Peer-to-Peer Communication between Android Mobiles

Ajmeera Suresh

A Thesis Submitted to

Indian Institute of Technology Hyderabad

In Partial Fulfillment of the Requirements for

The Degree of Master of Technology

Department of Elecctrical Engineering

June 2016

Declaration

I declare that this written submission represents my ideas in my own words, and where ideas or words of others have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited, or from whom proper permission has not been taken when needed.

18/06/16
(Signature)

Ajmeera Suresh.
(Ajmeera Suresh)

EE14mtech11001
(Roll No.)

Approval Sheet

This Thesis entitled Peer-to-Peer Communication between Android Mobiles by Ajmeera Suresh is approved for the degree of Master of Technology from IIT Hyderabad

(Dr. Sumohana Channappayya) Examiner
Dept. of Electrical Eng
IITH

(Dr. Abhinav Kumar) Examiner
Dept. of Electrical Eng
IITH

(Dr. G. V. V. Sharma) Adviser
Dept. of Electrical Eng
IITH

Acknowledgements

I sincerely thank my advisor Dr. G. V. V. Sharma. for his immese throughout the course. I benefited a lot from discussions with him. He had always believed in me and supported my ideas. I also thank all my professors from the department and other disciplines who supported me.

I would like to thank Ms. Rayapati Sushma for supporting and helping me in whole M.tech program.

Finally I would like to thank my family and my friends for the support and encouragement they have provided me during the ups and downs of my studies.

Dedication

I dedicate this thesis to my family without them i wouldn't be here.

Abstract

In the current days Voice telephony over mobile is possible considering GSM system which is cost consuming. Wi-Fi technology is a form of telecommunication that allows data and voice transmissions over a wide range of interconnected networks. In this thesis we provides a mechanism for live communication over IP using mobile phones at no cost. The purpose of this research is to design and implement a telephony program that uses WI-FI in p2p (Peer-to-Peer) or WLAN (Wireless Local Area Network) as a means of communication between mobile phones. The system will allow users to establish p2p voice connection through Access Points (AP) and then allow user to make voice conversation, sending SMS (Short Message Service). The current system will only allow for one call per connection, and no call waiting, or conference calls. The group chat application is the number of users connected to the server.

Contents

Chapter 1

Introduction

The main objective of this thises is to present how Peer-to-Peer services can be efficiently used in next-generation mobile networks. Currently, GSM service provider provide services over mobile phones but at a high cost. Where as using IP telephony would reduce the cost compared to the existing GSM system. The aim is to provide live communication services over mobile phone over IP. Two approaches are suggested in this thises ar as follows:

1. Client to Server model
2. Peer to Peer model

This group chat application was created to address communication issue for people tied sitting in front of their computer. Its very easy to use the company group chat application among co-workers. It provides them with an additional way real-time communication in a busy office environment. For this application we creat our own server. For this Group chatting application we don't need WI-FI, and the server is always runs with a specific port.

In this work, we have chosen native android as the programming language as it covers an adequate range of functions and classes to develop this socket-based programming application. The clear implementation of group chat application is in chapter[2].

A telephone call is between two parties - the calling party (or caller) and the called party(or callee) who are connected by one or more switches at various carrier companies exchanges. These switches form an electrical connection between both end-users, and their setting is electronically determined by pulses or tones generated by the dialed number. When a connection is established, the caller and callee subsequently go in speech, their voices are transported as analog and digital signals between the switches in the network. In order to successfully realize this process, the telecom exchange companies charge for this. Each time a number is dialed, each of these companies sees it as an attempt, which may either be success or a failure. They make a very small profit margin for each successful call but rely on the minutes generated by the huge amounts of successful calls in order to make a noticeable profit. The clear implementation of voice call application is in chapter[3].

Our application can be configured in client-server (infrastructure networking). The client-server configuration typically consists of multiple Mobile phones using wireless links to communicate with a server or central access point (Router) in the network.

Chapter 2

Group chatting application

2.1 Introduction

The basic idea of our approach is to develop group chat application which can transfer files over the interconnected devices to server. For reliable data transfer we chose TCP protocol. TCP provides a reliable, point-to-point communication, which use client-server applications on the internet for communication. The Socket and ServerSocket classes in java.net provide a system-independent communication channel using TCP.

A network socket is an endpoint of a connection across a computer network. Todays, most of the communication between computers is based on the Internet Protocol (IP); therefore most network sockets are internet sockets. More precisely, a socket is a handle that a local program can pass to the networking application programming interface (API) to use the connection, for example "send this data on this socket".

2.2 Client-Server architechture

The introduction of client-server architecture has greatly improved large-scale productivity as thousands of employees can work on their client computers, performing daily tasks and checking e-mails, while the less frequently accessed data is stored on a high-speed server that only performs large data-related pulls and computations, thus increasing speed and accessibility for all workers.

we have several computers and, each resources shoud be available to the other computers, then we should connect all the computers. This is called a network. A network represents interconnection of computers either by using a cable or a satellite where no cable is needed. In a network there may be several computers-some of them receiving the services and some providing the services to others. The computer which receives services is called "client" and the computer which provides the services is called "server". Here client sometimes acts as a server and a server acts as a client.
There are 3 requirements to establish a network:
Hardware:includes the computers, cables, modems, hubs, etc.
Software:includes programes to communicate between servers and clients.
Protocol:represents a way to establish connection and helps in sending and receving data in a standed format.

2.2.1 TCP/IP Protocol

The protocal represents a set of rules to be followed by every computer on the network. Protocal is useful to physically move data from one plae to another place on a network. TCP (Transmission Control Protocol) /IP (Internet Protocol) is the standed protocol model used on any network, including Internet.

TCP/IP model has got the following 5 layers:

1. Application layer
2. TCP
3. IP
4. Data link layer
5. Physical layer

Application layer is the topmost of the TCP/IP model that directly interacts with an application (or data). This layer receives data from the application and formates the data. Then it sends that data to the next layer called TCP/IP in the form of continus streem of bytes. The TCP, upon receiving the data from the appliction layer, will divided into small segments called 'packets'. A packet contains a group of bytes of data. These packets are then sent to the next IP layer. IP layer inserts the packets into envelopes called 'frames'. Each frame contains a packet, the IP address of destination computes, the IP address ofsource computers, and some additional bits useful in error detection and correction. These frames are then sent to Data link layer which dispatches them to corect destination computers on the network. The last layer, which is called the Physical layer, is used to physically transmit data on the network using appropriate hardware.

To send data from one place to another place, first of all computers should be correctly identified on the network. This is done with the help of IP address. An IP address is unique identification namber given to every computer on the network. It contains four intege numbers in the range of 0 to 255 and seperated by a dat as: **87.248.113.14**
This IP address may represent, for example a website on server machine on Internet as: **www.yahoo.com**
Therefore, to open 'yahoo.com site', we can type the site address as 'www.yahoo.com' or IP address as "87.248.113.14". But when we type the IP address in numaric form, that number is mapped to the website automatically. This mapping service is available in Internet, which is called 'DNS' (Domin Namming service).

On Internet, IP address of 4 bytes are used and this version is called IP address version 4. The next new version of IP address is version 6, which uses 16 bytes to identify a computer.

TCP/IP takes care of number of bits sent and whether all the bits are received duly by the destination computer. So it is called "connection orented reliable protocol". Every transmitted bit is accountable in this protocal. Hence, this protocol is highly suitable for transmitting data reliably on a network. Almost all the protocols on Internet uses TCP/IP model internally.

HTTP (hyper text transfer protocol) is the mostly widely used protocol on Internet, which is used to transfer web pages (.html files) from one computer to anther computer on network. FTP (file transfer protocol) is used to download or upload files from and to the server. SMTP (simple mail

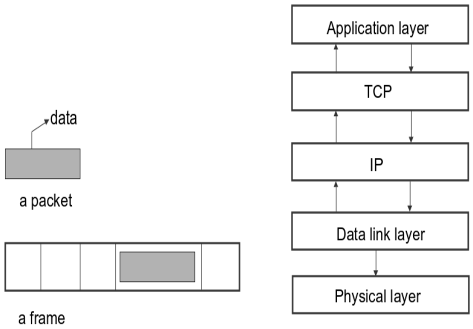


Figure 2.1: Packet, frame, TCP/IP layer

transfer protocol) is used to send mails on network. POP (post office protocol) is used to receive mails into the mail boxes.

Technology that separates computers and application software into two categories clients, and servers to better employ available computing resources and share data processing loads. A client computer provides the user interaction-facility (interface) and some or all application processing, while the a server computer might provide high-volume storage capacity, heavy data crunching, and/or high resolution graphics. Typically, several client computers are connected through a network (or networks) to a server which could be a large PC, minicomputer, or a mainframe computer.

2.2.2 User Datagrame Protocol (UDP)

UDP is a another protocol that transfer data in a connection less and unreliable manner. It will not check how many bits are sent or how many bits are receiver at the other side. During transmission of data, there may be loss of some bits. Hence, UDP is used to send images, audio files, and vedio files. Even if some bits are lost, still the image or audio file can be composed with a slight variation that will not distrub the original image or audio. Here the UDP packets are transmission and receiving through sockets.

Sockets

It is possible to establish a logical connecting point betwwn a server and client so that communication can be done through that point. This point is called "socket".

Each socket is given an identification number, which is called "port number". Port number takes 2 bytes and can be form 0 to 65,535. Establishing communication betwwen a server and a client using sockets is called "socket programming".

We should use a new port number for each new socket. Similarly, we should allot a new port number depending on the service provided on a socket. Every new service on the net should be assigned a new port number. There are already allocated port numbersfor the services (Table:2.1).

A socket, at server side is called 'server socket' and is created using ServerSocket class in Java. A socket, at client side is called 'Socket' and is created using Socket class. Both the ServerSocket and Socket class are available in java.net package. Of course, a server socket may not be neccessarily at server side; it may be created at client side also, if the client acts as server. similarly, a client socket

Port number	Application of service
13	Data and time services
21	FTP which transfers files
23	Telnet, which provides remote login
25	SMTP, which delivers mails
67	BOOTP, which provides configuration at boot time
80	HTTP, which transfers web pages
109	POP, which accesses mail boxes

Table 2.1: Allocated port numbers

may also exist at server side, if the sever acts as client.

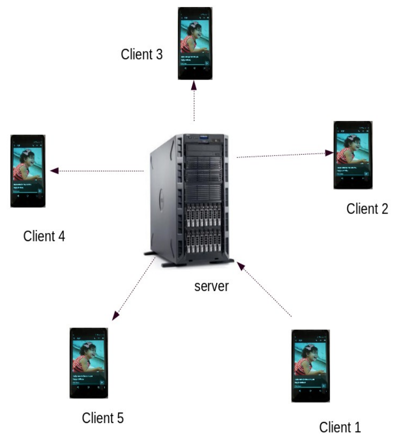


Figure 2.2: Client Server Architecture

2.3 Detail Implementation

A socket address is the combination of an IP address and a port number. Sockets need not have an address (for example for only sending data), but if a program binds a socket to an address, the socket can be used to receive data sent to that address. Based on this address, internet sockets deliver incoming data packets to the appropriate application process or thread. TCP is a connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages.

User interface layout of android application

In the user interface layout(Fig: 2.3) contains toolbar, activity layout sections. The toolbar intern contains buttons such as Call button,Attachment button and Camera buttons. Activity layout section contains Text view and Send buttons in it. Pressing on call button of toolbar will lead you into a new layout whose details were mentioned in the voice calling section of this report. Pressing Attachment button of toolbar leads to gallery of the device where we can select the item that are to be sent. Pressing send button of the activity layout will send the information to the server. Previous data that is sent to the server will be displayed in the Text view section of activity layout.

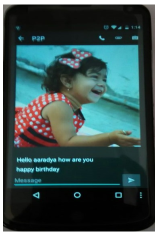


Figure 2.3: Chat activity layout

For example, to send “Hello world” via TCP to port 8080 of the host with address 192.168.17.58, one might get a socket, connect it to the remote host, send the string, then close the socket.

```
private Socket socket;{
 try{
 socket=IO.socket("http://172.16.17.58:8080");
    }catch(URISyntaxException e) {
          throw new RuntimeException(e);
         }
 }
```

To send a message, a source text, an image in which the text should be embedded, and a key are needed. The key is used to a id in encryption and to decide where the information should be hidden in the image.

Encoding: The encoding is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

```
private String encodeImage(String path){
   File imagefile = new File(path);
   FileInputStream fis = null;
    try{
     fis = new FileInputStream(imagefile);
      }catch(FileNotFoundException e){
          e.printStackTrace();
       }
```

```
Bitmap bm = BitmapFactory.decodeStream(fis);
ByteArrayOutputStream baos=new ByteArrayOutputStream();
bm.compress(Bitmap.CompressFormat.JPEG,100,baos);
byte[] b=baos.toByteArray();
  String encImage=Base64.encodeToString(b,Base64.DEFAULT);
      return encImage;
}
```

Decoding: The decoding is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden in that.

```
private Bitmap decodeImage(String data){
byte[] b =Base64.decode(data,Base64.DEFAULT);
Bitmap bmp=BitmapFactory.decodeByteArray(b,0,b.length);
return bmp;
    }
```

After pressing send button The encoded data(text or image) directy goes to the server. The serevr is bind to the particular address and port.

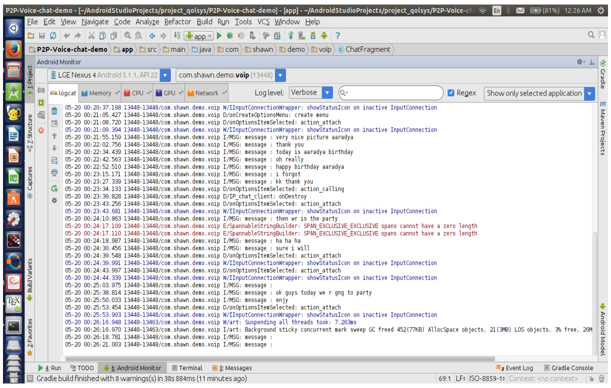


Figure 2.4: Server

See the above figure the data is received from the client. The server is sending the received data to the particular client destined. If the number of users are connected to a same port, all the clients receive the same data from the server.

```
var app = require('express')();
var http = require('http').Server(app);
var io = require('socket.io')(http);
app.get('/',function(req,res){
    res.sendFile(dirname+'/index.html');
})
 io.on('connection',function(socket){
 console.log('user connected'+socket.id);
```

```
 socket.on('message',function(data){
 console.log('arravied msg: +data.text');
 var sockets = io.sockets.sockets;
  socket.broadcast.emit('message',data);
    })
 socket.on('disconnect',function(){
console.log('disconnected'+socket.id);
    })
})
http.listen(8080,function(){
console.log('server listening on 8080');
})
```

2.4 Summary

In this chapter to make a Group Chat application (File transfer and Chatting) program using TCP/IP Protocal for reliable data transfer in this appication we create our own Server. In this case all the clients are connected to a Server with specific port. For this Group chatting application we don't need WI-FI, and the server always runs with a specific port.

In this work, we have chosen native android as the programming language as it covers an adequate range of functions and classes to develop this socket-based programming application.

Chapter 3

Voice call over Wi-Fi

3.1 Introduction

Voice over Internet Protocol (VoIP) is one of the rising voice communication technologies over packet-switched networks, such as the Internet and other IP networks. It uses the internet technologies and web linked environment in a highly efficient way to offer much more versatile services with reduced or no costs. Additionally combined with the embedded technology, Voice over IP allows a wide range of hand-held devices to have their real-time access to voice communication on the Internet, making a new era to the future internet technologies. Wireless LAN systems providing broadband wireless access in hand held devices have become more popular in recent years. There has been growing interest on Internet telephony, mainly on hand held devices running applications such as web browsing and email. Internet telephony allows the Users to make voice and video calls over the internet. The main advantage of IP telephony over a wireless network is that it allows mobility of the people while they are talking.

The motive behind the system is to enable the cost effective voice communication. We have designed a client server model based system to implement it. We has implemented the system using native android. The backbone of the android programming is JAVA which is platform independent. Various methods have been deployed for communication. There are some popular digital wireless transmission techniques can be divided into three categories according to their applications. The first category is pulse transmission technique used mostly in IR (Infrared) applications. The second category is basic modulation techniques widely used in TDMA (Time division multiple access) cellular, as well as a number of mobile data networks. The third category is spread spectrum systems used in the CDMA (Code division multiple access), as well as WLANs operating in ISM (industrial, scientific and medical) bands. The main advantage of using wireless LAN (Local area network) is that it provides the ability to change the network infrastructure of an organization easily and without the need for expensive re-routing of cable or the installation of new cable runs.

Voice over Internet Protocol (VoIP) technology facilitates packet based IP networks to carry digitized voice. With VoIP, competitive carriers and service providers can offer telephony (voice) services together with traditional data services over the same IP infrastructure.

3.2 IEEE802.11 architechture

Wireless LANs are most important access networks technologies in the Internet. Most popular is the IEEE802.11 wireless LAN, also known as Wi-Fi. An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called Basic Service Set, or BSS, in the 802.11 nomenclature) is controlled by a Base Station (Access Point). Although a wireless LAN may be formed by a single cell, with a single Access Point, most installations will be formed by several cells, where the Access Points are connected through some kind of backbone DS (Distribution System). This backbone is typically Ethernet and, in some cases, is wireless itself.

The Most wireless networks are based on IEEE 802.11 standards. Basic wireless network consist of set of service stations, communicating each other using radio signals which broadcast in either the 2.4GHz or 5GHz band. Neighbouring channels are 5 MHz apart. IEEE 802.11 standards services include managing associations, delivering data and security. There are mainly three parameters that characterize Wired and Wireless LANs. Those are transmission media, topology and medium access control techniques. There are several standards for wireless LAN technology.

IEEE802.11 Standards

Protocol	Release Date	Op.Frequency	Data Rate (Typ)	Data Rate (Max)	Rande (Indoor)	Range (Outdoor)
Legacy	1997	2.4-2.5GHz	1 Mb/s	2 Mb/s	?	?
802.11a	1999	5.15-5.35/5.47-5.725/ 5.725-5.875GHz	25 Mb/s	54 Mb/s	25 meters	75 meters
802.11b	1999	2.4-2.5GHz	5.5 Mb/s	11 Mb/s	35 meters	100 meters
802.11g	2003	2.4-2.5GHz	25 Mb/s	54 Mb/s	25 meters	-75 meters
802.11n	2007 (unapproved draft)	2.4GHz or 5 GHz band	200 Mb/s	540 Mb/s	50 meters	126 meters

Table 3.1: IEEE802.11 Standards

The whole interconnected Wireless LAN, including the different cells, their respective Access Points and the Distribution System, is seen as a single 802 network to the upper layers of the OSI model and is known in the Standard as Extended Service Set (ESS).

The main concept of OSI is that the process of communication between two endpoints in a telecommunication network can be divided into seven distinct groups of related functions, or layers. Each communicating user or program is at a computer that can provide those seven layers of function. So in a given message between users, there will be a flow of data down through the layers in the source computer, across the network and then up through the layers in the receiving computer. The seven layers of function are provided by a combination of applications, operating systems, network card device drivers and networking hardware that enable a system to put a signal on a network cable or out over Wi-Fi or other wireless protocol.

OSI Referance Model:

The seven Open Systems Interconnection layers are:

Application layer: This is the layer at which communication partners are identified (Is there someone to talk to?), network capacity is assessed (Will the network let me talk to them right now?), and that creates a thing to send or opens the thing received. (This layer is not the application it-self, it is the set of services an application should be able to make use of directly, although some

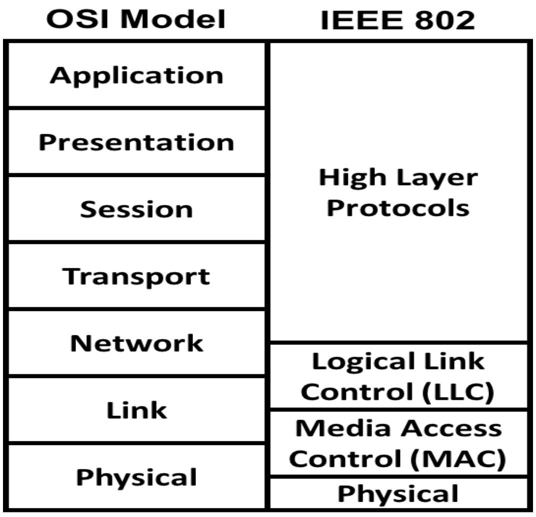


Figure 3.1: OSI Referance model

applications may perform application layer functions.)
Presentation layer: This layer is usually part of an operating system (OS) and converts incoming and outgoing data from one presentation format to another (for example, from clear text to encrypted text at one end and back to clear text at the other).
Session layer: This layer sets up, coordinates and terminates conversations. Services include authentication and reconnection after an interruption. On the Internet, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) provide these services for most applications.
Transport layer: This layer manages packetization of data, then the delivery of the packets, including checking for errors in the data once it arrives. On the Internet, TCP and UDP provide these services for most applications as well.
Network layer: This layer handles the addressing and routing of the data (sending it in the right direction to the right destination on outgoing transmissions and receiving incoming transmissions at the packet level). IP is the network layer for the Internet.
Data-link layer: This layer sets up links across the physical network, putting packets into network frames. This layer has two sub-layers, the Logical Link Control Layer and the Media Access Control Layer. Ethernet is the main data link layer in use.
Physical layer: This layer conveys the bit stream through the network at the electrical, optical or radio level. It provides the hardware means of sending and receiving data on a carrier network.

Considering the topology of IEEE802.11 standard networks, it supports two types of modes of basic service set (BSS).

- Infrastructure mode

In this mode, one station (STA) acts as master which is called AP (access point) and all other stations associate to the AP. In this BSS, if any station wants to communicate with another station, communication should be done through AP and messages should pass via AP.

- Ad-hoc mode

In this mode, stations will communicate directly without an AP. It is also known as Independent BSS (IBSS).

IEEE802.11 model:

The Physical Layer: The Physical layer (PHY) provides a frame exchange between MAC and PHY under the control of the physical layer convergence procedure (PLCP) sub layer and using signal carrier and spread spectrum modulation to transmit data frames over the media under the control of the physical medium dependent (PMD) sub player. Finally, the PHY provides a carrier sense indication back to the MAC to verify the activity on the media.

There are three different physical layer specifications are described in Wireless LAN.

1. Spread Spectrum

    - FHSS(frequency hopping spread spectrum)

      2.4GHz ISM band at 1Mbps and 2Mbps

      PHY uses 79 non-overlapping 1 MHz channels to transmit 1 Mbps data signal

    - DSSS(direct sequence spread spectrum)

      2.4GHz ISM band at 1Mbps and 2Mbps

      IEEE 802.11 uses a simple 11 chip barker code with QPSK or BPSK modulation

2. Infra-red signal

Medium Access Control (MAC): IEEE802.11 medium access control (MAC) provides a functionality to make a reliable data transmission over wireless media, which is noisy and unreliable. MAC also gives functionality to access control and security. Due to noise, interference and propagation effects, there might be a chance of having loss of frames in the result, errors in correction codes and also frames may not receive properly. To reduce frame loss we can implement MAC functionality at higher layers like TCP but retransmission timers will be order of seconds so that it is more efficient to deal with errors at MAC level.

IEEE 802.11 MAC takes MSDUs and adds headers and tailors (MAC service data unit) which takes from the higher layers of the protocol stack to send equivalent layers of the protocol stack to another station. These MSDUs are known as MAC protocol data unit (MPDU). IEEE 802.11 defined MAC protocol frame format is shown below. It contains three different frame types:

- Control frames
- Data frames
- Management frames

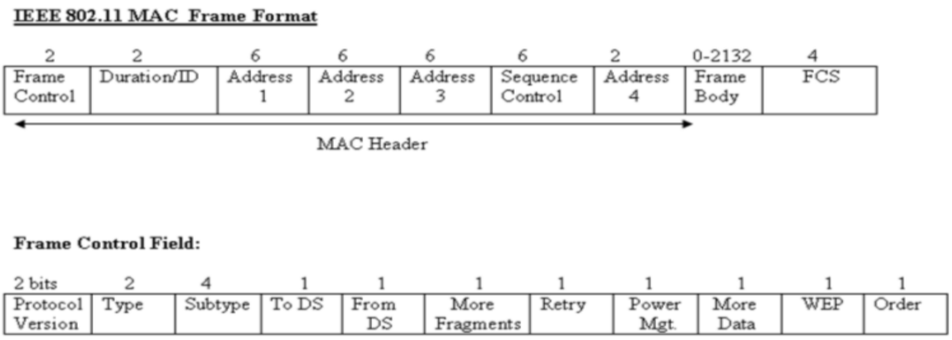
Control frames: These frames are used for handshaking and positive acknowledgement during data exchange.
In control frames, subtypes defining RTS,CTS,ACK,Power Save Poll,CF-End and CF-End + ACK.
Data frames: These frames are used for the transmission of data. MAC header provides information on frame control, duration, sequence control and addressing.
Data frames are again divided into eight subtypes in two groups. The first group of frames associates with simple data, data with contention-free acknowledgement (CF-ACK), data with CF- Poll, data

with CF-ACK and CF-Poll. The second group frames associates with CF- ACK, CF-Poll, and CF-ACK+ CF-Poll.

Management frames: These frames are used for station association/disassociation with AP, timing and synchronization among stations with AP and authentication and de authentication.

In management frames, we have several subtypes. Those are Beacon frames, Probe request and response frames, Authentication and De-Authentication frames, Association request and response frames, Re-association request and response frames, Disassociation frames and Announcement traffic indication map frame. The first function of the MAC is to provide a reliable data delivery service to the Users of the MAC through frame exchange protocol at the MAC level. The minimal MAC frame exchange protocol consists of two frames, a frame sent from the source to the destination and an acknowledgement from destination to the source. WLAN has 'hidden node problem' which does not exist in Wired LAN. In order to overcome this, two more frames are added, one is Request to send frame (RTS) and another is clear to send (CTS) frame. The second function of MAC is to fairly control access to the shared wireless medium. MAC has a basic access mechanism called distributed coordination function (DCF) and centrally controlled access mechanism called point coordination function (PCF).

IEEE802.11 Frame



IEEE 802.11 MAC Frame Format

2	2	6	6	6	6	2	0-2132	4
Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

MAC Header

Frame Control Field:

2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More Data	WEP	Order

Figure 3.2: IEEE802.11 frame format

3.3 Voice over Internet Protocol (VoIP)

In the recent years the internet has further developed itself into providing Internet Telephony or Voice over Internet Protocol (VoIP). This allows Users to make voice or video calls over the internet. All the User needs is a computer with a network connection, a soundcard, and a microphone. Enterprises, ISPs, ITSPs (Internet Telephony Service Providers), and carriers view VoIP as aviable way to implement voice over packet. VoIP is a cheaper way of communicating over the internet. Various infrastructures have been developed to increase both the efficiency and effectiveness of both the VOIP systems and the VOIP architecture.

Voice over Internet Protocol (VoIP) is the technology used to transmit conversations digitally over the Internet. Voice-over-IP (VoIP) is getting widespread adoption both from business and residential customers as it enables combined communication and network infrastructure. The Main reasons for implementing the VoIP are it allows long distance communication such as voice, video and data which can be carried over a single network infrastructure, which leads into reducing costs, by simplifying the network management through the common use of equipment. VoIP makes good use of internet technology so that it is able to offer more services with lower or even no cost. VoIP combined with embedded technology can offer a wide range of handheld devices for communicating over the internet.

3.3.1 VoIP Components

The basic steps involved in originating an Internet telephone call are conversion of the analogue voice signal to digital format and compression/translation of the signal into internet protocol packets for transmission over the internet; the process is reversed at the receiving end. The VoIP components must perform functions such as:
Signaling: Signaling is the way that devices communicate within the network, activating and co-ordinating the various components needed to complete a call (accomplished by exchange of data grams between end terminals).
Database services: A VoIP network uses an IP address and port number to locate an end point, address abstraction could be accomplished with DNS.
Call bearer control: The connection of a call is made by two endpoints opening a communication session between each other. In a VoIP implementation, connection is a multimedia stream transported in real time. Once communication is complete, the IP sessions are released and optionally network resources are freed.
Codec Operations: The process of converting analogue waveforms to digital information is done with a coder-decoder (VOCODER), the data stream from the VOCODER is put into IP packets and transported across the network to the end terminals. Two end points will use the same ITU encoding standards (ex: G.7 family) and common set of CODEC parameters.

3.4 Compression Technology

There are few codec techniques like G711, G722, Speex and alaw. which are used for compressed the voice data so that it can be transfered over IEEE802.11 standard. This section how voice compression technology works. In VoIP applications, codecs are used for compression and decompression of voice. The codecs take the voice signal input from the microphone and compresses according to the available best bit rate. The compressed signal from codec is passed to the VoIP controller, and then it transferred from there to a destination over the internet. When the voice is received from its destination, the VoIP controller sends that signal to codec for decompression. After decompression, codec sends that signal to the speaker.

3.4.1 G711 and Speex codec

1. **G711:** It describes a relatively simple way to digitize analog data by using a semi logarithamic scale, called the companded pulse code modulation (PCM). Its goal is to increase the resolution for small signals, while large signals are treated proportionally. The encoded stream is 64 kbps, consisting of 8 kHz sampling of 8 bit signals. The frame length is eight 125 s samples.

2. **Speex codec:** Speex is an open source codec, based on the popular Code Exited Linear Prediction (CELP) algorithm with a wide range of bit rate. It is a flexible audio codec for the development of Voice over IP (VoIP) on Linux and other free operating systems. Speex is considered to be optimized for speech and is designed for low latency communication over an unreliable packet switching network. Speex has modest complexity and it is targeted at wide range of devices.

Some of the main Speex codec are:
Sampling rate: It is designed for 3 sampling rates referred to as narrowband (8kHz), wideband (16 kHz), ultra wideband (32 kHz).
Quality: Speex quality parameter ranges from 0to 10. In constant bit (CBR) operation, the quality parameter is an integer while for variable bit-rate, and it is float.
Complexity: Speex allows varying the complexity allowed for the encoder by controlling how the search is performed with the quality parameter.
Variable bit rate: It allows audio codec to change its bit rate dynamically to adapt to the hardness of the audio being encoded. Speex codec encodes the high energy transients with high bit rate to achieve good quality while fricatives encoded sufficient with less bits. Regardless of its advantages, there is no guaranty about the final average bit-rate and for the real time applications like VoIP it counts maximum bit-rate without considering the communication channel capacity.
Average bit rate: Average bit-rate solves the problems of VBR. It adjusts VBR quality dynamically in order to meet specific bit rate. Also includes

- Voice activity detection (VAD,integrated with VBR) and discontinuous transmission(DTX),
- Variable complexity, Ultra-wideband sampling rate 32 kHz,
- Embedded wideband structure(Scalable sampling rate)
- Intensity stereo encoding option, Fixed-point implementation

3.5 Session Initiation Protocal (SIP)

SIP is an IETF defined signaling protocol for voice and video over IP. It is an open standard for Internet telephony. From version 2.3 or higher Android includes SIP protocol stack to support Internet telephony. Android SIP API does not provide direct IP to IP call in a local network so that we obtained some required code from the open source project of Linphone Android application. Each device must have an IP address according to the SIP standards. According to solution for achieving peer-to-peer voice calling functionality, we have to make a voice call between two clients by using an Access-point (AP).

Session Initiation Protocol is a signaling protocol specified by the Internet Engineering Task Force used to set up and tear down two-way communications sessions. It provides the necessary tools for location services, call establishment, call management, and call termination. Session initiation protocol operates on the application level so it can be used with several different protocols.

The Access point allocates IP addresses to the connected clients in a network. According to the SIP standards VoIP session can be established between connected devices using IP address. SIP

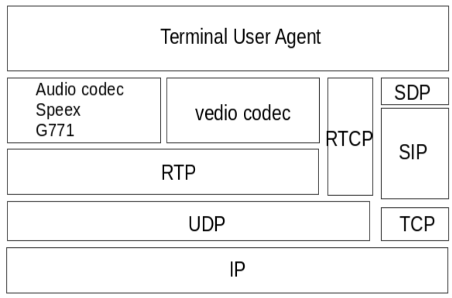


Figure 3.3: Session Initiation Protocol

program creates a SIP session between two clients and transfers RTP packets. Mainly there are only three SIP applications are available for an Android operating system. Android has API for developing a SIP application but it requires registration in the proxy server or SIP server. In this thesis work we are going to make just an IP to IP call without registration or maintaining a proxy server. Therefore an Android SIP application API is not suitable for our application development. An open source project Linphone Android application includes direct IP to IP call in local network. This SIP application can establish IP to IP call between two devices.

3.5.1 SIP Components

SIP supports functionalities to establish and end multimedia sessions: location, availability, resource use, and negotiation features. In order to implement these functionalities, there are different SIP components. There are two main elements:

1. **User Agents (UA):** User Agent have two different parts, User Agent Client (UAC) and User Agent Server (UAS). An UAC is a logical entity which sends SIP requests and receives answers to those requests. An UAS is a logical entity that sends answers to SIP requests. Both entities are in every user agent, to allow the communication between different user agents in a client-server and peer-to-peer communication.

2. **SIP Servers:** Three deffirent types of SIP Servers:

   (a) **Proxy Server:** Proxy Server resend requests and they decide the server they must send the messages to, altering the request fields if necessary. It is an intermediate entity that acts as a client and as a server in order to establish calls between users. This server has a similar functionality to an HTTP Proxy. It has the task of routing the requests that receive from other entities.
   There are two types of Proxy Server:

   - **Stateful Proxy:** Stateful Proxy keep the state of the transaction during the request processing. It allows the division of a request message in several ones (forking), with the purpose to find in parallel the location of the called in order to obtain the best path.

- **Stateless Proxy:**Stateless Proxy do not keep the state of the transaction during the requests processing, They only resend messages.

(b) **Registrar Server:**Registrar Server is a server which accepts register requests of the users and keep the information from these requests. It provides a location and address translation service in its domain

(c) **Redirect Server:**Redirect Server is a server which generates redirection answers to the received requests. This server routes again the requests to the next server.

These categories are just conceptual, they can be all placed in the same machine. They can be also in different machines for scalability or processing matters.

3.5.2 Real Time Transport Protocol (RTP)

Real time transport protocol provides general transport capabilities for the multimedia applications, including both stream based applications and conversational applications.

RTP works in combination with the User Datagram Protocol to transfer the data packets to the receiver node. VoIP data is inserted into data packets using the RTP protocol, which are then enclosed inside the UDP packets, are then transmitted to the receiving end. VoIP uses UDP protocol, because it transmits the voice data rapidly. Packet loss and delay jitter are the main problems when we send directly, by using UDP. For overcoming packet loss, a retransmission mechanism is not possible in VoIP for real-time services.

To overcome this problem, the receiver must know when the packet is sent. By using time stamping on the data packets while sending we can know when the data is sent at the receiver side. For this we are using a separate protocol called RTP. The main features of RTP are time stamping and sequence numbering. RTP uses a UDP port for communicating with other protocols. Services include payload type identification, sequence numbering, time stamping and delivery monitoring.

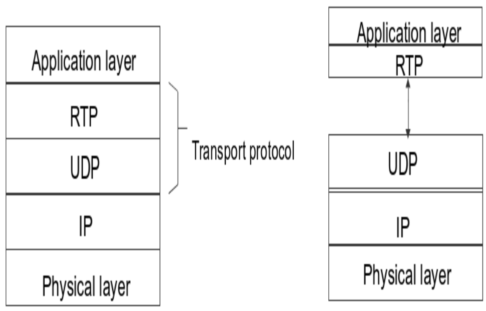


Figure 3.4: Real Time Transport Protocol

From programmer view point, RTP is a part of an application layer for a voice over IP. From Network theory viewpoint, it is more like a transport protocol.

Payload: In the RTP header, pay load indicates type of encoding used for the multimedia stream (audio/video). It is allowed to send the payload size as 7 bits (27= 128). If a sender changes the payload type on fly, it should be updated in the pay load header, so that the receiver will adjust the

Table 3.2: RTP Header

Payload Type	Sequence number	Time Stamp	SSRI
7 bits	16 bits	16 bits	32 bits

VOCODER as per the encoding technique updated. In the RTP payload header we can send 128 types of payload types, some of them are standardized and the remaining are free.
Ex: Payload:

- 0 PCM - law
- 7 LPC (8 kHz)
- 14 - mpeg(90 khz)-audio
- 31 - mpeg-1 video
- 32-mpeg-2 video

Sequence number: Incremented by 1 for each RTP packet and sequence number is used for detecting packet loss.
Time stamping: It denotes sampling instant of first byte in the RTP data and to remove packet jitter. It is derived from sampling clock at the sender.
Synchronization source identifier: This is different from an IP address, the sender chooses a random number while using. The main use of SSRI is to identify a particular RTP stream between 2 hosts, which is for identifying the source of the RTP stream.

3.6 Detail Implementation

3.6.1 User interface layout of android application

Wi-Fi phone works by accessing wireless internet connections such as a wireless router in your home or office, or Wi-Fi hotspots around the globe. We can access open Wi-Fi hotspots quickly and easily, as well as various secure hotspots. Voice over Internet Protocol (Voice over IP, VoIP) is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms frequently encountered and often used synonymously with VoIP are IP VoIP is available on many smartphones and Internet devices so that users of portable devices that are not phones may place calls or send SMS text messages over 3G or Wi-Fi. On the receiving side, similar steps (usually in the Reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone. It works at many hotels, airports, coffee shops, and etc.

Figure 3.5: Voice call activity layout

The user interface layout (Fig: 3.5) of the application contains a text view, a text box and three user buttons. After that by clicking on Call button the voice call is initiated. Stop button is used to end the voice call.

3.6.2 Voice Recording and Encoding

Voice Recording: The voice data from the microphone is handled using AudioRecord Android API (Application Program Interface). The sampling rate is kept at 8 Kbps. The audio encoding format used is 16 bit PCM (Pulse Coded Modulation). The buffer size is 4096 bytes for the above mentioned sampling rate and recording format.

Voice Encoding: There are few codec techniqes like G711, G722, Speex and alaw. which are used for compressed the voice data so that it can be transfered over IEEE 802.11 standard. Speex encoder operates in frames. client-1 frame contains raw voice data of voice. In Narrowband operation mode (8Khz) and for the parameters used in voice recording section, the frame size is 160 samples (320 bytes). These frames are read from the temporary file (created while recording voice) and given as input to the Speex encoder, which compresses the given frame and returns encoded voice data.

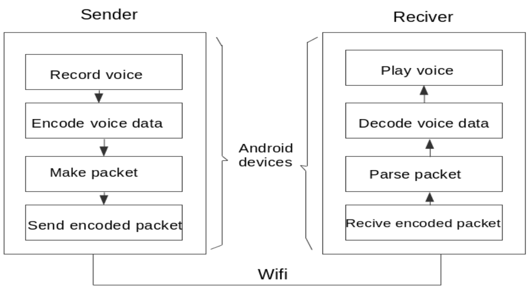


Figure 3.6: Flowchat

3.6.3 Voice Decoding and Playing

At the receiving end, encoded voice data is received from client-1. The recived encoded data is stored in receive buffer and this buffer is given as input to the decode method, which decodes the data and returns (160 samples) 320 bytes of voice data. These 320 bytes are stored in a dynamic buffer and every time after decoding, 320 bytes are appended to this dynamic buffer. This dynamic buffer is used for playing the voice. Write and Play methods of AudioTrack Android API are used for this purpose. When 320 bytes are decoded for the first time, Play method is initiated and starts playing the voice. Write method is used for writing the data from dynamic buffer to Play method. As the dynamic buffer will be modified every time, the voice will be played in real time until the sender ends the voice call.

Figure 3.7: P2P Voice calling over Wi-Fi

In this scenario our android mobiles are connected to Access-point in a centralized network. In centralized network, connected devices will get an IP address from the access-point. Using this IP address a voice call can be established between the connected devices.

3.7 Summary

In this chapter to make a VoIP (Voice over Intenet Protocol) based Voice Call using WI-FI. In this case the communication between android mobiles was done by connecting them to an AP (Access Point or Router). Voice over Internet Protocol is used for communication of two persons by sending voice packets in a real time fashion. Various protocols are involved in implementing VoIP. One of the main advantages of SIP is that it is human readable and is less complex. So, in this application we implemented SIP as our signaling protocol.

The Main reasons for implementing the VoIP are, it allows long distance communication such as voice, video and data which can be carried over a single network infrastructure reducing its cost by simplifying the network management through the common use of equipment. VoIP makes good use of Internet technology so that it is able to offer more services at lower or even no cost. VoIP combined with embedded technology can offer a wide range of communication over the Internet.

Chapter 4

Conclusion

This thesis presents the detail implementation of a chat,file transfer and voice chat application that is using socket programming method. In this work, we have chosen native android as the programming language as it covers an adequate range of functions and classes to develop this socket-based programming application. The application is subject to further improvement in the future in which other functionalities may be included to enhance its overall function.

In this thesis we defined two test scenarios:
In first scenario to make a Group Chat application (File transfer and Chatting) program for this appication we create our own Server. In this case all the clients are connected to a Server with specific port. For this Group chatting application we don't need WI-FI, and the server is always runs with a specific port.

In second scenario to make a VoIP (Voice over Intenet Protocol) based Voice Call using WI-FI. In this case the communication between android mobiles was done by connecting them to an AP (Access Point or Router). Voice over Internet Protocol is used for communication of two persons by sending voice packets in a real time fashion. Various protocols are involved in implementing VoIP. One of the main advantages of SIP is that it is human readable and is less complex. So, in this application we implemented SIP as our signaling protocol.

References

[1] Android web site:*http://www.android.com/*http://www.android.com

[2] *http://www.p2psip.org*http://www.p2psip.org

[3] Forouzan Behrouz, *TCP/IP Protocol Suite*, 3rd. NY: McGraw Hill, 2006.

[4] https://nodejs.org/api/dgram.htmlhttps://nodejs.org/api/dgram.html

[5] Law, K.L.E., Leung, R. 2002. *Design and implementation of active network socket programming.* Computer Communications and Networks.

[6] Malhotra, A., Sharma, V., Gandhi, P., Purohit, N. UDP based chat application. Computer Engineering and Technology (ICCET), 2010 2nd International Conference vol.6: pp.V6-374-V6-377.

[7] Stefan Tilkov and Steve Vinoski, Node.js: *Using JavaScript to Build High Performance Network Programs*,IEEE Computer Society in IEEE Internet Computing.

[8] Hac, and Anna, *Mobile Telecommunication Protocolsfor Data Networks*, 1st.London: John Wiley and SonsLTD,2000.

[9] Ghassan Kbar , Wathiq Mansoor , Aryan Naim, *Voice Over IP mobile telephony using WIFI p2p* , 2010 Sixth International Conference on Wireless and Mobile Communications.

[10] B. Regis J, and D. W. Gregory, *Voice and Data Communication*, 4rth ed. California, Berkeley: McGraw Hill, 2001.