NEAR EAST UNIVERSITY

FACULTY OF ENGINEERING

Department of Electrical and Electronic Engineering

THE PERFORMANCE OF VOICE OVER INTERNET PROTOCOL OVER WIRELESS LOCAL AREA NETWORK

Graduation Project
EE-400

Student: Yazan ALZaghah (20000923)

Supervisor: Mr. Izzet Agoren

Nicosia - 2004

ACKNOWLEDGMENT

First of all I would like to thanks Allah {God} for guiding me through m study.

As well as I would like to thanks my parents and my family for supporting an encouraging me accomplish my dream under their custody, and I want handset this project to my parents because without their endless support and love for me, I would never achieve my current position. I wish my mother lives happy always and my father in the heaven is proud of me.

Secondary I have to thanks my supervisor Mr. Izzet Agoren for his prosecutions and his limitless help until I complete my project. Under his guidance, I successfully overcome many difficulties and learn a lot from him. He always help me a lot either in my study or my life.

Also I will not forget my friends in NEU, as they were with me during my stud and I will never forget our nice times in Cyprus, they are really good friends and I hope to them more success in their study and their future life.

List of Abbreviations

Acronym	Definition
ATM	Asynchronous Transfer Mode
CNG	Comfort Noise Generator
DSP	Digital Signal Processor
DSSS	Direct Sequence Spread Spectrum
EST	Eastern Standard Time
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industry, Scientific, and Medical
ITU-T	International Telecommunication Union-Telecommunication
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI/RM	Open Systems Interconnected Reference Model
PCF	Point Coordination Function
PCM	Pulse Code Modulation
VOIP	Voice Over internet protocol
IP	Internet Protocol
LAN	Local Area Network
TCP	Transmission Control Protocol
CCK	Code Complementary Keying
HR	High Rate
WLAN	Wireless Local Area Network
SIP	Session Initiation Protocol
RTP	Real Time Protocol
ROHC	Robust Header Compression
802.11b	IEEE Wireless LAN
CSMA/CD	(Carrier Sense Multiple Accesses/Collision Detection)
CSMA/CA	(Carrier Sense Multiple Accesses/Collision Avoidance)
DSSS	Direct Sequence Spread Spectrum
UDP	User Datagram Protocol

ABSTRACT

(Future wireless) devices and systems must deliver voice, data, messaging, multimedia, and entertainment seamlessly between one another.

This project focuses on the future of VOIP (Voice over Internet Protocol) over wireless infrastructure and devices. The adoption of high bandwidth internet connectivity as well as the proliferation of wireless web enabled devices should accelerate the development of wireless voice and data services over IP. As users access the Internet through high speed and 'always on" connections, the quality and convenience of web based calling increases.

Improved quality, reduced costs and additional value added features for mobiles workforces, and voice and data conferencing will drive VOIP usage. In fact, IP telephony may be the primary industry driver for the build out of wireless LANs. The proliferation of wireless LANs may reduce the demand for capita intensive 3G wireless systems by providing the connectivity that most people need without the high costs associated with 3G.

TABLE OF CONTENTS

INTRODUCTION

The incredible growth of two leading technologies, wireless LAN and Voice over IP (VOIP), has come together to provide an exciting new application, Voice over Wireless LANs (VOWLANs). The most prevalent usage of VOWLAN today is in the retail, warehousing, manufacturing, and healthcare, education, and hospitality industries. Employees in these industries are more mobile than the average office worker and have specific application needs that lend well to handheld devices. Adding VOWLAN can increase productivity and responsiveness for mobile employees in the workplace.

The aim of this project is to test the performance of Voice Over Internet Protocol over Wireless Local Area Network. This project contains four chapters, Introduction To Voice Over IP Over WLAN, Background, Experiments, and Results.

In the first chapter I will give an overview of Voice Over IP Over WLAN and the protocols that are used in VOIP over WLAN.

In the second chapter I will discuss in detail about the background and functions of different protocols that are being used in my project.

In the third chapter we will practically demonstrate applications of voice over IP over WLAN.

In the fourth chapter we will discuss the results that were obtained from the tests performed and described in experiment chapter.

CHAPTER ONE

INTRODUCTION TO VOICE OVER IP OVER WLAN

The emergence of VOIP technology has presented network managers with a practical solution for combining voice and data over one network. VOIP has proven to be a viable and cost-effective alternative to circuit-switched voice networks, and is promising to extend those same benefits to high-performance teams of mobile employees within your enterprise.

As the pace of business continues to accelerate, mobile communication is a tool of ever-increasing strategic importance. Success or failure on an objective can result from the ability or inability to immediately access and distribute information throughout the enterprise.

Utilizing IP as the ubiquitous transport offers the enterprise significant statistical gains in bandwidth efficiency, lower overall bandwidth requirements, ease of management, and the ability to deploy new applications rapidly. On the WLAN, data and voice share a common infrastructure. By contrast, legacy disparate networks constitute a use-it or lose-it model. When voice is quiescent, data can utilize the available bandwidth; when voice applications are active, they can be guaranteed the bandwidth required. Therefore, the ability to converge voice and data over a single wireless local area network can result in significant cost savings and allows for the development of new applications that increase productivity and efficiency.

The incredible growth of two leading technologies, wireless LAN and Voice over IP (VOIP), has come together to provide an exciting new application, Voice over Wireless LANs (VOWLANs). The most prevalent usage of VOWLAN today is in the retail, warehousing, manufacturing, and healthcare, education, and hospitality industries. Employees in these industries are more mobile than the average office worker and have specific application needs that lend well to handheld devices. Adding VOWLAN can increase productivity and responsiveness for mobile employees in the workplace.

Enabling VOWLAN requires a WLAN infrastructure capable of providing seamless mobility to allow for high-quality voice connections. Some manufacturers have designed unique WLAN solution that allows mobile users to roam throughout the network without requiring the Access Point (AP) AP-to-AP hand-off delays that plague traditional WLAN deployments. Instead of requiring users to re-associate and re-authenticate as they mobilize throughout the network, with commensurate delays in the hundreds of milliseconds, the Airflow solution provides a WLAN deployment that eliminates the re-association and re-authentication requirements. The end result is seamless mobility that reduces the 300-500ms delay common with AP-to-AP hand-offs to under 20ms, enabling high-quality VOWLAN deployments.

1.1 Overview of TCP/IP

TCP/IP is made up of two acronyms, TCP, for Transmission Control Protocol, and IP, for Internet Protocol. TCP handles packet flow between systems and IP handles the routing of packets. However, that is a simplistic answer that we will expand on further.

All modern networks are now designed using a layered approach. Each layer presents a predefined interface to the layer above it. By doing so, a modular design can be developed so as to minimize problems in the development of new applications or in adding new interfaces.

1.2 Overview of H.323

H.323 is the globally accepted standard for audio/video/data communication. It specifically describes how multimedia communications occur between user terminals, network equipment, and assorted services on Local and Wide Area Internet Protocol (IP) networks.

Activity around H.323 is especially high due to the unified support of a global coalition of companies, including personal computer and communications systems manufacturers, and operating systems makers.H.323-compliance has also been promoted and accepted by Internet Phone and Voice-Over-IP manufacturers as the standard for interoperability.

H.323 is sometimes referred to as an "umbrella" specification, meaning that in the document itself there are references to other recommendations. Other recommendations in the H.323 series include H.225.0 packet and synchronization, H.245 control, H.261 and H.263 video codes, G.711, G.722, G.728, G.729, and G.723 audio codes, and the T.120 series of multimedia communications protocols.

Together, these specifications define a number of new network components -- H.323 terminal, H.323 Gatekeeper and H.323 Gateway)--all of which interoperate with other standards-compliant end points and networks by virtue of an H.323/H.32X gateway.

1.3 802.11b Overview

The IEEE 802.11b is a Direct Sequence Spread Spectrum (DSSS) system very similar in concept to the CDMA Wireless, using a spread spectrum chip sequence.

In the 802.11b the transmission medium is wireless and the operating frequency band is 2.4 GHz. 802.11b provides 5.5 and 11 Mbps payload data rates in addition to the 1 and 2 Mbps rates provided by 802.11. To provide the higher rates, 8 chip Complementary Code Keying (CCK) is employed as the modulation scheme. The CCK uses 6 bits to encode the code sent, this increase the speed of the 802.11 by 6.The chipping rate is 11 MHz, which is the same as the DSSS system as described in 802.11, thus providing the same occupied channel bandwidth.

802.11b describes an optional mode replacing the CCK modulation with packet binary convolution coding (HR/DSSS/PBCC).

Another optional mode of 802.11b allows data throughput at the higher rates (2, 5.5, and 11 Mbps) to be significantly increased by using a shorter PLCP preamble. This mode is called HR/DSSS/short. This Short Preamble mode can coexist with DSSS, HR/DSSS under limited circumstances, such as on different channels or with appropriate CCA mechanisms.

The High Rate PHY contains three functional entities: the PMD function, the physical layer convergence function, and the layer management function. For the purposes of

MAC and MAC Management when channel agility is both present and enabled, the High Rate PHY shall be interpreted to be both a High Rate and a frequency hopping physical layer. The High Rate PHY service shall be provided to the MAC through the PHY service primitives.

CHAPTER TWO

BACKGROUND

2.1 Introduction

Here by this chapter we will discuss in detail about the background and functions of different protocols that are being used in my project. We will discuss the background and functions of the following protocols:

1. H.323 (Multimedia Protocol)

2. RTP (Real Time Protocol)

3.802.11b (IEEE Wireless LAN)

4. TCP/IP (Transmission Control Protocol/Internet Protocol)

5. UDP (User Datagram Protocol)

6. CSMA/CD (Carrier Sense Multiple Accesses / Collision Detection.)

7. CSMA/CA (Carrier Sense Multiple Accesses / Collision Avoidance)

2.2 Background of H.323

H.323 is the globally accepted standard for audio/video/data communication. It specifically describes how multimedia communications occur between user terminals, network equipment, and assorted services on Local and Wide Area Internet Protocol (IP) networks.

Activity around H.323 is especially high due to the unified support of a global coalition of companies, including personal computer and communications systems manufacturers, and operating systems makers. H.323-compliance has also been promoted and accepted by Internet Phone and Voice-Over-IP manufacturers as the standard for interoperability.

H.323 is sometimes referred to as an "umbrella" specification, meaning that in the document itself there are references to other recommendations. Other recommendations in the H.323 series include H.225.0 packet and synchronization, H.245 control, H.261 and H.263 video codes, G.711, G.722, G.728, G.729, and G.723 audio codes, and the T.120 series of multimedia communications protocols.

Together, these specifications define a number of new network components -- H.323 terminal, H.323 Gatekeeper and H.323 Gateway--all of which interoperate with other standards-compliant end points and networks by virtue of an H.323/H.32X gateway.

In the past, computer product designers and manufacturers were less clearly influenced by (or allowed to influence) the telecommunications industry than they are today. Telecommunications design specifications evolved gradually over nearly a century, and, for a substantial portion of this time, with the support and direction of government regulation. Telecommunications products customers demand 99.9% reliability and end point equipment interoperability.

In contrast, the computer industry is renown for releasing products early in test markets, and customers tolerate a relatively low level of reliability and interoperability, accepting defector standards whenever necessary (e.g., lowest cost of ownership). Until the industry wide adoption of the H.320 standard for multimedia communications over

ISDN, computer systems and peripheral manufacturers had little to do with specifications published by international telecommunications standards bodies.

Collaboration between telecommunications and computer industry leaders rose dramatically during the development of H.323. The result is that the specification has progressed rapidly and draws upon experiences and innovation from both industries. Global adoption of the ITU-T H.323 assures developers, manufacturers and their customer's interoperability and highly functional products and services more quickly than would otherwise be possible. And the fact that H.323 promises these products and services on non-guaranteed Quality of Service networks is even more significant.

The Internet protocol for non-guaranteed Quality of Service networks offers ubiquity unlike any earlier networking protocols. Ubiquity and ease of use fueling the emergence of IP telephony and multimedia conference as a mass market phenomenon.

2.2.1 H.323 Goes Mainstream

H.323 applications are becoming mainstream for the following reasons:

• IP LANs are becoming more powerful. Ethernet bandwidth is migrating from 10 Mbps to 100 Mbps, and Gigabit Ethernet is already on the horizon.

• By providing device-to-device, application-to-application, and vendor-to-vendor interoperability, H.323 allows customer's products to interoperate with other H.323-compliant products.

• PCs are becoming more powerful multimedia platforms due to faster processors, enhanced instruction sets, and powerful multimedia accelerator chips.

• H.323 provides standards for interoperability between LANs and other networks.

• Network loading can be managed. With H.323, the network manager can restrict the amount of network bandwidth available for conferencing. Multicast support also reduces bandwidth requirements.

• H.323 has the support of many computing and conferencing companies and organizations, including Intel, Microsoft and Netscape. Their efforts will generate a higher level of awareness in the market.

The size of the market potential and pace of innovation in this environment makes the H.323 standard the critical building block for a broad new range of collaborative LAN/WAN-based applications for multimedia communications.

2.3 Background of (RTP)

2.3.1 RTP - Real-time Transport Protocol

Real-time transport protocol (RTP) is an IP-based protocol providing support for the transport of real-time data such as video and audio streams. The services provided by RTP include time reconstruction, loss detection, security and content identification. RTP is primarily designed for multicast of real-time data, but it can be also used in unicast. It can be used for one-way transport such as video-on-demand as well as interactive services such as Internet telephony.

RTP is designed to work in conjunction with the auxiliary control protocol RTCP to get feedback on quality of data transmission and information about participants in the on-going session.

2.3.2 How Does RTP Works

As discussed in the first section, Internet is a shared datagram network. Packets sent on the Internet have unpredictable delay and jitter. But multimedia applications require appropriate timing in data transmission and playing back. RTP provides timestamping, sequence numbering, and other mechanisms to take care of the timing issues. Through these mechanisms, RTP provides end-to-end transport for real-time data over datagram network.

Timestamping is the most important information for real-time applications. The sender sets the timestamp according to the instant the first octet in the packet was sampled. Timestamps increase by the time covered by a packet. After receiving the data packets, the receiver uses the timestamp to reconstruct the original timing in order to play out the data in correct rate. Timestamp is also used to synchronize different streams with timing properties, such as audio and video data in MPEG. However, RTP itself is not responsible for the synchronization. This has to be done in the application level.

UDP does not deliver packets in timely order, so sequence numbers are used to place the incoming data packets in the correct order. They are also used for packet loss detection. Notice that in some video format, when a video frame is split into several RTP packets, all of them can have the same timestamp. So just timestamp is not enough to put the packets in order.

The payload type identifier specifies the payload format as well as the encoding/compression schemes. From this payload type identifier, the receiving application knows how to interpret and play out the payload data. Default payload types are defined in RFC 1890. Example specifications include pulse code modulation (PCM), MPEG1/MPEG2 audio and video, JPEG video, Sun Cell B video, H.261 video streams, et al. More payload types can be added by providing a profile and payload format specification. At any given time of transmission, an RTP sender can only send one type of payload, although the payload type may change during transmission, for example, to adjust to network congestion.

Another function is source identification. It allows the receiving application to know where the data is coming from. For example, in an audio conference, from the source identifier a user could tell who is talking.

RTP is typically run on top of UDP to make use of its multiplexing and checksum functions. TCP and UDP are two most commonly used transport protocols on the Internet. TCP provides a connection-oriented and reliable flow between two hosts, while UDP provides a connectionless but unreliable datagram service over the network. UDP was chosen as the target transport protocol for RTP because of two reasons. First, RTP is primarily designed for multicast; the connection-oriented TCP does not scale well and therefore is not suitable. Second, for real-time data, reliability is not as important as timely delivery. Even more, reliable transmission provided by retransmission as in TCP is not desirable. For example, in network congestion, some packets might get lost and the application would result in lower but acceptable quality.

If the protocol insists a reliable transmission, the retransmitted packets could possibly increase the delay, jam the network, and eventually starve the receiving application.

RTP and RTCP packets are usually transmitted using UDP/IP service. However, efforts have been made to make them transport-independent so they can be also run on CLNP (Connectionless Network Protocol), IPX (Internet work Packet Exchange), AAL5/ATM or other protocols.

In practice, RTP is usually implemented within the application. Many issues, such as lost packet recovery Multimedia over IP: RSVP, RTP, RTCP, RTSP and congestion control, have to be implemented in the application level.

To set up an RTP session, the application defines a particular pair of destination transport addresses (one network address plus a pair of ports for RTP and RTCP). In a multimedia session, each medium is carried in a separate RTP session, with its own RTCP packets reporting the reception quality for that session. For example, audio and video would travel on separate RTP sessions, enabling a receiver to select whether or not to receive a particular medium.

An audio-conferencing scenario presented in RFC 1889 illustrates the use of RTP. Suppose each participant sends audio data in segments of 20 ms duration. Each segment of audio data is preceded by an RTP header, and then the resulting RTP message is placed in a UDP packet. The RTP header indicates the type of audio encoding that is used, e.g., PCM. Users can opt to change the encoding during a conference in reaction to network congestion or, for example, to accommodate low-bandwidth requirements of a new conference participant. Timing information and a sequence number in the RTP header are used by the receivers to reconstruct the timing produced by the source, so that in this example, audio segments are contiguously played out at the receiver every 20 ms.

2.4 Background of 802.11b

IEEE 802.11 specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps using either Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS). In IEEE 802.11b data is encoded using DSSS (Direct Sequence Spread Spectrum) technology. DSSS works by taking a data stream of zeros and ones and modulating it with a second pattern, the chipping sequence. In 802.11, that sequence is known as the Barker code, which is an 11 bits sequence (10110111000) that has certain mathematical properties making it ideal for modulating radio waves. The basic data stream is XOR'd with the Barker code to generate a series of data objects called chips. Each bit is "encoded" by the 11bits Barker code, and each group of 11 chips encodes one bit of data.

IEEE 802.11b uses 64 Complementary Code Keying (CCK) chipping sequences to achieve 11 Mbps. Rather than using the Barker code, CCK uses a series of codes called Complementary Sequences. Because there are 64 unique code words that can be used to encode the signal, up to 6 bits can be represented by any one particular code word (instead of the 1 bit represented by a Barker symbol).

The wireless radio generates a 2.4 GHz carrier wave (2.4 to 2.483 GHz) and modulates that wave using a variety of techniques. For 1 Mbps transmission, Binary Phase Shift Keying (BPSK) is used (one phase shift for each bit). To accomplish 2 Mbps transmission, Quadrate Phase Shift Keying (QPSK) is used. QPSK uses four rotations (0, 90, 180 and 270 degrees) to encode 2 bits of information in the same space as BPSK encodes 1. The trade-off is increase power or decrease range to maintain signal quality. Because the Federal Communications Commission (FCC) regulates output power of portable radios to 1 watt equivalent isotropic radiated power (EIRP), range is the only remaining factor that can change. On 802.11 devices, as the transceiver moves away from the radio, the radio adapts and uses a less complex (and slower) encoding mechanism to send data.

The MAC layer communicates with the PLCP via specific primitives through a PHY service access point. When the MAC layer instructs, the PLCP prepares MPDUs for transmission. The PLCP also delivers incoming frames from the wireless medium to the

MAC layer. The PLCP sub layer minimizes the dependence of the MAC layer on the PMD sub layer by mapping MPDUs into a frame format suitable for transmission by the PMD.

Under the direction of the PLCP, the PMD provides actual transmission and reception of PHY entities between two stations through the wireless medium. To provide this service, the PMD interfaces directly with the air medium and provides modulation and demodulation of the frame transmissions. The PLCP and PMD communicate using service primitives to govern the transmission and reception functions.

The CCK code word is modulated with the QPSK technology used in 2 Mbps wireless DSSS radios. This allows for an additional 2 bits of information to be encoded in each symbol. Eight chips are sent for each 6 bits, but each symbol encodes 8 bits because of the QPSK modulation. The spectrum math for 1 Mbps transmission works out as 11 M chips per second times 2 MHz equals 22 MHz of spectrum. Likewise, at 2 Mbps, 2 bits per symbol are modulated with QPSK, 11 M chips per second, and thus have 22 MHz of spectrum. To send 11 Mbps 22 MHz of frequency spectrum is needed.

It is much more difficult to discern which of the 64 code words is coming across the airwaves, because of the complex encoding. Furthermore, the radio receiver design is significantly more difficult. In fact, while a 1 Mbps or 2 Mbps radio has one correlate (the device responsible for lining up the various signals bouncing around and turning them into a bit stream), the 11 Mbps radio must have 64 such devices.

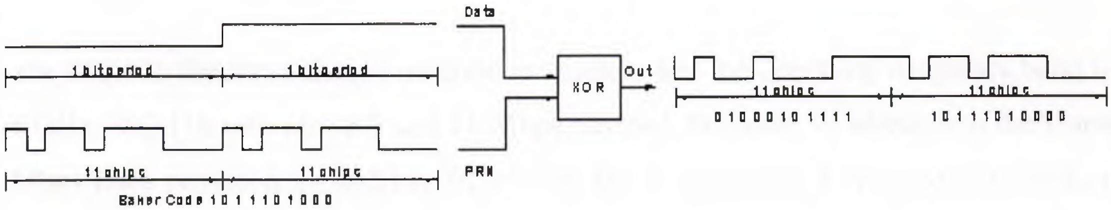

Figure 2.1 Digital Modulation of Data with PRN sequence

The wireless physical layer is split into two parts, called the PLCP (Physical Layer Convergence Protocol) and the PMD (Physical Medium Dependent) sub layer. The

PMD takes care of the wireless encoding. The PLCP presents a common interface for higher-level drivers to write to and provides carrier sense and CCA (Clear Channel Assessment), which is the signal that the MAC (Media Access Control) layer needs so it can determine whether the medium is currently in use.

The PLCP consists of a 144 bits preamble that is used for synchronization to determine radio gain and to establish CCA. The preamble comprises 128 bits of synchronization, followed by a 16 bits field consisting of the pattern 1111001110100000. This sequence is used to mark the start of every frame and is called the SFD (Start Frame Delimiter).

The next 48 bits are collectively known as the PLCP header. The header contains four fields: signal, service, length and HEC (header error check). The signal field indicates how fast the payload will be transmitted (1, 2, 5.5 or 11 Mbps). The service field is reserved for future use. The length field indicates the length of the ensuing payload, and the HEC is 16 bits CRC of the 48 bits header.

In a wireless environment, the PLCP is always transmitted at 1 Mbps. Thus, 24 bytes of each packet are sent at 1 Mbps. The PLCP introduces 24 bytes of overhead into each wireless Ethernet packet before we even start talking about where the packet is going. Ethernet introduces only 8 bytes of data. Because the 192 bits header payload is transmitted at 1 Mbps, 802.11b is at best only 85 percent efficient at the physical layer.

The IEEE 802.11b is a Direct Sequence Spread Spectrum (DSSS) system very similar in concept to the CDMA Wireless, using a spread spectrum chip sequence.

In the 802.11b the transmission medium is wireless and the operating frequency band is 2.4 GHz. 802.11b provides 5.5 and 11 Mbps payload data rates in addition to the 1 and 2 Mbps rates provided by 802.11. To provide the higher rates, 8 chip Complementary Code Keying (CCK) is employed as the modulation scheme. The CCK uses 6 bits to encode the code sent, this increase the speed of the 802.11 by 6.The chipping rate is 11 MHz, which is the same as the DSSS system as described in 802.11, thus providing the same occupied channel bandwidth.

802.11b describes an optional mode replacing the CCK modulation with packet binary convolution coding (HR/DSSS/PBCC).

Another optional mode of 802.11b allows data throughput at the higher rates (2, 5.5, and 11 Mbps) to be significantly increased by using a shorter PLCP preamble. This mode is called HR/DSSS/short.

This Short Preamble mode can coexist with DSSS, HR/DSSS under limited circumstances, such as on different channels or with appropriate CCA mechanisms.

The High Rate PHY contains three functional entities: the PMD function, the physical layer convergence function, and the layer management function. For the purposes of MAC and MAC Management when channel agility is both present and enabled, the High Rate PHY shall be interpreted to be both a High Rate and a frequency hopping physical layer. The High Rate PHY service shall be provided to the MAC through the PHY service primitives.

2.5 Background of TCP/IP

TCP/IP is made up of two acronyms, TCP, for Transmission Control Protocol, and IP, for Internet Protocol. TCP handles packet flow between systems and IP handles the routing of packets. However, that is a simplistic answer that we will expound on further.

All modern networks are now designed using a layered approach. Each layer presents a predefined interface to the layer above it. By doing so, a modular design can be developed so as to minimize problems in the development of new applications or in adding new interfaces.

The ISO/OSI protocol with seven layers is the usual reference model. Since TCP/IP was designed before the ISO model was developed it has four layers; however the differences between the two are mostly minor. Below, is a comparison of the TCP/IP and OSI protocol stacks.

2.5.1 OSI Protocol Stack

1. Physical -- The cable or physical connection itself.

2. Data Link -- Transmit and receive packets.

3. Network -- Packet routing.

4. Transport -- Guarantee end-to-end delivery of packets.

5. Session -- Authentication and authorization.

6. Presentation -- Data problems and data compression.

7. Application -- End user services such as email.

2.5.2 TCP/IP Protocol Stack

Below are the major difference between the OSI and TCP/IP:

- The application layer in TCP/IP handles the responsibilities of layers 5, 6, and 7 in the OSI model.
- The transport layer in TCP/IP does not always guarantee reliable delivery of packets as the transport layer in the OSI.
- Model does. TCP/IP offers an option called UDP that does not guarantee reliable packet delivery.

2.6 Background of (UDP): User Datagram Protocol

Contents

1. **What is UDP.**
2. **How it's used.**
3. **Bad things about UDP.**
4. **Good things about UDP.**
5. **Security.**

2.6.1 What is UDP

UDP stands for User Datagram Protocol and is mostly used for broadcasting data over the Internet. Like TCP, UDP runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services and methods. Instead, it offers a way to directly connect to send and receive datagram's over an IP network. UDP is said to be connectionless because there is no use of any kind of "handshaking" method on server or client side. It's always a direct connection. Since TCP/IP is the widely used standard for internet applications a lot of people tend to look down on UDP because of its differences and faults. The good thing about UDP however is that it's straight forward and isn't too complex.

2.6.2 How UDP is used

There are many programs and services that people use that use UDP.I am going to list a few of these services and programs:

- Video Conferencing systems.
- NetBIOS Datagram Service. (Port 138)
- Microsoft Common Internet File System. (Port 445)
- Multiplayer Online Games (Quake 3, UT Series)
- Streaming Multimedia
- Computer Phones.

2.6.3 Bad things about UDP

UDP do little error checking, so if a packet is lost or corrupted it is lost forever.

Not 100% Guaranteed to send all data.

The receipt of a burst of multiple datagram's. The packet information could have been tampered with.

All these bad things about UDP may make the protocol seem very unappealing but UDP can be useful in some situations, and it enjoys one key advantage over TCP: speed. The reliability features built into TCP can be expensive in terms of execution time. Also note that UDP does not preclude reliable message delivery, it merely defers those details to a higher level of the network stack.

2.6.4 Good things about UDP

- Speed.
- There's no real connection establishment. UDP is simply just underlying.
- Unregulated send rate. The sending rate can go to its full potential.

2.6.5 Security Issues

When it comes to UDP and security it all depends on the UDP service that is running on a port and how secure the service is. The service could be vulnerable to hacking if the service has an exploit or a bug in it that allows remote access, overflow, etc. Another aspect of UDP security is the fact that it's underlying, this meaning that there aren't too many user applications that run it so a user wouldn't know that their actually running for example Microsoft Common Internet File System on Port 445 where as in TCP, you could check to see if your running a NetBIOS Session and disable it or see if you have a trojan.

2.7 Background of the CSMA/CD Protocol

The CSMA/CD protocol functions somewhat like a dinner party in a dark room. Everyone around the table must listen for a period of quiet before speaking (Carrier Sense). Once a space occurs everyone has an equal chance to say something (Multiple Accesses). If two people start talking at the same instant they detect that fact, and quit speaking (Collision Detection).

To translate this into Ethernet terms, each interface must wait until there is no signal on the channel, and then it can begin transmitting. If some other interface is transmitting there will be a signal on the channel, which is called carrier. All other interfaces must wait until carrier ceases before trying to transmit, and this process is called Carrier Sense.

All Ethernet interfaces are equal in their ability to send frames onto the network. No one gets a higher priority than anyone else, and democracy reigns. This is what is meant by Multiple Access. Since signals take a finite time to travel from one end of an Ethernet system to the other, the first bits of a transmitted frame do not reach all parts of the network simultaneously. Therefore, it's possible for two interfaces to sense that the network is idle and to start transmitting their frames simultaneously. When this happens, the Ethernet system has a way to sense the "collision" of signals and to stop the transmission and resend the frames. This is called Collision Detect.

The CSMA/CD protocol is designed to provide fair access to the shared channel so that all stations get a chance to use the network. After every packet transmission all stations use the CSMA/CD protocol to determine which station gets to use the Ethernet channel next.

2.8 Background of CSMA/CA

The most important differences between the wireless LAN and the MAC protocol of most wired networking applications is the impossibility to detect collisions. With the receiving and sending antennas immediately next to each other, a station is unable to see any signal but its own. As a result, the complete packet will be sent before the incorrect checksum reveals that a collision has happened. It is therefore of utmost importance that the number of collisions be limited to the absolute minimum.

This is achieved by a protocol called Carrier Sense Multiple Access with Collision Avoidance. The idea is to prevent collisions at the moment they are most likely to occur, i.e. when the bus is released. All clients are forced to wait for a random number of timeslots and then sense the medium again, before starting a transmission. If the medium is sensed to be busy, the client freezes its timer until it becomes free again. Thus, the chance of two clients starting to send simultaneously is reduced.

Of course, the overhead introduced by the Collision Avoidance delays should be as small as possible. On the other hand, the protocol should keep the number of collisions to a minimum, even under the highest possible load. To this end, the range of the random delay, or the contention window, is set to vary with the load. In the case of a collision, the delay is doubled progressively: 15, 31, 63...1023, until a successful transmission occurs and the delay is reset to the minimal value. The 802.11 standard does not fix the minimum and maximum values of the contention window. However, it does advise a minimum of 15 or 31 and a maximum of 1023. The figure below follows the Random Delay (red) and the timer (green) through a collision and a successful transmission. During the whole period the timer can be seen to reset and restart due to the transmissions of other clients.

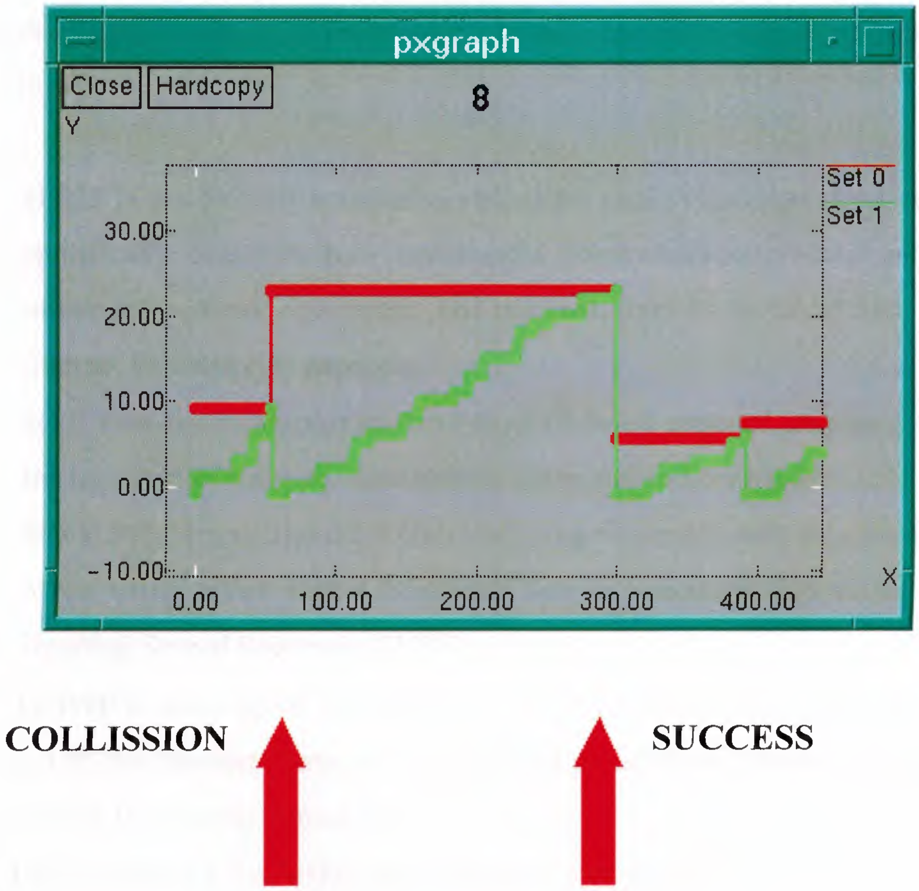

Figure 2.2 Random Delay and the timer through a collision and a successful transmission

2.9 SUMMARY

As we discussed the details of the protocols in this chapter the outline of these protocols is as follows:

- **H.323** is the globally accepted standard for audio/video/data communication. It specifically describes how multimedia communications occur between user terminals, network equipment, and assorted services on Local and Wide Area Internet Protocol (IP) networks.
- **RTP** Real-time transport protocol is an IP-based protocol providing support for the transport of real-time data such as video and audio streams.
- **IEEE 802.11** specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps using either Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS).
- **TCP/IP** is made up of two acronyms, TCP, for Transmission Control Protocol, and IP, for Internet Protocol. TCP handles packet flow between systems and IP handles the routing of packets.
- **UDP** stands for User Datagram Protocol and is mostly used for broadcasting data over the Internet.
- **CSMA/CD** functions as CSMA/CD functions as each interface must wait until there is no signal on the channel, and then it can begin transmitting. If some other interface is transmitting there will be a signal on the channel, which is called carrier. All other interfaces must wait until carrier ceases before trying to transmit, and this process is called Carrier Sense.
- **CSMA/CA** in Carrier Sense Multiple Access with Collision Avoidance. The idea is to prevent collisions at the moment they are most likely to occur.

CHAPTER THREE

EXPERIMENTS

3.1 Introduction

In this chapter we will practically demonstrate applications of voice over IP over WLAN. In this chapter we will perform four experiments from which one is based on wired local area networking and the rest of the three are based on wireless local area networking, we will establish voice communication over IP by using MS Net meeting and check the quality of voice.

3.2 Description of the software and hardware used in the experiments

3.2.1 Winpcap

WinPcap is an architecture for packet capture and network analysis for the Win32 platforms. It includes a kernel-level packet filter, a low-level dynamic link library (packet.dll), and a high-level and system-independent library (wpcap.dll, based on libpcap version 0.6.2).

The packet filter is a device driver that adds to Windows 95, 98, ME, NT, 2000 and XP the ability to capture and send raw data from a network card, with the possibility to filter and store in a buffer the captured packets.

Packet.dll is an API that can be used to directly access the functions of the packet driver, offering a programming interface independent from the Microsoft OS.

Wpcap.dll exports a set of high level capture primitives that are compatible with libpcap, the well known Unix capture library. These functions allow capturing packets in a way independent from the underlying network hardware and operating system.

WinPcap is released under a BSD-style license.

3.2.2 NetMeeting

Microsoft NetMeeting® provides whiteboard, chat, file transfer, application sharing, audio, and video conferencing capabilities intra-ship, ship-to-ship, ship-to-shore, and shore-to-shore. All capabilities are available on SIPRNet. A secure means of conducting ship-to-shore Net Meetings on NIPRNet is not currently available.

NetMeeting is a form of multimedia communication that virtually brings parties together. Originally fielded on some carriers as TeleMaintenance, NetMeeting is a means to virtually collaborate through existing ship/shore hardware and software via satellite connectivity (SIPRNet and NIPRNet) to exchange real time information. NetMeeting is a generic communication tool that can be utilized to address and support virtually any issue or subject area: Medical, Supply, Chaplain, Aviation, Maintenance, Combat Systems, Training, etc.

3.2.3 Windows XP

Microsoft Windows XP is short for Windows Experienced and is the convergence of the two major Microsoft operating systems into one.

Windows XP is available in the following versions:

- Home Edition - Full / Upgrade
- Professional - Full / Upgrade

Windows XP is designed more for users who may not be familiar with all of Windows features and has several new abilities to make the Windows experience easier for those users.

Windows XP includes various new features not found in previous versions of Microsoft Windows.

- New interface - a completely new look and ability to change the look.
- Updates - new feature that automatically obtains updates fro the Internet.
- Internet Explorer 6 - Includes internet explorer 6 and new IM.
- Multilingual support - added support for different languages.

In addition to the above features, Windows XP does increase reliability when compared to previous versions of Microsoft Windows.

3.2.4 Ethereal

Ethereal is a free network protocol analyzer for UNIX and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.

3.2.5 DWL 650+

The DWL-650+ is an enhanced 802.11b card bus featuring advanced silicon chip technology from Texas Instruments. The DWL-650+ is fully compatible with the IEEE 802.11b standard making it inter-operable with all existing 802.11b compliant devices. The DWL-650+ also features 256-bit WEP encryption providing you a higher level of security for your data and communications. Notice that the Trx power is 16 dbm and the RX sensitivity is 80 dbm.

3.3 Test One

In this experiment we will establish a connection between two portable computers using cables (wired). The distance which separates them will be 50 cm.

We will make a voice connection over the internet using MS-net meeting and measure the quality of the voice.

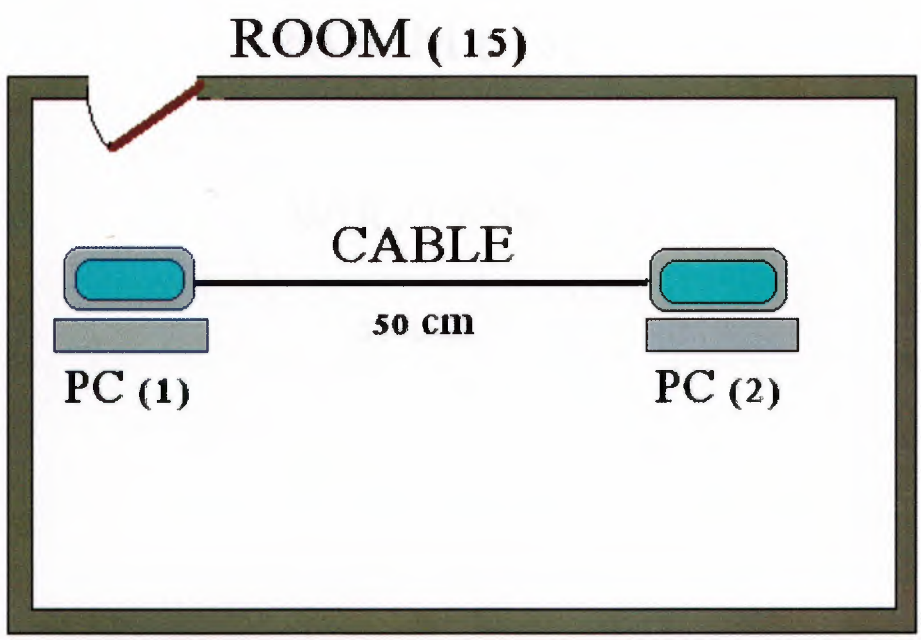

Figure 3.1 wired connections between two portable computers

3.4 Test Two

In this experiment we will establish a wireless connection between two portable computers. The distance which separates them will be 50 cm.

We will make a voice connection over the internet using MS-net meeting and measure the quality of the voice.

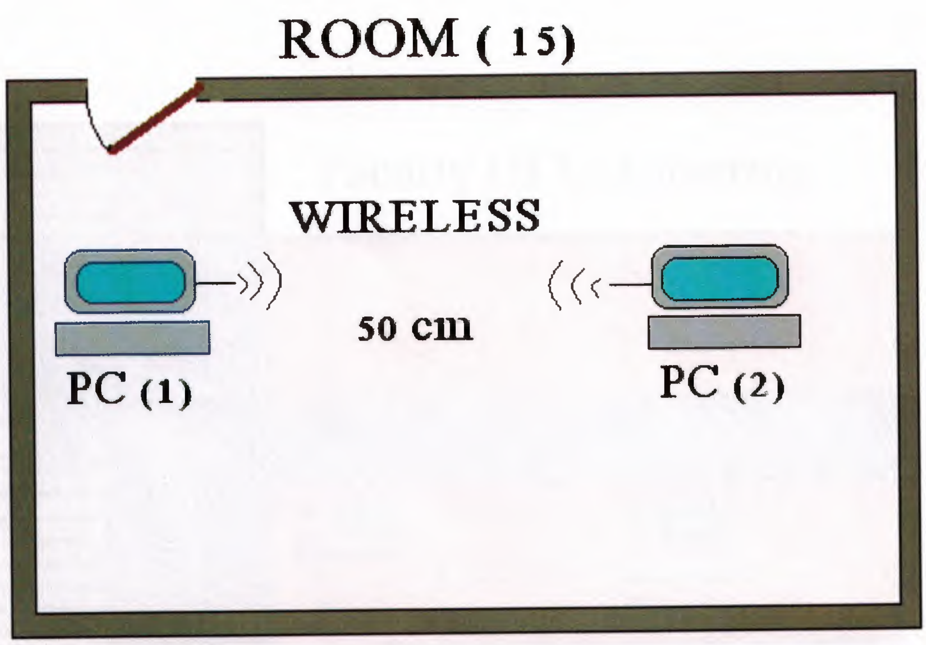

Figure 3.2 Wireless connections between two portable computers

3.5 Test Three

In this experiment we will establish a wireless connection between two portable computers. One which is located at room (15) and the other will be located at the faculty door (approximately separated by 25 m).

Then we will try to establish a call from the portable computer located at the faculty door by using MS-net meeting.

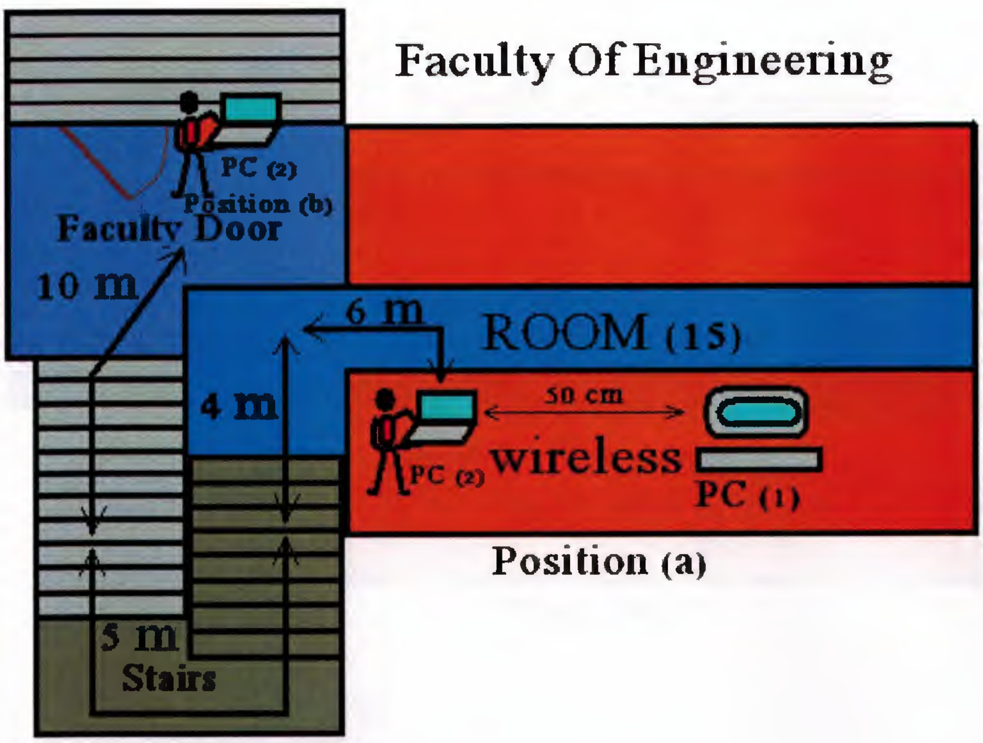

Figure 3.3 Wireless connections between two portable computers which separate by high range

3.6 Test Four

In this experiment we will establish a wireless connection between two portable computers separated at the beginning by 50 cm where we will start a call using MS-net meeting.

During the experiment we will expand the distance between them so we have many points where we are going to check the voice connection and see in which point the connection will be dropped.

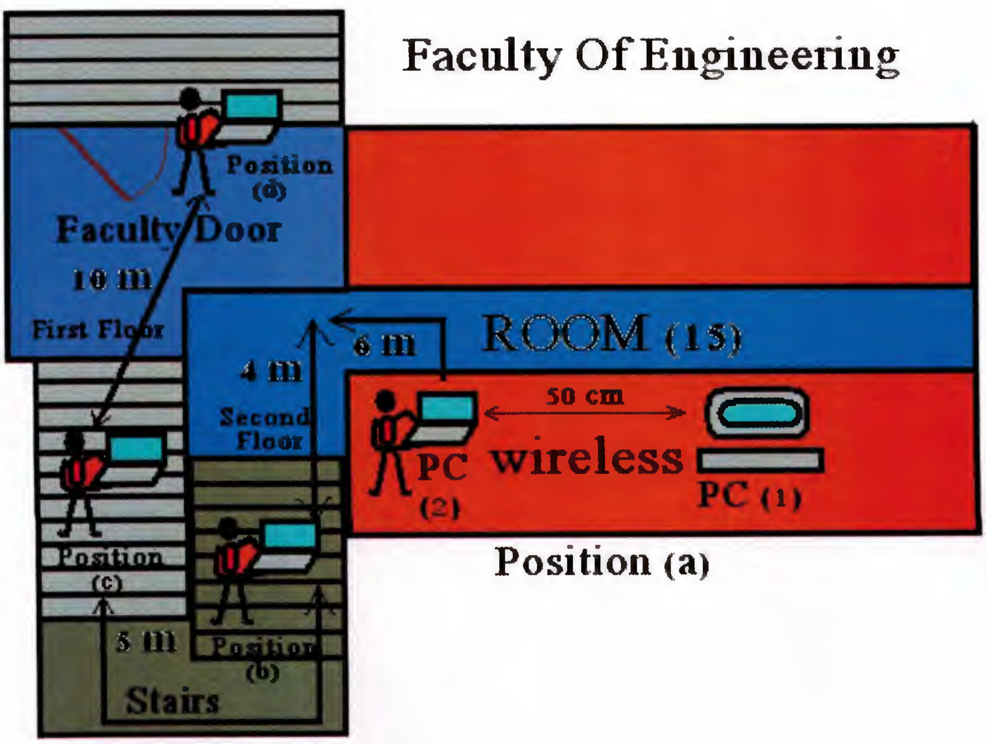

Figure 3.4 Wireless connections between two portable computers which separate by multiple ranges

3.7 SUMMARY

In this chapter we discussed about the practical tests that I conducted in order to check the voice over IP over wireless local area network. I conducted four different tests from which one was a wired local area network and the rest three were wireless local area network implementations each at a different range or we can say at different distances in between the two stations.

CHAPTER FOUR

RESULTS

4.1 Introduction

In this chapter we will discuss about the results that were obtained from the tests performed and described in chapter 3.The aim is to establish whether VOIPOWLAN is suitable for various in door mobile scenarios, detailed in chapter 3.

Having established a working knowledge of the performance ,in terms through-put and usability it will because possible to determine the issues involved in either improving the performance or making VOIPOWLAN communications more efficient .

Efficiency becomes a major concern if VOIPOWLAN is to become ubiquitous in society especially in terms of capacity and available bandwidth.

4.2Test One

In this test I connected two portable computers through wired local area network connection and I have found out that the transmission and receiving of the voice over IP in this connection is very clear as shown in the histogram of figure 4.1.

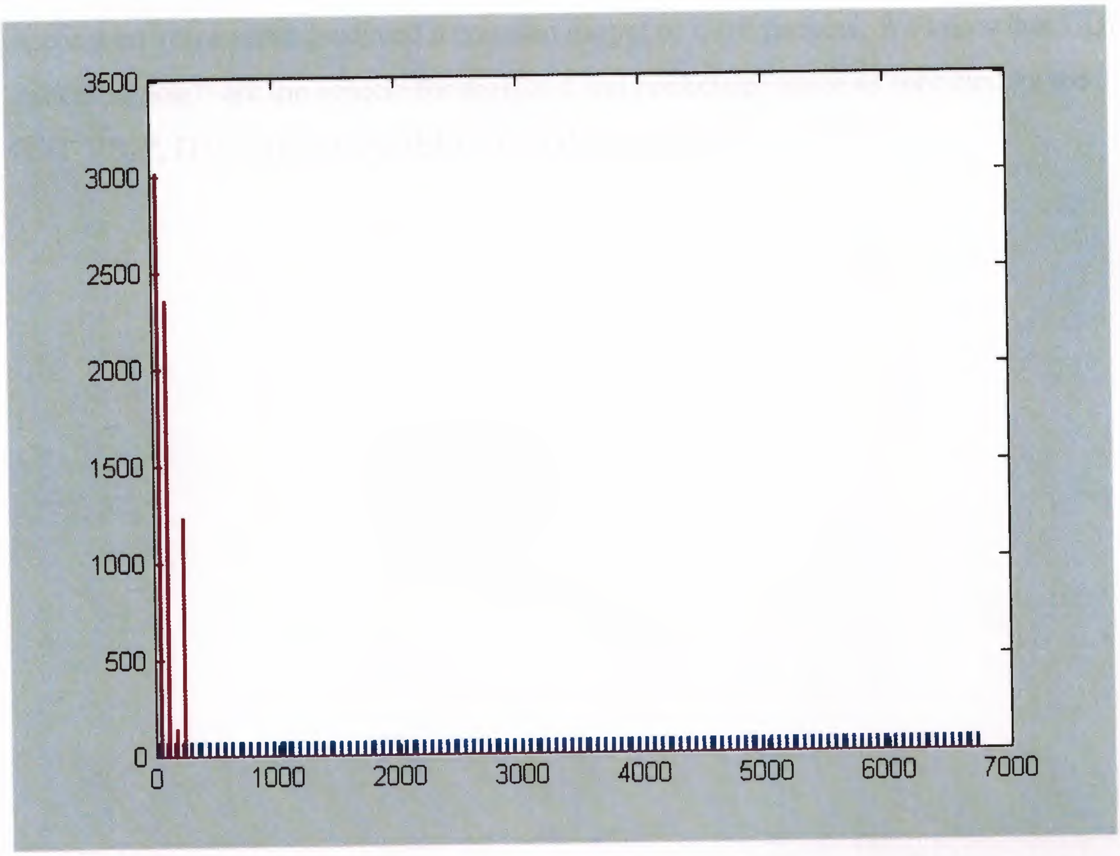

Figure 4.1 The capture data of experiment (1)

No variation was found in the UDP flow. This met expectations precisely and established our base line for comparison. It further confirms that our apparatus is suitable for further examination of the performance.

Exactly 6732 packets were transmitted of which 98% were UDP.

A constant voice input produced a constant output of UDP packets. We know that UDP Packet payloads are the vehicle for digitized and pocketsize voice as specified by the IETF VOIP, ITU-T H3.23 and IEEE 802.11B standards.

4.3 Test Two

In this test I have connected the two portable computers through a wireless local area network connection and I found out that the transmission and receiving of the voice over IP over the wireless local area network at the point where the computers were placed was the similar as the wired local area network connection as shown in the histogram of figure 4.2.

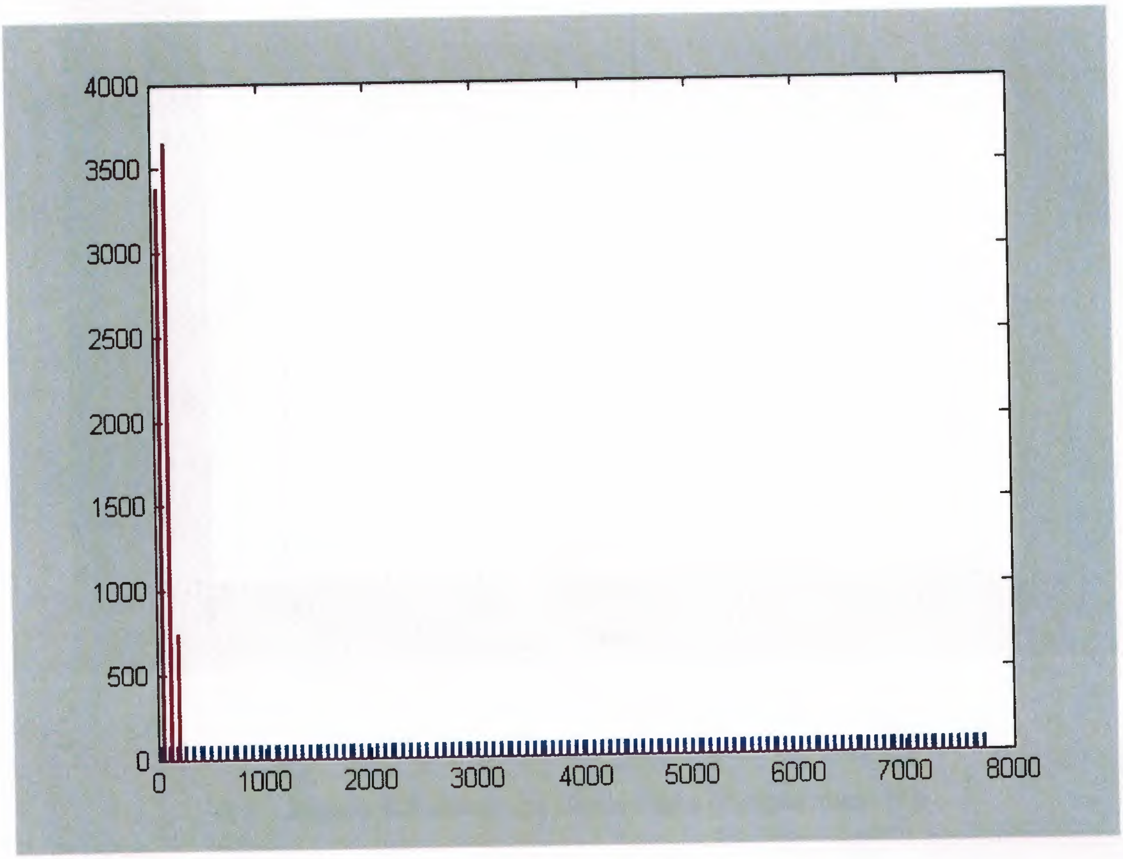

Figure 4.2 The capture data of experiment (2)

[Stress that the result were almost exactly the same as that found in experiment one]. Then WLAN is ok for two users, but what would have happened if there were 32 users simultaneously?

4.4 Test Three

In this test again we have the same scenario as test number 2 but the distance between the computers is too long so there was no UDP packet transfer just TCP/IP transferring was occurred as shown in the histogram of figure 4.3.

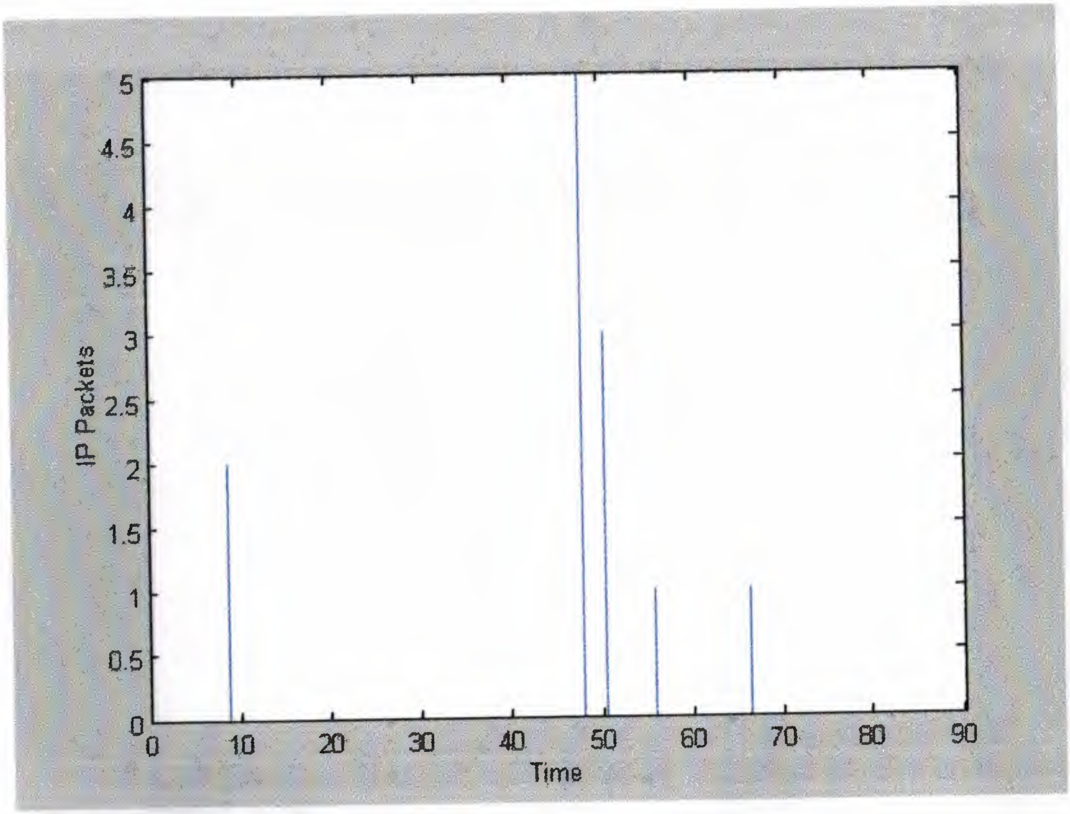

Figure 4.3 shows the capture data of experiment (3).

4.5 Test Four

In this test again we have the same scenario as test 2 and in this test again the computers were near to each other and there was TCP/IP and UDP packet transferring. Then I slowly moved one of the portable computers slowly away from the other till the point the UDP packet transferring was disabled as shown in the histogram of figure 4.4. The level of UDP transmissions were measured at the various points detailed in the chapter 3.

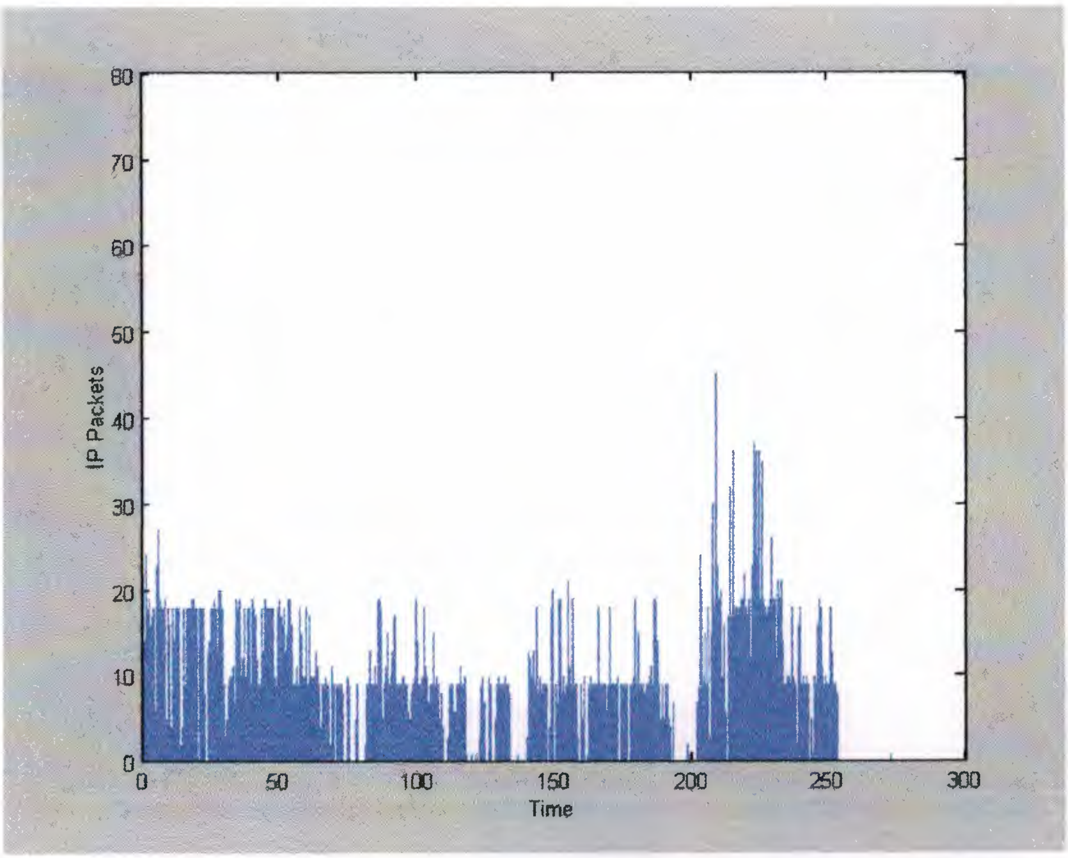

Figure 4.4 shows the capture data of experiment (4).

4.6 SUMMARY

In this chapter I have described the test results of the four experiments performed in chapter 3 about voice over IP over wireless local area network.

CONCLUSIONS

My project contains four chapters: an introduction to the topics involved in voice over internet protocol over wireless local area networks, the background of the wireless standard 802.11, experiments that examine the performance of voipowlan and results that we conclude about the experiments.

1. Background

In this chapter we discussed in detail, the background and functions of different protocols that are being examined in my project. We discussed the background and functions of the following protocols:

1-H323

2-RTP (Real Time Protocol)

3-802.11b

4-TCP/IP (Transmission Control Protocol/Internet Protocol)

5-UDP (User Datagram Protocol)

6-CSMA/CA (Carrier Sense Multiple Accesses / Collision Avoidance).

2. Experiments

In this chapter we practically demonstrate applications of voice over IP over WLAN. In this chapter we performed four experiments from which one is based on wired local area networking and the rest of the three are based on wireless local area networking, we established voice communication over IP by using MS Net meeting, ethereal, and check the quality of voice.

3. Results

In this chapter we discussed about the results that are adapted from the tests performed in the last chapter.

The aim of this project was to test the performance of voice over internet protocol over WLAN.

My expectations almost meet the actual results as in the experiments. The performance of voice over IP over WLAN when the portable computers are close to each other is same as the performance of wired connections.

On the other hand when the distance between portable computers is far away, my expectation for the performance did not meet the actual results.

Future Work

My advice to the one who is going to take my project as a reference to handle these points:

- Create interference using either access points, more users or other devices that operate at 2.4GHz.
- The performance of Robust Header Compression algorithms.

REFERENCES

[1] Mr.Izzet Agoren, E430 Lecture Notes

[2] Tanebaum Andrew S., Computer Networks, 1996

[3] http://www.ti.com/voip over WLAN

[4] http://www.voip-fourm.com

[5] http://www.voip-info.org

[6] Draft standard IEEE 802.11. Wireless LAN Medium Access Control (MAC) an Physical Layer (PHY) Specifications. IEEE, 1996

[7] http://www.dlink.com

[8] http://www.Ethereal.com

[9] http://www.microsoft.com/xp