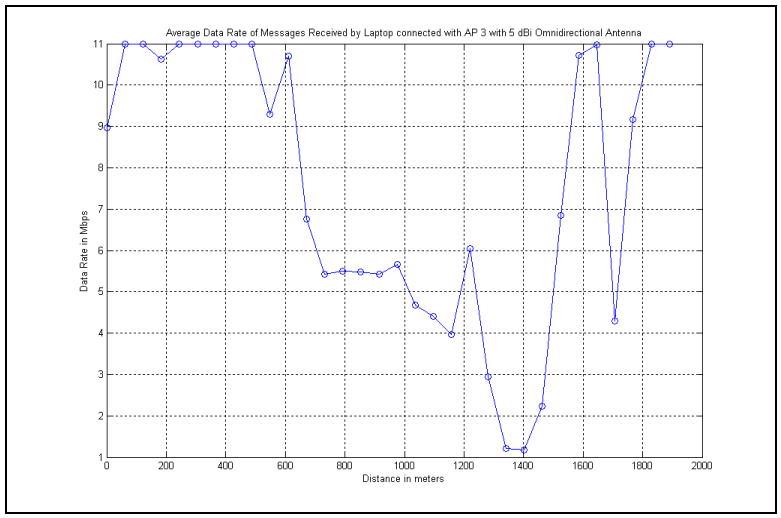

Figure 4. 3: Average Data Rate of End-User Wireless Link with 5-dBi *Laptop* Antenna

The percentage of data loss with 5-dBi omnidirectional antenna is shown in Figure 4.4. The plot identifies patches on the road where one may observe data loss. Average data loss is calculated by averaging the number of test messages which are lost over total number of test messages sent by the access point.

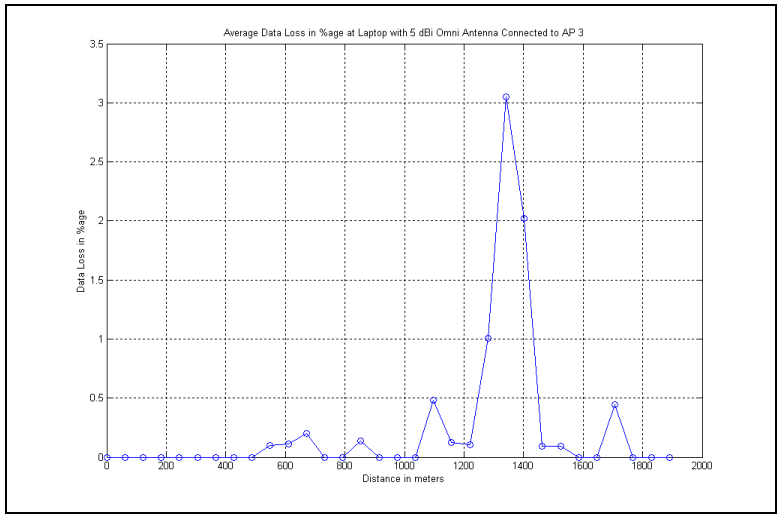

Figure 4. 4: End-User Wireless Link' Average Data Loss with 5-dBi *Laptop* Antenna

4.2.2 3-dBi Omnidirectional Antenna

This section elucidates throughput and coverage measurement results taken with a 3-dBi omnidirectional *Laptop* antenna. Figure 4.5 shows average SNR values measured at *Laptop* and AP-3 versus distance. These measurements are taken at the last section of the road starting from AP-3 location, similar to previous section. The SNR values are recorded at every 200 feet using *ORiNOCO Client Manager*.

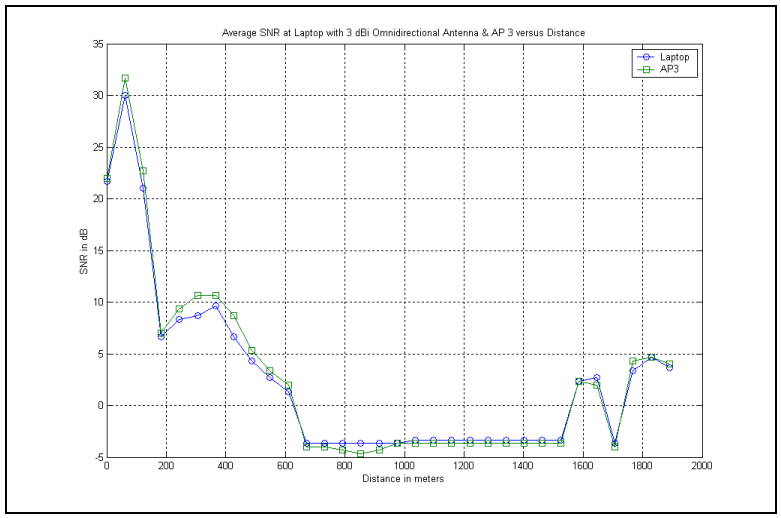

Figure 4. 5: Average SNR at AP-3 and *Laptop* with 3-dBi Antenna

Figure 4.5 exhibits the same SNR and coverage pattern as shown in Figure 4.1 with 5-dBi antenna. It accounts for the specific site details and characteristics like terrain, surrounding hills and variation in elevation. The received signal power and noise level also follows the same pattern as shown in Figure 4.2.

Figure 4.6 shows a plot of average data rate of end-user wireless link versus distance with 3-dBi *Laptop* antenna. It is to be noticed here that the data rate drops significantly in low SNR regions when compared with Figure 4.3.

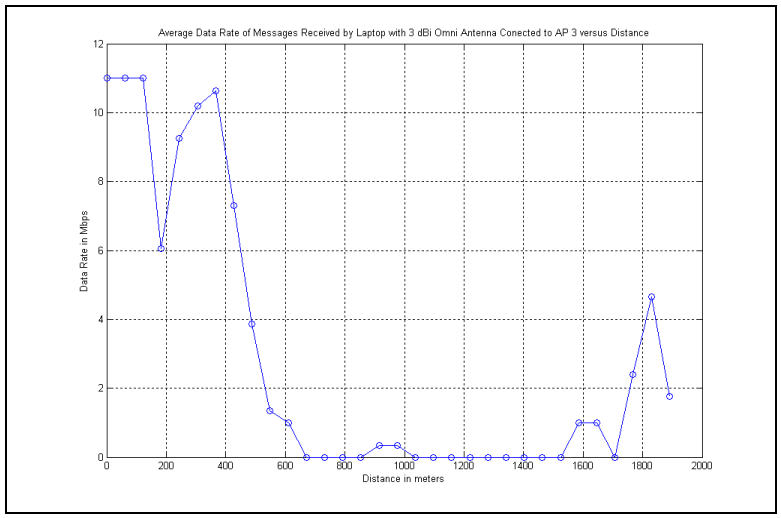

Figure 4. 6: End-user Wireless Link's Average Data Rate with 3-dBi *Laptop* Antenna

Below is a plot of average data loss versus distance with a 3-dBi *Laptop* antenna. Figure 4.7 shows more data loss in regions with low SNR when compared with Figure 4.4. It can be deduced from Figures 4.5 and 4.7 that SNR values of 8-dB and above guarantee absolutely no data loss. Also, it can be deduced from these two figures that below 0-dB SNR, almost no coverage can be expected down the road.

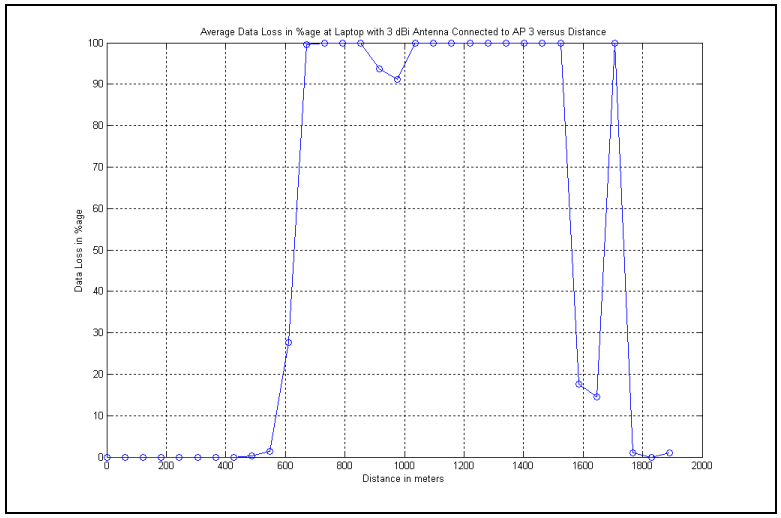

Figure 4. 7: End-User Wireless Link's Average Data Loss with 3-dBi *Laptop* Antenna

4.2.3 3-dBi versus 5-dBi

The above graphs show that we get poor coverage, and hence less available data rate, with 3-dBi antenna as compared to 5-dBi, verifying the basic radio propagation principles [Rap01]. Figure 4.8 compares the SNR at measuring *Laptop* with both antennas. The network exhibits similar coverage pattern down the road with both the antennas, but with different SNR values. It also verifies the basic radio propagation principles discussed in texts like [Rap01]. At some points along the road the difference between the two readings is more than 2 dBs. It is probably due to the manufacturing errors in omnidirectional antennas.

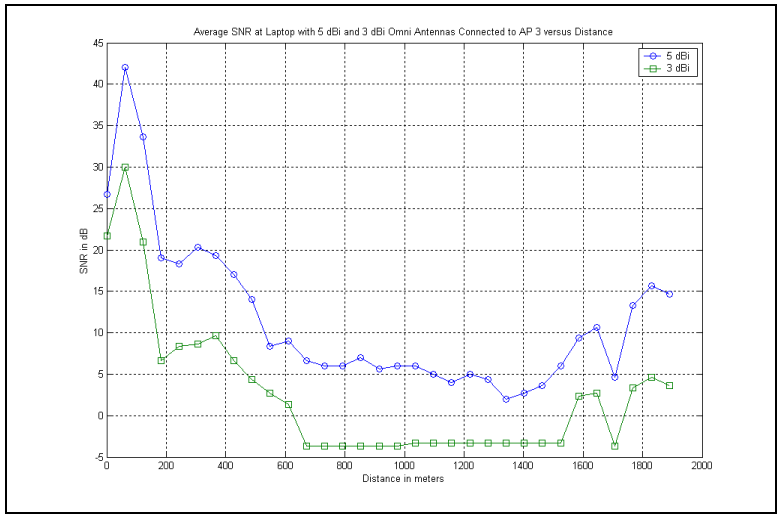

Figure 4. 8: Average SNR at *Laptop* with 5-dBi and 3-dBi Omni Antennas

Figure 4.9 compares available data rates for end-user wireless link with both the antennas. The two antennas follow the same pattern, but 3-dBi antenna is incapable of supporting high data rates when compared with 5-dBi.

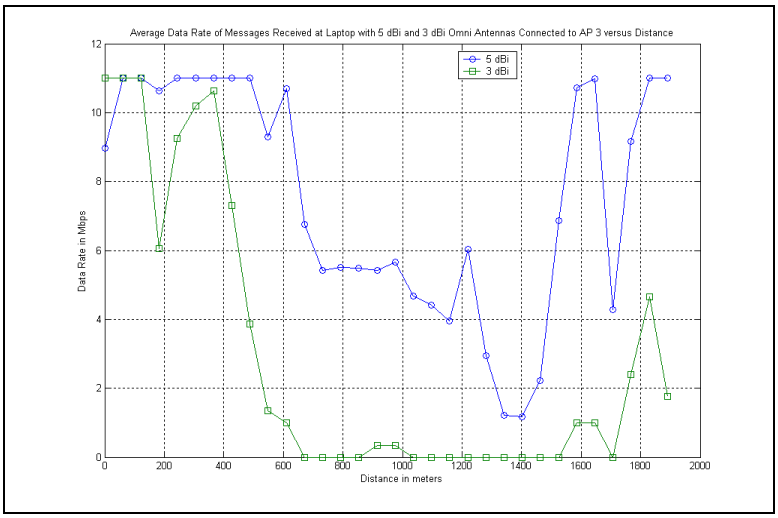

Figure 4. 9: End-User Wireless Link Data Rate with 5-dBi and 3-dBi Omni Antennas

The data loss with both antennas is compared in Figure 4.10. The 3-dBi antenna causes huge data loss in poor coverage regions along the road when compared with 5-dBi. It causes almost no coverage in certain regions, where 5-dBi antenna causes data loss up to 3%. Further investigations (not reported in this document) show that the data loss can be practically eliminated on this site by using *Laptop* antennas with gain 7-dBi or above.

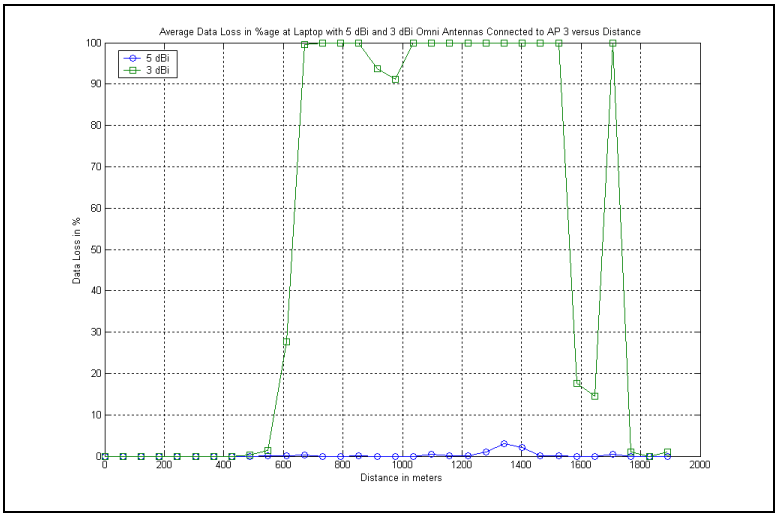

Figure 4. 10: Average Data Loss with 5-dBi and 3-dBi Omni Antennas

Discussion

Wireless coverage and supported data rate for end-user wireless link depends also on site details. The network is capable of supporting 11 Mbps data rate from wireless end-user to the access point if the SNR is at least 15 dB. Our observations show that the SNR values below 8 dB may cause data loss and hence less throughput. A 5-dBi omnidirectional antenna provides much better coverage and data rates as compared to 3-dBi omni, and is more appropriate for measuring network performance as it seldom loses network connection down the road.

4.3 Network Delays

This section presents and discusses network latency results recorded with the help of *NetIQ Chariot* and *ORiNOCO Client Manager*. *Chariot* helps us testing the network response time under different testing conditions and the *Client Manager* helps us recording the local wireless link SNR. 5-dBi omnidirectional antenna was used with the *Laptop 1* throughout these measurements.

The latency test is performed by *Chariot* from different locations on the road to the *Desktop* using *TCP/IP* and *UDP/IP* protocols. *Chariot* sends a data file of 100 bytes from *Laptop 1* to *Desktop* and requests for a reply of 100 bytes in response. This transfer is performed 50 times in order to calculate the accurate value for this test.

Some typical results are shown in this section, rest of them can be found in Section A.1 of Appendix A. All of these test results are summarized and discussed in the following section.

4.3.1 Using TCP

Response time test is performed from different locations on the road using *TCP* as transport layer protocol. The *TCP* Default Send Size for all of *TCP* tests is 32767 bytes. The test is run on network's uplink (wireless link from *Laptop 1* to *Desktop)* and downlink (wireless link from *Desktop* to *Laptop 1)* simultaneously (and in some cases separately) to get a fair idea about network delays in both the directions. Since the data size is only 100 bytes in each test, it is unlikely that the simultaneous testing saturate the network. Hence running a full-duplex test is safe and reliable from network performance measurement point of view.

While Connected to AP-2

The test is run while connected to AP-2 at a static location with reasonable SNR. Some of the test details are given below.

- *Laptop* SNR: 29 dB
- AP-2 SNR: 20 dB
- Frequency Channel #: 5
- Pair 1: Uplink
    - Average Response Time: 26 ms
    - Bytes Sent By *Laptop*: 245,000
    - Bytes Received By *Laptop*: 245,000
- Pair 2: Downlink
    - Average Response Time: 26 ms
    - Bytes Sent By *Desktop*: 250,000
    - Bytes Received By *Desktop*: 250,000
- Totals:
    - Average Response Time: 26 ms

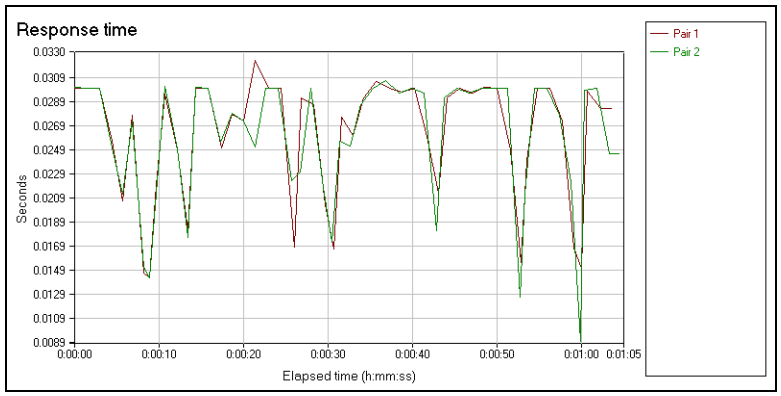

Figure 4. 11: Full-Duplex TCP Response Time @ AP-2

Discussion

Table 4.2 presents a summary of *TCP* response time tests. The variation of response time with number of total hops (including one from *Laptop* to the access point) is shown in Figure 4.12.

The figure 4.12 shows that the average response time increases almost linearly with increasing number of hops. Uplink and downlink response time is almost the same when *TCP* is used as the transport layer protocol. The temporal variations in Figure 4.11 and so on when measuring network's static performance are caused by random nature of wireless signals and sometimes by network congestion.

Table 4. 2: Average *TCP* Response Time Summary

***Laptop* Connected To**	***Laptop* SNR (dB)**	**AP SNR (dB)**	**Average Response Time (ms)**
AP-1	28	33	6
AP-2	29	20	26
AP-3	33	36	56
AP-4	22	24	89

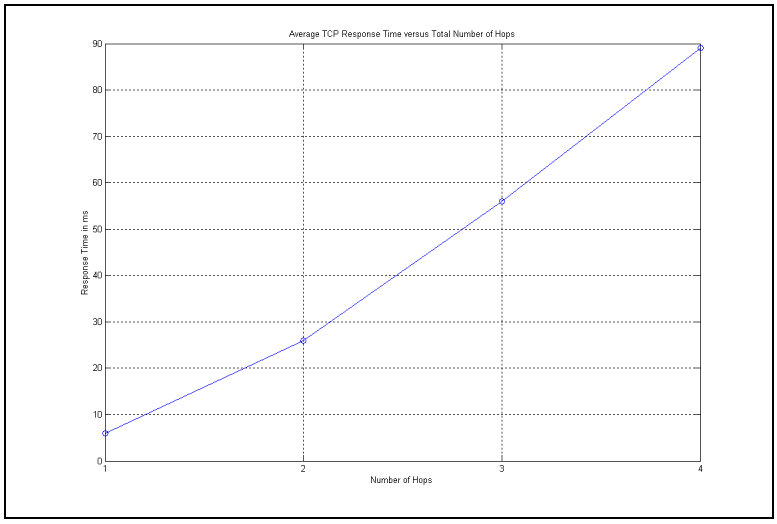

Figure 4. 12: Average TCP Response Time versus Number of Hops

4.3.2 Using UDP

The response time test as described earlier is repeated with *UDP* as transport layer protocol. The *UDP* Default Send Size is 8183 bytes for all the tests mentioned with *UDP* in this document.

While Connected to AP-2

The full-duplex *UDP* response time test is run on the network while connected to AP-2. Some of the test details and results are given below.

- *Laptop* SNR: 29 dB
- AP-2 SNR: 16 dB
- Frequency Channel #: 5
- Pair 1: Uplink
    - Average Response Time: 35 ms
    - Bytes Sent By *Laptop*: 180,000
    - Bytes Received By *Laptop*: 180,000
- Pair 2: Downlink
    - Average Response Time: 26 ms
    - Bytes Sent By *Desktop*: 250,000
    - Bytes Received By *Desktop*: 250,000
- Totals:
    - Average Response Time: 30 ms

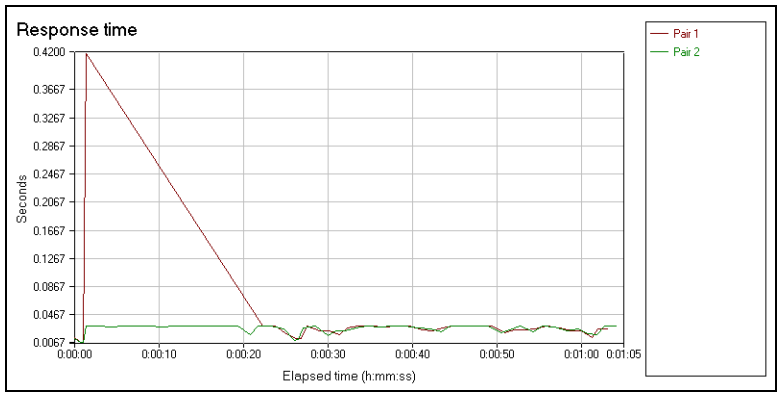

Figure 4. 13: Full-Duplex UDP Response Time @ AP-2

Discussion

Table 4.3 summarizes average *UDP* response times for different locations on the road. It is evident that uplink and downlink response times are different when *UDP* is used for the transport layer. The major reason for this asymmetry is the *UDP* protocol itself. *UDP* is a best-effort

connectionless transport layer protocol by design and cannot provide packet delivery guarantees [Pet00]. Other reasons include wireless networking (the *Laptop*'s IP address does not indicate its physical location) and the use of an asymmetric network (the experimental network is asymmetric, by design, as discussed in Chapter 3).

Table 4. 3: Average *UDP* Response Time Summary

Laptop **Connected To**	***Laptop*** **SNR (dB)**	**AP SNR (dB)**	**Uplink Response Time (ms)**	**Downlink Response Time (ms)**	**Total Average Response Time (ms)**
AP-1	30	33	3	16	10
AP-2	29	19	35	26	30
AP-3	32	36	56	60	58
AP-4	21	23	89	102	95

Figure 4.14 shows the variation of the total average *UDP* response time with increasing number of hops.

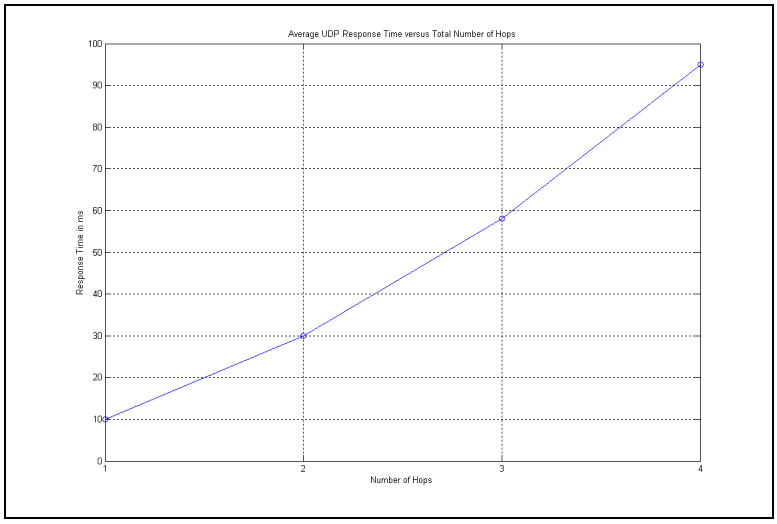

Figure 4. 14: Average UDP Response Time versus Number of Hops

4.3.3 Response Time – TCP versus UDP

Figure 4.15 compares *TCP* and *UDP* total average response time graphically. The figure indicates total average response time with both the protocols versus total number of hops. It is clear from Figure 4.15 that *UDP* response time is always a little higher than with *TCP*, because *UDP* is a best-effort connectionless protocol and can not address problems like network congestion and data loss. It is also obvious from Figure 4.15 that both *TCP* and *UDP* response time increase almost linearly with increasing number of hops.

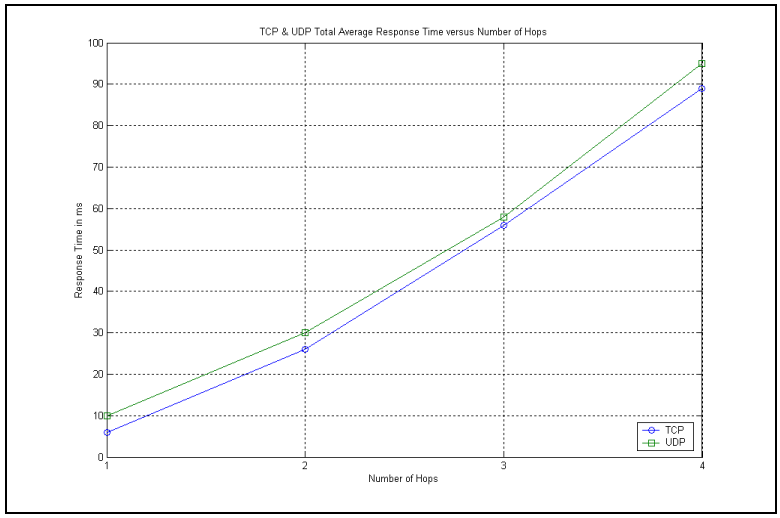

Figure 4. 15: TCP and UDP Total Average Response Time versus Number of Hops

4.4 Single-User Uplink Throughput

As discussed earlier, *Uplink* is defined as the wireless link from *Laptop* connected to the wireless access network along the road to the *Desktop.* Single-user uplink throughput is measured from *Laptop 1* to *Desktop*. *Chariot* is used for testing network performance and to measure throughput. *Client Manager* is used for recording SNR values. Some typical test results are shown in this section. All other results are presented in Section A.2 of Appendix A.

4.4.1 Throughput Test with TCP

Throughput test is run by *Chariot.* This test sends a data file of 100,000 bytes from source host to destination host and records the time it takes to be received by it. This practice is repeated 100

times and the results are averaged later on to get a reliable measure of network throughput. This test is performed with *TCP/IP* protocol stack while connected to different access points along the road with reasonable SNR.

While Connected to AP-1

The test results while connected to AP-1 are shown in Figure 4.16.

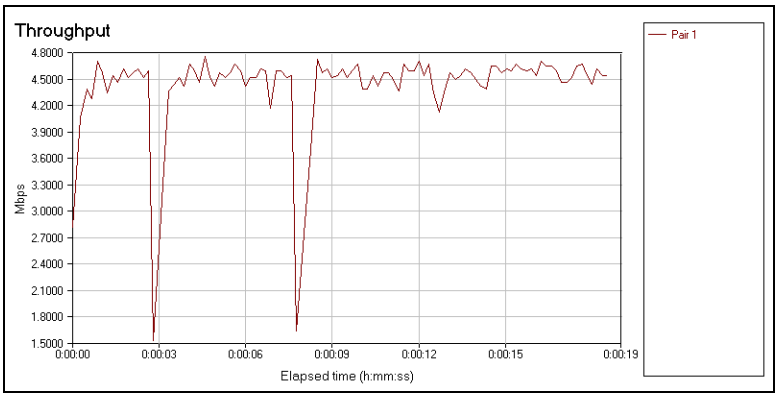

Figure 4. 16: Uplink *TCP* Static Throughput @ AP-1

The test details are given below.

- Average Uplink Throughput: 4.337 Mbps
- Average Response Time: 184 ms
- Average SNR at *Laptop*: 30 dB
- Average SNR at AP-1: 33 dB
- Total Bytes Sent by *Laptop*: 10,000,000
- Total Bytes Received by *Laptop*: 100
- Frequency Channel #: 11.

Discussion

The following is a summary of uplink *TCP* throughput tests.

Table 4. 4: Uplink *TCP* Throughput Test Summary

***Laptop* Connected To**	**AP SNR (dB)**	**Average Throughput (Mbps)**	**Response Time (ms)**
AP-1	33	4.337	184
AP-2	19	3.383	237
AP-3	36	2.233	358
AP-4	23	1.049	762

Figure 4.17 shows a graphical variation of uplink *TCP* throughput versus total number of hops. It shows that when *TCP/IP* protocol is used, the uplink average throughput degrades almost linearly with increasing number of total hops, which is a characteristic of the network under consideration. It is to be noted here that this throughput is measured from *Laptop* connected to an access point along the road, to the *Desktop* connected to the first backbone router ROR-1 via a wired connection, and the backbone is also built on point-to-point wireless link. Hence, the *Desktop* is connected to the first wired interface of the network. Thus, the data transfer does not encounter any wired connection but the one that is connected to the *Desktop.*

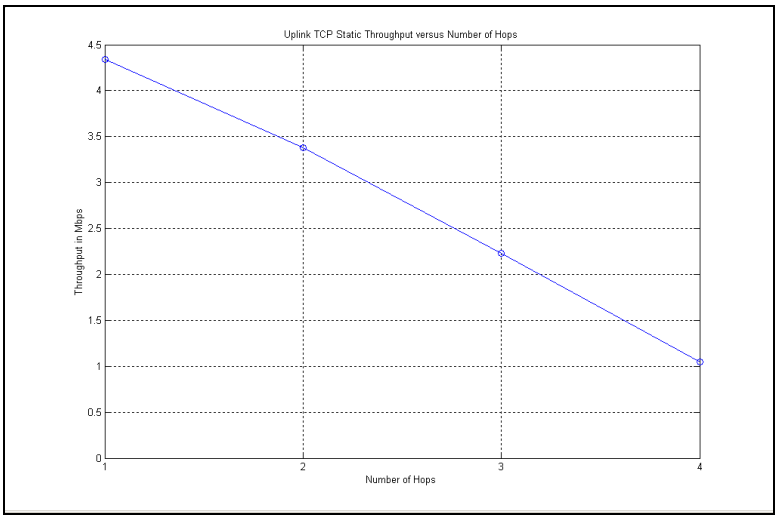

Figure 4. 17: Uplink *TCP* Average Throughput versus Number of Hops

4.4.2 10-Mbps Streaming Test with UDP

Chariot is used to perform 10-Mbps streaming test running on *UDP/IP* protocol stack. The *UDP* is best-effort connectionless protocol and can be used to estimate a network's *saturated throughput. Chariot* sends an *MPEG* video-streaming file at a rate of 10-Mbps from source host to destination host and repeats the practice 100 times in this test. The average results provide us an estimate of the network's saturated throughput, or in other words the maximum data rate that it can support with *UDP/IP* protocol stack.

While Connected to AP-1

The test results and some details are shown as follows.

- Average Uplink Throughput: 5.844 Mbps
- *Laptop*'s Send Data Rate: 9.772 Mbps
- Bytes Lost from *Laptop* to *Desktop*: 40.2%
- Max Consecutive Lost Datagrams: 8
- Average SNR at *Laptop*: 25 dB
- Average SNR at AP-1: 25 dB
- Total Bytes Sent by *Laptop*: 36,500,000
- Total Bytes Received by *Desktop*: 21,827,000
- Frequency Channel #: 11.

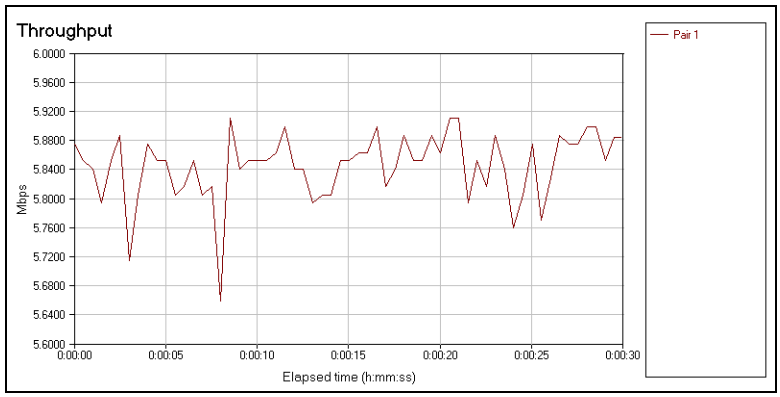

Figure 4. 18: Uplink *UDP* 10-Mbps Streaming Throughput @ AP-1

Discussion

Table 4.5 summarizes the uplink *UDP* 10-Mbps streaming test results.

Table 4. 5: Uplink *UDP* 10-Mbps Streaming Test Summary

***Laptop* Connected To**	**AP SNR (dB)**	**Average Throughput (Mbps)**	**Max Consecutive Lost Datagrams**
AP-1	25	5.844	8
AP-2	18	4.234	25
AP-3	36	3.237	63
AP-4	25	1.448	92

Figure 4.19 shows a graphical degradation the saturated throughput of the uplink with increasing number of hops with *UDP/IP* protocols. This figure gives us an idea of the maximum possible data rates at different locations on the road. The supportable throughput does not degrade as linearly as Figure 4.28.

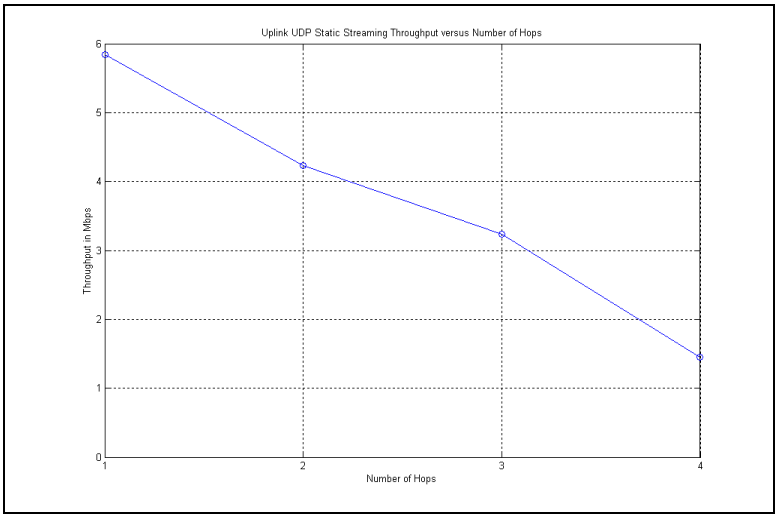

Figure 4. 19: Uplink UDP 10-Mbps Average Streaming Throughput versus Number of Hops

4.4.3 Uplink Throughput - TCP versus UDP

Figure 4.21 shows a comparison of *TCP* throughput and *UDP* saturated streaming throughput versus number of hops. Since *TCP* is a connection-oriented transport layer protocol with congestion control capabilities, it deals with the network data loss and latency issues better than *UDP*. It, however, requires handshaking all the time with the host destination to address network congestion and data loss issues more intelligently. *UDP*, on the other hand, is a best-effort, connectionless protocol that has no way of confirming a packet delivery or loss and, hence, is not treated as a reliable transport layer protocol [Pet00]. The *UDP* streaming throughput gives us an idea of network's saturation. *TCP* throughput, therefore, comes out to be less than that with *UDP*.

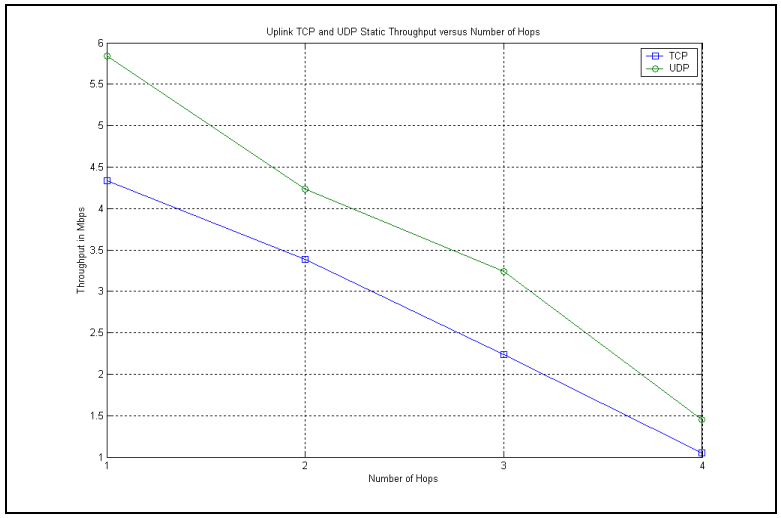

Figure 4. 20: Uplink Average *TCP* Throughput and *UDP* Streaming Throughput

4.5 Single-User Downlink Throughput

The network's *downlink* is defined as the wireless link from the *Desktop* connected to the first router ROR-1 to the *Laptop* connected to an access point along the road. *Laptop 1* is used to measure *downlink throughput* from the *Desktop* to itself. It is to be noted here that the network is asymmetric by design; hence different throughput results are expected at this time. Some typical results are shown in this section, rests of them are given in Section A.3 of Appendix A.

4.5.1 Throughput Test with TCP

The same *TCP* throughput test is performed on downlink with *Chariot,* as discussed in the Section 4.4.1. The test is run from different locations along the road connected to various access points with reasonable SNR.

While Connected to AP-1

The test results are shown in Figure 4.21.

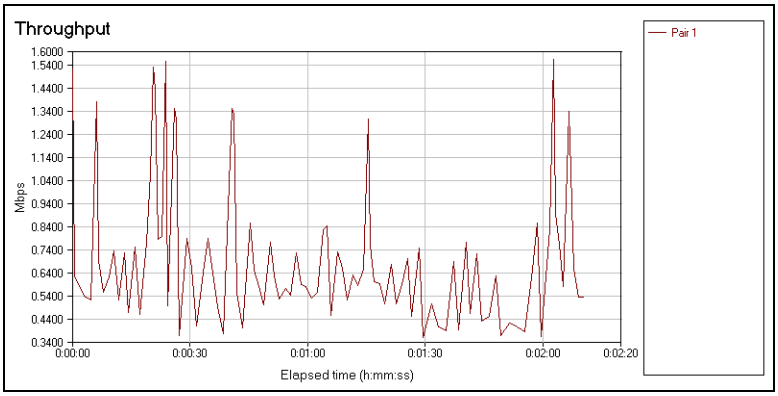

Figure 4. 21: Downlink *TCP* Throughput @ AP-1

Some of the test details are given below.

- Average Downlink Throughput: 0.613 Mbps
- Average Response Time: 1.306 seconds
- Average SNR at *Laptop*: 31 dB
- Average SNR at AP-1: 33 dB
- Total Bytes Sent by *Desktop*: 10,000,000
- Total Bytes Received by *Desktop*: 100
- Frequency Channel #: 11.

Discussion

Table 4.6 presents a summary of *TCP* throughput tests performed on the network's downlink.

Table 4. 6: Downlink *TCP* Throughput Test Summary

***Laptop* Connected To**	***Laptop* SNR (dB)**	**Average Throughput (Mbps)**	**Response Time (seconds)**
AP-1	31	0.613	1.306
AP-2	30	0.495	1.617
AP-4	20	0.245	3.265

Figure 4.22 shows degradation of downlink *TCP* throughput with increasing number of hops graphically. The downlink throughput degrades linearly with increasing number of hops as studied in uplink case but with a different rate because the network is designed asymmetrically. The test results at AP-3 are not presented in this section because they follow the same pattern as shown here.

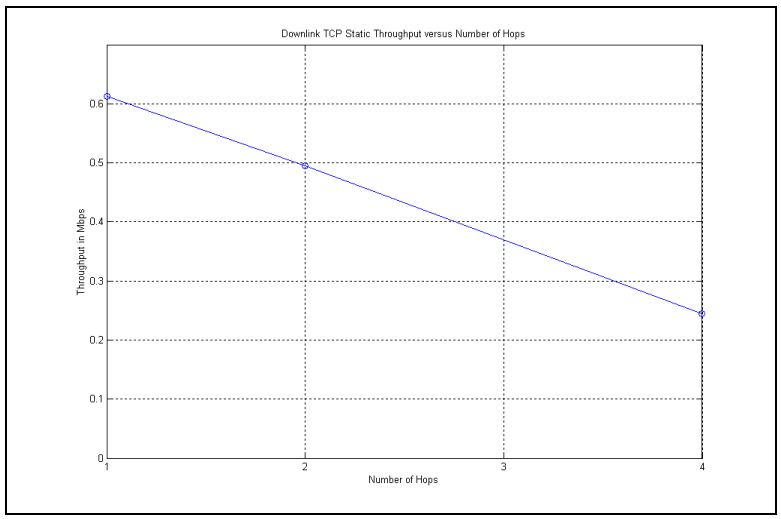

Figure 4. 22: Downlink TCP Average Throughput versus Number of Hops

4.5.2 10-Mbps Streaming Test with UDP

The same 10-Mbps MPEG streaming test is run on downlink as discussed in the Section 4.4.2. The *UDP* streaming test helps us in estimating the maximum data rate limit for the network.

While Connected to AP-1

Some of the test details and the results are given as follows.

- Average Downlink Throughput: 1.650 Mbps
- *Desktop* Send Data Rate: 8.474 Mbps
- Bytes Lost from *Desktop* to *Laptop*: 80.531%
- Max Consecutive Lost Datagrams: 16
- Average SNR at *Laptop*: 24 dB
- Average SNR at AP-1: 24 dB
- Total Bytes Sent by *Desktop*: 36,491,240
- Total Bytes Received by *Laptop*: 7,104,360
- Frequency Channel #: 11.

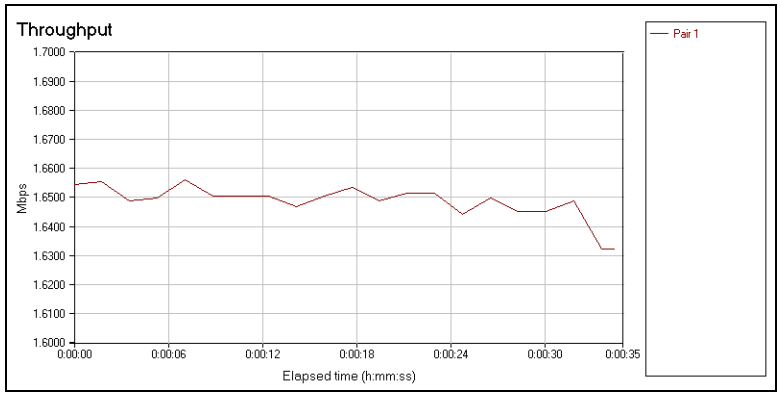

Figure 4. 23: Downlink UDP 10-Mbps Streaming Throughput @ AP-1

Discussion

Table 4.7 presents a summary of *UDP* 10-Mbps streaming tests performed on downlink. The saturated throughput of the downlink is less than that with the uplink due to asymmetric design of the network as expected. The throughput is almost constant over different number of hops (except at AP-1) because the *Desktop* has a wired connection to ROR-1 and the *Laptop* has a fairly good SNR. The streaming throughput within the first *Basic Service Area (BSA)* (region along the road covered by AP-1) is far less than that in other areas. This discrepancy can be explained from the fact that the first backbone router ROR-1 and the first access point AP-1 share the same router

hardware *ROR-1000.* It is due to this resource sharing that we get less than half streaming throughput in first *BSA* as compared to other regions along the road.

Table 4. 7: Downlink *UDP* 10 Mbps Streaming Test Summary

***Laptop* Connected To**	***Laptop* SNR (dB)**	**Average Throughput (Mbps)**	**Max Consecutive Lost Datagrams**
AP-1	24	1.650	11
AP-2	29	3.855	12
AP-3	32	3.900	7
AP-4	23	3.755	13

Figure 4.43 presents a graphical representation of the average saturated throughput of the downlink versus increasing number of hops.

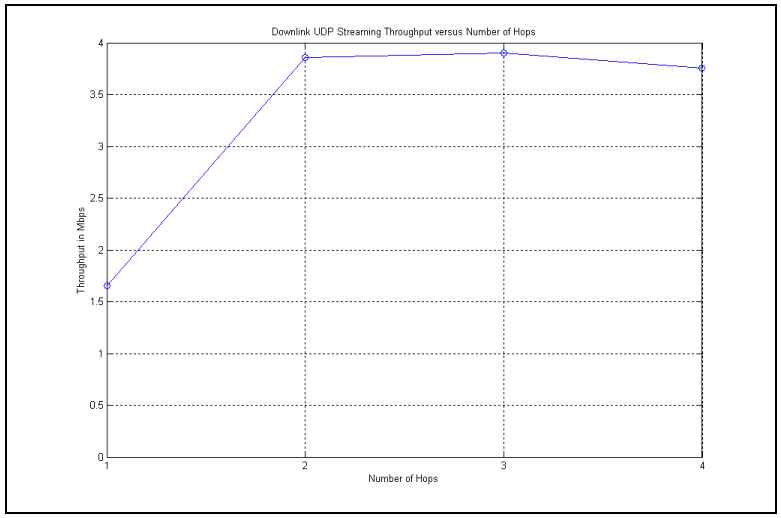

Figure 4. 24: Downlink UDP 10-Mbps Average Streaming Throughput versus No. of Hops

4.5.3 TCP versus UDP

Figure 4.25 shows a comparison of the average *TCP* throughput of the downlink and *UDP* saturated throughput. The *UDP* throughput is always higher than the *TCP* throughput for the reasons discussed earlier.

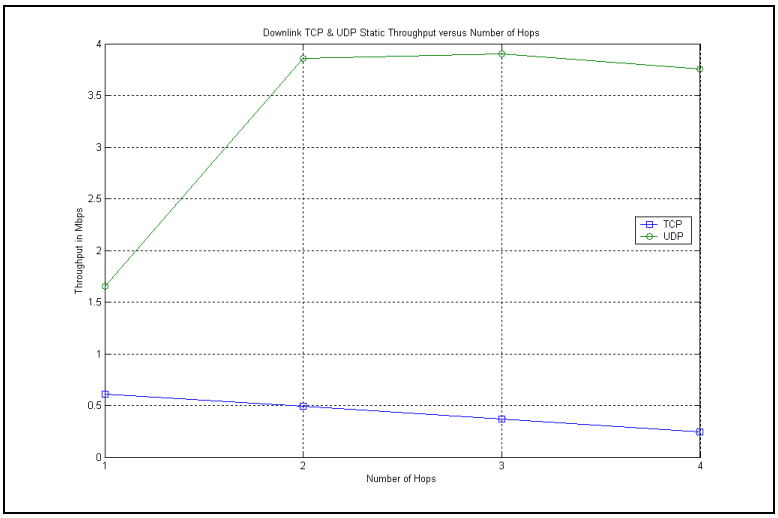

Figure 4. 25: Downlink Average *TCP* Throughput and *UDP* Streaming Throughput

4.6 Uplink versus Downlink

This section compares uplink and downlink performance. Due to inherent network asymmetry, different throughputs are expected, as discussed.

4.6.1 TCP Average Throughput

Figure 4.26 compares the uplink and downlink average *TCP* throughput. It is evident from the graph that average *TCP* throughput degrades almost linearly with increasing number of hops. The graph also shows that the downlink average throughput is far less than the uplink due to the asymmetric network design. Also, the rates at which the two throughputs degrade are different due to the same reason.

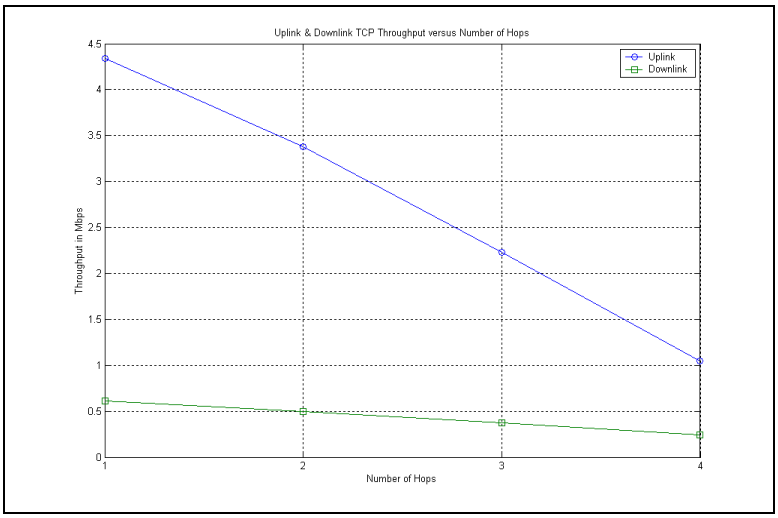

Figure 4. 26: Uplink and Downlink Average *TCP* Throughput versus Number of Hops

4.6.2 UDP 10-Mbps Streaming Throughput

In order to drive the network to saturation level, the *UDP* streaming tests use 10 Mbps send data rate (for an *802.11b* compliant network, the theoretical upper limit for supportable data rate is 11 Mbps). *UDP* is used for delay-sensitive and multimedia-streaming applications around the world as discussed in Chapter 2.

Figure 4.27 compares the saturated throughputs for uplink and downlink cases. As shown earlier, uplink throughput degrades with increasing number of hops, whereas downlink throughput almost remains the same except at AP-1. It is due to the reason that the *Desktop* is connected via a wired connection and the *Laptop* is mobile (or at least portable in these measurements) and connected to the wireless network. The streaming test just continues to send data irrespective of whether it has been actually received by the destination or not. For the case of the uplink, the network needs to transport data from *Laptop* to fixed *Desktop* via wireless backbone, and as the hops increase data loss on the network increases and hence the throughput decreases. In contrast, in the downlink, *Desktop* sends streaming data via a wired connection, which, however, does not need to travel through wireless links. Hence, downlink throughput remains practically constant.

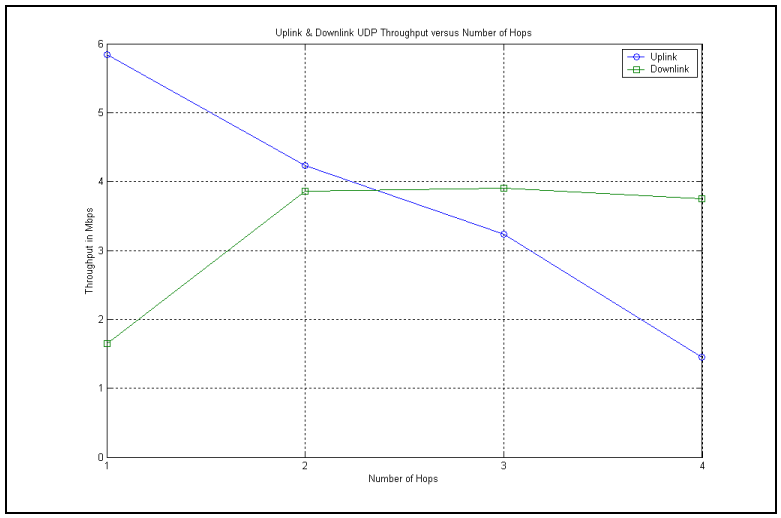

Figure 4. 27: Uplink and Downlink *UDP* Average Streaming Throughput versus No. of Hops

4.7 Two-User Throughput

Laptop 1 and *Laptop 2* are used in these tests behaving as two different users. *Laptop 1* is equipped with 5-dBi omnidirectional antenna, and *Laptop 2* is equipped with 3-dBi omnidirectional antenna as described in Chapter 3.

4.7.1 Mutual Performance Tests at AP-1

In these tests both the laptops are connected to AP-1 with reasonable SNR. Since the network is configured in *Infrastructure mode* of *802.11b* topologies, the laptops communicate with each other via AP-1 only using the wireless network as medium for data transfer. This section measures and analyses the performance of the mutual wireless.

TCP Response Time

This test measures response time from *Laptop 1* to *Laptop 2* using the same response time test performed by *Chariot as* discussed earlier. The test details and the corresponding results are shown below.

- Average SNR at *Laptop 1*: 30 dB
- Average SNR at *Laptop 2*: 28 dB
- Average SNR at AP-1: 29 dB

- Frequency Channel #: 11
- Average Response Time: 6 ms
- Bytes Sent By *Laptop 1*: 250,000
- Bytes Received By *Laptop 1*: 250,000

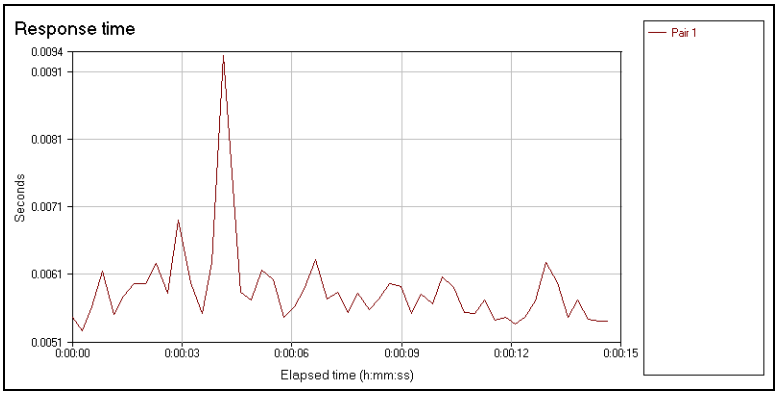

Figure 4. 28: Two-User Mutual *TCP* Response Time @ AP-1

UDP Response Time

The test details and the results are given below.

- Average SNR at *Laptop 1*: 30 dB
- Average SNR at *Laptop 2*: 30 dB
- Average SNR at AP-1: 31 dB
- Frequency Channel #: 11
- Average Response Time: 6 ms
- Bytes Sent By *Laptop 1*: 250,000
- Bytes Received By *Laptop 1*: 250,000

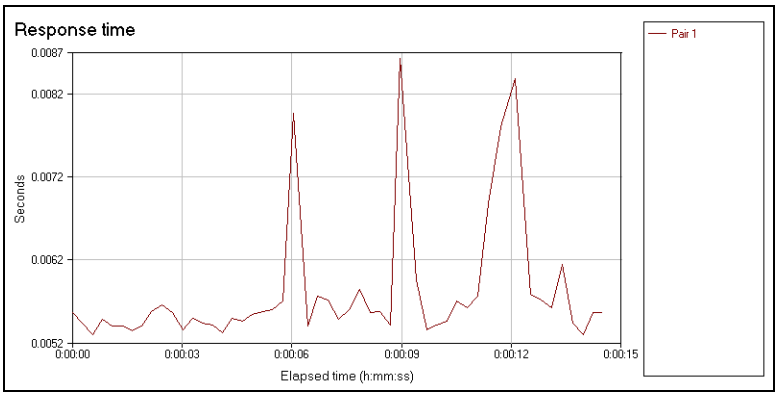

Figure 4. 29: Two-User Mutual *UDP* Response Time @ AP-1

Discussion

From the above two tests, it is clear that the average mutual response time is the same (6 ms) both for *TCP* and *UDP*, as both the laptops are connected to AP-1 with reasonable SNR.

TCP Mutual Throughput

The following test measures TCP mutual throughput from *Laptop 1* to *Laptop 2* when both are connected to AP-1. The same throughput test is run from *Laptop1* to *Laptop 2* using *Chariot* as described earlier. The test details and the results are given below.

- Average SNR at *Laptop 1*: 29 dB
- Average SNR at *Laptop 2*: 17 dB
- Average SNR at AP-1: 24 dB
- Frequency Channel #: 11
- Average Throughput: 0.814 Mbps
- Average Response Time: 0.983 seconds
- Bytes Sent By *Laptop 1*: 10,000,000
- Bytes Received By *Laptop 1*: 100

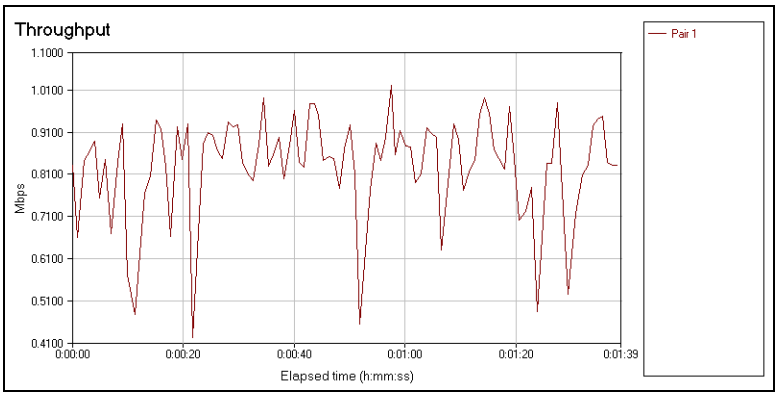

Figure 4. 30: Two-User Mutual *TCP* Throughput @ AP-1

10-Mbps UDP Streaming Test

In order to measure maximum supportable *UDP* data rate by the mutual wireless link between the two laptops, 10-Mbps *UDP MPEG* video streaming test is performed from *Laptop 2* to *Laptop 1*. The test details and the corresponding results are given below.

- Average SNR at *Laptop 1*: 29 dB
- Average SNR at *Laptop 2*: 16 dB
- Average SNR at AP-1: 24 dB
- Average Streaming Throughput: 0.655 Mbps
- *Laptop 2* Send Data Rate: 9.231 Mbps
- Total Bytes Sent by *Laptop 2*: 36,491,240
- Total Bytes Received by *Laptop 1*: 2,590,040
- Bytes Lost from *Laptop 2* to *Laptop 1*: 92.902%
- Max Consecutive Lost Datagrams: 113
- Frequency Channel #: 11.

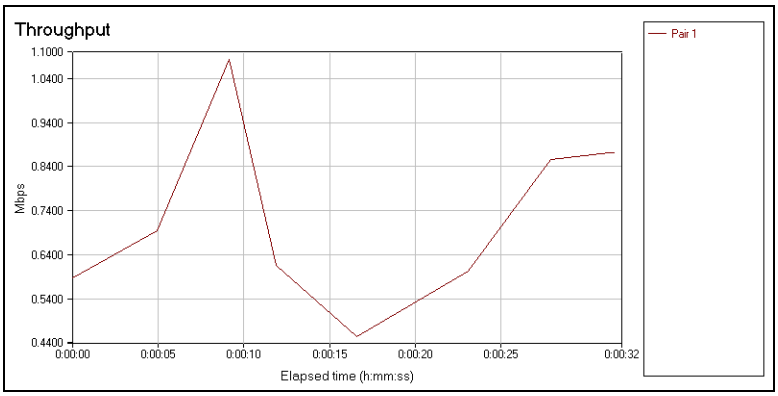

Figure 4. 31: Two-User Mutual 10-Mbps *UDP* Streaming Throughput @ AP-1

Discussion

The mutual throughput between the two laptops is given below.

- Average *TCP* Throughput from *Laptop 1* to *Laptop 2:* 0.814 Mbps
- Average *UDP* Streaming Throughput from *Laptop 2* to *Laptop 1*: 0.655 Mbps

The difference between the two throughputs is due to the use of different protocols in two different directions. It is, however, obvious that the network does not support very optimistic data rate between two static users. We assume that using the same hardware for backbone routing and access network at first node resulted in low values of mutual throughputs.

4.7.2 TCP Throughput Tests at AP-4

The network throughput is measured with *TCP/IP* protocols to and from two simultaneous users connected at AP-4. Both the laptops access the wireless network via the last access point AP-4 down the road.

Uplink Throughput

In an effort to measure network performance with two simultaneous users connected at the same access point, we run *Chariot* throughput test with *TCP* on the network. In this test two simultaneous throughput tests from *Laptop 1* and *Laptop 2* to the *Desktop* are run. The test details and the corresponding results are as follows.

- Average SNR at *Laptop 1*: 22 dB
- Average SNR at *Laptop 2*: 16 dB
- Average SNR at AP-4: 18 dB
- Frequency Channel #: 1
- Bytes Sent By *Laptop 1*: 10,000,000
- Bytes Received By *Laptop 1*: 100
- Bytes Sent By *Laptop 2*: 8,000,000
- Bytes Received By *Laptop 2*: 80
- Uplink *1* Average Throughput: 0.836 Mbps
- Uplink *2* Average Throughput: 0.671 Mbps
- Total Average Throughput: 1.501 Mbps

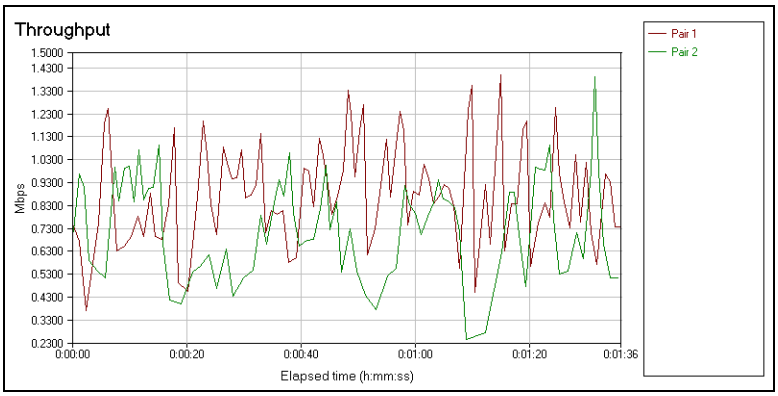

Figure 4. 32: Two-User Uplink Simultaneous *TCP* Throughput @ AP-4

Downlink Throughput

The *TCP* throughput test, as discussed earlier, is run from the *Desktop* to *Laptop 1* and *Laptop 2* simultaneously. The test results and some details are given below.

- Average SNR at *Laptop 1*: 22 dB
- Average SNR at *Laptop 2*: 16 dB
- Average SNR at AP-4: 18 dB
- Frequency Channel #: 1
- Bytes Sent By *Desktop* to *Laptop 1*: 3,900,000
- Bytes Received By *Desktop* from *Laptop 1*: 39

- Bytes Sent By *Desktop* to *Laptop 2*: 2,600,000
- Bytes Received By *Desktop* from *Laptop 2*: 26
- Downlink 1 Average Throughput: 0.168 Mbps
- Downlink 2 Average Throughput: 0.112 Mbps
- Total Average Throughput: 0.275 Mbps

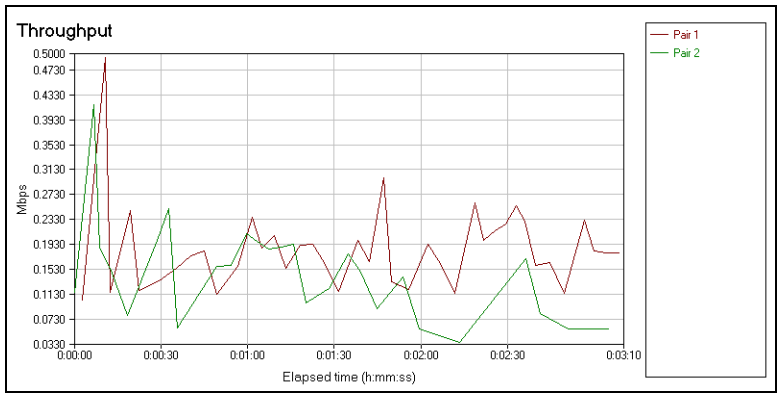

Figure 4. 33: Two-User Downlink Simultaneous *TCP* Throughput @ AP-4

Discussion

Single-user and two-users *TCP* throughputs at AP-4 are as follows.

- Single-User Uplink Average Throughput: 1.049 Mbps.
- Two-Users' Uplink Total Average Throughput: 1.501 Mbps.
    - *Laptop 1's* Uplink Throughput: 0.836 Mbps.
    - *Laptop 2's* Uplink Throughput: 0.671 Mbps.
- Single-User Downlink Average Throughput: 0.245 Mbps.
- Two-Users' Downlink Total Average Throughput: 0.275 Mbps.
    - *Laptop 1's* Downlink Throughput: 0.168 Mbps.
    - *Laptop 2's* Downlink Throughput: 0.112 Mbps.

The results clearly show that the two laptops share the network bandwidth fairly equally in proportion to their signal-to-noise ratios (consider 22 dB at *Laptop 1* as compared to 16 dB at *Laptop 2*) and the total average throughput for two-users case is a little more than single-user

case. This behavior is typical of direct-sequence spread spectrum systems such as *802.11b* networks (for further details, see [Rap01]).

4.8 Summary

In this chapter, *Smart Road's* experimental wireless network's static performance is discussed. It clarifies that wireless coverage and end-user data rate depends on site details in addition to location of the antenna and the type used. An SNR value of 15 dB or more may guarantee 11 Mbps data rate between end-user and an access point down the road. An SNR of 8 dB or less may cause data loss along the road. Better results can be obtained by using 5-dBi omnidirectional antenna than 3-dBi, and hence 5-dBi antenna should be used for laptop for performance measurement. The uplink and downlink exhibit different throughputs due asymmetric design of the network. The average response time of the *TCP* is practically same in both directions and increases almost linearly with increasing number of hops. On the other hand, the average response time of the *UDP* is a little different for the two directions and increases with increasing number of hops. The total average response time of the *UDP* is a little more than that of *TCP*. The single-user average *TCP* throughputs in both the directions degrade almost linearly with increasing number of hops but with different rates. The *UDP* streaming throughput is used to measure the saturated throughput of the network, which is almost always more than *TCP* throughput, and found to be different for different data transfer directions. Two simultaneous users may transfer mutual data using wireless network at a lower rate than accessing network's *Desktop*. Two simultaneous users share the network bandwidth fairly in accordance with their signal-to-noise ratios. The total throughput of two-users is a little more than a single-user throughput at the same location.

Chapter 5: Network Performance Results & Analysis - Mobile

This chapter presents and analyzes network performance results while moving at a constant speed along the road. The *NetIQ Chariot* and *ORiNOCO Client Manager* are used for performance measurement purposes.

5.1 Wireless Link Measurements

The *Client Manager* is used to measure signal-to-noise ratio (SNR) for both the moving station (*Laptop*s in this case) and access point. Wireless link's SNR is measured and recorded with each performance test described later in this chapter. In order to avoid repetition, these measurements are reported in this section, once for each speed. In addition to SNR values, corresponding access point numbers, and frequency channel are also reported with SNR results.

5.1.1 Wireless Link at 40 mph

The network performance tests have been performed at three different, but constant speeds of 20, 40 and 60 mph moving on the eastbound lane of the *Smart Road*. All the wireless link tests follow the same SNR pattern. The SNR measurements at 40 mph along with corresponding access point number, and frequency channel during the course is reported in this section. SNR measurements at 20 and 60 mph are given in the Section B.1 of Appendix B.

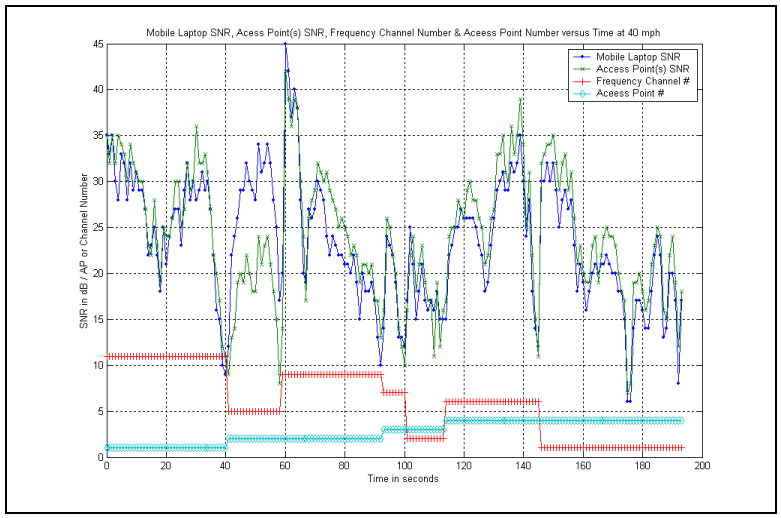

Figure 5. 1: End-User Wireless Link SNR, Access Point and Frequency Channnel @ 40 mph

Discussion

Figures 5.1, B.1, and B.2 show the SNR variation pattern along the road while moving at some constant speed. They all exhibit similar behavior, which can be understood from Figure 5.1. The network performance tests are conducted with 3-dBi and 5-dBi omnidirectional antennas used for *Laptop*. The details of access point, and backbone antennas are described in Chapter 3. From the above-mentioned figures, network hand-off points can be easily identified. Each access point (except AP-1) has two different *PC Cards,* and hence can have two different frequency channels as verified by these figures. There is a very short time span in which an end-user connects to the Channel # 7 (AP-3) (see Figure 5.1) while moving along the road, and even sometimes it does not need to connect to that channel as shown in Figures B.1 and B.2. AP-3 is installed to cover the curvature of the road as shown in Chapter 3 and Channel # 7 spans over very small, but curved region of the road. It is due to this reason that sometimes a mobile user does not need to access it in order to retain its connectivity to the rest of the network.

5.2 Network Delays

This section reports network's response time measurements. The *Chariot* is used to run these tests on network's uplink and downlink. This section also discusses measurement results at a speed of 40 mph. *Laptop 1* is used in all of these measurements unless otherwise stated.

5.2.1 Using TCP at 40 mph

The *Chariot* is used to send data files of size 100 bytes from source host to the destination host and requests for a reply of size 100 bytes while moving on the road. The test is run from the start of the road until the road end. The definitions of *uplink* and *downlink* remain the same as defined in Chapter 4. The following are the full-duplex TCP response time results and some details while moving at 40 mph along the road.

- Pair 1: Uplink
  - Average Response Time: 19 ms
  - Bytes Sent By *Desktop*: 990,000
  - Bytes Received By *Desktop*: 990,000
- Pair 2: Downlink
  - Average Response Time: 19 ms
  - Bytes Sent By *Laptop*: 1,005,000
  - Bytes Received By *Laptop*: 1,005,000
- Totals:
  - Average Response Time: 19 ms

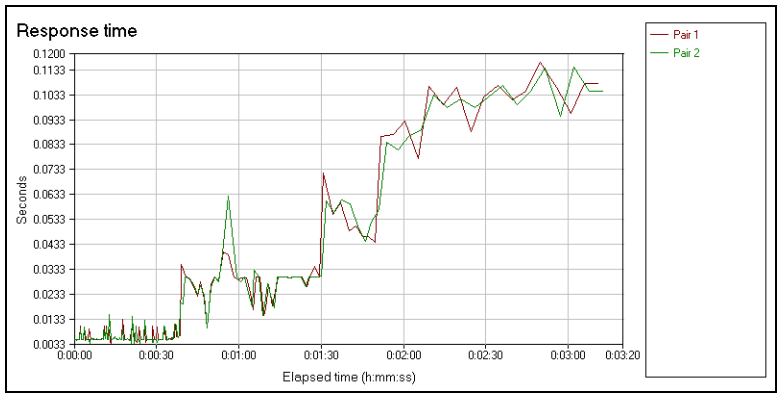

Figure 5. 2: Full-Duplex TCP Response Time @ 20 mph

Figure 5.2 shows the pattern of network's response time change at different locations on the road when moving at 40 mph. The uplink and downlink show nearly the same average response time, as also noticed in Chapter 4. As we move on the road, the response time increases gradually (on average) due to increasing number of hops. However, it is to be noticed here that it remains almost constant when the *Laptop* is connected to a particular access point. Hence, the change in response time is a

function of number of hops, not of distance from the entrance. Small variation is observed in response time due to mobility and location of vehicle at a particular instant. Different locations along the road have different signal strength due to small-scale fading as discussed in [Rap01]. Figure 5.2 also shows the hand-off points at which response time shoots to next possible value. Average value presented above does not give us an insight into network performance because this average is based on complete data set, and in our case, number of hops increases as we move ahead.

5.2.2 Using UDP at 40 mph

Response time test is conducted on the network in both the directions simultaneously using *UDP/IP* protocols and moving at 40 mph in eastbound lane of the road. The test results and some details are given below.

- Pair 1: Uplink
  - Average Response Time: 75 ms
  - Bytes Sent By *Desktop*: 260,000
  - Bytes Received By *Desktop*: 260,000
- Pair 2: Downlink
  - Average Response Time: 75 ms
  - Bytes Sent By *Laptop*: 260,000
  - Bytes Received By *Laptop*: 260,000
- Totals:
  - Average Response Time: 75 ms

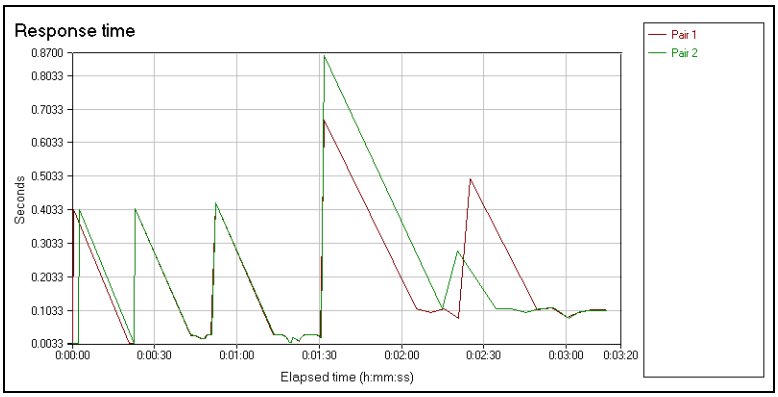

Figure 5. 3: Full-Duplex UDP Response Time @ 40 mph

Similar to *TCP*, the response time increases with increasing number of hops. Although the average values for both the uplink and downlink are the same, these averages are taken over all the measured values along the road, and do not take into account the fact that number of hops changes as we move forward.

5.2.3 TCP versus UDP

Both TCP and UDP exhibit same kind of behavior as discussed in Chapter 4. The response time values increase with increasing number of hops, and UDP offers a little worse (more) response time characteristics than TCP. The average values presented above do not give us a reliable insight into network performance because these values are taken over complete data set, and do not consider the fact that number of hops change during the test. The transitional values at hand-off points in Figure 5.3 force the average value to be much higher than that with Figure 5.2. However, in reality, the stable regions in both the figures exhibit comparable values of response time. *UDP* connection, however, encounters more problems due to use of best-effort connectionless transport layer protocol. Due to this reason, UDP response time is a little more than that with TCP.

5.3 Single-User Uplink Throughput

Throughput tests are conducted by *Chariot* at various constant speeds moving in the eastbound lane of the road. *Laptop 1* is used in these measurements unless otherwise stated. Various throughput tests are conducted at constant speeds of 20, 40, and 60 mph. Some of these tests are reported in this section. Rests of them are given in the Section B.2 of Appendix B.

5.3.1 TCP Throughput Test

The same throughput test is conducted on the network while moving at different speeds as discussed in Chapter 4. This test transfers a data file of size 100,000 bytes from source host to destination host and is run from the road entrance to the end.

At 20 mph

The test results and some of the details are given below.

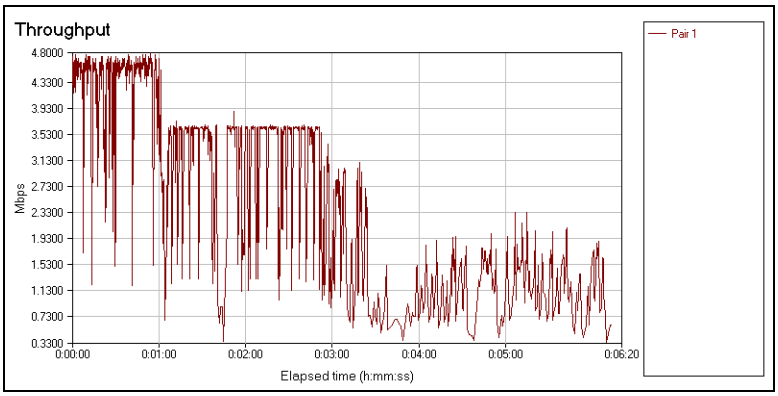

Figure 5. 4: Uplink TCP Throughput @ 20 mph

- Average Uplink Throughput: 2.173 Mbps
- Average Response Time: 368 ms
- Total Bytes Sent by *Laptop*: 101,300,000
- Total Bytes Received by *Laptop*: 1,013

Figure 5.6 shows uplink throughput at different instances, while moving at 20 mph along the road. The network experiences different throughputs at different locations on the road. The throughput decreases as the number of hops increases. However, it remains the same (on average) when the end-user is connected to a particular access point. From the data set, average values are calculated for throughput at a particular access point. These averages do not include the throughput values at hand-off points.

- Average Throughput When Connected to AP-1: 4.4023 Mbps
- Average Throughput When Connected to AP-2: 3.3645 Mbps
- Average Throughput When Connected to AP-3: 2.1893 Mbps
- Average Throughput When Connected to AP-4: 1.1986 Mbps

Discussion

The uplink throughput degrades as the number of hops increases during our tests. The average throughput values reported by *Chariot* do not serve as a reliable network performance measure. Therefore, the average values have been calculated from measured throughput values for each access point.

Static versus Mobile

Table 5.1 summarizes the average throughput values at each access point for static and mobile measurements discussed in this thesis.

Table 5. 1: Static & Mobile Average Uplink TCP Throughput Summary

***Laptop* Connected To**	**Static Throughput (Mbps)**	**20 mph Throughput (Mbps)**	**40 mph Throughput (Mbps)**	**60 mph Throughput (Mbps)**
AP-1	4.337	4.4023	4.1322	4.2823
AP-2	3.383	3.3654	3.1561	3.1568
AP-3	2.233	2.1893	2.1543	2.0258
AP-4	1.049	1.1986	1.1940	0.9824

Figure 5.5 plots these values versus number of hops.

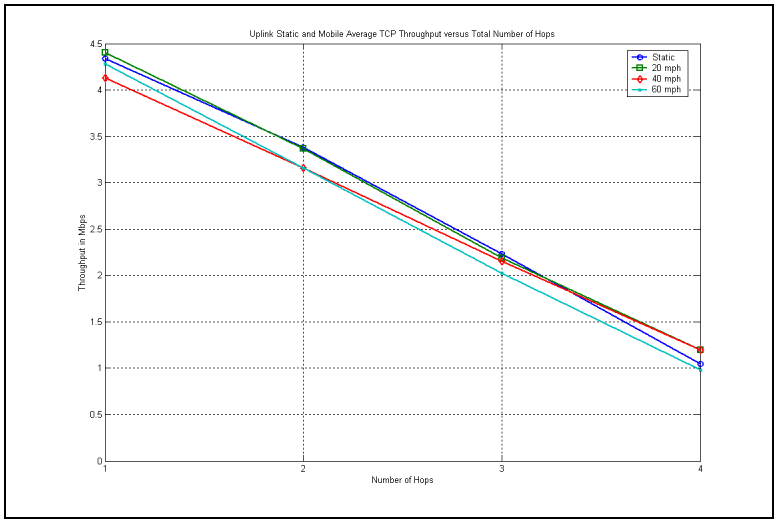

Figure 5. 5: Uplink Static & Mobile Average TCP Throughput versus Number of Hops

The above figure shows that the average uplink TCP throughput decreases almost linearly with increasing number of hops, which is a characteristic of this network. There is a very slight degradation of throughput with mobility as shown in Figure 5.6. Hence, the dominating factor affecting the network's throughput is number of hops and network can still provide reasonable bandwidth while a user is in motion.

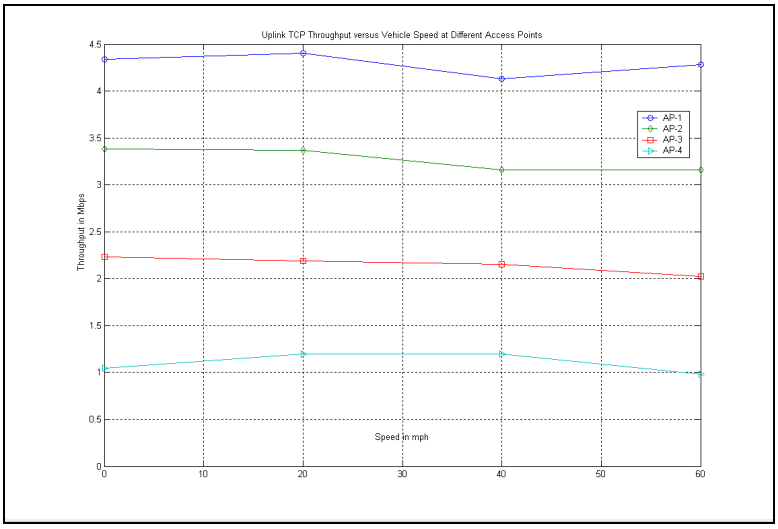

Figure 5. 6: Average Uplink TCP Throughput versus Vehicle Speed

Hence, if TCP connection retains, *802.11b* networks can be used to provide high-mobility data networking. It is worth mentioning here that during these tests, sometimes TCP loses its connection due to intolerable packet loss, poor coverage or excessive network delays. This problem needs to be addressed in future researches.

5.3.2 UDP 10-Mbps Streaming Test

The 10-Mbps *UDP MPEG* video-streaming test is run by *Chariot* as discussed in Chapter 4. The test starts from the road entrance and stopped at the road end (note that the road length is 2.2 miles), and sends continuous streaming data at a rate of 10 Mbps from *Laptop* to *Desktop.* The test is run at 20, 40, and 60 mph, but due to TCP connection time-out error, the test stops in middle of the road at speeds of 20, and 40 mph. However, the test runs successfully at 60 mph. It is to be noted here that the *Chariot Console* runs at *TCP.* The main reason behind this discrepancy is network congestion and excessive network delays. The 10-Mbps data rate is quite high for the network especially for later access points, which can be verified from uplink saturated throughput values as discussed in Chapter 4. For 20, and 40 mph tests, the *Laptop* needs to be connected to the network for a longer time as compared to 60 mph test. This causes more network congestion at lower speeds, hence timing out of TCP connection. The 60 mph test results are given below.

At 60 mph

The test results and some of its details are given below.

- Average Uplink Throughput: 2.769 Mbps
- *Laptop*'s Send Data Rate: 8.781 Mbps
- Bytes Lost from *Laptop* to *Desktop*: 68.473%
- Max Consecutive Lost Datagrams: 2,580
- Total Bytes Sent by *Laptop*: 163,146,240
- Total Bytes Received by *Desktop*: 51,435,800

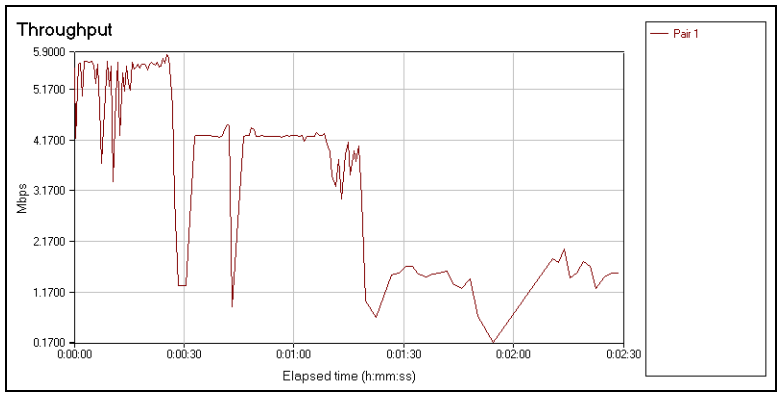

Figure 5. 7: Uplink UDP 10-Mbps Streaming Throughput @ 60 mph

As discussed above, the mobile throughput decreases with increasing number of hops during the test. The average value presented above does not serve as a reliable measure of network performance. Hence, the throughput averages at different access points are given below.

- Average Streaming Throughput When Connected to AP-1: 5.3480 Mbps
- Average Streaming Throughput When Connected to AP-2: 4.2845 Mbps
- Average Streaming Throughput When Connected to AP-3: 3.6721 Mbps
- Average Streaming Throughput When Connected to AP-4: 1.5026 Mbps

Static versus Mobile

Table 5.2 summarizes static and mobile (60 mph) UDP streaming throughput.

Table 5. 2: Static & Mobile Uplink UDP 10-Mbps Streaming Throughput Summary

***Laptop* Connected To**	**Static (Mbps)**	**60 mph (Mbps)**
AP-1	5.844	5.4063
AP-2	4.234	4.1564
AP-3	3.237	3.1569
AP-4	1.448	1.3503

Figure 5.8 presents a graphical comparison of these throughputs.

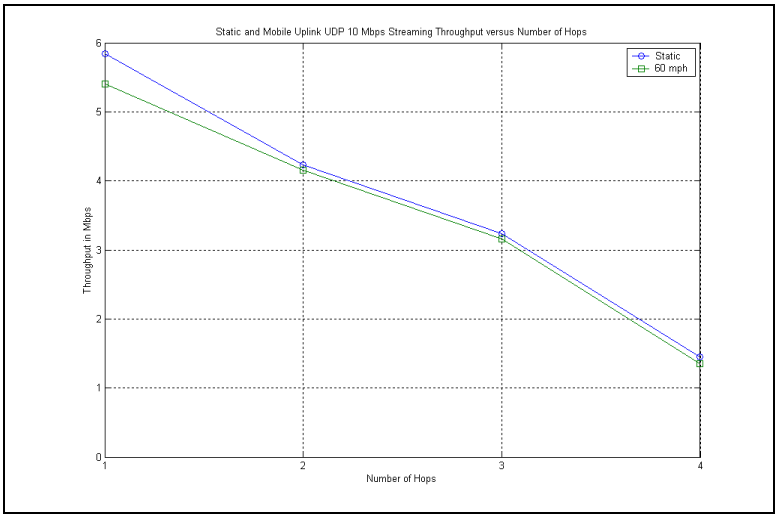

Figure 5. 8: Static & Mobile UDP 10-Mbps Streaming Throughput versus Number of Hops

Figure 5.8 shows that the saturated throughput of the network decreases slightly due to mobility. At AP-1, however, this difference is a little more pronounced as AP-1 shares the processing power of the same hardware as ROR-1.

5.3.3 UDP Throughput Test

The *UDP* is designed to be a best-effort, connectionless transport layer protocol with no built-in mechanism to acknowledge or verify a packet delivery or loss. The *Throughput Test* run by *Chariot* needs to get an acknowledgement back from the destination host in order to calculate the network's real throughput. In the absence of such a mechanism in the *UDP* protocol, *NetIQ* incorporates a way to get acknowledgement in *Chariot scripts,* when *UDP* is used for *throughput*

tests. This makes *UDP Throughput* less than what is expected (for more details on it, see [NetIQ]).

The throughput test is conducted on the network with *UDP* as transport layer protocol. The test is run in the same way as is done for *TCP*. The source host sends a data file of 100,000 bytes and gets a reply of a single byte in response from the destination host. The test is run at the road entrance until reached at the road end, at various vehicle speeds.

At 20 mph

The test results and some details are given below.

- Average Uplink Throughput: 0.792 Mbps
- Average Response Time: 1.010 seconds
- Total Bytes Sent by *Laptop*: 37,100,000
- Total Bytes Received by *Laptop*: 371

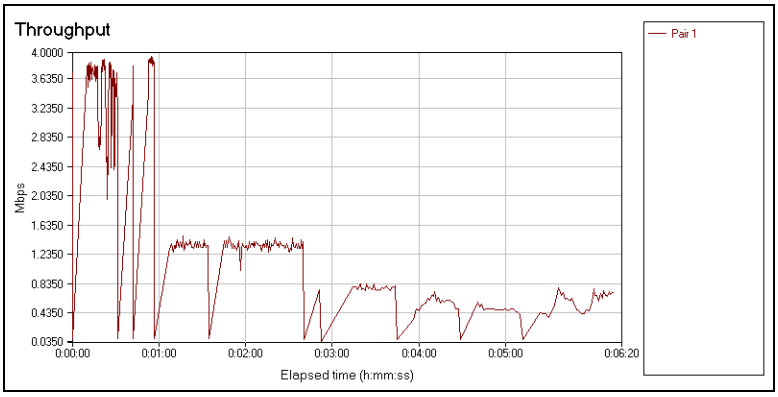

Figure 5. 9: Uplink UDP Throughput @ 20 mph

Below is a summary of average throughputs when connected to different access points.

- Average Throughput When Connected to AP-1: 3.4961 Mbps
- Average Throughput When Connected to AP-2: 1.3608 Mbps
- Average Throughput When Connected to AP-3: 0.7729 Mbps

- Average Throughput When Connected to AP-4: 0.5826 Mbps

Discussion

Table 5.3 summarizes the corresponding results.

Table 5. 3: Uplink UDP Average Throughput Summary

***Laptop* Connected To**	**20 mph (Mbps)**	**40 mph (Mbps)**	**60 mph (Mbps)**
AP-1	3.4961	3.3544	3.3255
AP-2	1.3608	1.3227	1.2568
AP-3	0.7729	0.6837	0.5844
AP-4	0.5826	0.6634	0.5157

These results are plotted in Figure 5.16 versus total number of hops. It shows that the *UDP* throughput does not degrade linearly with increasing number of hops. Also, there is very slight throughput degradation due to mobility.

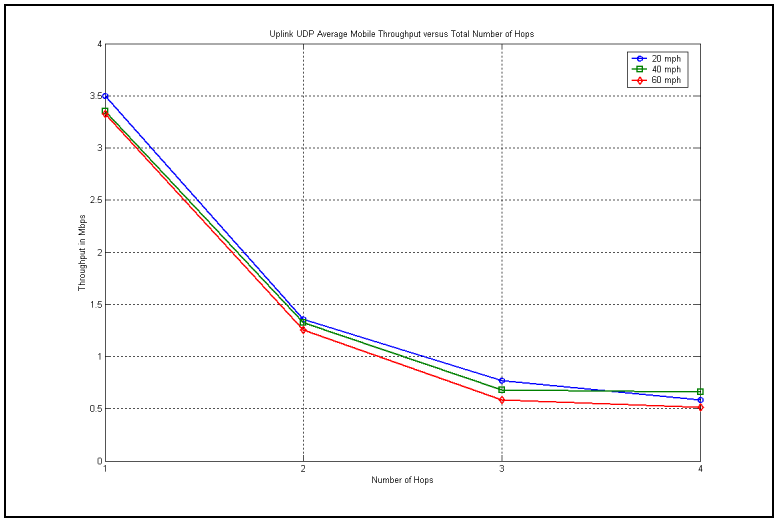

Figure 5. 10: Uplink UDP Average Mobile Throughput versus Number of Hops

5.3.4 TCP versus UDP

The performance of TCP and UDP at a speed of 60 mph is compared in Figure 5.11. The TCP throughput degrades almost linearly with increasing number of hops. But, the UDP throughput (both streaming and file transfer) does not degrade linearly with increasing number of hops due to its best-effort, connectionless design. The UDP streaming throughput is the highest achievable data rate of the network and serves as a ceiling for the network throughput. The TCP throughput is higher than corresponding UDP throughput (file transfer) due to reasons discussed earlier.

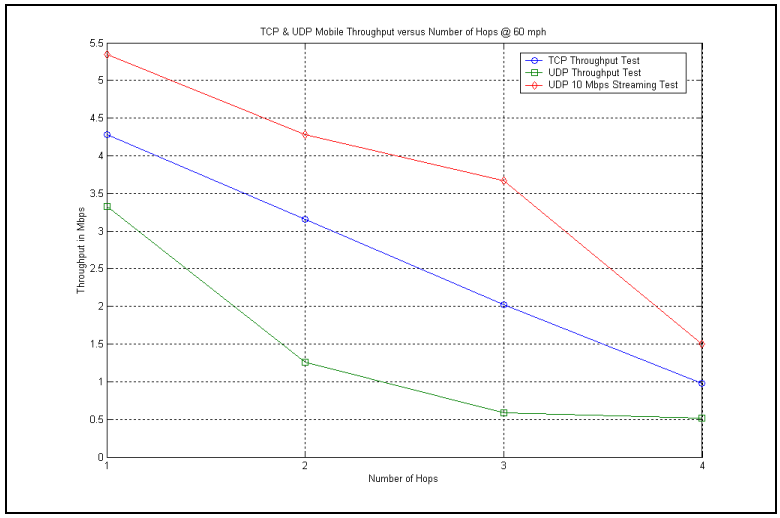

Figure 5. 11: TCP & UDP Uplink Mobile Throughputs versus Number of Hops @ 60 mph

5.4 Single-User Downlink Throughput

As defined in Chapter 4, the *Desktop* serves as the source host, and the *Laptop* as the destination host. *Laptop 1* is used in all the measurements unless stated otherwise. Similar tests are run on the downlink as discussed earlier in order to measure and analyze its performance. Below are some test results and their details. Other test results are given in the Section B.3.

5.4.1 TCP Throughput Test

The same test is conducted on downlink as described for uplink.

At 20 mph

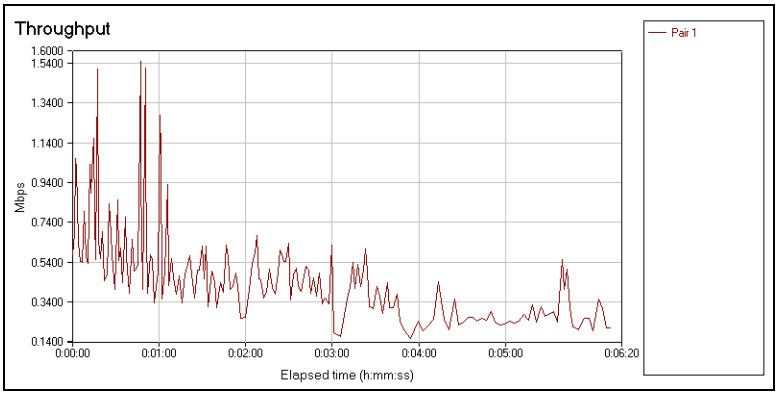

Figure 5. 12: Downlink TCP Throughput Test @ 20 mph

- Average Downlink Throughput: 0.390 Mbps
- Average Response Time: 2.051 seconds
- Total Bytes Sent by *Desktop*: 18,200,000
- Total Bytes Received by *Desktop*: 182

Discussion

Due to asymmetric design of the network, downlink throughput is much less than that with uplink. The throughput degrades with increasing number of hops, but not very rapidly. Also, there is a slight degradation in the throughput due to mobility, which can be seen from the average values presented above.

5.4.2 UDP 3-Mbps Streaming Test

The downlink capacity is far less than that of uplink due to the inherent asymmetry of the network. A lower streaming rate is used to measure downlink saturated throughput under mobility. *UDP MPEG* video-streaming test is run on the downlink at a rate of 3 Mbps in order to measure and analyze the saturated throughput performance of the network under mobility.

At 40 mph

The test results and some of its details are given below.

- Average Downlink Throughput: 2.573 Mbps
- *Desktop*'s Send Data Rate: 2.990 Mbps
- Bytes Lost from *Desktop* to *Laptop*: 13.957%
- Max Consecutive Lost Datagrams: 910
- Total Bytes Sent by *Desktop*: 64,605,000
- Total Bytes Received by *Laptop*: 55,588,040

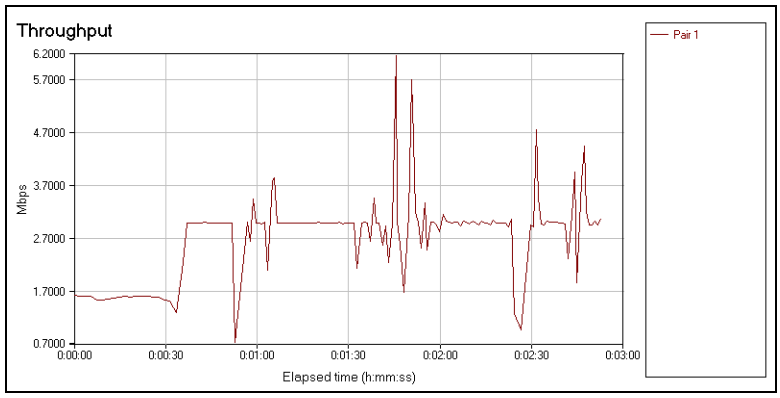

Figure 5. 13: Downlink UDP 3-Mbps Streaming Throughput @ 40 mph

At 60 mph

The test results and some details are as follows.

- Average Downlink Throughput: 2.489 Mbps
- *Desktop*'s Send Data Rate: 2.990 Mbps
- Bytes Lost from *Desktop* to *Laptop*: 16.753%
- Max Consecutive Lost Datagrams: 1,065
- Total Bytes Sent by *Desktop*: 46,720,000
- Total Bytes Received by *Laptop*: 38,892,940

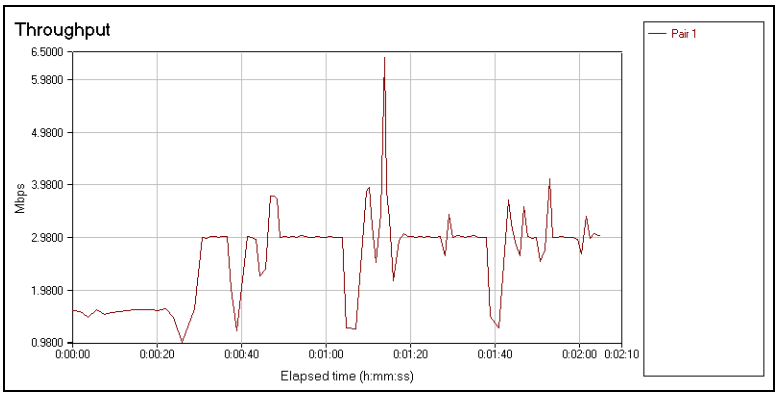

Figure 5. 14: Downlink UDP 3-Mbps Streaming Throughput @ 60 mph

Discussion

The streaming test results shown in Figures 5.15, and 5.16 indicate that the network's downlink is capable of supporting data rate of 3 Mbps with minimal data loss all over the road, except when the *Laptop* is connected to AP-1. The reduced data rate at AP-1 is due to the fact that single hardware is used at ROR-1 and AP-1, and network performance is limited by its processing power.

5.4.3 UDP Throughput Test

The throughput test is run on the network's downlink with *UDP/IP* protocol stack. The corresponding test results and their details are given as under.

At 20 mph

The test results and some details are given below.

- Average Downlink Throughput: 0.416 Mbps
- Average Response Time: 1.925 seconds
- Total Bytes Sent by *Desktop*: 19,400,000
- Total Bytes Received by *Desktop*: 194

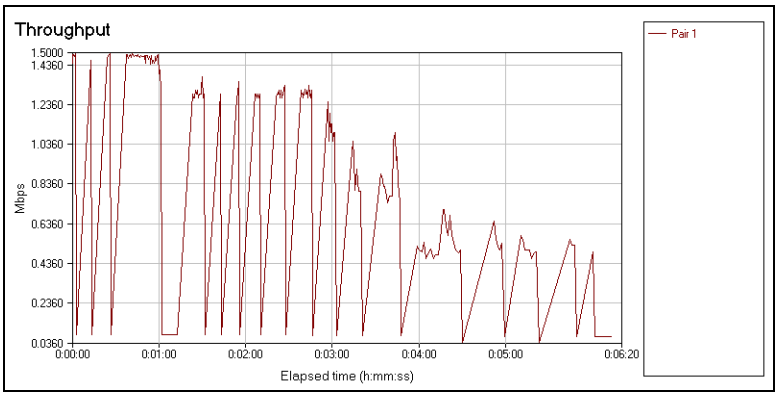

Figure 5. 15: Downlink UDP Throughput @ 20 mph

Discussion

The average downlink throughput degrades gradually, but not linearly with increasing number of hopes. This decreased rate is lower than that of uplink throughput due to inherent network symmetry. Also, the throughput degrades slightly with mobility.

5.5 Single-User Full-Duplex TCP Throughput

The throughput test is conducted on the uplink and downlink simultaneously with *TCP/IP* protocol stack. Source host transfers data file of 100,000 bytes to destination host in each direction. The test is run from the road entrance to the road end at various speeds. The following are some of the test results and their corresponding details.

At 20 mph

The test results and some details are given below.

- Pair 1: Uplink
  - Average Throughput: 1.565 Mbps
  - Average Response Time: 0.511 seconds
  - Bytes Sent By *Laptop*: 72,900,000
  - Bytes Received By *Laptop*: 729
- Pair 2: Downlink

- Average Throughput: 0.199 Mbps
- Average Response Time: 4.030 seconds
- Bytes Sent By *Desktop*: 9,300,000
- Bytes Received By *Desktop*: 93

- Totals:
  - Total Average Throughput: 1.754 Mbps
  - Average Response Time: 2.271 seconds

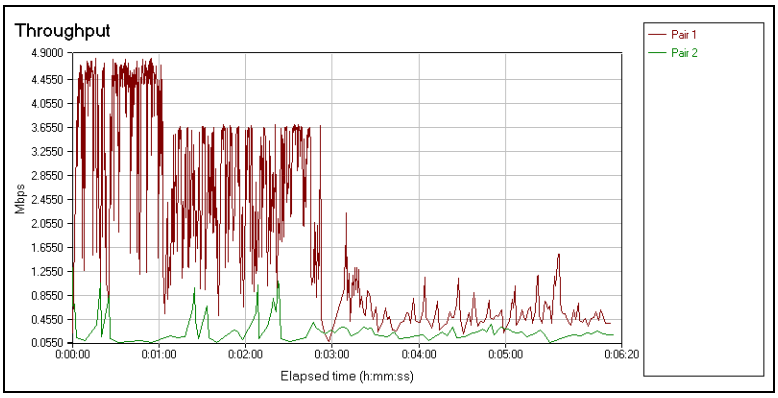

Figure 5. 16: Full-Duplex TCP Throughput @ 20 mph

At 40 mph

The test results and some details are as follows.

- Pair 1: Uplink
  - Average Throughput: 1.410 Mbps
  - Average Response Time: 0.568 seconds
  - Bytes Sent By *Laptop*: 33,700,000
  - Bytes Received By *Laptop*: 337
- Pair 2: Downlink
  - Average Throughput: 0.256 Mbps
  - Average Response Time: 3.127 seconds
  - Bytes Sent By *Desktop*: 6,200,000
  - Bytes Received By *Desktop*: 62
- Totals:

- Total Average Throughput: 1.646 Mbps
- Average Response Time: 1.847 seconds

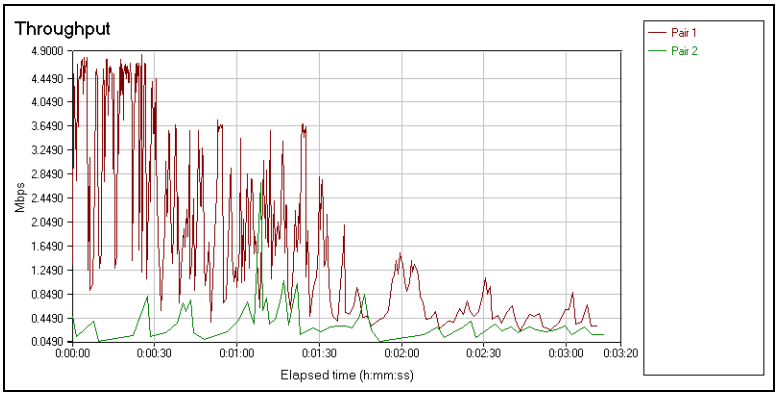

Figure 5. 17: Full-Duplex TCP Throughput @ 40 mph

Discussion

Figures 5.20 and 5.21 clearly show the network's inherent asymmetry. The uplink throughput is much higher than downlink, and degrades at a higher rate with increasing number of hops. Moreover, the throughput, in both the cases degrades very slightly due to mobility.

5.6 Two-User Mutual Full-Duplex Throughput

Mutual throughput is measured between two different mobile stations moving at approximately the same speed besides each other. Existence of an infrastructure mode network requires these two mobile stations to communicate via wireless data network at the *Smart road* in order to communicate with each other. Both *Laptop 1,* and *Laptop 2* are used in these measurements. Both laptops are installed in two different vehicles moving in the eastbound lane of the road at some constant speed. Some of the test results are given in this section. Others can be found in the Section B.4 of Appendix B.

5.6.1 TCP/IP File Transfer Test

The *Chariot's* file transfer script for short Internet connections is used for measuring mutual throughput between the two laptops. Data file of size 100,000 bytes is transferred from source

host to destination host in each direction; using data transfer protocol for short Internet connections. This test starts at the road entrance and stops at the road end. It is to be noted here that the data is transferred between the two laptops, and the *Desktop* does not participate in these measurements. Hence, the term full duplex refers here to simultaneous data transfer from one laptop to the other.

At 20 mph

- Pair 1: From *Laptop 1* to *Laptop 2*
  - Average Throughput: 0.963 Mbps
  - Average Response Time: 831 ms
  - Bytes Sent By *Laptop* 1: 41,200,000
  - Bytes Received By *Laptop* 1: 412
- Pair 2: From *Laptop 2* to *Laptop 1*
  - Average Throughput: 0.980 Mbps
  - Average Response Time: 816 ms
  - Bytes Sent By *Laptop* 2: 41,900,000
- Bytes Received By *Laptop* 2: 419
- Totals:
  - Total Average Throughput: 1.940 Mbps
  - Average Response Time: 824 ms

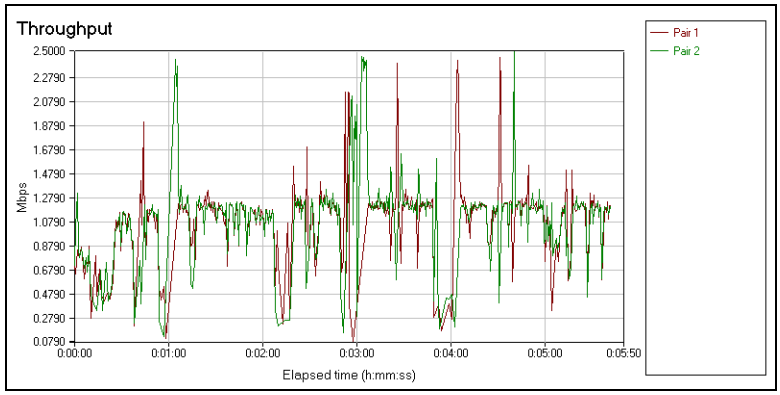

Figure 5. 18: Two-User Mutual Full-Duplex TCP File Send Test Throughput @ 20 mph

Discussion

The mutual wireless link between the two mobile users is almost symmetric as shown in above figures. The mutual throughput degrades slightly due to mobility, but the physical location on the road doesn't affect their mutual throughput, because the hosts always communicate with each other via wireless backbone and their inter-communication always involve two hops down the road.

5.6.2 UDP/IP File Transfer Test

The same test as described above is repeated with *UDP/IP* protocols stack. Some of the test results and their details are given below. Others can be found in Appendix B.

At 20 mph

- Pair 1: From *Laptop* 1 to *Laptop* 2
  - Average Throughput: 0.648 Mbps
  - Average Response Time: 1.235 seconds
  - Bytes Sent By *Laptop* 1: 31,300,000
  - Bytes Received By *Laptop* 1: 313
- Pair 2: From *Laptop* 2 to *Laptop* 1
  - Average Throughput: 0.666 Mbps
  - Average Response Time: 1.201 seconds
  - Bytes Sent By *Laptop* 2: 32,200,000
  - Bytes Received By *Laptop* 2: 322
- Totals:
  - Total Average Throughput: 1.313 Mbps
  - Average Response Time: 1.218 seconds

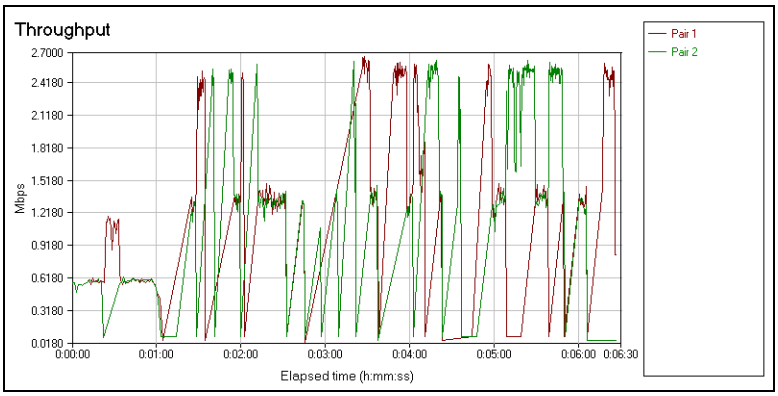

Figure 5. 19: Two-User Mutual Full-Duplex UDP File Send Test Throughput @ 20 mph

Discussion

The test results show that the average UDP mutual throughput remains same irrespective of end-user location as discussed earlier. The mutual wireless link between the two mobile stations is almost symmetric, and is slightly sensitive to mobility.

5.7 Summary

From the results and discussions presented in this chapter, it can be concluded that both *TCP* and *UDP* throughput degrades with increasing number of hops and mobility. However, the throughput degradation due to mobility is slight. The dominating factor controlling the network throughput is the number of hops not the vehicle speed. Hence, these networks can live with mobility if proper hand-offs can be made and *TCP* connection doesn't time out. The network's inherent asymmetry requires different uplink and downlink throughputs, and they both degrade at a different rate with increasing number of hops. The *TCP* throughput decreases almost linearly with increasing number of hops, but this characteristic is not pronounced in *UDP*. Also, mutual throughput between two mobile end-users does not depend on stations location, and almost always comes out to be symmetric. *UDP* can be used to measure the network's saturated throughput, which is always higher than *TCP* throughput. Sometimes, TCP connection terminates or times out due to network congestion, excessive delays, or poor coverage, which needs to be taken care.

Chapter 6: Conclusion

This chapter concludes this document by summarizing the findings of the study followed by some suggestions for future work in this direction.

6.1 Summary of Findings

The document presents feasibility and characteristics of the use of the *IEEE 802.11b* [802.11b] networks for outdoor high mobility applications. The *IEEE 802.11b* [802.11b] typically represents the family of wireless LANs and is one of the most widely deployed, and commercially available wireless LANs around the world. Its success as an outdoor high mobility wireless LAN standard leads us to use it as a low-cost high-rate outdoor wireless data network. During the course of this research, the following key results are obtained

- End-user throughput depends on many factors including its location, antenna gain and type used, noise level, and site details.
- *TCP* throughput decreases almost linearly with increasing number of hops, which is a characteristic of the designed network.
- *UDP* streaming throughput can be used to estimate saturated throughput of a network, which is always equal to or higher than the *TCP* and *UDP* file transfer throughput.
- Two users share the network's bandwidth in a fair proportion of their signal-to-noise ratios (SNR).
- Throughput degrades slightly with mobility if proper hand-offs are made.
- Mutual throughput between two mobile users does not depend on backbone.
- *TCP* connection often terminates or times out due to network congestion, excessive delays, or poor coverage.

Although some of these results are characteristic of the designed network, we can certainly conclude that the network performance is mainly based on number of hops rather than mobility. Wireless LANs can provide us substantial throughput even with high Doppler. The topology and structure of this network can be implemented along highways and other areas for more coverage and easier scalability. Moreover, it can be said that the *TCP/IP* throughput does not degrade with

higher exponents with number of hops. Hence, it can be used for wireless data networks if can be modified to tolerate excessive delays, poor coverage and data loss or corruption, which are frequently encountered in wireless world.

6.2 Future Work

The following are some suggestions for future research in this direction.

- A reliable communication protocol for wireless data networks needs to be devised.
- Performance of other wireless LAN standards should also be tested and analyzed under high mobility outdoor conditions.
- Network performance may be analyzed with specific protocols and applications for real world networks according to their scope and need.
- Use of computer simulations, and hardware emulations, in addition to real measurements may also provide support and directive for future research.

6.3 Final Word

This study shows that the *802.11b* [802.11b] networks can be used for high mobility applications, if *TCP* connections are retained in motion and proper hand-offs can be guaranteed. However, most of the time number of hops in an outdoor wireless network dictates the network performance.

Appendix A: Network Static Performance – Additional Results

A.1 Network Delays

The following test results are in continuation of Section 4.3.

A.1.1 Using TCP

While Connected to AP-1

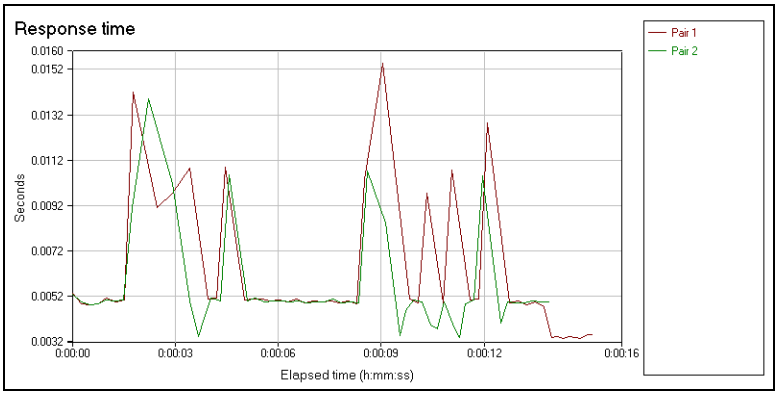

Figure A. 1: Full-Duplex TCP Response Time @ AP-1

- *Laptop* SNR: 28 dB
- AP-1 SNR: 33 dB
- Frequency Channel #: 11
- Pair 1: Downlink
    - Average Response Time: 6 ms
    - Bytes Sent By *Desktop*: 250,000
    - Bytes Received By *Desktop*: 250,000
- Pair 2: Uplink
    - Average Response Time: 6 ms

  - Bytes Sent By *Laptop*: 250,000
  - Bytes Received By *Laptop*: 250,000
- Totals:
  - Average Response Time: 6 ms

While Connected to AP-3

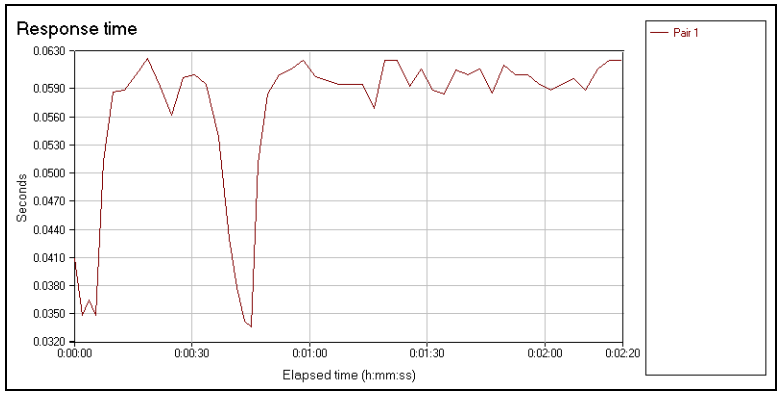

Figure A. 2: Uplink TCP Response Time @ AP-3

- *Laptop* SNR: 33 dB
- AP-3 SNR: 36 dB
- Frequency Channel #: 2
- Average Response Time: 56 ms
- Bytes Sent By *Laptop*: 250,000
- Bytes Received By *Laptop*: 250,000

While Connected to AP-4

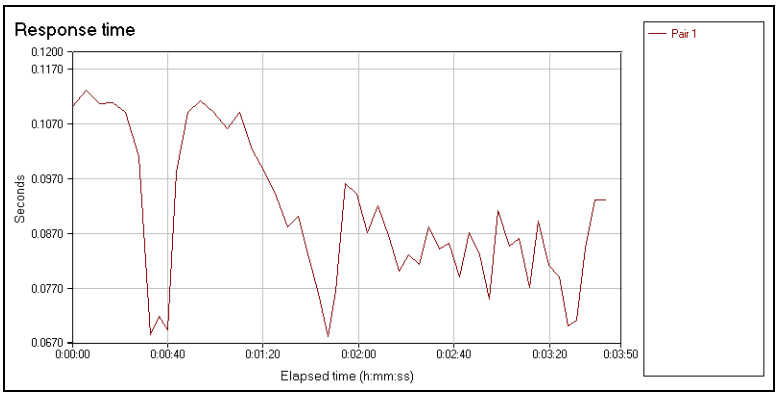

Figure A. 3: Uplink TCP Response Time @ AP-4

- *Laptop* SNR: 21 dB
- AP-4 SNR: 25 dB
- Frequency Channel #: 1
- Average Response Time: 89 ms
- Bytes Sent By *Laptop*: 250,000
- Bytes Received By *Laptop*: 250,000

A.1.2 Using UDP

While Connected to AP-1

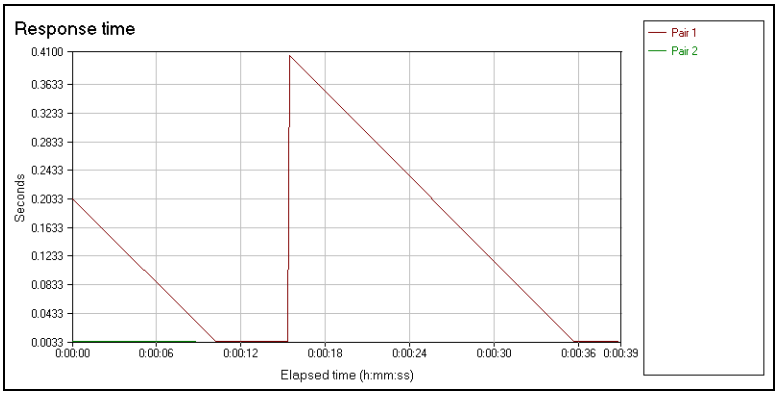

Figure A. 4: Full-Duplex UDP Response Time @ AP-1

- *Laptop* SNR: 30 dB
- AP-1 SNR: 33 dB
- Frequency Channel #: 11
- Pair 1: Downlink
    - Average Response Time: 16 ms
    - Bytes Sent By *Desktop*: 250,000
    - Bytes Received By *Desktop*: 250,000
- Pair 2: Uplink
    - Average Response Time: 3 ms
    - Bytes Sent By *Laptop*: 250,000
    - Bytes Received By *Laptop*: 250,000
- Totals:
    - Average Response Time: 10 ms

While Connected to AP-3

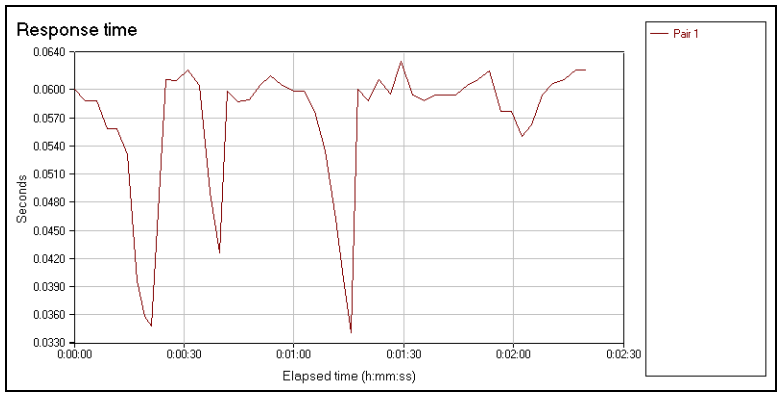

Figure A. 5: Uplink UDP Response Time @ AP-3

- *Laptop* SNR: 32 dB
- AP-3 SNR: 36 dB
- Frequency Channel #: 2
- Average Response Time: 56 ms
- Bytes Sent By *Laptop*: 250,000

- Bytes Received By *Laptop*: 250,000

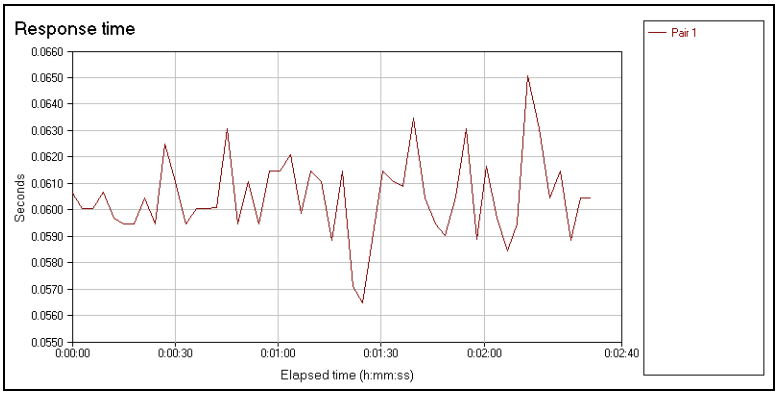

Figure A. 6: Downlink UDP Response Time @ AP-3

- *Laptop* SNR: 33 dB
- AP-3 SNR: 36 dB
- Frequency Channel #: 2
- Average Response Time: 60 ms
- Bytes Sent By *Desktop*: 250,000
- Bytes Received By *Desktop*: 250,000

While Connected to AP-4

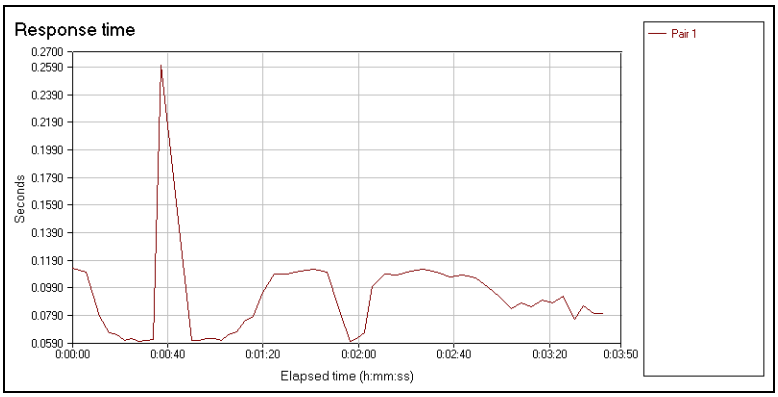

Figure A. 7: Uplink UDP Response Time @ AP-4

- *Laptop* SNR: 21 dB
- AP-4 SNR: 23 dB
- Frequency Channel #: 1
- Average Response Time: 89 ms
- Bytes Sent By *Laptop*: 250,000
- Bytes Received By *Laptop*: 250,000

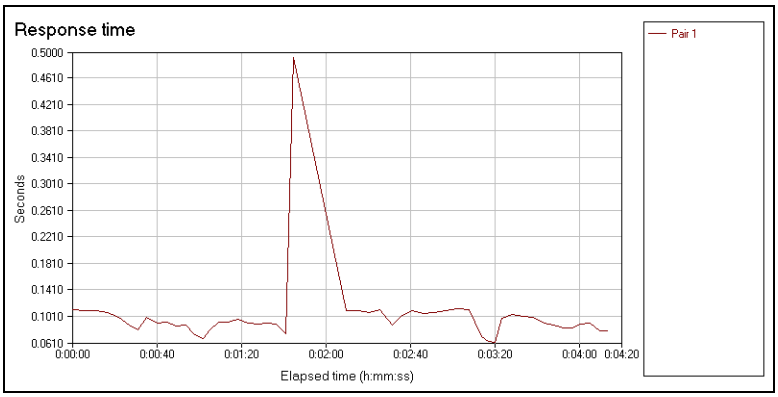

Figure A. 8: Downlink UDP Response Time @ AP-4

- *Laptop* SNR: 22 dB
- AP-4 SNR: 24 dB
- Frequency Channel #: 1
- Average Response Time: 102 ms
- Bytes Sent By *Desktop*: 250,000
- Bytes Received By *Desktop*: 250,000

A.2 Single-User Uplink Throughput

The test results presented in this section are a continuation of Section 4.4.

A.2.1 Throughput Test with TCP

While Connected to AP-2

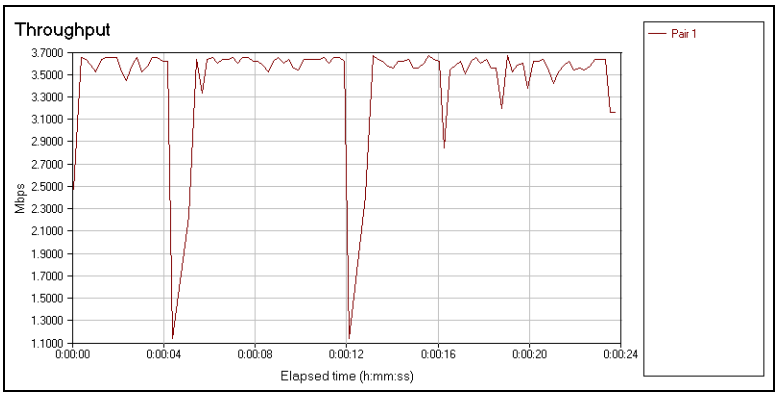

Figure A. 9: Uplink TCP Static Throughput @ AP-2

- Average Uplink Throughput: 3.383 Mbps
- Average Response Time: 237 ms
- Average SNR at *Laptop*: 30 dB
- Average SNR at AP-2: 19 dB
- Total Bytes Sent by *Laptop*: 10,000,000
- Total Bytes Received by *Laptop*: 100

While Connected to AP-3

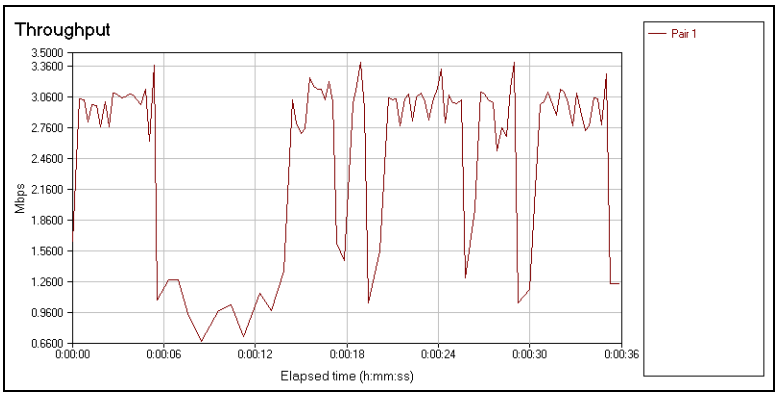

Figure A. 10: Uplink TCP Static Throughput @ AP-3

- Average Uplink Throughput: 2.233 Mbps
- Average Response Time: 358 ms
- Average SNR at *Laptop*: 32 dB
- Average SNR at AP-3: 36 dB
- Total Bytes Sent by *Laptop*: 10,000,000
- Total Bytes Received by *Laptop*: 100

While Connected to AP-4

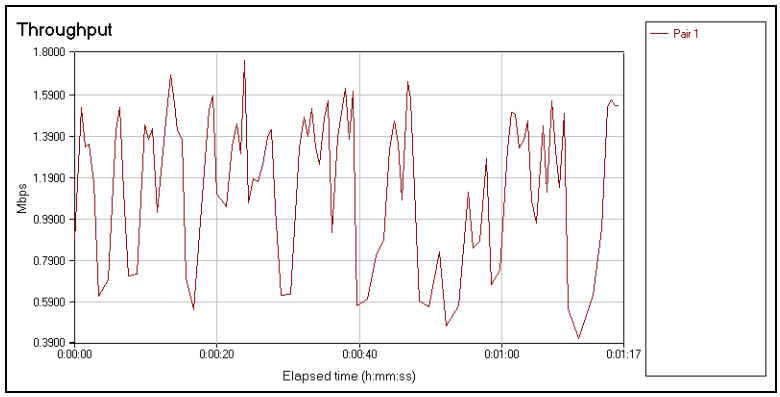

Figure A. 11: Uplink TCP Static Throughput @ AP-4

- Average Uplink Throughput: 1.049 Mbps
- Average Response Time: 762 ms
- Average SNR at *Laptop*: 21 dB
- Average SNR at AP-4: 23 dB
- Total Bytes Sent by *Laptop*: 10,000,000
- Total Bytes Received by *Laptop*: 100

A.2.2 10-Mbps Streaming Test with UDP

While Connected to AP-2

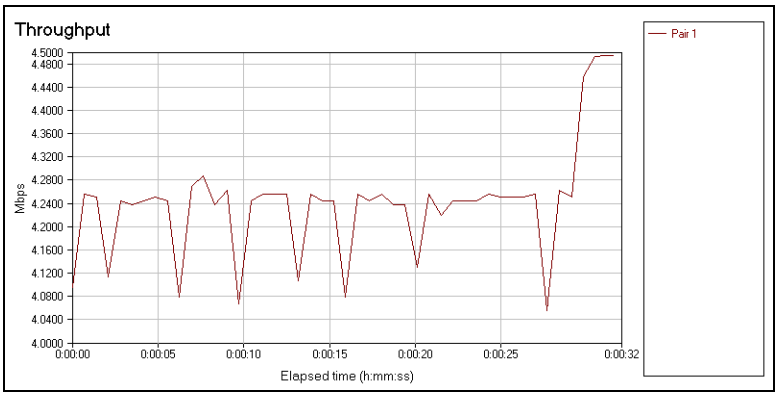

Figure A. 12: Uplink UDP 10-Mbps Streaming Throughput @ AP-2

- Average Uplink Throughput: 4.234 Mbps
- *Laptop*'s Send Data Rate: 9.260 Mbps
- Bytes Lost from *Laptop* to *Desktop*: 54.272%
- Max Consecutive Lost Datagrams: 25
- Average SNR at *Laptop*: 29 dB
- Average SNR at AP-2: 18 dB
- Total Bytes Sent by *Laptop*: 36,500,000
- Total Bytes Received by *Desktop*: 16,690,720

While Connected to AP-3

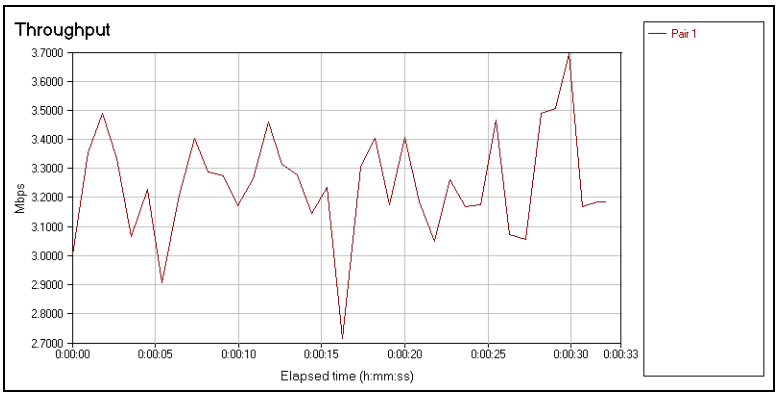

Figure A. 13: Uplink UDP 10-Mbps Streaming Throughput @ AP-3

- Average Uplink Throughput: 3.237 Mbps
- *Laptop*'s Send Data Rate: 9.102 Mbps
- Bytes Lost from *Laptop* to *Desktop*: 64.436%
- Max Consecutive Lost Datagrams: 63
- Average SNR at *Laptop*: 32 dB
- Average SNR at AP-3: 36 dB
- Total Bytes Sent by *Laptop*: 36,500,000
- Total Bytes Received by *Desktop*: 12,980,860

While Connected to AP-4

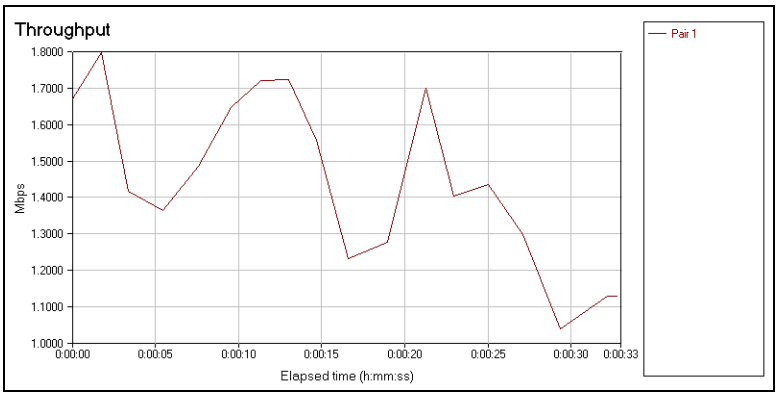

Figure A. 14: Uplink UDP 10-Mbps Streaming Throughput @ AP-4

- Average Uplink Throughput: 1.448 Mbps
- *Laptop*'s Send Data Rate: 8.913 Mbps
- Bytes Lost from *Laptop* to *Desktop*: 83.756%
- Max Consecutive Lost Datagrams: 92
- Average SNR at *Laptop*: 22 dB
- Average SNR at AP-3: 25 dB
- Total Bytes Sent by *Laptop*: 36,500,000
- Total Bytes Received by *Desktop*: 5,929,060

A.3 Single-User Downlink Throughput

The test results presented here are a continuation of Section 4.5.

A.3.1 Throughput Test with TCP

While Connected to AP-2

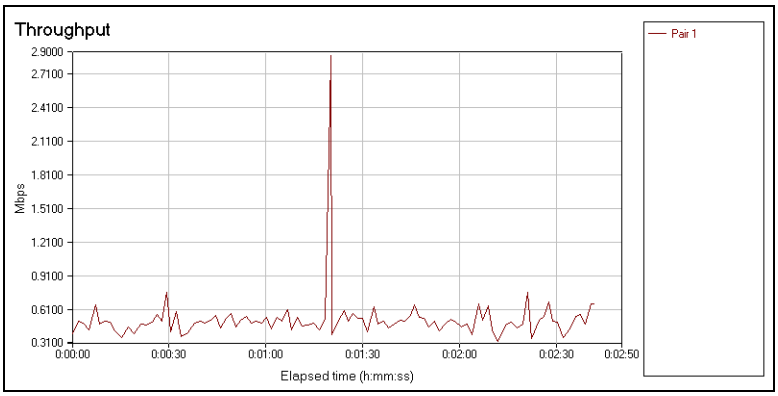

Figure A. 15: Downlink TCP Static Throughput @ AP-2

- Average Downlink Throughput: 0.495 Mbps
- Average Response Time: 1.617 seconds
- Average SNR at *Laptop*: 30 dB
- Average SNR at AP-2: 18 dB
- Total Bytes Sent by *Desktop*: 10,000,000
- Total Bytes Received by *Desktop*: 100

While Connected to AP-4

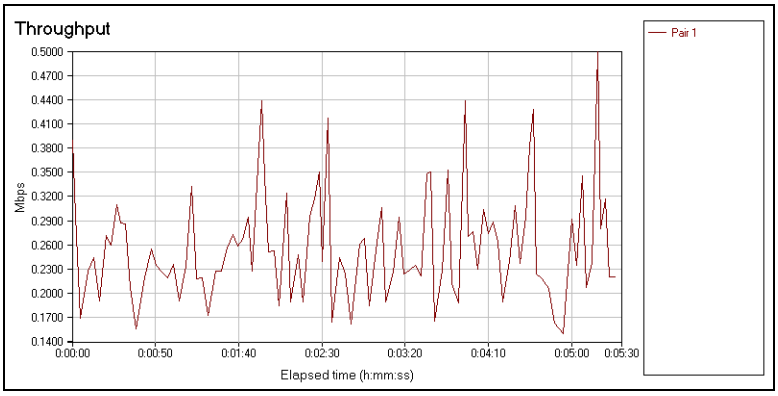

Figure A. 16: Downlink TCP Static Throughput @ AP-4

- Average Downlink Throughput: 0.245 Mbps
- Average Response Time: 3.265 seconds
- Average SNR at *Laptop*: 20 dB
- Average SNR at AP-2: 24 dB
- Total Bytes Sent by *Desktop*: 10,000,000
- Total Bytes Received by *Desktop*: 100

A.3.2 10-Mbps Streaming Test with UDP

While Connected to AP-2

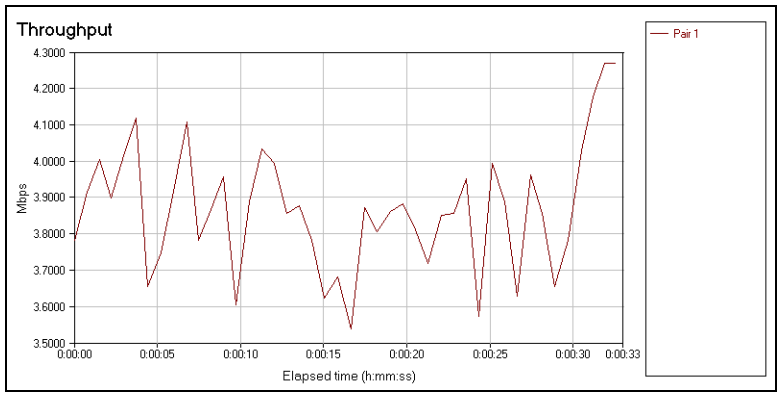

Figure A. 17: Downlink UDP 10-Mbps Streaming Throughput @ AP-2

- Average Downlink Throughput: 3.855 Mbps
- *Desktop* Send Data Rate: 8.980 Mbps
- Bytes Lost from *Desktop* to *Laptop*: 57.064%
- Max Consecutive Lost Datagrams: 12
- Average SNR at *Laptop*: 29 dB
- Average SNR at AP-2: 18 dB
- Total Bytes Sent by *Desktop*: 36,500,000
- Total Bytes Received by *Laptop*: 15,671,640

While Connected to AP-3

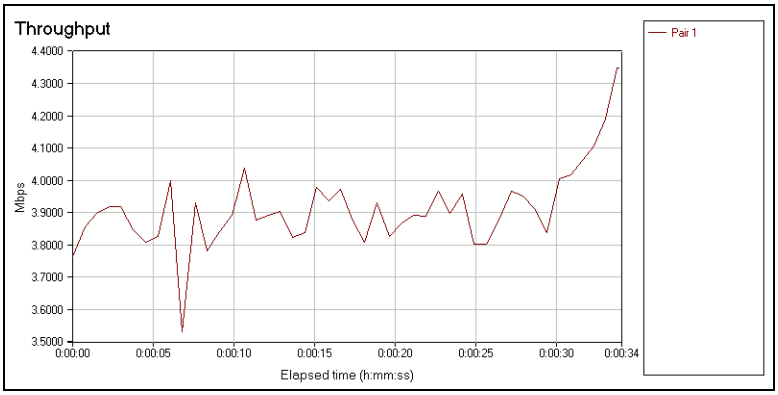

Figure A. 18: Downlink UDP 10-Mbps Streaming Throughput @ AP-3

- Average Downlink Throughput: 3.900 Mbps
- *Desktop* Send Data Rate: 8.613 Mbps
- Bytes Lost from *Desktop* to *Laptop*: 54.720%
- Max Consecutive Lost Datagrams: 7
- Average SNR at *Laptop*: 32 dB
- Average SNR at AP-3: 36 dB
- Total Bytes Sent by *Desktop*: 36,500,000
- Total Bytes Received by *Laptop*: 16,527,200

While Connected to AP-4

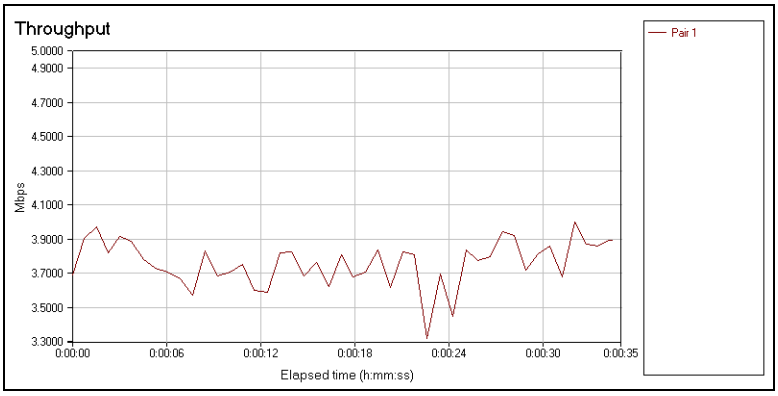

Figure A. 19: Downlink UDP 10-Mbps Streaming Throughput @ AP-4

- Average Downlink Throughput: 3.755 Mbps
- *Desktop* Send Data Rate: 8.473 Mbps
- Bytes Lost from *Desktop* to *Laptop*: 55.684%
- Max Consecutive Lost Datagrams: 13
- Average SNR at *Laptop*: 23 dB
- Average SNR at AP-3: 24 dB
- Total Bytes Sent by *Desktop*: 36,500,000
- Total Bytes Received by *Laptop*: 16,175,340

Appendix B: Network Mobile Performance – Additional Results

B.1 Wireless Link Measurements

The SNR measurement results reported in this section are a continuation of Section 5.1.

B.1.1 Wireless Link at 20 mph

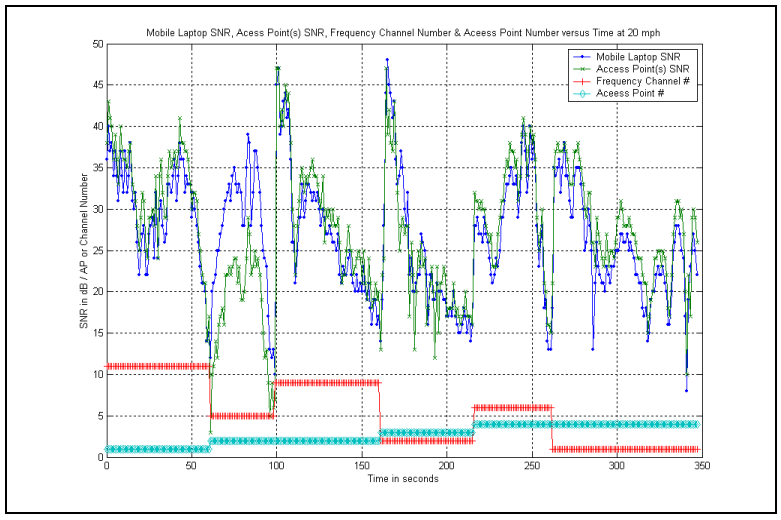

Figure B. 1: End-User Wireless Link SNR, Access Point and Frequency Channel @ 20 mph

B.1.2 Wireless Link at 60 mph

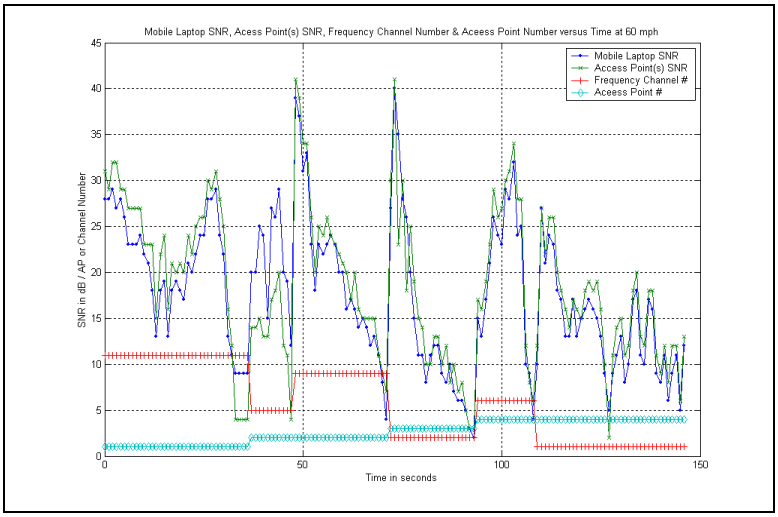

Figure B. 2: End-User Wireless Link SNR, Access Point and Frequency Channel @ 60 mph

B.2 Single-User Uplink Throughput

The following results are in continuation of the Section 5.3.

B.2.1 TCP Throughput Test

At 40 mph

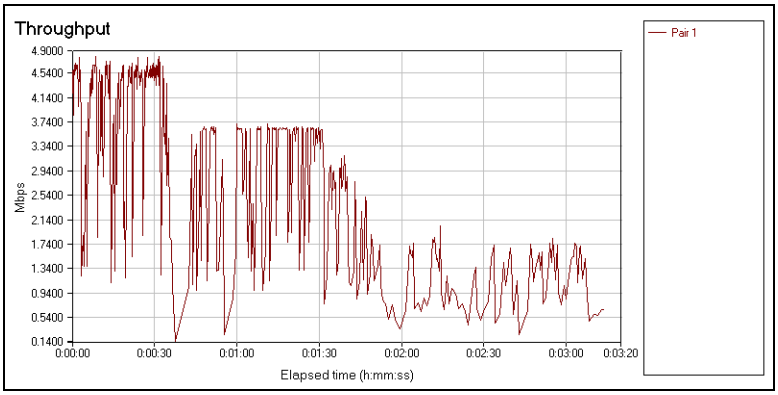

Figure B. 3: Uplink TCP Throughput @ 40 mph

- Average Uplink Throughput: 1.936 Mbps
- Average Response Time: 413 ms
- Total Bytes Sent by *Laptop*: 46,900,000
- Total Bytes Received by *Laptop*: 469

Figure B.3 shows the uplink throughput results while moving at 40 mph. The average value presented above does not indicate the network performance, as it does not take into effect the fact that the number of hops changes during the test. The following are the average throughput values at different access points, calculated from the test's results shown above.

- Average Throughput When Connected to AP-1: 4.1322 Mbps
- Average Throughput When Connected to AP-2: 3.1561 Mbps
- Average Throughput When Connected to AP-3: 2.1543 Mbps
- Average Throughput When Connected to AP-4: 1.1940 Mbps

At 60 mph

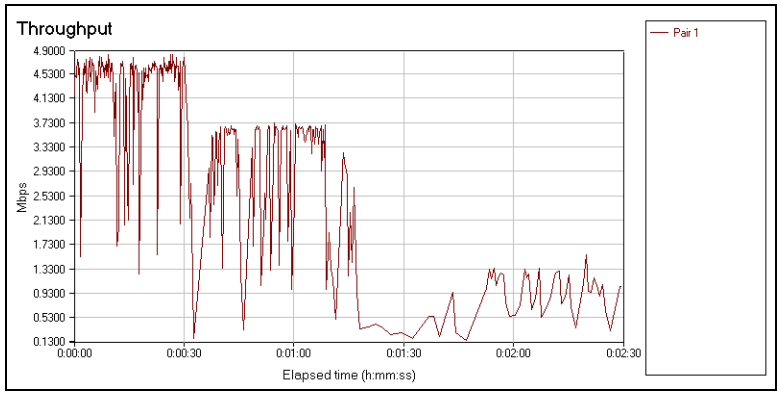

Figure B. 4: Uplink TCP Throughput @ 60 mph

- Average Uplink Throughput: 1.867 Mbps
- Average Response Time: 428 ms
- Total Bytes Sent by *Laptop*: 34,900,000
- Total Bytes Received by *Laptop*: 349

Below are the throughput averages at different access points calculated from the above results.

- Average Throughput When Connected to AP-1: 4.2823 Mbps
- Average Throughput When Connected to AP-2: 3.1568 Mbps
- Average Throughput When Connected to AP-3: 2.0258 Mbps
- Average Throughput When Connected to AP-4: 0.9824 Mbps

B.2.2 UDP Throughput Test

The results reported in this subsection are a continuation of the Section 5.3.3.

At 40 mph

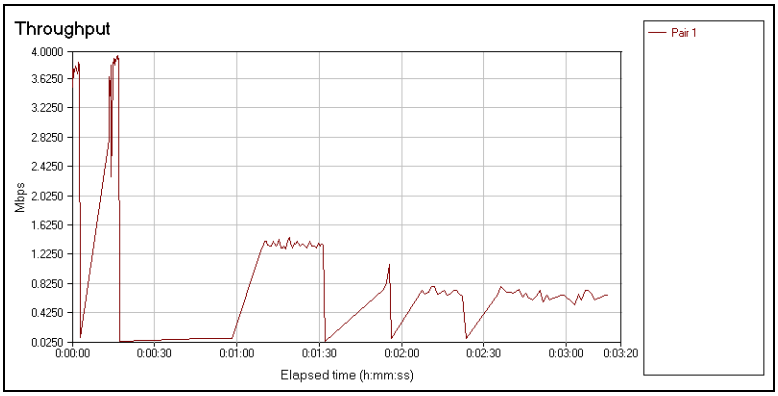

Figure B. 5: Uplink UDP Throughput @ 40 mph

- Average Uplink Throughput: 0.520 Mbps
- Average Response Time: 1.538 seconds
- Total Bytes Sent by *Laptop*: 12,700,000
- Total Bytes Received by *Laptop*: 127

The average uplink throughput while connected to different access points is given below.

- Average Throughput When Connected to AP-1: 3.3544 Mbps
- Average Throughput When Connected to AP-2: 1.3227 Mbps
- Average Throughput When Connected to AP-3: 0.6837 Mbps

- Average Throughput When Connected to AP-4: 0.6634 Mbps

At 60 mph

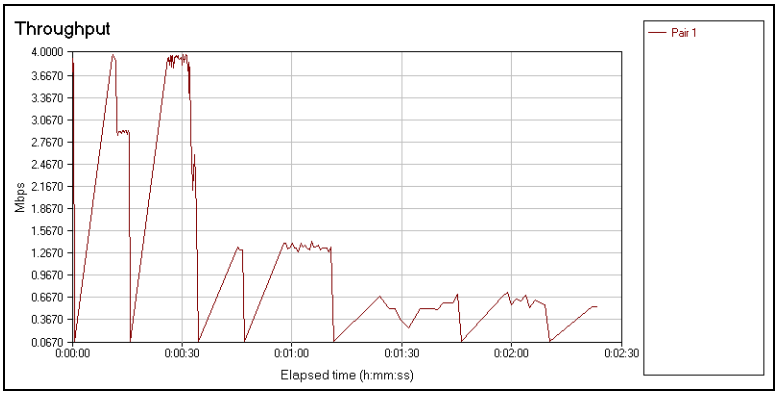

Figure B. 6: Uplink UDP Throughput @ 60 mph

- Average Uplink Throughput: 0.658 Mbps
- Average Response Time: 1.216 seconds
- Total Bytes Sent by *Laptop*: 11,800,000
- Total Bytes Received by *Laptop*: 118

Below are the throughput averages when the *Laptop* is connected to different access points.

- Average Throughput When Connected to AP-1: 3.3255 Mbps
- Average Throughput When Connected to AP-2: 1.2568 Mbps
- Average Throughput When Connected to AP-3: 0.5844 Mbps
- Average Throughput When Connected to AP-4: 0.5157 Mbps

B.3 Single-User Downlink Throughput

The following results are a continuation of the Section 5.4.

B.3.1 TCP Throughput Test

At 40 mph

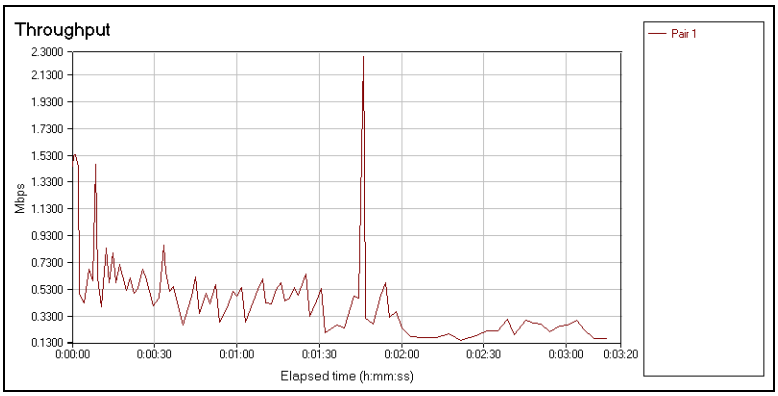

Figure B. 7: Downlink TCP Throughput @ 40 mph

- Average Downlink Throughput: 0.386 Mbps
- Average Response Time: 2.073 seconds
- Total Bytes Sent by *Desktop*: 9,400,000
- Total Bytes Received by *Desktop*: 94

At 60 mph

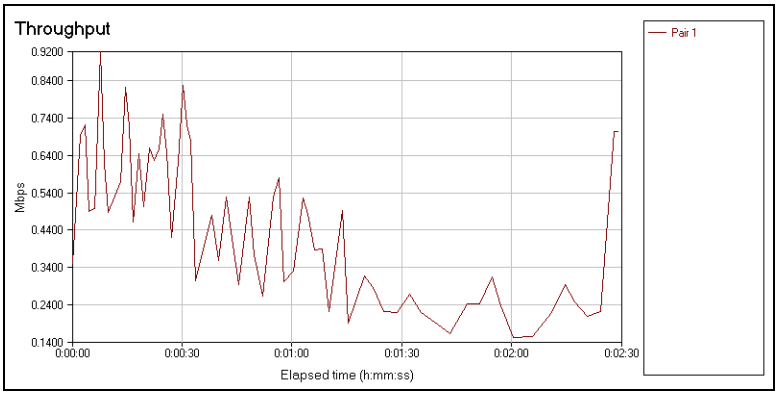

Figure B. 8: Downlink TCP Throughput @ 60 mph

- Average Downlink Throughput: 0.354 Mbps

- Average Response Time: 2.260 seconds
- Total Bytes Sent by *Desktop*: 6,600,000
- Total Bytes Received by *Desktop*: 66

B.3.2 UDP Throughput Test

At 40 mph

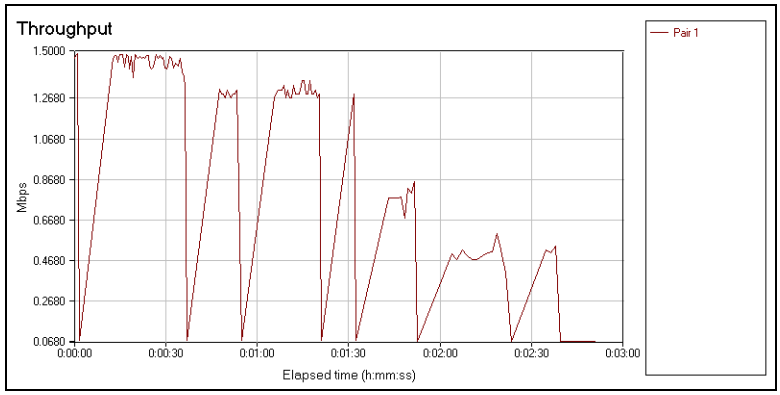

Figure B. 9: Downlink UDP Throughput @ 40 mph

- Average Downlink Throughput: 0.548 Mbps
- Average Response Time: 1.460 seconds
- Total Bytes Sent by *Desktop*: 11,700,000
- Total Bytes Received by *Desktop*: 117

At 60 mph

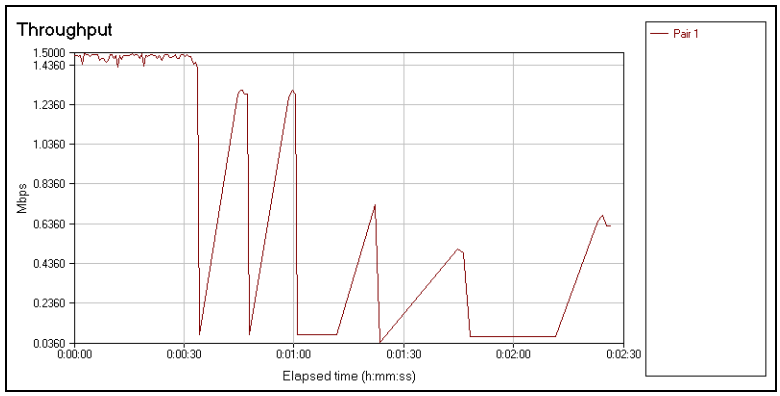

Figure B. 10: Downlink UDP Throughput @ 60 mph

- Average Downlink Throughput: 0.469 Mbps
- Average Response Time: 1.706 seconds
- Total Bytes Sent by *Desktop*: 8,600,000
- Total Bytes Received by *Desktop*: 86

B.4 Two-User Mutual Full-Duplex Throughput

The following results are a continuation of the Section 5.6.

B.4.1 TCP/IP File Transfer Test

At 40 mph

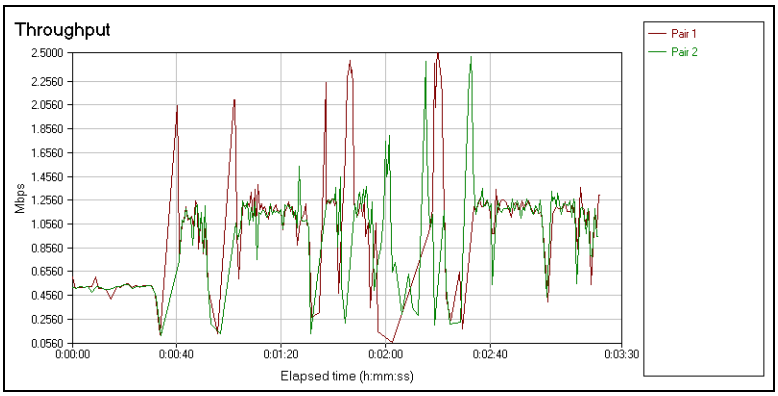

Figure B. 11: Two-User Mutual Full-Duplex TCP File Send Throughput @ 40 mph

- Pair 1: From *Laptop* 1 to *Laptop* 2
  - Average Throughput: 0.808 Mbps
  - Average Response Time: 990 ms
  - Bytes Sent By *Laptop* 1: 20,400,000
  - Bytes Received By *Laptop* 1: 204
- Pair 2: From *Laptop* 2 to *Laptop* 1
  - Average Throughput: 0.798 Mbps
  - Average Response Time: 1,002 ms
  - Bytes Sent By *Laptop* 2: 20,100,000
  - Bytes Received By *Laptop* 2: 201
- Totals:
  - Total Average Throughput: 1.603 Mbps
  - Average Response Time: 996 ms

At 60 mph

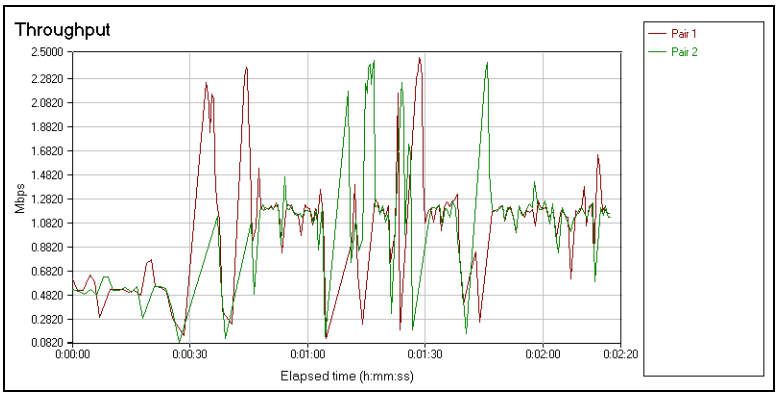

Figure B. 12: Two-User Mutual Full-Duplex TCP File Send Test Throughput @ 60 mph

- Pair 1: From *Laptop* 1 to *Laptop* 2
  - Average Throughput: 0.840 Mbps
  - Average Response Time: 952 ms
  - Bytes Sent By *Laptop* 1: 14,400,000
  - Bytes Received By *Laptop* 1: 144
- Pair 2: From *Laptop* 2 to *Laptop* 1
  - Average Throughput: 0.792 Mbps
  - Average Response Time: 1,010 ms
  - Bytes Sent By *Laptop* 2: 13,600,000
  - Bytes Received By *Laptop* 2: 136
- Totals:
  - Total Average Throughput: 1.630 Mbps
  - Average Response Time: 981 ms

B.4.2 UDP/IP File Transfer Test

At 40 mph

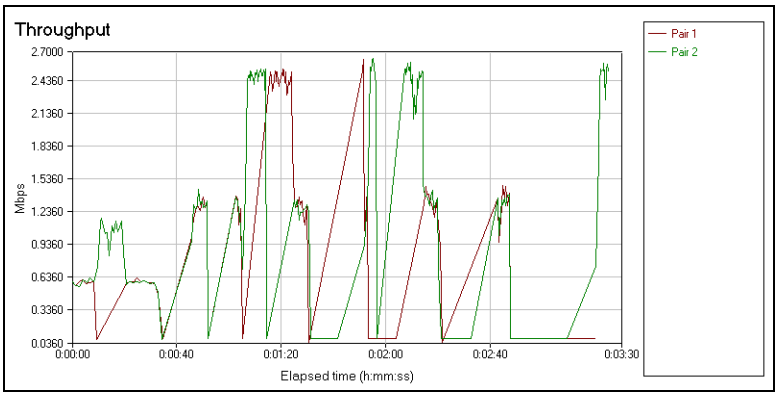

Figure B. 13: Two-User Mutual Full-Duplex UDP File Send Test Throughput @ 40 mph

- Pair 1: From *Laptop* 1 to *Laptop* 2
  - Average Throughput: 0.408 Mbps
  - Average Response Time: 1.962 seconds
  - Bytes Sent By *Laptop* 1: 10,200,000
  - Bytes Received By *Laptop* 1: 102
- Pair 2: From *Laptop* 2 to *Laptop* 1
  - Average Throughput: 0.612 Mbps
  - Average Response Time: 1.307 seconds
  - Bytes Sent By *Laptop* 2: 15,700,000
  - Bytes Received By *Laptop* 2: 157
- Totals:
  - Total Average Throughput: 1.009 Mbps
  - Average Response Time: 1.634 seconds

At 60 mph

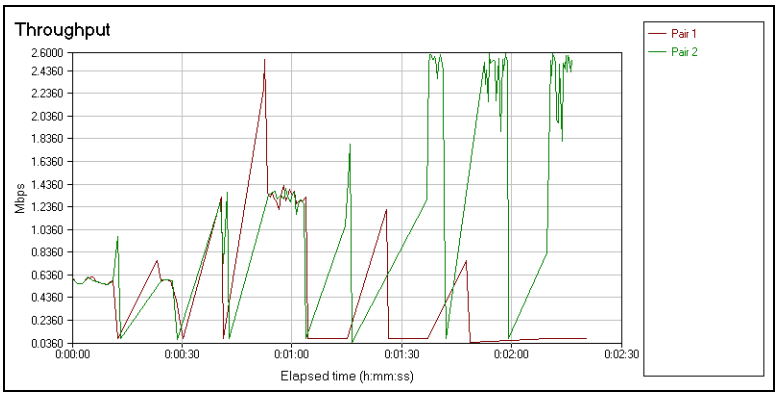

Figure B. 14: Two-User Mutual Full-Duplex UDP File Send Test Throughput @ 60 mph

- Pair 1: From *Laptop* 1 to *Laptop* 2
  - Average Throughput: 0.267 Mbps
  - Average Response Time: 2.991 seconds
  - Bytes Sent By *Laptop* 1: 4,700,000
  - Bytes Received By *Laptop* 1: 47
- Pair 2: From *Laptop* 2 to *Laptop* 1
  - Average Throughput: 0.568 Mbps
  - Average Response Time: 1.409 seconds
  - Bytes Sent By *Laptop* 2: 9,700,000
  - Bytes Received By *Laptop* 2: 97
- Totals:
  - Total Average Throughput: 0.819 Mbps
  - Average Response Time: 2.200 seconds

References and Bibliography

[802.11] IEEE, "IEEE Std. 802.11 – 1997, Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1997.

[802.11a] IEEE, "IEEE Std. 802.11a – 1999, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 1: High-Speed Physical Layer in the 5 GHz Band," 1999.

[802.11b] IEEE, "IEEE Std. 802.11b – 1999, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 2: Higher-Speed Physical Layer Extension in the 2.4 GHz Band," 1999.

[802.11b Cor 1] IEEE, "IEEE Std. 802.11b – 1999/Cor 1 – 2001, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 2: Higher-Speed Physical Layer Extension in the 2.4 GHz Band – Corrigendum 1," 2001.

[802.11d] IEEE, "IEEE Std. 802.11d – 2001, IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless

LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 3: Specification for Operation in Additional Regulatory Domains", 2001.

[8802-11] ISO/IEC, and ANSI/IEEE, "ISO/IEC 8802-11; ANSI/IEEE Std. 802.11, 1999 edition, Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.

[Ala01] J. Ala-Laurila, J. Mikkonen, and J. Rinnemaa, **"**Wireless LAN access network architecture for mobile operators,*" IEEE Communications Magazine*, vol. 39, no. 11, pp. 82 – 89, Nov 2001.

[Arr01] M.G. Arranz, R. Aguero, L. Munoz, and P. Mahonen, "Behavior of UDP-based applications over IEEE 802.11 wireless networks," in *Proc. of the 12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2001,* vol. 2, Sep/Oct 2001, pp. F-72 – F-77 vol. 2.

[Ban02] K. Ban, and H. Gharavi, " Video transmission for multi-hop networks using IEEE 802.11 FHSS," in *Proc. of the International Conference on Image Processing, 2002,* vol. 1, 2002, pp. I-13 – I-20 vol. 1.

[Bin99] B. Bing, "Measured Performance of the IEEE 802.11 wireless LAN," in *Proc. of the Conference on Local Computer Networks, 1999, LCN '99,* Oct 1999, pp. 34 – 42.

[Bluetooth] *The official Bluetooth website*. [Online]. Available: http://www.bluetooth.com

[CEPT] *The European Conference of Postal and Telecommunications Administrations*. [Online]. Available: http://www.cept.org

[Cla02] M.V. Clark, K. K. Leung, B. McNair, and Z. Kostic, "Outdoor IEEE 802.11 cellular networks: radio link performance," in *Proc. of the IEEE International*

Conference on Communications, 2002, ICC 2002, vol. 1, 2002, pp. 512 – 516.

[ETSI] *The European Telecommunications Standards Institute*. [Online]. Available: http://www.etsi.org

[FCC] United States' *Federal Communications Commission.* [Online]. Available: http://www.fcc.gov

[Fleeman] *Fleeman Anderson & Bird, Inc., USA.* [Online].
Available: http://www.fab-corp.com

[Fre01] M. Freytes, C. E. Rodriguez, and C. A. Marques, "Real-time H.263+ video transmission on 802.11 wireless LANs," in *Proc. of the International Conference on Information Technology: Coding and Computing, 2001*, Apr 2001, pp. 125 – 129.

[Gas02] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide,* Sebastopol, CA: O'Reilly & Associates, 2002.

[Gei02] J. Geier, *Wireless LANs: Implementing High Performance IEEE 802.11 Networks,* 2nd edition, Indianapolis, Indiana: Sams, 2002.

[H2GF] *HiperLAN/2 Global Forum*. [Online]. Available: http://www.hiperlan2.com

[Hil01] A. Hills, "Large-Scale Wireless LAN Design," *IEEE Communications Magazine*, vol. 39, no. 11, pp. 98 – 107, Nov 2001.

[HomeRF] *HomeRF Working Group*. [Online]. Available: http://www.homerf.org

[Hop99] M. Hope, and N. Linge, " Determining the propagation range of IEEE 802.11 radio LANs for outdoor applications," in *Proc. of the Conference on Local Computer Networks, 1999, LCN' 99*, Oct 1999, pp. 49 – 50.

[Hun02] Hsieh Hung-Yun, and R. Sivakumar, "IEEE 802.11 over Multi-hop Wireless

Networks: Problems and New Perspectives," in *Proc. of the 2002 IEEE 56th Vehicular Technology Conference, 2002, VTC 2002-Fall*, vol. 2, 2002, pp. 748 – 752 vol. 2.

[HyperLink] *HyperLink Technologies, Inc.* [Online]. Available: http://www.hyperlinktech.com

[IEEE] *The Institute of Electrical and Electronics Engineers, Inc., USA*. [Online]. Available: http://www.ieee.org

[IETF] *The Internet Engineering Task Force*. [Online]. Available: http://www.ietf.org

[Intel] *Intel Corporation.* [Online]. Available: http://www.intel.com

[ISO] *International Organization for Standardization.* [Online]. Available: http://www.iso.ch

[ITU] *International Telecommunication Union*. [Online]. Available: http://www.itu.int

[Kam02] M. Kamenetsky, and M. Unbehaun, "Coverage Planning for Outdoor Wireless LAN Systems," in *Proc. of the 2002 International Zurich Seminar on Broadband Communications, 2002, Access, Transmission, Networking,* 2002, pp. 49-1 – 49-6.

[Lar02] J. LaRocca, and R. LaRocca, *802.11 Demystified,* New York: McGraw-Hill, 2002.

[Leu02] K. K. Leung, B. McNair, L. J. Cimini Jr., and J. H. Winters, "Outdoor IEEE 802.11 Cellular Networks: MAC Protocol Design and Performance," in *Proc. of IEEE International Conference on Communications, 2002, ICC 2002,* vol. 1, 2002, pp. 595 – 599.

[Lin99] Ying-Dar Lin, Yu-Ching Hsu, Kuan-Wen Oyang, Tzu-Chieh Tsai, and Dong-

Su Yang, "Multihop Wireless IEEE 802.11 LANs: A Prototype Implementation," in *Proc. of the 1999 IEEE International Conference on Communications, 1999, ICC' 99*, vol. 3, 1999, pp. 1568 – 1572 vol. 3.

[Microsoft] *Microsoft Inc., USA*. [Online]. Available: http://www.microsoft.com

[MPRG] *The Mobile and Portable Radio Research Group at Virginia Tech*. [Online]. Available: http://www.mprg.org

[NetIQ] *NetIQ Inc., USA*. [Online]. Available: http://www.netiq.com

[Oht02] Y. Ohtani, H. Nakaoka, T. Tomaru, K. Maruyama, T. Chiba, T. Onoye, and L. Shirakawa, "Implementation of Wireless MPEG2 Transmission System Using IEEE 802.11b PHY," in *Proc. of the 2002 Asia-Pacific Conference on Circuits and Systems, 2002, APCCAS' 02,* vol. 1, 2002, pp. 39 – 44 vol. 1.

[ORiNOCO] *ORiNOCO*^{TM}. [Online]. Available: http://www.orinocowireless.com

[Par02] Jin-A Park, Seung-Keun Park, Pyung-Dong Cho, and Kyoung-Rok Cho, "Analysis of spectrum channel assignment for IEEE 802.11b wireless LAN," in *Proc. of the 5th International Symposium on Wireless Personal Multimedia Communications, 2002*, vol. 3, 2002, pp. 1073 – 1077.

[Pen01] Yong Peng, Haitao Wu, Keping Long, and Shiduan Cheng, "Simulation Analysis of TCP Performance on IEEE 802.11 Wireless LAN," in *Proc. of the 2001 International Conferences on Info-tech and Info-net, 2001, ICII 2001 – Beijing*, vol. 2, 2001, pp. 520 – 525 vol. 2.

[Pet95] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications,* Upper Saddle River, NJ: Prentice Hall, 1995.

[Pet00] L. L. Peterson, and B. S. Davie, *Computer Networks: A Systems Approach*, 2nd edition, San Diego, CA: Academic Press, 2000.

[PLLAN] "Power Line Local Area Networking," *IEEE Communications Magazine,* vol. 41, no. 4, pp. 32 – 70, April 2003.

[Pra99] A. R. Prasad, "Performance Comparison of Voice over IEEE 802.11 Schemes," in *Proc. of the IEEE VTS 50th Vehicular Technology Conference, 1999, VTC 1999 – Fall,* vol. 5, 1999, pp. 2636 – 2640 vol. 5.

[Pro01] J. G. Proakis, *Digital Communications,* 4th edition, New York: McGraw-Hill, 2001.

[Pro02] C. Prommak, J. Kabara, D. Tipper, and C. Charnsripinyo, "Next Generation Wireless LAN System Design," in *Proc. of the MILCOM 2002,* vol. 1, 2002, pp. 473 – 477.

[Rag02] S. Raghavan, R. Jordan, H. N. Jerez, and C. T. Abdallah, "Real-time Streaming over an IEEE 802.11b Based Wireless LAN Test Bed," in *Proc. of the 2002 IEEE International Conference on Personal Wireless Communications,* 2002, pp. 155 – 158.

[Rap01] T. S. Rappaport, *Wireless Communications: Principles and Practice,* 2nd edition, Upper Saddle River, NJ: Prentice-Hall, 2001.

[Rui03] Jiang Rui, V. Gupta, and C. V. Ravishankar, "Interactions Between TCP and the IEEE 802.11 MAC Protocol," in *Proc. of the DARPA Information Survivability Conference and Exposition, 2003,* vol. 1, 2003, pp. 273 – 282.

[Sin02] J. P. Singh, N. Bambos, B. Srinivasan, and D. Clawin, "Wireless LAN Performance Under Varied Stress Conditions in Vehicular Traffic Scenarios," in *Proc. of the 2002 IEEE 56th Vehicular Technology Conference, 2002, VTC 2002-Fall,* vol. 2, 2002, pp. 743 – 747 vol. 2.

[Smart Road] *Virginia's Smart Road,* Montgomery County, Virginia. [Online]. Available: http://www.virginiadot.org/projects/constsal-smartrd.asp

[Suz99] T. Suzuki, and S. Tasaka, "Performance Evaluation of Integrated Video and Data Transmission with the IEEE 802.11 Standard MAC Protocol," in *Proc. of the Global Telecommunications Conference, 1999, GLOBECOM' 99,* vol. 1B, 1999, pp. 580 – 586 vol. 1b.

[Telex] *Telex Communications, Inc. : Telex Wireless Networking Technology.* [Online]. Available: http://www.telexwireless.com

[Ter01] J. Terry, and J. Heiskala, *OFDM Wireless LANs: A Theoretical and Practical Guide,* Indianapolis, Indiana: Sams, 2001.

[VDOT] *Virginia Department of Transportation*. [Online]. Available: http://virginiadot.org

[Vee01] M. Veeraraghavan, N. Cocker, and T. Moors, "Support of Voice Services in IEEE 802.11 Wireless LANs," in *Proc. of the IEEE 20th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2001,* vol. 1, 2001, pp. 488 – 497 vol. 1.

[VTTI] *The Virginia Tech Transportation Institute*, Blacksburg, Virginia. [Online]. Available: http://www.vtti.vt.edu

[WECA] *Wireless Ethernet Compatibility Alliance*. [Online]. Available: http://www.weca.net

[Wu01] Haitao Wu, Yong Peng, Keping Long, and Shiduan Cheng, "A simple model of IEEE 802.11 Wireless LAN," in *Proc. of the 2001 International Conference on Info-tech and Info-net, 2001, ICII 2001 – Beijing*, vol. 2, 2001, pp. 514 – 519 vol. 2.

[Xyl01] G. Xylomenos, G. C. Polyzos, P. Mahonen, and M. Saaranen, "TCP Performance Issues over Wireless Links," *IEEE Communications Magazine,* vol. 39, no. 4, pp. 52 – 58, Apr 2001.

[Xyl99] G. Xylomenos, and G. C. Polyzos, "TCP and UDP Performance over a Wireless LAN," in *Proc. of the IEEE 18th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM' 99*, vol. 2, Mar 1999, pp. 439 – 446 vol. 2.

[Zah00] A. Zahedi, and K. Pahlavan, "Capacity of a Wireless LAN with Voice and Data Services," *IEEE Trans. on Communications,* vol. 48, no. 7, pp. 1160 – 1170, Jul 2000.

Vita

Farhan Muhammad Aziz was born on October 7, 1977 in Karachi, Pakistan. He completed his Bachelor of Engineering degree in Electrical Engineering from NED University of Engineering & Technology, Karachi, Pakistan in May 1999 with second merit position out of 158 students. During his studies at NED, he had a chance to work with Siemens Pakistan Engineering Company Private Limited as an Intern for three months and developed a *SIMATIC S-7* PLC (Programmable Logic Controller) based control and automation test bed. After graduating from NED, he worked with Alcatel Pakistan Private Limited as a Field Engineer for a year. His responsibilities with Alcatel were to ensure smooth and continuous operation of a countrywide voice and data communication network consisting of more than sixty communication nodes. Farhan Aziz joined Virginia Polytechnic Institute and State University as a graduate student in the Bradley Department of Electrical & Computer Engineering in Fall 2000. Since March 2001, he has been working with Mobile and Portable Radio Research Group (MPRG), Virginia Tech under the supervision of Prof. Dr. Brian D. Woerner. His primary areas of research and interest include wireless local area networks, space-time codes, and CDMA techniques. He is continuing his studies into the Ph. D. program at Virginia Tech with Prof. Woerner from Fall 2003. Farhan Aziz is a continuing student member of IEEE Inc., USA and IEEE Communications Society since 1998.