STUDY OF IP MULTIMEDIA SUBSYSTEMS AND IMPLEMENTATION OF PoC ON MOBILE SETS

Thesis report submitted towards the partial fulfillment of requirements for the award of the degree of

Master of Engineering
in
Electronics and Communication
to
Thapar Institute of Engineering & Technology, Patiala

Submitted by

HAZEL SAXENA

Roll No: 8044112

Under the Guidance of

Ms.NAVJOT KAUR

Lecturer

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

THAPAR INSTITUTE OF ENGINEERING & TECHNOLOGY
(Deemed University)
Patiala– 147001, Punjab, INDIA

June- 2006

ACKNOWLEDGEMENTS

It is with the deepest sense of gratitude that I am reciprocating the magnanimity, which my guide ***Ms. Navjot Kaur***, Lecturer, Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala, has bestowed on me by providing guidance and support throughout the thesis work.

I am also thankful to ***Dr. A.K. Chatterjee***, P.G. Coordinator, Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala for the motivation and inspiration that triggered me for my thesis work.

I am also thankful to ***Mr. Sameer Bhatia***, I.T.A, Tata Consultancy Services Ltd., Gurgaon and ***Ms. Ira Acharya***, Group Leader, Tata Consultancy Services Ltd., Gurgaon for their guidance and support throughout the thesis work.

I convey my sincere thanks to ***Dr. R.S Kaler***, Head of Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala for his encouragement and co-operation.

At this occasion, I would not like to miss the opportunity to show my gratitude to ***Dr.T.P Singh***, dean of Academic Affairs (Thapar Institute of Engineering and Technology, Patiala) for hi co-operation.

I would also like to thank all the staff members and my co-students who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of my thesis.

I am also thankful to the authors whose works I have consulted and quoted in this work. Last but not the least I would like to thank God for not letting me down at the time of crisis and showing me the silver lining in the dark clouds.

Hazel Saxena
Date:
Place: T.I.E.T, Patiala

ABSTRACT

Over past few years many major industry developments have taken place resulting in audio, video and data-enhanced, real-time communications out from the realm of highly specialized applications. Multimedia systems have become one of the popular services provided on the wireless networks. The modern view of multimedia communications and multimedia networks has its roots in videoconferencing. The traditional view of multimedia-enabled networks often looks for tangible value in terms of cost savings, especially reduced travel expenses. IP multimedia Subsystems have a vision to combine two most successful and important technologies in communications: wireless cellular networks and internet. IMS provides a single platform to all the present technologies as well as to the future technologies.

The next generation networks provided a new face to the telecommunication world. Earlier the main emphasis was on speech and speech related services, but nowadays the main aim is to enable faster data rates and various multimedia services. IP Multimedia Subsystems (IMS) provide a single platform for all the present as well as future technologies. IMS enables a whole new set of services such as Push to talk Over Cellular (PoC) which is a novel concept of combining converging digital content formats, IP protocols and cellular packet bearers to provide a proven case –Voice Group Call .PoC is a type of communication service that sets up a channel between two or more users without the need to dial a connection or a set up a call. PoC is a new type of service with distinctive features. Many times, PoC is marketed or regarded in the press as a cheaper telephony replacement. The characteristics of PoC makes it very suitable for packet networks, and it has the potential to significantly increase the GPRS traffic in today's networks. It is also a forerunner to the peer-to-peer services over IP for which the IMS architecture provides the capabilities and foundation.

The recent buzzword, PoC, introduces the next wave of technology serving the basic human interaction mode of group communication.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ACELP	: Algebraic Coder Excited Linear
AMR	: Adaptive Multi Rate
API	: Application Interface
ATM	: Asynchronous Transfer Mode
B2BUA	: Back-To-Back User Agent
BGCF	: Breakout Gateway Control Function
CAMEL	: Customized Application for Mobile Network
CAP	: CAMEL Application Part
CK	: Ciphering Key
CSCF	: Call Session Control Function
DNS	: Domain Name System
DSL	: Digital Subscriber Line
EFR	: Enhanced Full Rate
FSM	: Finite State Machine
2G	: Second Generation
3G	: Third Generation
GGSN	: Gateway GPRS Support Node
GLMS	: Group List Management Server
GPRS	: General Packet Radio Service
HLR	: Home Location Register
HSS	: Home Subscriber Services
ICSCF	: Interrogating Call Session Control Function
IETF	: Internet Engineering Task Force
IK	: Integrity Key
IMS	: IP Multimedia Subsystems
IMSI	: International Mobile Subscriber Identity
IPCAN	: IP Connectivity Access Network
ISDN	: Integrated Services Digital Line
ISIM	: IP Multimedia Services Identity Module
LAN	: Local Area Network
MGFC	: Media Gateway Control Function
MRFC	: Media Resource Control Function

MSISDN	: Mobile Subscriber ISDN Number
NAI	: Network Access Identifier
NAT	: Network Address Translation
OMA	: Open Mobile Alliance
PAMR	: Public Access Mobile Radio System
PCSCF	: Proxy Call Session Control Function
PLMN	: Public Land Mobile Network
PMR	: Private Mobile Radio
PoC	: Push to talk Over Cellular
QoS	: Quality of Service
SCF	: Session Control Function
SCSCF	: Serving Call Session Control Function
SIGCOMP	: Signal Compression
SIP	: Session Initiation Protocol
SS7	: Signaling System 7
THIG	: Topology Hiding Internet work Gateway
UAC	: User Agent Client
UAS	: User Agent Server
UDVM	: Universal Decompressor Virtual Machine
UMTS	: Universal Mobile Telecommunication System
USIM	: Universal subscriber Identity Module
WAP	: Wireless Application Protocol

Chapter-1

INTRODUCTION

The IP Multimedia Subsystems is the Next Generation Networking architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3GPP-standardized implementation of SIP, and runs over the standard Internet Protocol (IP). Existing phone systems, both packet-switched and circuit-switched are supported.

As the Internet and mobile telecommunications becomes more and more integrated, new ways to communicate appears. Some of them, like WAP and MMS, have already made their way into every day life and others are on the way. One of the new upcoming applications is Push-to-talk (PTT), a walkie-talkie type of service that gives the user the capability to simultaneously communicate with one or more persons. Push-to-talk uses Voice over IP (VoIP), a way of packaging and transmitting voice data over the Internet, or any other packet data network. Since Push-to-talk uses some kind of network to transport the data, unlike a walkie-talkie that sends it directly to the receivers, it has the potential to communicate worldwide. It also minimizes the bandwidth needed by only sending data when someone is talking, which makes it very cost-efficient when used with a packet-switched network like GPRS.

To achieve interoperability between operators, terminals and networks, a Push-to talk specification over standard mobile networks, PoC (Push-to-talk over Cellular), is being developed by the mobile industry leaders, Ericsson, Nokia, Motorola and Siemens.

1.1 Purpose

The aim of IMS is to provide a single platform to all the current and future services. In addition, users have to be able to execute all their services when roaming as well as from their home networks. To achieve these goals, IMS uses open standard IP protocols, defined by the IETF. So, a multimedia session between two IMS users, between an IMS user and a user on the Internet, and between two users on the Internet is established using exactly the same protocol. Moreover, the interfaces for service developers are also based on IP protocols. This is why IMS truly merges the Internet with

the cellular world; it uses cellular technologies to provide easy access and Internet technologies to provide appealing services.

The main purpose of this project was to design two mobile clients and set up an IMS session between them and implementing PoC service using library called ReSIProcate.

1.2 Reading Guidelines

This thesis starts by presenting the theoretical background needed to understand the basic structure of an IP multimedia subsystems as described in chapter 2 and 3 and PoC as an application of IMS which is described in chapter 5.

At the end, the outputs logs of the mobile clients are also included. The outputs are based on VC 7 (dot net) with use of reSIProcate library to include SIP stack. A brief summary of all the chapters is given below:

Chapter 2:Introduction to IP Multimedia Subsystems

In this chapter a brief introduction to IMS is discussed. A view of both Internet and the cellular world is given. Importance and need of IMS is also discussed.

Chapter 3: Basic architecture of IMS

A detailed introduction to architecture of IMS. All the basic elements and their working is discussed in this chapter.

Chapter 4: Working of Session Initiation Protocol

The protocol used in the project- SIP is explained in this chapter. The structure of SIP messages and working of SIP is also described.

Chapter 5: Basics of Implementation of PoC

A basic introduction to how the PoC service is being implemented and what are the requirements to implement this service on cellular system.

Chapter 6: Implementation of API to check PoC functionality on mobile sets

The detail design of the PoC service, which was to be implemented on the test sets, is discussed here. The outputs are also shown in this chapter.

Chapter 7: Conclusions & Future Scope

In this chapter various benefits of PoC are listed and the future utility of the thesis is described.

Appendix I- A brief introduction to SIGCOMP.

Appendix II- AMR Codec

Appendix III- OMA Standards

Chapter-2

INTRODUCTION TO IP MULTIMEDIA SUBSYSTEMS

Third Generation (3G) networks aim to merge two of the most successful paradigms in communications: cellular networks and the Internet. The IP Multimedia Subsystem (IMS) is the key element in the 3G architecture that makes it possible to provide ubiquitous cellular access to all the services that the Internet provides.

2.1 The Internet World

The Internet has experienced a dramatic growth in the last years. It has evolved from a small network linking a few research sites to a massive worldwide network. The main reason for this growth has been the ability to provide a number of extremely useful services that millions of users like. The best-known examples are the World Wide Web and email, but there are many more, such as instant messaging, presence, VoIP (Voice Over IP), videoconferencing, and shared white boards [1].

2.2 The Cellular World

At present, cellular telephone networks provide services to over one billion users worldwide. These services include, of course, telephone calls, but are not limited to them. Modern cellular networks provide messaging services ranging from simple text messages (e.g., SMS) to fancy multimedia messages that include video, audio and text (e.g., MMS). Cellular users are able to surf the Internet and read email using data connections, and some operators even offer location services, which notify users when a friend or colleague is nearby.

Still, cellular networks did not become so attractive to users only for the services they offered. Their main strength is that users have coverage virtually everywhere. Within a country, users can use their terminals not only in cities, but also in the countryside. In addition, there exist international roaming agreements between operators that allow users to access cellular services when they are abroad [1].

Reduction in terminal size also helped the spread of cellular networks. Old brick-like terminals gave way to modern small terminals that work several days without having

their batteries recharged. This allows people to carry their terminals everywhere with little difficulty.

2.3 Need of IMS

The circuit-switched domain is an evolution of the technology used in 2G networks. The circuits in this domain are optimized to transport voice and video, although they can also be used to transport instant messages. Although circuit-switched technology has been in use since the birth of the telephone the current trend is to substitute it with the more efficient packet-switched technology. Cellular networks follow this trend and, as we said earlier, 3G networks have a packet-switched domain.

The packet-switched domain provides IP access to the Internet. While 2G terminals can act as a modem to transmit IP packets over a circuit, 3G terminals use native packet-switched technology to perform data communications. This way, data transmissions are much faster and the available bandwidth for Internet access increases dramatically. Users can surf the web, read email, download videos, and do virtually everything they can do over any other broadband Internet connection, such as ISDN (Integrated Services Digital Line) or DSL (Digital Subscriber Line) [1]. This means that any given user can install a VoIP client in their 3G terminals and establish VoIP calls over the packet-switched domain. Such a user can take advantage of all the services that service providers on the Internet offer, such as voice mail or conferencing services.

The need of IMS can be described in three reasons:

1) **QoS (Quality of Service)**
2) **Charging**
3) **Integration of different services.**

The main issue with the packet-switched domain to provide real-time multimedia services is that it provides a best effort service without QoS. That is, the network offers no guarantees about the amount of bandwidth a user gets for a particular connection or about the delay the packets experience. Consequently, the quality of a VoIP conversation can vary dramatically throughout its duration [1]. At a certain point the voice of the person at the other end of the phone may sound perfectly clear and, instants later, it can become impossible to understand. Trying to maintain a conversation (or a videoconference) with poor QoS can soon become a nightmare.

So, one of the reasons for creating the IMS was to provide the QoS required for enjoying, rather than suffering, real time multimedia sessions. The IMS takes care of

synchronizing session establishment with QoS provision so that users have a predictable experience.

Another reason for creating the IMS was to be able to charge multimedia sessions appropriately. A user involved in a videoconference over the packet-switched domain usually transfers a large amount of information (which consists mainly of encoded audio and video). Depending on the 3G operators the transfer of such an amount of data may generate large expenses to the user, since operators typically charge based on the number of bytes transferred [1]. The user's operator cannot follow a different business model to charge the user because the operator is not aware of the contents of those bytes: they could belong to a VoIP session, to an instant message, to a web page, or to an email.

On the other hand, if the operator is aware of the actual service that the user is using, the operator can provide an alternative charging scheme that may be more beneficial for the user. For instance, the operator might be able to charge a fixed amount for every instant message, regardless of its size. Additionally, the operator may charge for a multimedia session based on its duration, independently of the number of bytes transferred.

Providing integrated services to users is the third main reason for the existence of the IMS. Although large equipment vendors and operators will develop some multimedia services, operators do not want to restrict themselves to these services. Operators want to be able to use services developed by third parties, combine them, integrate them with services they already have, and provide the user with a completely new service. For example, an operator has a voicemail service able to store voice messages and a third party develops a text-to-speech conversion service [1]. If the operator buys the text-to-speech service from the third party, it can provide voice versions of incoming text messages for blind users.

Chapter-3

BASIC ARCHITECTURE OF IMS

The IMS architecture enables the efficient creation and delivery of an exciting range of emerging multimedia services that can be delivered over mobile, fixed, or converged mobile and fixed networks. It introduces a multimedia session model that enables consistency in the user experience, accelerated service development, and the efficient and flexible delivery of rich multimedia content and services.

3.1 Basic Functions

IMS distributes much of the intelligence to the communications device or the edge of the network, allowing carriers to develop multimedia services that can be delivered and managed across diverse access networks. Because service intelligence is largely distributed to the edge of the network or to the communications device, network operators can more swiftly create enhanced services that can be provisioned across multiple networks [1]. IMS is a strategic technology for next-generation services, and it is offers a standards-based architecture for critical functions such as:

1) Call control
2) Presence
3) Location
4) Content-based billing
5) Profile management
6) Convergence
7) Service interaction
8) Abstract data management and distribution

Network operators create a single IP, asynchronous transfer mode (ATM), or multi-protocol label switching (MPLS) core network for transport, and they can implement IMS architecture across mobile and/or fixed networks. Subscribers can be provided with flexible means of accessing services delivered over IMS infrastructure. They can access IMS services by dialing up over the PSTN, or they can benefit from more rich multimedia services by accessing the infrastructure through the PSTN using digital subscriber line (DSL) services [1]. They can also access IMS services via

broadband cable technology, and mobile users can reap the benefits of IMS via cell phones or WiFi connections.

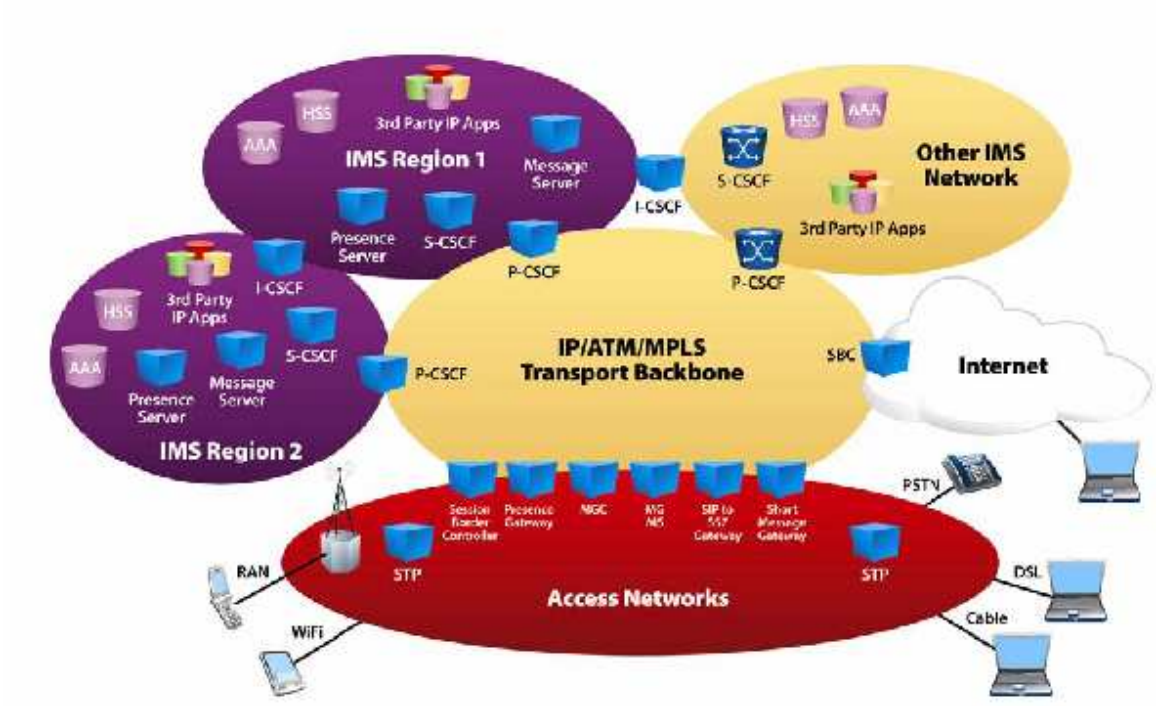

Figure-3.1 Architecture of IMS

In this converged network architecture, IMS provides an underlying infrastructure mechanism for the intelligent interaction of applications and services. Common features and capabilities can be reused across many applications in a "develop once, use many" fashion. For example, presence information can be re-used for applications ranging from push-to-talk to multimedia conferencing [1]. This flexible, open architecture enables service brokering to work in an intelligent way to support feature interaction across multiple applications.

3.2 Key Logical Elements of IMS

The IMS architecture defines the logical elements necessary to implement next-generation multimedia services across multiple network types. It is important to note that these logical functions do not necessarily have a one-to-one relationship with physical equipment. The components of the IMS architecture refer to functions, not platforms.

Multiple functions can be mapped to a single network device, and, conversely, a single function can conceivably be implemented across multiple physical platforms [1]. The following are descriptions of elements and concepts of IMS, which are shown in figure3.1:

a) Home Subscriber Service Function:

The home subscriber service (HSS) manages subscriber information and enables users or servers to locate targets. The profile and the preferences of each user are stored in the HSS database. By centralizing this information, service providers can simplify administration and ensure a consistent view of active subscribers across all services. With IMS, managing mobility is easier than ever. The HSS contains the subscriber information and allows subscribers to locate each other. The Home Subscriber Server (HSS) is the central repository for user-related information. Technically, the HSS is an evolution of the HLR (Home Location Register), which is a GSM node. The HSS contains all the user-related subscription data required to handle multimedia sessions. These data include, among other items, location information, security information (including both authentication and authorization information), user profile information (including the services that the user is subscribed to), and the S-CSCF (Serving-CSCF) allocated to the user [1].

A network may contain more than one HSS, in case the number of subscribers is too high to be handled by a single HSS. In any case, all the data related to a particular user are stored in a single HSS. Networks with a single HSS do not need an SLF(Subscriber Location Function). On the other hand, networks with more than one HSS do require an SLF .The SLF is a simple database that maps users' addresses to HSSs. A node that queries the SLF, with a user's address as the input, obtains the HSS that contains all the information related to that user as the output [2].

b) Call Session Control Function:

The CSCF (Call/Session Control Function), which is a SIP server, is an essential node in the IMS. The CSCF processes SIP signaling in the IMS. There are three types of CSCFs, depending on the functionality they provide [2]. All of them are collectively known as CSCFs, but any CSCF belongs to one of the following three categories:

i) ***P-CSCF (Proxy-CSCF)***

ii) ***S-CSCF (Serving-CSCF)***

iii) ***I-CSCF (Interrogating-CSCF)***

i) Proxy-Call Session Control Function:

IMS enables mobile IP services by its ability to find users in the network and establish sessions. The proxy-call session control function (P-CSCF) is often the entry into the signaling network, and the policy control function (PCF) is a logical entity of the P-CSCF and it provides tight coupling with SIP (Session Initiation Protocol) session control. The P-CSCF helps setup and manage sessions, and it forwards messages between IMS networks [2]. It is the first point of contact for a client accessing the IMS network, whether that client is in its home network or roaming in a visited network. However the subscriber accesses the IMS infrastructure—whether via the PSTN or via a mobile, cable, or WiFi access network—the initial signaling goes straight to the P-CSCF. The chief responsibility of the P-CSCF is to swiftly direct incoming and outgoing messages. Network operators will deploy many of these platforms at the edges of the network. From the SIP point of view the P-CSCF is acting as an outbound/inbound SIP proxy server. This means that all the requests initiated by the IMS terminal or destined to the IMS terminal traverse the P-CSCF [2] . The P-CSCF forwards SIP requests and responses in the appropriate direction (i.e., toward the IMS terminal or toward the IMS network).

The P-CSCF is allocated to the IMS terminal during IMS registration and does not change for the duration of the registration (i.e., the IMS terminal communicates with a single P-CSCF during the registration). The P-CSCF includes several functions, some of which are related to security [2]. First, it establishes a number of IPsec security associations toward the IMS terminal.

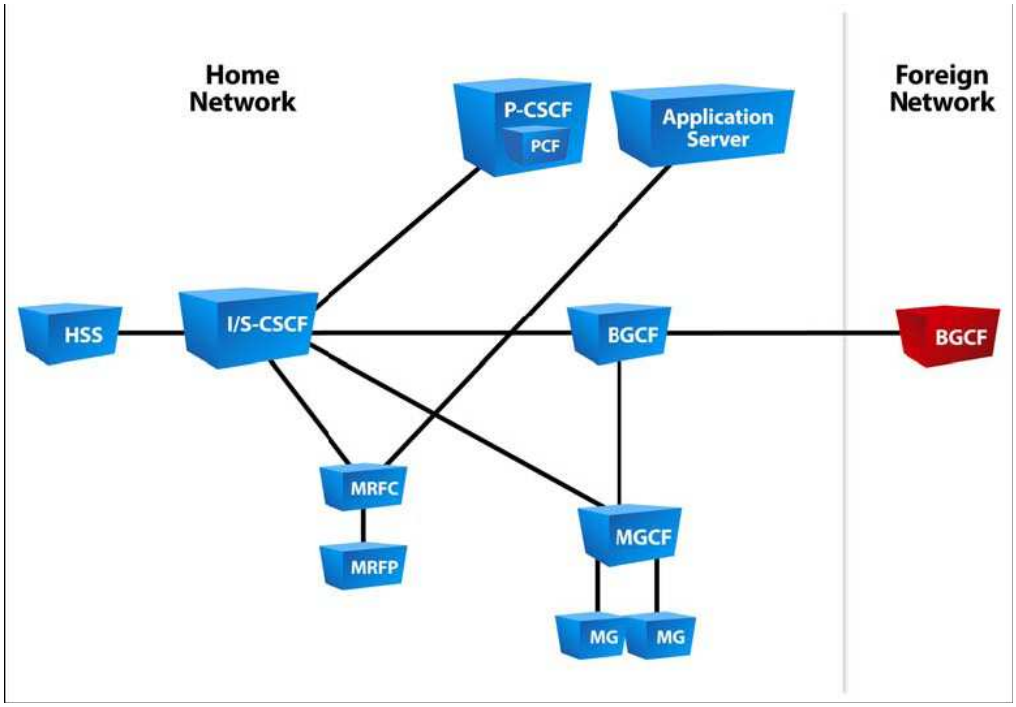

Figure-3.2 Interconnection of CSCF in home network and foreign network

These IPsec security associations offer integrity protection (i.e., the ability to detect that the contents of the message have changed since its creation).Once the P-CSCF authenticates the user (as part of security association establishment) the P-CSCF asserts the identity of the user to the rest of the nodes in the network [2] . This way, other nodes do not need to further authenticate the user, because they trust the P-CSCF. The rest of the nodes in the network user's identity (asserted by the P-CSCF) have a number of purposes, such as providing personalized services and generating account records. Additionally, the P-CSCF verifies the correctness of SIP requests sent by the IMS terminal. This verification keeps IMS terminals from creating SIP requests that are not built according to SIP rules.

The P-CSCF also includes a compressor and a decompressor (see Appendix-I) of SIP messages (IMS terminals include both as well). SIP messages can be large, given that SIP is a text-based protocol [2]. While a SIP message can be transmitted over a broadband connection in a fairly short time, transmitting large SIP messages over a narrowband channel, such as some radio links, may take a few seconds. The mechanism used to reduce the time to transmit a SIP message is to compress the message, send it over the air interface, and decompress it at the other end. The P-CSCF may include a PDF (Policy Decision Function). The PDF may be integrated with the P-CSCF or be

implemented as a stand-alone unit. The PDF authorizes media plane resources and manages Quality of Service over the media plane. The P-CSCF also generates charging information toward a charging collection node [2]. An IMS network usually includes a number of P-CSCFs for the sake of scalability and redundancy. Each P-CSCF serves a number of IMS terminals, depending on the capacity of the node.

The P-CSCF may be located either in the visited network or in the home network. In case the underlying packet network is based on GPRS, the P-CSCF is always located in the same network where the GGSN (Gateway GPRS Support Node) is located. So both P-CSCF and GGSN are either located in the visited network or in the home network [2]. Due to current deployments of GPRS, it is expected that the first IMS networks will inherit this mode and will be configured with the GGSN and P-CSCF in the home network. It is also expected that once IMS reaches the mass market, operators will migrate the configuration and will locate the P-CSCF and the GGSN in the visited network.

ii) Serving Call Session Control Function:

The serving-CSCF (S-CSCF) performs the session control services for subscribers. It maintains session state as needed by the network operator for support of the services and is the core session control function for IMS. It maintains session state for each current user and enables communications with servers of applications and content. The S-CSCF manages all session control messages, and it sends information to the users involved in a session, such as alerts to conference callers about an attendee entering or leaving the session. The S-CSCF is the central node of the signaling plane [2]. The S-CSCF is essentially a SIP server, but it performs session control as well. In addition to SIP server functionality the S-CSCF also acts as a SIP registrar. This means that it maintains a binding between the user location (e.g., the IP address of the terminal the user is logged on) and the user's SIP address of record (also known as a Public User Identity). The main reasons to interface the HSS are:

- To download the authentication vectors of the user who is trying to access the IMS from the HSS. The S-CSCF uses these vectors to authenticate the user.
- To download the user profile from the HSS. The user profile includes the service profile, which is a set of triggers that may cause a SIP message to be routed through one or more application servers.

- To inform the HSS that this is the S-CSCF allocated to the user for the duration of the registration.

The entire SIP signaling the IMS terminals sends, and the entire SIP signaling the IMS terminal receives, traverses the allocated S-CSCF. The S-CSCF inspects every SIP message and determines whether the SIP signaling should visit one or more application servers en route toward the final destination [2]. Those application servers would potentially provide a service to the user.

One of the main functions of the S-CSCF is to provide SIP routing services. If the user dials a telephone number instead of a SIP URI the S-CSCF provides translation services. The S-CSCF also enforces the policy of the network operator. For example, a user may not be authorized to establish certain types of sessions. The S-CSCF keeps users from performing unauthorized operations [2]. A network usually includes a number of S-CSCFs for the sake of scalability and redundancy. Each S-CSCF serves a number of IMS terminals, depending on the capacity of the node. The S-CSCF is always located in the home network.

iii) Interrogating Call Session Control Function:

The interrogating-CSCF (I-CSCF) is the contact point within an operator's network for all connections destined to a subscriber of that network operator, or for a roaming subscriber currently located within that network operator's service area. The I-CSCF is responsible for topology hiding to prevent foreign networks from gaining visibility into a network operator's infrastructure. It identifies which S-CSCF will process SIP requests for a given user, and it leverages information from the HSS to forward all session-related messages to the right S-CSCF. The I-CSCF is a SIP proxy located at the edge of an administrative domain. The address of the I-CSCF is listed in the DNS (Domain Name System) records of the domain [2]. When a SIP server follows SIP procedures to find the next SIP hop for a particular message the SIP server obtains the address of an I-CSCF of the destination domain.

Besides the SIP proxy server functionality the I-CSCF has an interface to the SLF and the HSS. The I-CSCF retrieves user location information and routes the SIP request to the appropriate destination (typically an S-CSCF).

Additionally, the I-CSCF may optionally encrypt the parts of the SIP messages that contain sensitive information about the domain, such as the number of servers in the

domain, their DNS names, or their capacity [2]. This functionality is referred to as THIG (Topology Hiding Inter-network Gateway). THIG functionality is optional and is not likely to be deployed by most networks. A network will include typically a number of I-CSCFs for the sake of scalability and redundancy. The I-CSCF is usually located in the home network, although in some especial cases, such as an I-CSCF (THIG), it may be located in a visited network as well.

c) Application Server:

Network operators deploy application servers to host applications that support the delivery of services. For example, operators can deploy application servers to support services such as IP Centrex, shared white boarding, or presence management. The AS (Application Server) is a SIP entity that hosts and executes services [2] . Depending on the actual service the AS can operate in SIP proxy mode, SIP UA (User Agent) mode (i.e., endpoint), or SIP B2BUA (Back-to-Back User Agent) mode (i.e., a concatenation of two SIP User Agents) [2]. The AS interfaces the S-CSCF using SIP. There are three types of servers which behave as SIP application servers toward the IMS network (i.e., they act as either a SIP proxy server, a SIP User Agent, a SIP redirect server or a SIP Back-to-back User Agent).The interconnection is shown in figure3.3 .

- SIP AS (Application Server): This is the native Application Server that hosts and executes IP Multimedia Services based on SIP. It is expected that new IMS-specific services will likely be developed in SIP Application Servers.
- OSA-SCS (Open Service Access—Service Capability Server): This application server provides an interface to the OSA framework Application Server. It inherits all the OSA capabilities, especially the capability to access the IMS securely from external networks. This node acts as an Application Server on one side (interfacing the S-CSCF with SIP) and as an interface between the OSA Application Server and the OSA Application Programming Interface [2].

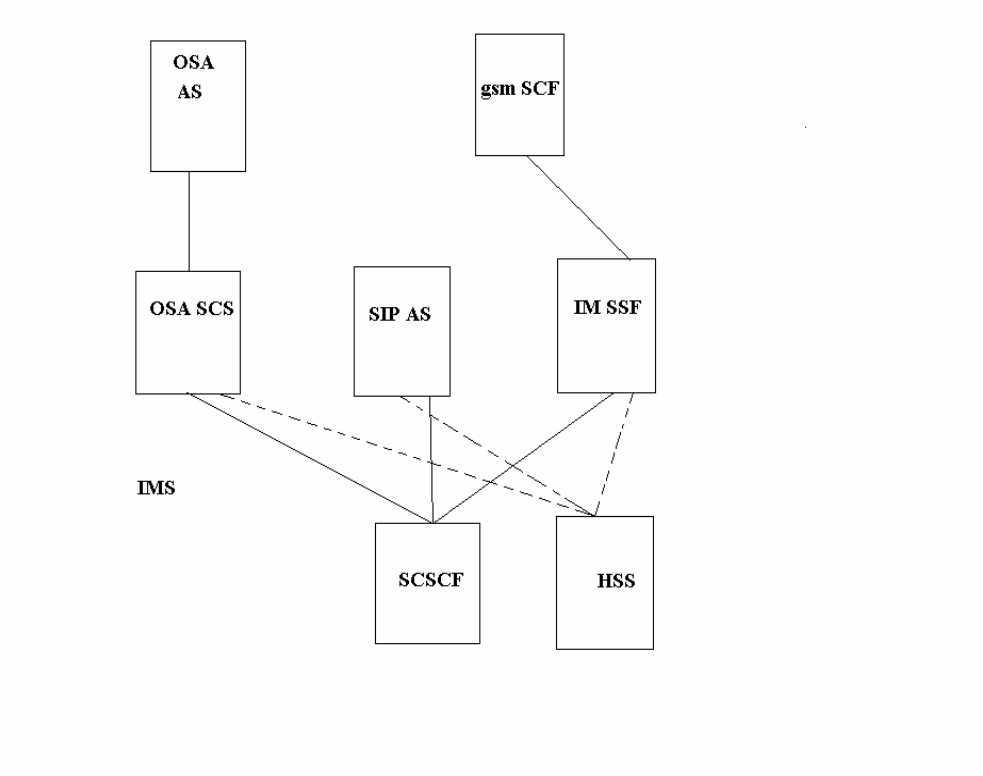

Figure-3.3 Three types of Application Servers

- IM-SSF (IP Multimedia Service Switching Function):This specialized application server allows us to reuse CAMEL (Customized Applications for Mobile network Enhanced Logic) services that were developed for GSM in the IMS. The IM-SSF allows a gsm SCF (GSM Service Control Function) to control an IMS session. The IM-SSF acts as an Application Server on one side (interfacing the S-CSCF with SIP). On the other side, it acts as an SCF (Service Switching Function) [2] , interfacing the gsm SCF with a protocol based on CAP (CAMEL Application Part).

The AS can be located either in the home network or in an external third-party network to which the home operator maintains a service agreement. In any case, if the AS is located outside the home network, it does not interface the HSS.

d) Media Resources:

Media resources stream basic media content to IP endpoints, allow control of those streams, and enables jitter buffering, control error rates, etc. for all IP-based

services. Injecting tones, announcements, or other multimedia content into calls or sessions is enabled by the media resource function control (MRFC) and media resource function processor (MRFP) [2]. While the MRFC provides the intelligence, the MRFP provides the heavy processing required for multimedia services.

e) Gateway Control Functions:

The gateway control functions manage media gateways (MGs) and handle the communications between the IP and SS7 networks to enable interworking with the PSTN (Public Switched Telephone Network). The breakout gateway control function (BGCF) selects the network in which the connection to the PSTN is to occur for a given session. If the BGCF determines that the breakout is to occur in the same network in which the BGCF is located, then the BGCF will select a media gateway control function (MGCF) element, which will be responsible for the interworking with the PSTN for signaling [2] . If the breakout is in another network, the BGCF will forward this session signaling to another BGCF, or an MGCF, depending on the configuration, in the selected network. The BGCF is essentially a SIP server that includes routing functionality based on telephone numbers. The BGCF is only used in sessions that are initiated by an IMS terminal and addressed to a user in a circuit-switched network, such as the PSTN or the PLMN (Public Land Mobile Network). The main functionality of the BGCF is:

1) To select an appropriate network where interworking with the circuit-switched domain is to occur.

2) To select an appropriate PSTN/CS gateway, if interworking is to occur in the same network where the BGCF is located [2].

The PSTN gateway provides an interface toward a circuit-switched network, allowing IMS terminals to make and receive calls to and from the PSTN (or any other circuit-switched network). Figure3.4 shows a BGCF and a decomposed PSTN gateway

that interfaces the PSTN. The PSTN gateway is decomposed into the following functions:

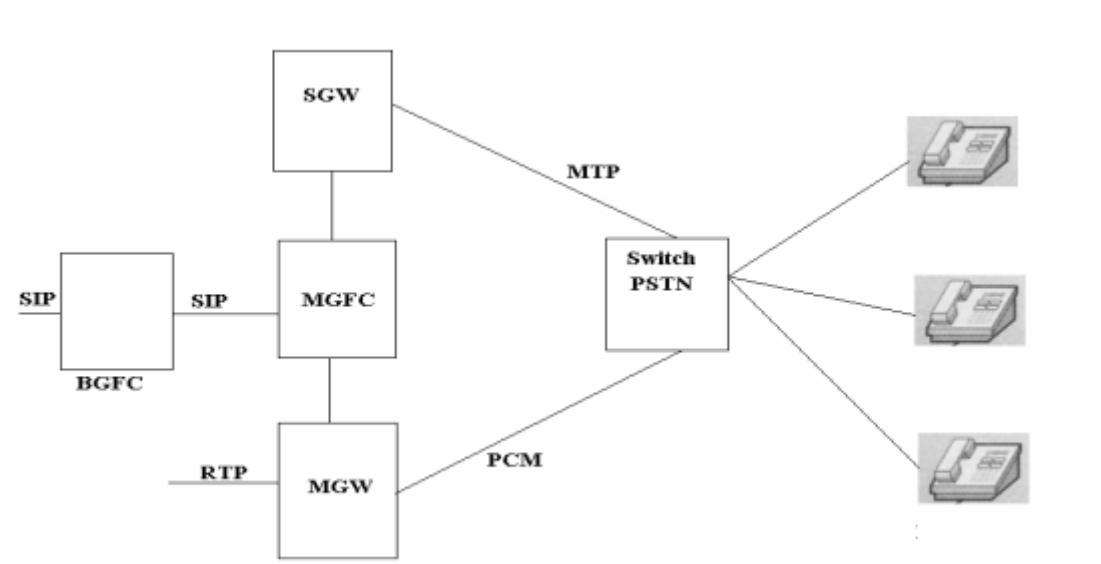

Figure-3.4 The PSTN/CS gateway interfacing a CS network

- SGW (Signaling Gateway): the Signaling Gateway interfaces the signaling plane of the CS network (e.g., the PSTN). The SGW performs lower layer protocol conversion [2] . For instance, an SGW is responsible for replacing the lower MTP transport with SCTP (Stream Control Transmission Protocol) over IP.
- MGCF (Media Gateway Control Function): the MGCF is the central node of the PSTN/CS gateway. It implements a state machine that does protocol conversion and maps SIP (the call control protocol on the IMS side) to either ISUP over IP or BICC over IP (both BICC and ISUP are call control protocols in circuit-switched networks)[2] . In addition to the call control protocol conversion the MGCF controls the resources in an MGW (Media Gateway).
- MGW (Media Gateway): the Media Gateway interfaces the media plane of the PSTN or CS network. On one side the MGW is able to send and receive IMS media over the Real-Time Protocol (RTP). On the other side the MGW uses one or more PCM (Pulse Code Modulation) time slots to connect to the CS network [2] . Additionally, the MGW performs transcoding when the IMS terminal does not support the codec used by the CS side.

3.3 Home Networks and Visited Networks

The IMS borrows a few concepts from GSM and GPRS, such as having a home and a visited network. In the cellular model, when we use our cell phones in the area where we reside, we are using the infrastructure provided by our network operator. This infrastructure forms the so-called home network [3]. On the other hand, if we roam outside the area of coverage of our home network (e.g., when we visit another country), we use an infrastructure provided not by our operator, but by another operator. This infrastructure is what we call the visited network, because effectively we are a visitor in this network. In order to use a visited network the visited network operator has to have signed a roaming agreement with our home network operator. In these agreements both operators negotiate some aspects of the service provided to the user, such as price of calls, quality of service, or how to exchange accounting records.

The IMS reuses the same concept of having a visited and a home network. Most of the IMS nodes are located in the home network, but there is a node that can be either located in the home or the visited network. That node is the P-CSCF (Proxy-CSCF). The IMS allows two different configurations, depending on whether the P-CSCF is located in the home or visited network. Additionally, when the IP-CAN (IP Connectivity Access Network) is GPRS the location of the P-CSCF is subordinated to the location of the GGSN. In roaming scenarios, GPRS allows location of the GGSN either in the home or in the visited network (the SGSN is always located in the visited network).

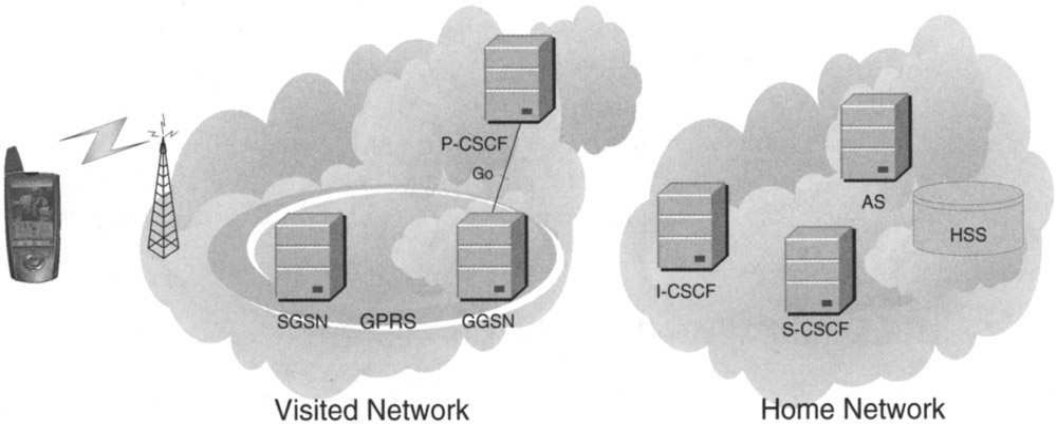

Figure-3.5 The P-CSCF located in the visited network

In the IMS, both the GGSN and the P-CSCF share the same network. This allows the P-CSCF to control the GGSN over the so-called Go interface. As both the P-CSCF and the

GGSN are located in the same network the Go interface is always an intra-operator interface, which makes its operation simpler [3].

Figure3.5 shows a configuration where the P-CSCF (and the GGSN) is located in the visited network. This configuration represents a longer-term vision of the IMS, because it requires IMS support from the visited network.

It is not expected that all networks in the world will deploy IMS simultaneously.

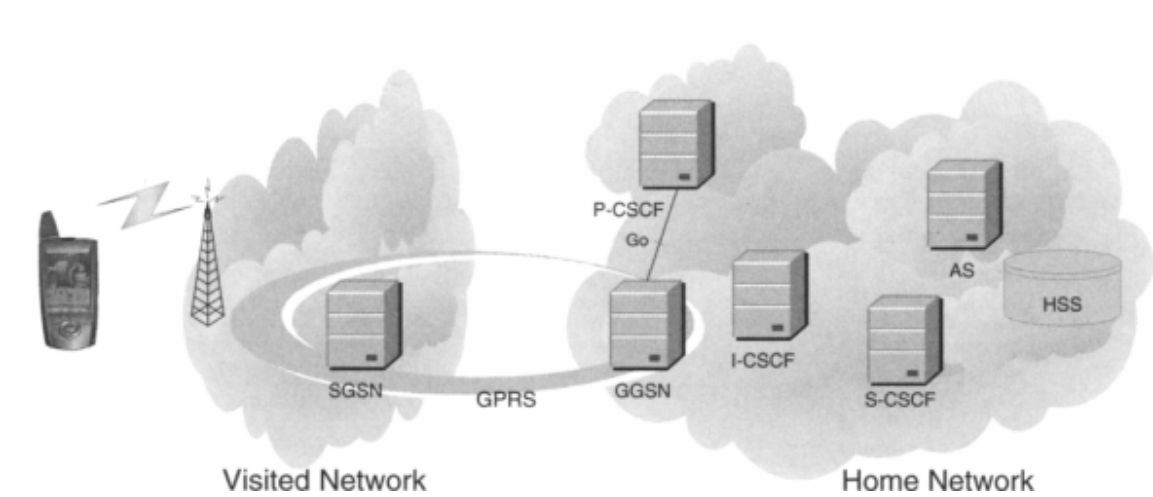

Figure- 3.6 The P-CSCF located in the home network

Consequently, it is not expected that all roaming partners will upgrade their GGSNs at the same time the home network operator starts to provide the IMS service. So, we expect that early IMS deployments will locate the P-CSCF in the home network, as shown in Figure 3.6. This figure shows a near term configuration where both the P-CSCF and the GGSN are located in the home network [3]. This configuration does not require any IMS support from the visited network. Particularly, the visited network does not need to have a 3GPP Release 5 compliant GGSN. The visited network only provides the radio bearers and the SGSN. So, this configuration can be deployed from the very first day of the IMS. As a consequence, it is expected that this will be the most common configuration in the early years of IMS deployments [3].

Even so, this configuration has a severe disadvantage with respect to the configuration where the P-CSCF and GGSN are located in the visited network. Since the media plane traverses the GGSN and the GGSN is located in the home network the media are first routed to the home network and then to their destination. This creates an undesired trombone effect that causes delays in the media plane.

There is a misconception that compression between the IMS terminal and the P-CSCF is enabled just to save a few bytes over the air interface. This is not the motivation lying behind compression. Particularly, it is not worth saving a few bytes of signaling when the IMS terminal will be establishing a multimedia session (e.g., audio, video) that will use much more bandwidth than the signaling [3]. The main motivation for compression is to reduce the time to transmit SIP messages over the air interface.

3.4 IMS and the Delivery of Next-Generation Services

One way to learn about the IMS architecture is to review a sample implementation. For example, the following diagram visually represents how IMS logical functions interact to support a few sample applications. In this example, push-to-talk, short messaging, and instant messaging all leverage a common infrastructure to enable the efficient delivery of multimedia services [3]. Services are developed in SIP and hosted on application servers.

The network operator can swiftly create additional services that repurpose application code and can leverage the underlying infrastructure to offer new services in the future. These applications leverage data layer logical functions, elements, and features. For example, all of these applications rely on the HSS to manage subscriber information and enable users or servers to locate targets.

The SIP applications also leverage user presence information. The network operator would only have to write the logic to manage presence once, and allow current and future applications to tap into this logic to incorporate presence information.

The I-CSCF and S-CSCF functions provide access to the signaling network for the applications and prevent foreign networks from gaining visibility into the network. The MRFC provides the intelligence to instruct the MFRP to process the media resources, while the MGCF instructs the MG to deliver the media services to the session. Together, the MGCF and MG deliver media services to-and-from the PSTN. The P-CSCF at the edge of the packet access network serves as a proxy [3] . If the session

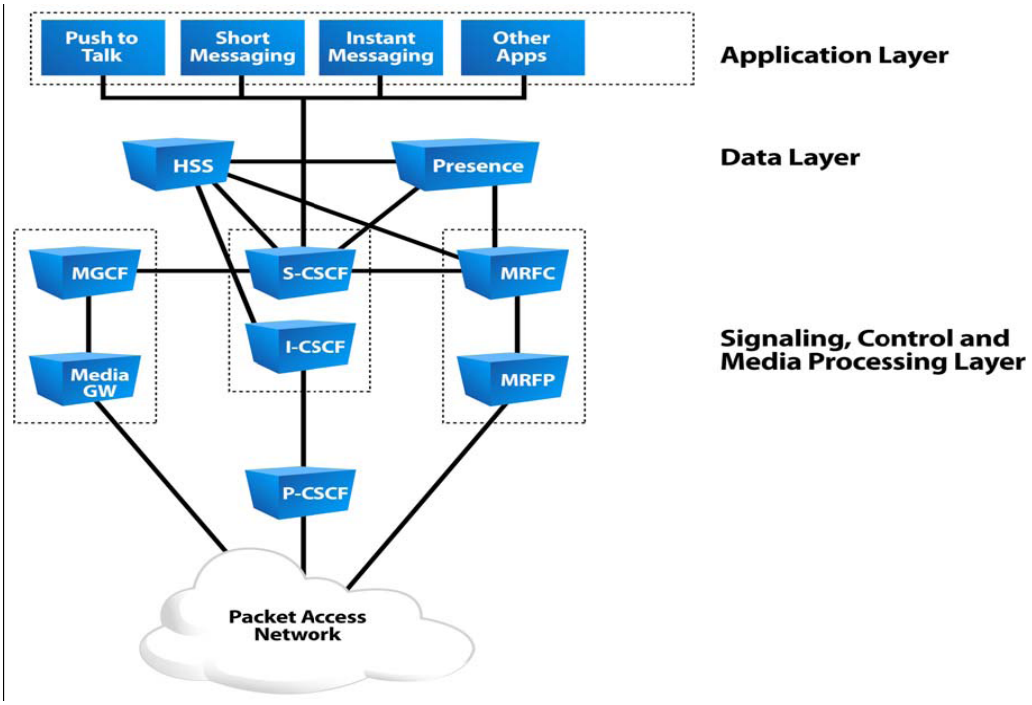

Figure-3.7 Three layers of IMS

involves more than two members, multiple P-CSCFs might be involved in the session control function.

3.5 Identification in IMS

In a network of any kind, it must be possible to uniquely identify users. This is the property that allows a particular phone to ring (as opposed to a different telephone) when we dial a sequence of digits in the PSTN (Public Switched Telephone Network).

Central to any network is the ability of the operator to identify users, so that calls can be directed to the appropriate user. In the PSTN, users are identified by a telephone number (i.e., a collection of ordered digits that identify the telephone subscriber). The telephone number that identifies a subscriber may be represented in different formats: a local short number, a long-distance number, or an international number. In essence, these are just different representations of the same telephone subscriber [3] . The length of the digits depends on the destination of the call (e.g., same area, another region, or another country).

Additionally, when a service is provided, sometimes there is a need to identify the service. In the PSTN services are identified by special numbers, typically through a special prefix, such as 800 numbers. IMS also provides mechanisms to identify services. In the IMS there is also a deterministic way to identify users. An IMS user is allocated

with one or more *Public User Identities.* The home operator is responsible for allocating these Public User Identities to each IMS subscriber [3] . A Public User Identity is either a SIP URI or a TEL URL. Public User Identities are used as contact information on business cards. In the IMS, Public User Identities are used to route SIP signaling. If we compare the IMS with GSM, a Public User Identity is to the IMS what an MSISDN (Mobile Subscriber ISDN Number) is to GSM.

When the Public User Identity contains a SIP URI, it typically takes the form of sip: first.last@operator.com, although IMS operators are able to change this scheme and address their own needs. Additionally, it is possible to include a telephone number in a SIP URI using the following format:

sip:+1–212–555–0293@operator.com;user=phone

This format is needed because SIP requires that the URI under registration be a SIP URI. So, it is not possible to register a TEL URL in SIP, although it is possible to register a SIP URI that contains a telephone number.

The TEL URL is the other format that a Public User Identity can take. The following is a TEL URL representing a phone number in international format:

tel:+1–212–555–0293

TEL URLs are needed to make a call from an IMS terminal to a PSTN phone, because only digits represent PSTN numbers. On the other hand, TEL URLs are also needed if a PSTN subscriber wants to make a call to an IMS user, because a PSTN user can only dial digits [3] .

We envision that operators will allocate at least one SIP URI and one TEL URL per user. There are reasons for allocating more than one Public User Identity to a user, such as having the ability to differentiate personal (e.g., private) identities, that are known to friends and family from business Public User Identities (that are known to colleagues), or for triggering a different set of services.

The IMS brings an interesting concept: *a set of implicitly registered public user identities.* In regular SIP operation, each identity that needs to be registered requires a SIP REGISTER request. In the IMS, it is possible to register several Public User Identities in one message, saving time and bandwidth [3].

Each IMS subscriber is assigned a *Private User Identity.* Unlike Public User Identities, Private User Identities are not SIP URIs or TEL URLs; instead, they take the format of a NAI (Network Access Identifier). The format of a NAI is username@operator.com.

Unlike Public User Identities, Private User Identities are not used for routing SIP requests; instead, they are exclusively used for subscription identification and authentication purposes. A Private User Identity performs a similar function in the IMS as an IMSI (International Mobile Subscriber Identifier) does in GSM. The user need not know a Private User Identity, because it might be stored in a smart card, in the same way that an IMSI is stored in a SIM (Subscriber Identity Module).

Operators assign one or more Public User Identities and a Private User Identity to each user. In the case of GSM/UMTS the smart card stores the Private User Identity and at least one Public User Identity. The HSS, as a general database for all the data related to a subscriber, stores the Private User Identity and the collection of Public User Identities allocated to the user. The HSS and the S-CSCF also correlate the Public and Private User Identities [3] . The relation between an IMS subscriber, the Private User Identity and the Public User Identities is shown in figure 3.8.

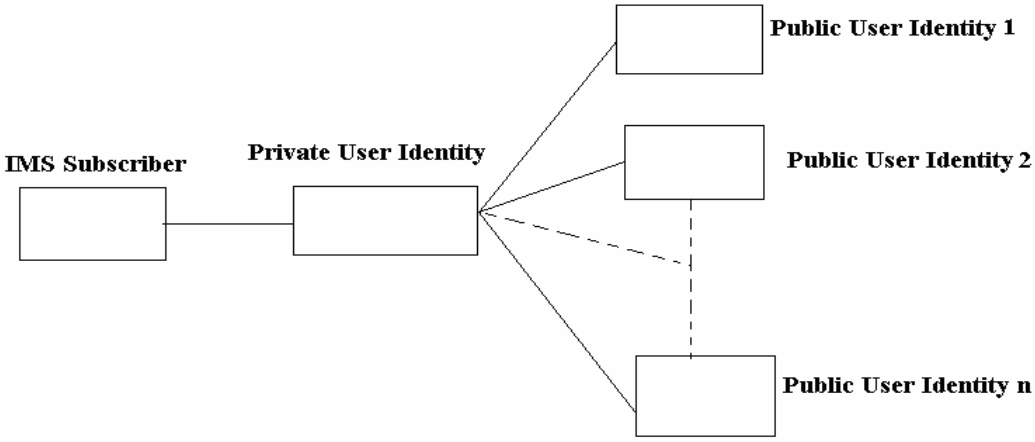

Figure- 3.8 Relation of Private and Public User Identities in 3GPRS

An IMS subscriber is assigned one Private User Identity and a number of Public User Identities. 3GPP Release 6 has extended the relationship of Private and Public User Identities, as shown in figure 3.9. An IMS subscriber is allocated not with one, but with a number of Private User Identities. In the case of UMTS, only one Private User Identity is stored in the smart card, but users may have different smart cards that they insert in different IMS terminals.

It might be possible that some of those Public User Identities are used in combination with more than a single Private User Identity. This is the case of Public User Identity #2 in Figure 3.9, because it is assigned to both Private User Identity #1 and #2.

This allows Public User Identity #2 to be used simultaneously from two IMS terminals, each one assigned with a different Private User Identity (e.g., different smart cards are inserted in different terminals).

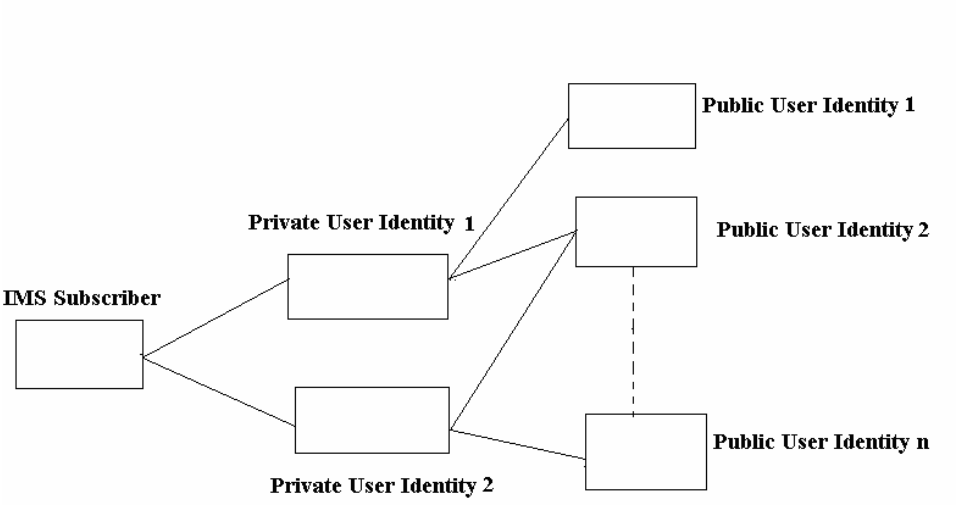

Figure-3.9 Relation of Private and Public User Identities in 3GPP R6

Central to the design of 3GPP terminals is the presence of a UICC (Universal Integrated Circuit Card). The UICC is a removable smart card that contains a limited storage of data [3]. The UICC is used to store, among other things, subscription information, authentication keys, a phonebook, and messages.

GSM and 3GPP specifications rely on the presence of a UICC in the terminal for its operation. Without a UICC present in the terminal the user can only make emergency calls. The UICC allows users to easily move their user subscriptions (including the phonebook) from one terminal to another. The user simply removes the smart card from a terminal and inserts it into another terminal. UICC is a generic term that defines the physical characteristics of the smart card (like the number and disposition of pins, voltage values, etc.). The interface between the UICC and the terminal is standardized.

A UICC may contain several logical applications, such as a SIM (Subscriber Identity Module), a USIM (Universal Subscriber Identity Module), and an ISIM (IP multimedia Services Identity Module). Additionally, a UICC can contain other applications; such as a telephone book Figure 3.10 represents a UICC that contains several applications.

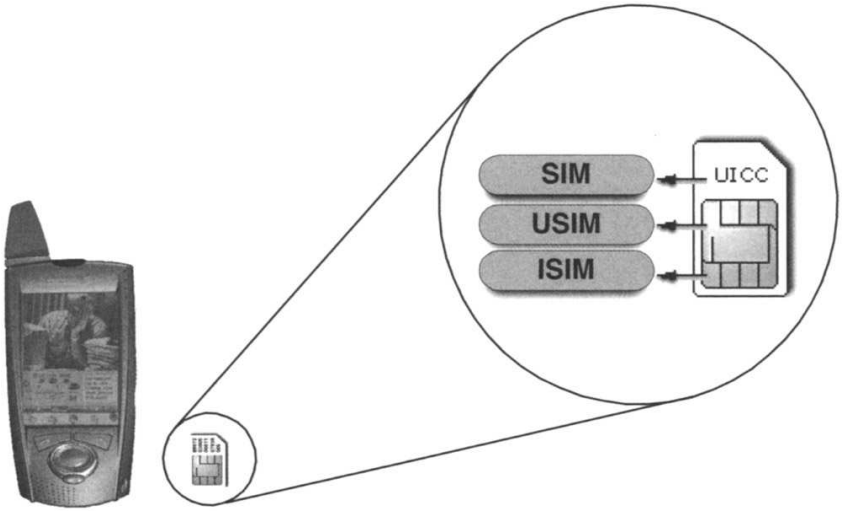

Figure-3.10 SIM, USIM, and ISIM in the UICC of 3GPP IMS terminals

SIM provides storage for a collection of parameters (e.g., user subscription information, user preferences, authentication keys, and storage of messages) that are essential for the operation of terminals in GSM networks [3] . Although the terms UICC and SIM are often interchanged, UICC refers to the physical card, whereas SIM refers to a single application residing in the UICC that collects GSM user subscription information. SIM is widely used in 2G (Second Generation) networks, such as GSM networks.

USIM is another example of an application that resides in third-generation UICCs. USIM provides another set of parameters (similar in nature, but different from those provided by SIM) which include user subscriber information, authentication information, payment methods, and storage for messages [3] . USIM is used to access UMTS (Universal Mobile Telecommunication) networks, the third-generation evolution of GSM.A USIM is required if a circuit-switched or packet-switched terminal needs to operate in a 3G (Third Generation) network. Obviously, both SIM and USIM can co-exist in the same UICC, so that if the terminal is capable, it can use both GSM and UMTS networks.

Figure 3.10 shows a simplified version of the structure of USIM. USIM stores, among others, the following parameters:

- IMSI (International Mobile Subscriber Identity): IMSI is an identity assigned to each user. This identity is not visible to users themselves, but only to the network. IMSI

is used as the user identification for authentication purposes. The Private User Identity is the equivalent of the IMSI in IMS.

- MSISDN (Mobile Subscriber ISDN Number): this field stores one or more telephone numbers allocated to the user. A Public User Identity is the equivalent of the MSISDN in the IMS.
- CK (Ciphering Key) and IK (Integrity Key): these are the keys used for ciphering and integrity protection of data over the air interface. USIM separately stores the keys

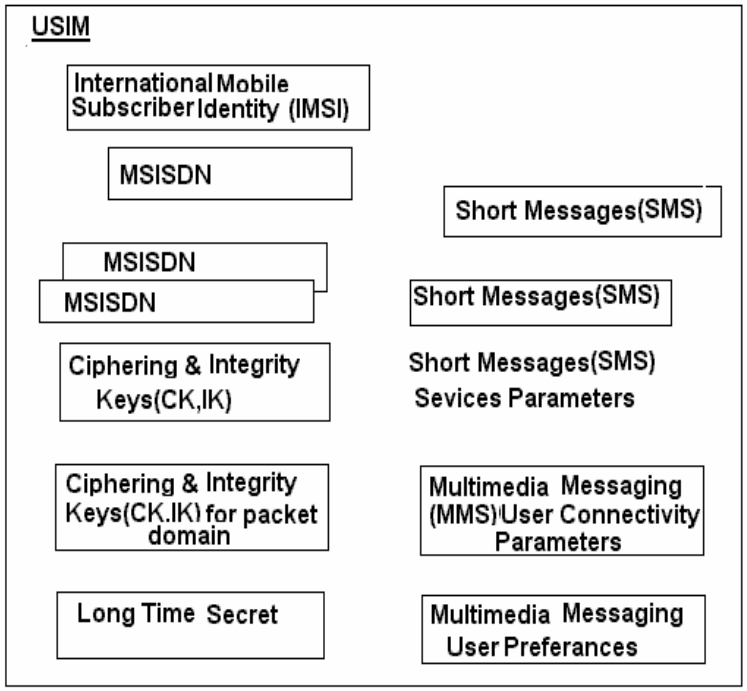

Figure-3.11 Simplified representation of the structure of the USIM application

used in circuit-switched and packet-switched networks [3] .

- Long term secret: USIM stores a long-term secret that is used for authentication purposes and for calculating the integrity and cipher keys used between the terminal and the network.
- SMS (Short Messages Service): USIM provides storage for short messages and their associated data (e.g., sender, receiver, and status).
- SMS (Short Message Service) parameters: this field in the USIM stores configuration data related to the SMS service, such as the address of the SMS center or the protocols that are supported.
- MMS (Multimedia Messaging Service) user connectivity parameters: this field stores configuration data related to the MMS service, such as the address of the MMS server and the address of the MMS gateway.

- MMS user preferences: this field stores the user preferences related to the MMS service, such as the delivery report flag, read-reply preference, priority, and time of expiration [3] .

A third application that may be present in the UICC is ISIM. ISIM is of special importance for the IMS, because it contains the collection of parameters that are used for user identification, user authentication, and terminal configuration when the terminal operates in the IMS. ISIM can co-exist with a SIM, a USIM, or both applications in the same UICC.

Figure 3.12depicts the structure of the ISIM application. The relevant parameters stored in ISIM are:

- Private User Identity: ISIM stores the Private User Identity allocated to the user. There can only be one Private User Identity stored in ISIM.
- Public User Identity: ISIM stores one or more SIP URIs of Public User Identities allocated to the user.
- Home Network Domain URI: ISIM stores the SIP URI that contains the home network domain name. This is used to find the address of the home network during the registration procedure [3]. There can only be one home network domain name URI stored in ISIM.

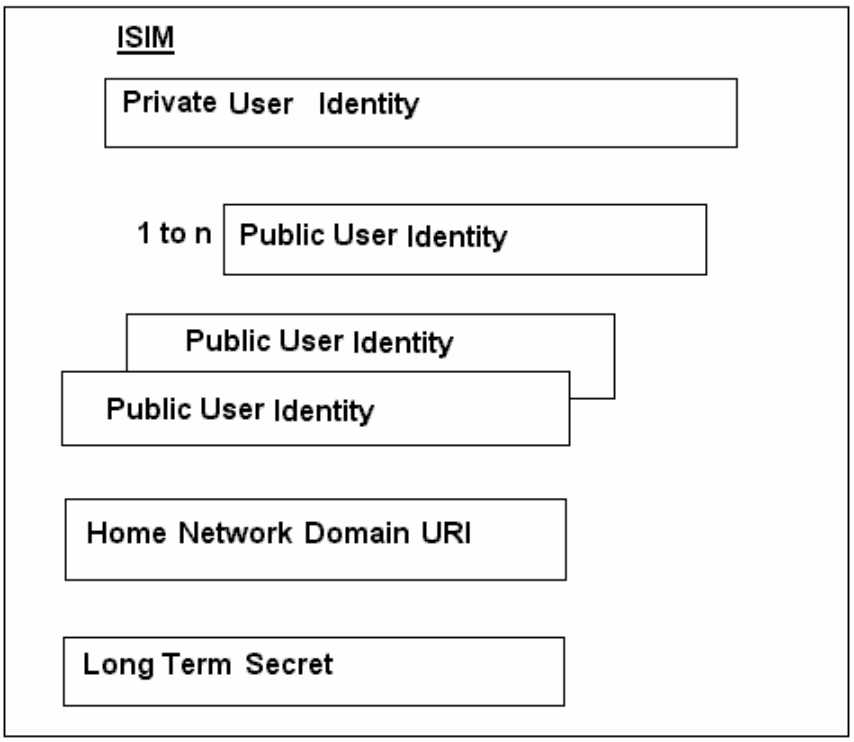

Figure-3.12 Structure of an ISIM application

- Long-term secret: ISIM stores a long-term secret that is used for authentication purposes and for calculating the integrity and cipher keys used between the terminal and the network. The IMS terminal uses the integrity key to integrity protect the SIP signaling that the IMS terminal sends to or receives from the P-CSCF. If the signaling is ciphered, the IMS terminal uses the cipher key to encrypt and decrypt the SIP signaling that the IMS terminal sends to or receives from the P-CSCF [3] . All the above mentioned fields are read-only, meaning that the user cannot modify the values of the parameters.

Equation 1

Chapter-4

WORKING OF SESSION INITIATION PROTOCOL

4.1 Introduction

IMS relies on the session initiation protocol (SIP) for the development of applications and services. SIP is a signaling protocol specifically designed for multimedia. It offers advantages over signaling system 7 (SS7), which is used throughout the public switched telephone network (PSTN) and was designed specifically for voice services. Unlike SS7, SIP was designed to support voice, data, and multimedia services. SIP is focused on session control—establishing, changing and terminating sessions—and it supports dynamic modification of multimedia streams for any given session. SIP was originally developed within the SIP working group in the IETF. Even though SIP was initially designed to invite users to existing multimedia conferences, today it is mainly used to create, modify and terminate multimedia sessions [4]. In addition, there exist SIP extensions to deliver instant messages and to handle subscriptions to events.

Protocols developed by the IETF have a well-defined scope. The functionality to be provided by a particular protocol is carefully defined in advance before any working group starts working on it. In our case the main goal of SIP is to deliver a session description to a user at their current location [4]. Once the user has been located and the initial session description delivered, SIP can deliver new session descriptions to modify the characteristics of the ongoing sessions and terminate the session whenever the user wants.

Session Initiation Protocol (SIP) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. SIP is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more end points [4]. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP provides the capabilities to:

• Determine the location of the target end point—SIP supports address resolution, name mapping, and call redirection.

• Determine the media capabilities of the target end point—Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between the end points. Conferences are established using only the media capabilities that can be supported by all end points.

• Determine the availability of the target end point—If a call cannot be completed because the target end point is unavailable, SIP determines whether the called party is already on the phone or did not answer in the allotted number of rings. It then returns a message indicating why the target end point was unavailable.

• Establish a session between the originating and target end point—If the call can be completed, SIP establishes a session between the end points [4]. SIP also supports mid-call changes, such as the addition of another end point to the conference or the changing of a media characteristic or codec.

• Handle the transfer and termination of calls—SIP supports the transfer of calls from one end point to another. During a call transfer, SIP simply establishes a session between the transferee and a new end point (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of the following roles:

• User agent client (UAC)—A client application that initiates the SIP request.

• User agent server (UAS)—A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

Typically, a SIP end point is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiated the request.

4.2 Architecture of SIP network

From an architecture standpoint, the physical components of a SIP network can be grouped into two categories: clients and servers. Figure 4.1 illustrates the architecture of a SIP network [5].

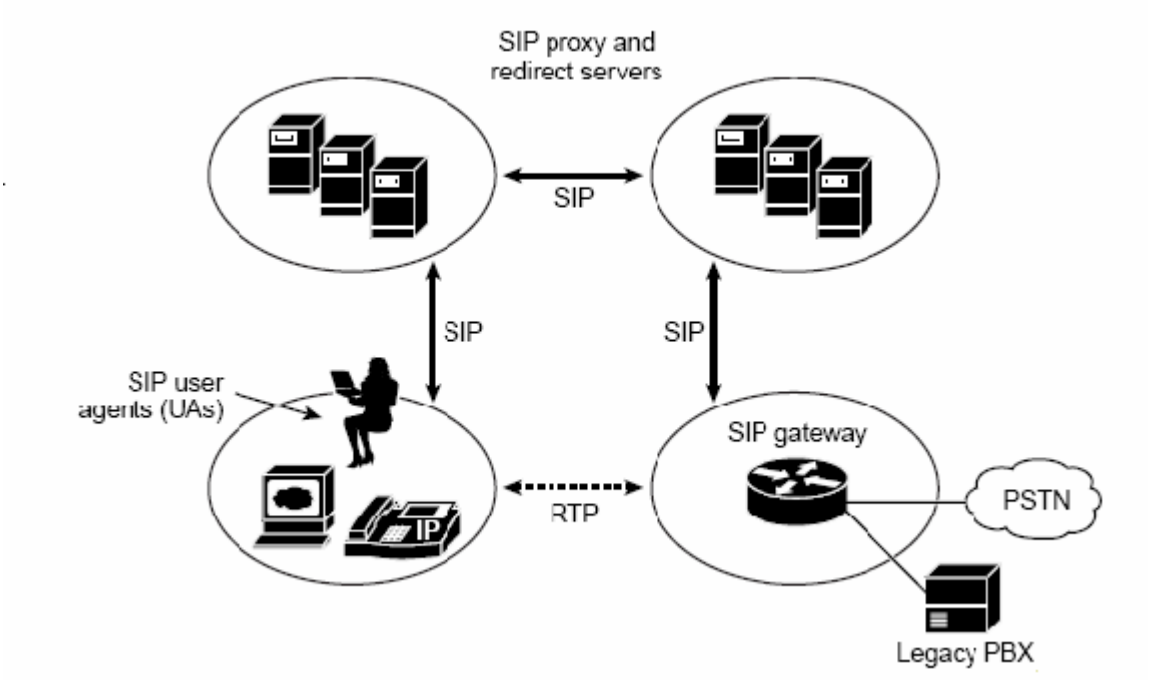

Figure-4.1 Architecture for SIP

a) SIP Clients

SIP clients include:

• Phones—Can act as either a UAS or UAC. Soft phones (PCs that have phone capabilities installed) and SIP IP phones can initiate SIP requests and respond to requests.

• Gateways—Provide call control. Gateways provide many services, the most common being a translation function between SIP conferencing endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway translates between audio and video codecs and performs call setup and clearing on both the LAN side and the switched-circuit network side [5].

b) SIP Servers

SIP servers include:

• Proxy server—The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on the client's behalf. Basically, proxy servers receive SIP messages and forward them to the next SIP server in the network [5]. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.

• Redirect server—Provides the client with information about the next hop or hops that a message should take and then the client contacts the next hop server or UAS directly.

• Registrar server—Processes requests from UACs for registration of their current location. Registrar servers are often co-located with a redirect or proxy server.

4.3 SIP Messages

They are basically of two types requests and responses. These requests and responses include different headers to describe the details of the communication.

a) Header fields:

SIP header fields are similar to HTTP header fields in both syntax and semantics. Messages use header-fields to specify such things as caller, callee, the path of the message, type and length of message body [6]. There are 44 SIP headers. These headers can be divided into four different groups of headers:

- General header fields
- Entity header fields
- Request header fields
- Response header fields

General header fields apply to both request and response messages.

Entity header fields define information about the message body or, if no body is present, about the resources identified by the request.

Request header fields act as request modifiers and allow the client to pass additional information about the request, and about the client itself, to the server.

Response header fields allow the server to pass additional information about the response, which cannot be placed in the Start-Line (in responses it is called Status-Line). These header fields give information about the server and about further access to the resource [6].

Table- 4.1 Different types of Header Fields

Header	Explanation
1) Contact	Provides URLs where user can be reached for further communications. It is used in INVITE, OPTIONS, ACK and REGISTER
2) Content Length	Indicates the size of message body sent to recipient.
3) Content Type	Indicates the media type of message body sent to recipient.
4) Cseq	Command Sequence uniquely identifies a request within a call ID
5) Encryption	Specifies that the content has been encrypted.
6) From	Indicates the initiator of the requests.
7) Route	Route request header field determines the route taken by a request.
8) Subject	Indicates the nature of call
9) To	Specifies the recipient of request

b) SIP Requests:

The request is characterized by the Start-Line, called Request-Line and starts with a method token followed by a Request-URI and the protocol version. There are six different kinds of requests in the current version of SIP They are referred to as methods and are here listed with their functionality [6].

- **REGISTER:** Conveys information about a user's location to a SIP server.
- **INVITE:** The INVITE method indicates that the user or service is being invited to participate in a session.
- **ACK:** The ACK request confirms that the client has received a final response to an INVITE. ACK is used only with INVITE requests.
- **OPTIONS:** The OPTIONS method queries the capabilities of the server/end system, but does not set up a connection.
- **BYE:** The user agent client uses BYE to indicate to the server that it wishes to release the call.

- **CANCEL:** The CANCEL request cancels a pending request with the same Call-ID, To, from and CSeq (sequence number only) header field values, but does not affect a completed request or existing calls.

The following table shows an example of a SIP requests

Table- 4.2 Example of Sip Request

Cseq: 1 INVITE Content Length…	Command sequence number and type Length of body SIP method

Blank line separates header from body

v = 0 o=anil289607830INIPG 157.227.12.184 s = Urgent phone call from anil c = INIPG anilworkstation.com t = 312688749 3126289399 m = audio 5002 RTP/AVP 03.5	SDP version Owner/Creator and Session Identifier Name of the session Connection information Time the session is active Media name and Transport address

Table- 4.3 Meaning of the symbols used in the SIP messages

Type	Meaning
v	Protocol Version
b	Bandwidth Information
o	Owner of session and session identifier
z	Time zone adjustments
s	Name of session
k	Encryption key
i	Information about session
a	Attribute lines

u	URL containing a description of session
t	Time when the session is active
e	Email address to obtain information about session
t	Times when session will be repeated
p	Phone number to obtain information about session
m	Media line
c	Connection information
i	Information about media line

c) SIP Responses:

The recipient, after receiving and interpreting a request message, responds with a SIP response message, indicating the status of the server, success or failure. The responses can be of different kinds and the type of response is identified by a status code, a 3-digit integer [7]. The responses are divided into six different classes as shown in the table.

Table- 4.4 Different Types of Responses

Response Code Series	Explanation	Example Response Codes
1xx	Informational	100-Trying 180-Ringing 181-Call is being forwarded
2xx	Successful	200-ok
3xx	Redirection	301-Moved permanently 302-Moved temporarily 305-Use proxy
4xx	Request Failure	400-Bad request

		401-Unauthorized 403-Forbidden 404-Not found 407-Proxy Authentication Registered
5xx	Server failure	500-Server internal error 501-Not implemented 502-Bad gateway 504-Server timeout
6xx	Global Failures	600-Busy everywhere 603-Decline

4.4 How SIP works?

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more end points. Users in a SIP network are identified by unique SIP addresses [8]. A SIP address is similar to an e-mail address and is in the format of sip: userID@gateway.com. The user ID can be a user name. Users register with a registrar server using their assigned SIP addresses. The registrar server provides this information to the location server upon request. When a user initiates a call, a SIP request is sent to a SIP server (either a proxy or a redirect server). The request includes the address of the caller (in the From header field) and the address of the intended callee (in the To header field). Over time, a SIP end user might move between end systems. The location of the end user can be dynamically registered with the SIP

server. The location server can use one or more protocols to locate the end user. Because the end user can be logged in at more than one station and because the location server can sometimes have inaccurate information, it might return more than one address for the end user. If the request is coming through a SIP proxy server, the proxy server will try each of the returned addresses until it locates the end user [8]. If the request is coming through a SIP redirect server, the redirect server forwards all the addresses to the caller in the contact header field of the invitation response.

4.5 An Example of working of IMS using SIP

Suppose Bobby is a student in France and now visiting Finland. He calls his sister Anne who is working in Germany but presently visiting America [9]. Both are IMS users. Choosing GPRS as IPCAN for this example we will study the session establishment and algorithms in IMS using SIP. We can say that Bobby is registered in France and is roaming in Finland whereas Anne is registered in Germany but roaming in America. So for session control in an IMS network following are the prerequisites:

a) Getting an IPCAN (IP Connectivity Access Network)

b) IMS level registration

c) PCSCF discovery

d) Basic Session Set Up

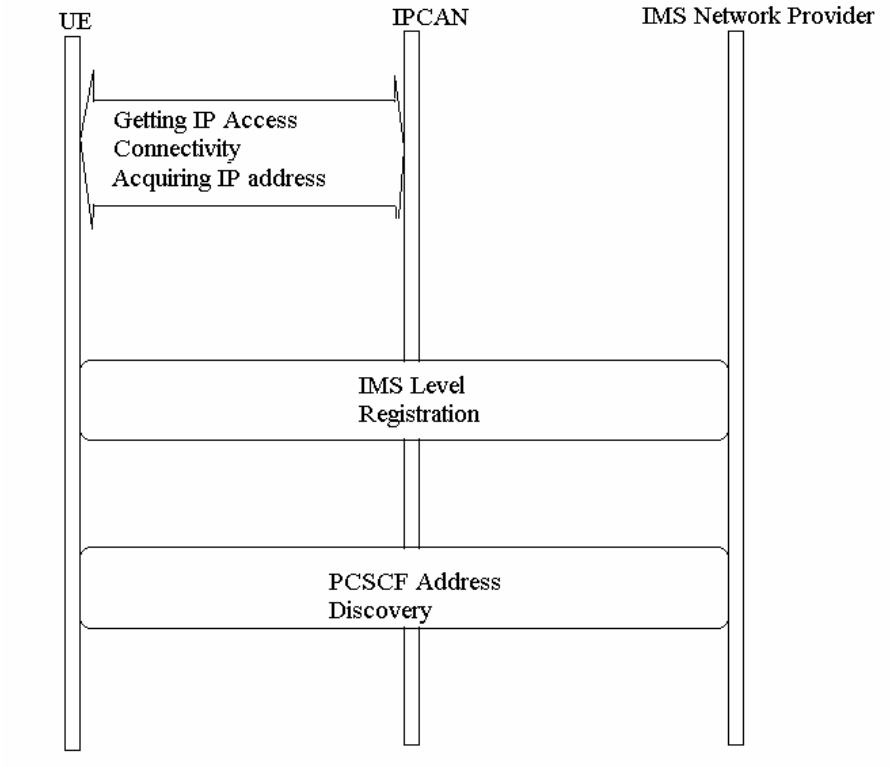

Figure-4.2 The Prerequisites of the IMS session setup

a) Getting IPCAN:

In GPRS, the IMS terminal first undertakes a set of procedures, globally known as *GPRS attach procedures*. These procedures involve several nodes, ranging from the SGSN to the HLR and the GGSN [10]. The procedures are illustrated in Figure 4.3. Once these procedures are complete the terminal sends an Activate PDP Context Request message to the SGSN requesting connection to an IPv6 network. The message includes a request for connectivity to a particular APN (Access Point Name) and packet connection type. The APN identifies the network to connect and the address space where the IP address belongs. In the case of an IMS terminal the APN indicates a desired connection to the IMS network and the connectivity type indicates IPv6. The SGSN, depending on the APN and the type of network connection, chooses an appropriate GGSN. The SGSN sends a Create PDP (Packet Data Protocol) Context Request message to the GGSN. The GGSN is responsible for allocating IP addresses [10].

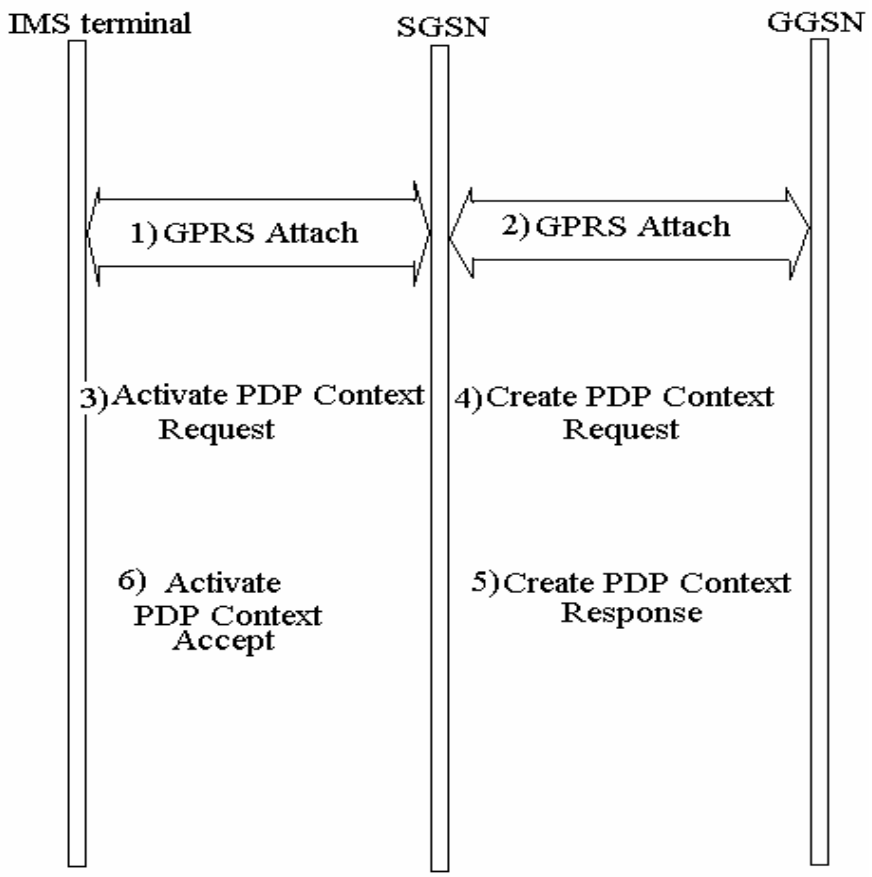

Figure-4.3 Getting an IP connect

In the case of the IMS the GGSN does not provide the terminal with an IPv6 address belonging to the IMS address space [10]. Instead, the GGSN provides the terminal with a 64-bit IPv6 prefix and includes it in a Create PDP Context Response message. The SGSN transparently forwards this IPv6 prefix in an Activate PDP Context Accept. When the procedure is completed the IMS terminal has got a 64-bit IPv6 prefix. The terminal is able to choose any 64-bit IPv6 suffix [10]. Together they form a 128-bit IPv6 address (i.e., the IPv6 address that the terminal will use for its IMS traffic).

b) IMS level registration:

After getting the access to GPRS the registration process is to be done. IMS registration is shown in the figure below and the steps are described [10]:

i) The UE sends a registration request to the PCSCF. This registration request contains RES, which is derived from ISIM from the mobile equipment.

ii) PCSCF further forwards this request to ICSCF, which forwards it to SCSCF.

iii) SCSCF compares the RES present in the request with the XRES, which is derived from the HSS by SCSCF.

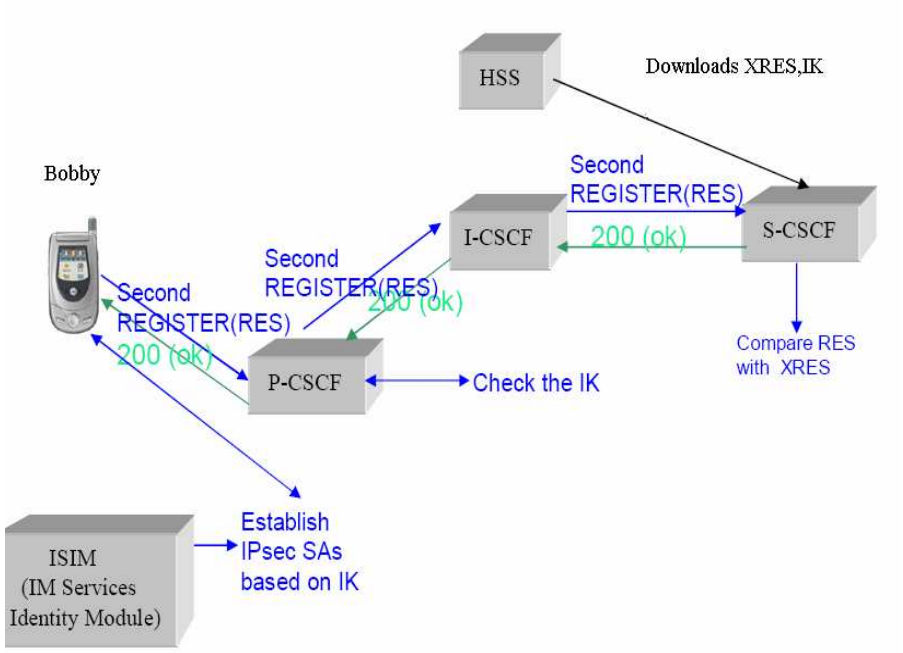

Figure- 4.4 IMS registration

iv) If the RES and XRES match then a 200 OK response is sent back to UE via ICSCF and PCSCF. If RES and XRES do not match then the registration fails.

The format of the registration request is shown below:

REGISTER sip: home1.fr SIP/2.0

Authorization: Digest username=user_private@home1.fr,

Realm="home1.fr",

nonce=A34Cm+Fva37UYWpGNB34JP, algorithm= AKAv1-MD5,

uri="sip: home1.fr",

Response="6629fae4939a05397450978507c4ef1**",** ……

Once Bobby is registered now he is authorized to access the IMS network through GPRS. In a similar way Anne is also registered.

c) PSCSF discovery:

P-CSCF discovery is the procedure by which an IMS terminal obtains the IP address of a P-CSCF. This is the P-CSCF that acts as an outbound/inbound SIP proxy server toward the IMS terminal (i.e., all the SIP signaling sent by or destined for the IMS terminal traverses the P-CSCF) [10].

P-CSCF discovery may take place in two different ways:

a. Integrated into the procedure that gives access to the IP-CAN.

b. As a stand-alone procedure.

The integrated version of P-CSCF discovery depends on the type of IP Connectivity Access Network. If IP-CAN is a GPRS network, once the GPRS attach procedures are complete the terminal is authorized to use the GPRS network. Then, the IMS terminal does a so-called Activate PDP Context Procedure [10]. The main goal of the procedure is to configure the IMS terminal with an IPv6 address, but in this case the IMS terminal also discovers the IPv6 address of the P-CSCF to which to send SIP requests.

The stand-alone version of the P-CSCF discovery procedure is based on the use of DHCPv6 (Dynamic Host Configuration Protocol for IPv6) and DNS (Domain Name System) [10].

d) Basic Session Setup:

When Bobby wants to connect to Anne he sends an INVITE request to Anne. The route of INVITE request from Bobby to Anne is illustrated in the Figure 4.5. The first observation noticed is that signaling (i.e., SIP) traverses a set of CSCFs. Another observation is that all SIP signaling traverses both the originating P-CSCF and the originating S-CSCF in all circumstances [10]. This is a significant difference with respect to other cellular networks where, if the user is roaming, signaling does not traverse the home network. The P-CSCF must be present in all the signaling exchanged with the terminal because it compresses/decompresses SIP (see Appendix-I) in the interface toward the terminal.

The S-CSCF is traversed in all requests to allow the triggering of services that the user may have requested. The S-CSCF plays an important role in service provision by

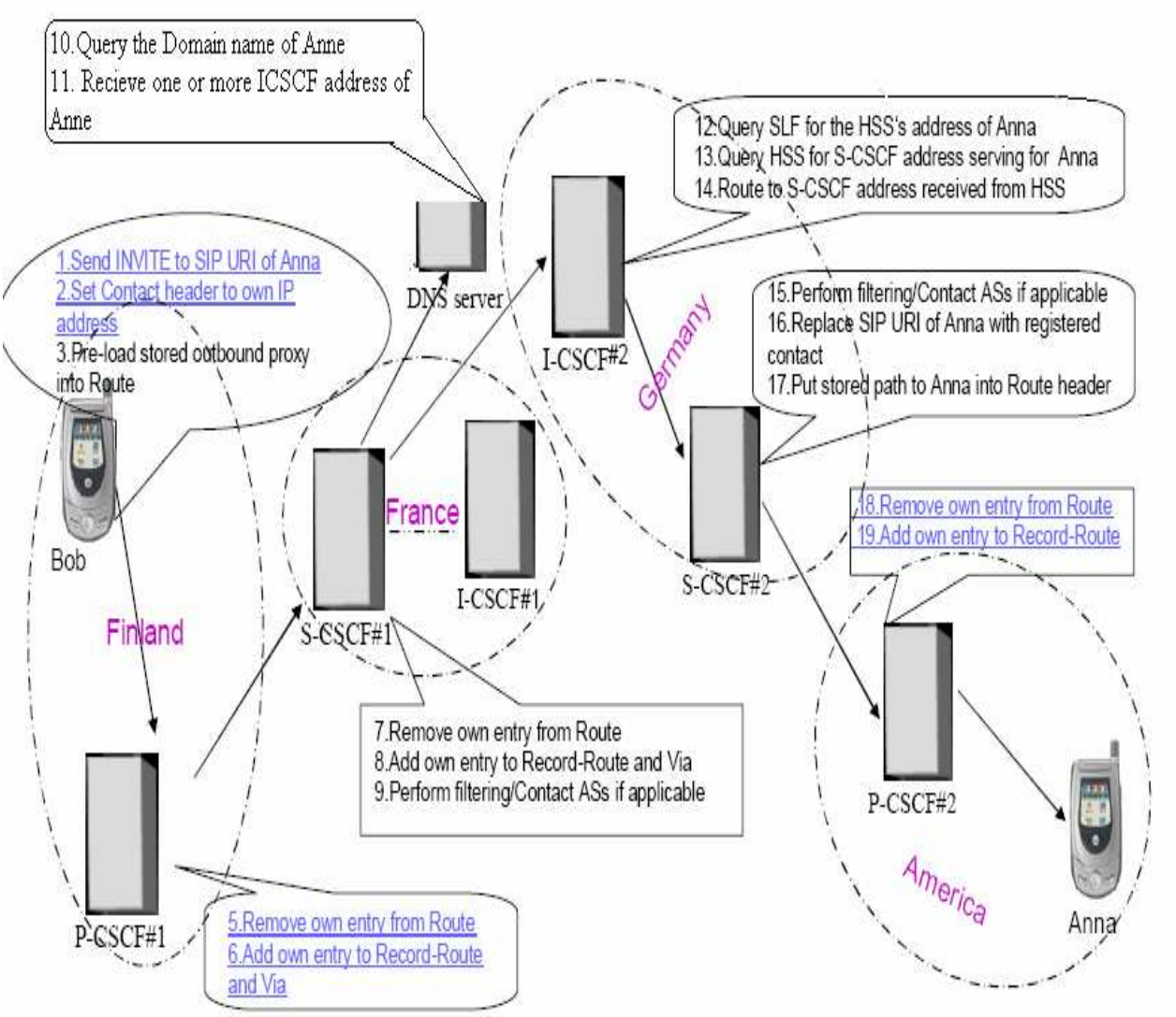

Figure-4.5 Routing of initial INVITE request

involving one or more Application Servers that implement the service logic. Since the S-CSCF is always located in the home network, services are always available to the user regardless of whether the user is roaming or not [10] . The *originating P-CSCF* and *originating S-CSCF* are the P-CSCF and S-CSCF that are serving the caller. Similarly, the *terminating P-CSCF* and *terminating S-CSCF* are the P-CSCF and S-CSCF that are serving the callee.

The format of the SIP requests is given in the subsequent sections:

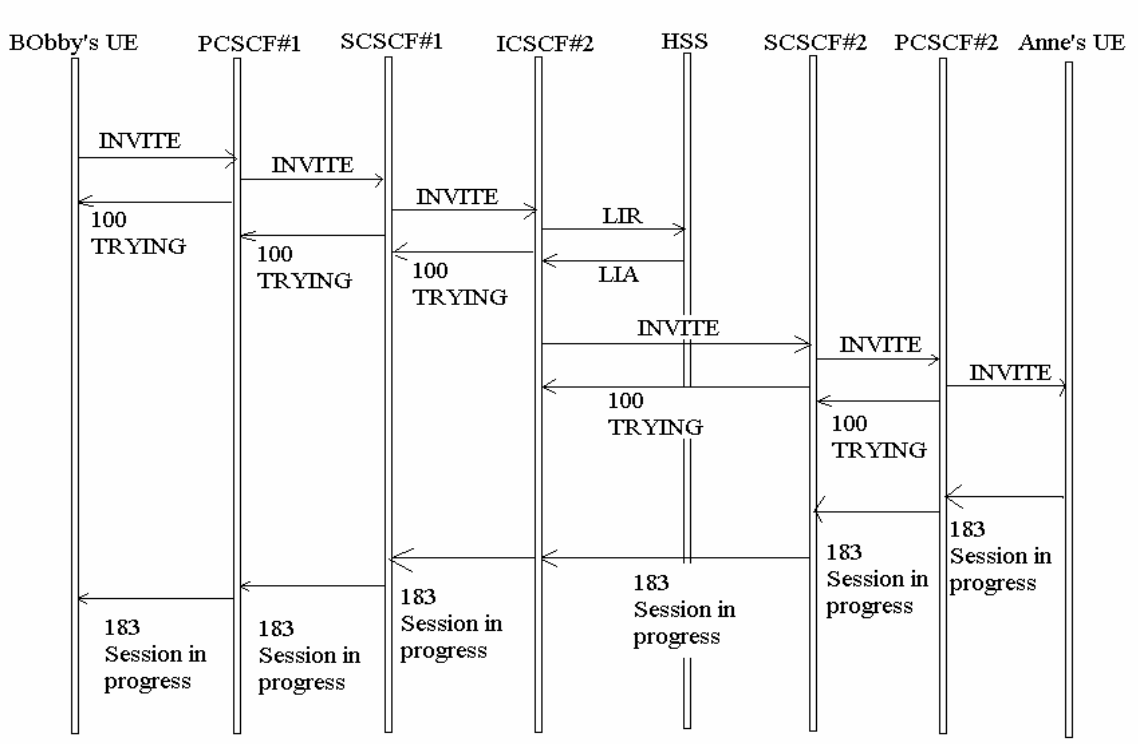

Figure- 4.6 IMS invite Basic Session Set up

1) INVITE request from UE1 to P-CSCF#1:

INVITE sip: anna@home2.de SIP/2.0

Via: SIP/2.0/UDP [1080::1:2:3:4]:1357; comp=sigcomp; branch=z9hG4bK9h9ab

Max-Forwards: 70

Route: <sip: pcscf1.visited1.fi: 5080; lr; comp=sigcomp>,

<sip: orign@scscf1.home1.fr ; lr>

P-Preferred-Identity: “Bob Smith”<sip: bob@home1.fr>

Privacy: none

P-Access-Network-Info: 3GPP-UTRAN-TDD;

utran-cell-id-3gpp=C359A3913B20E

From: <sip: bob@home1.fr>; tag=ty20s

To: <sip: anna@home2.de>

Call-ID: 3s09cs03

CSeq: 112 INVITE

Require: precondition, sec-agree

Proxy-Require: sec-agree

Supported: 100rel

Security-Verify: ipsec-3gpp; q=0.1;
alg=hmac-sha-1-96;
spi-c=98765432; spi-s=909786;
port-c=5057; port-s=5058
Contact: <sip: [1080:1:2:3:4]: 1357; comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: 590
…….. (Message body)

2) INVITE request from P-CSCF1 to S-CSCF#1:

INVITE sip: anna@home2.de SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.fi; branch=z9hG4bKoh2qrz
Via: SIP/2.0/UDP [1080::1:2:2:4]:1357; branch=z9hG4bK9h9ab
Max-Forwards: 69
Route: <sip: orign@scscf1.home1.fr; lr>
Record-Route: <sip: pcscf1.visited1.fi; lr>
P-Asserted-Identity: “Bob Smith”<sip: bob@home1.fr>
Privacy: none
P-Access-Network-Info: 3GPP-UTRAN-TDD;
utran-cell-id-3gpp=C359A3913B20E
P-Charging-Vector: icid-value=“W34h6dlg”
From: <sip: bob@home1.fr>; tag=ty20s
To: <sip: anna@home2.de>
Call-ID: 3s09cs03
CSeq: 112 INVITE
Require: precondition
Supported: 100rel
Contact: <sip: [1080::1:2:3:4]:1357; comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: 590
…….. (Message body)

3) INVITE request from S-CSCF1 to I-CSCF2

INVITE sip: anna@home2.de SIP/2.0

Via: SIP/2.0/UDP scscf1.home1.fr; branch=z9hG4Kpl8jqk

Via: SIP/2.0/UDP pcscf1.visited1.fi; branch=z9hG4bKoh2qrz

Via: SIP/2.0/UDP [1080:: 1:2:3:4]: 1357; branch=z9hG4bK9h9ab

Max-Forwards: 68

Route: <sip: icscf2.home2.de>

Record-Route: <sip: scscf1.home1.fr; lr>;

<sip: pcscf1.visited1.fi; lr>

P-Asserted-Identity: “Bob Smith”<sip: bob@home1.fr>;

<tel: +1-121-586-1234>

Privacy: none

P-Charging-Vector: icid-value=“W34h6dlg”; orig-ioi=home1.fr

From: <sip: bob@home1.fr>; tag=ty20s

To: <sip: anna@home2.de>

Call-ID: 3s09cs03

CSeq: 112 INVITE

Require: precondition

Supported: 100rel

Contact: <sip: [1080:: 1:2:3:4]: 1357; comp=sigcomp>

Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE

Content-Type: application/sdp

Content-Length: 590

…….. (message body)

4) INVITE request from P-CSCF2 to UE2

INVITE sip: [1080::5:6:7:8]:1006; comp=sigcomp SIP/2.0

Via: SIP/2.0/UDP pcscf2.visited2.com:5091; comp=sigcomp; branch=z9hG4Kpl8jqk

Via: SIP/2.0/UDP scscf2.home2.de; branch=z9hG4Kvp2yml

Via SIP/2.0/UDP icscf2.home2.de; branch=z9hG4Ksjeg8el

Via: SIP/2.0/UDP scscf1.home1.fr; branch=z9hG4Kpl8jqk

Via: SIP/2.0/UDP pcscf1.visited1.fi; branch=z9hG4bKoh2qrz

Via: SIP/2.0/UDP [1080::1:2:3:4]:1357; branch=z9hG4bK9h9ab

Max-Forwards: 64

Record-Route: <sip: pcscf2.visited2.com; lr>;

<sip: scscf2.home2.de; lr>;

<sip: scscf1.home1.fr; lr>;

<sip: pcscf1.visited1.fi; lr>

P-Asserted-Identity: “Bob Smith”<sip: bob@home1.fr>; <tel: +1-121-586-1234>

Privacy: none

P-Media-Authorization:

020000010010102565015 28e5462045e02245c55555266863240035052015 5415

From: <sip: bob@home1.fr>; tag=ty20s

To: <sip: anna@home2.de>

Call-ID: 3s09cs03

CSeq: 112 INVITE

Require: precondition

Supported: 100rel

Contact: <sip: [1080:: 1:2:3:4]: 1357; comp=sigcomp>

Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE

Content-Type: application/sdp

Content-Length: 590

…….. (Message body)

Equation 2

Chapter-5

BASICS OF IMPLEMENTING PUSH TO TALK OVER CELLULAR IN IMS

5.1 Introduction to PoC

> Push over Cellular (PoC) is a novel concept combining converging digital content formats; IP protocols and cellular packet bearers to provide proven use case, voice Group call. The developed solution in standardization is targeted to be applicable over any wireless system technology and therefore being able to serve customers globally. Push to talk is a type of communications service that sets up a channel between two or more users

without the need to dial a connection or set up a call. The paradigmatic example is a walkie-talkie or private mobile radio (PMR) system, where users page each other via a broadcast channel. Such systems are 'half duplex' – only one user at a time can be speaking, while all others must listen until the speaker relinquishes the channel. As with a walkie-talkie (or a PMR or public access mobile radio (PAMR) system), push to talk requires the participants in the conversation to manage who has the right to talk at any particular time – hence saying 'over' when one participant finishes speaking and invites others to reply. Like telephony, push to talk is a way of enabling two (or more) people to have a voice conversation [11]. Unlike telephony, it does not set up a circuit for the duration of the call; rather, the call is there as a background activity all the time and users drop in and out of it by pushing the big button on the side of the handset.

5.2 Evolution of PoC

Push to Talk (PTT) has its roots in military radios of the World War II. During the last 60 years PTT have probably been the most used paradigm of two-way and multiparty radio communication. Only the last 20 years have been era of dominating cellular radio technologies. PTT user paradigm is still very common in military and other professional radio systems (e.g. Terrestrial Trunked Radio, TETRA system) and it is also used broadly in private purposes such as coastal naval radio for leisure boating, deer hunting (VHF radios). Consumers would use PTT even more widely if it only were available anytime, anyplace. Traditional Push to Talk suffers limited coverage and poor privacy but on the other hand has no or very low usage charges. The golden era of Push to talk was probably some 30 years ago, when Citizen Band (CB) radios were used quite commonly by teenagers and by truck drivers [11]. Similar use cases have been addressed in the past

also by two variants of public cellular radio systems, namely so called GSM-R Radio system for European Railways Union (UIC) and proprietary radio system iDEN (Integrated Enhanced Digital Network) developed jointly by Motorola and their customer operator, NEXTEL.

The recent buzzword, PoC, Push (to talk) over Cellular introduces the next wave of technology serving the basic human interaction mode of group communication. The main differentiator between PoC and all the earlier technologies is that PoC is utilizing general packet packet radio and Internet Protocols (IP) versus earlier analog technologies or circuit switched digital radio technologies [11]. This new approach does not only bring some obvious advantages of IP, such as low operating and capital expenditure but it is also able to support various advanced services, which benefit from all digital content formats and broad compatibility throughout all the Internet [11].

5.3 PoC Standardization

The principal standardization bodies relevant for PoC include 3GPP, 3GPP2, OMA and IETF. Each one of them in principle has clear mandate but in practice the work plans are not fully inline.

The primary role of 3rd Generation Partnership Project (3GPP) is to develop technical specifications for GSM evolution to 3G, including maintenance of GSM core specification, future development of WCDMA radio specifications and for PoC most relevant work area is the Internet Multimedia Subsystem (IMS) specifications. The 3GPP develops specifications, which then will be approved by regional and national official standardization organizations, such as ETSI, ANSI, ARIB for Europe, USA and Japan, respectively, among others. The 3GPP has already completed, as part of their release 5 most of the fundamental features of IMS including the basic SIP (Session Initiation Protocol) based signaling, support of ISIM (IMS Subscriber Module) and related authentication and security protocols [11]. The 3GPP is responsible on the architecture and service aspects, not only the protocols. In practice all relevant players for Mobile Cellular business are participating the work in 3GPP. The 3GPP2 is similar organization set up later to carry out the standardization for CDMA2000 maintenance and evolution. Open Mobile Appliance (OMA), has been created parallel to 3GPP specifically to develop application and service enabler level specifications. Most of the OMA members are also actively participating 3GPP but specially the IT vendors are focusing their effort rather to OMA than to 3GPP [11] . The OMA has inherited any pre-IP era application

specifications, such as WAP Forum and Wireless Village, which on the other hand provide stable basis for further work but in many aspects are also a burden, since their compatibility to 3GPP IMS has not really been any goal. Additional source of friction is that the pre-IP era protocols are competing with IETF protocols, developed for similar purposes for the Internet. Co-operation between OMA and 3GPP is developing and going into better direction but still there are several complex and complicated areas to be sorted out. Related to PoC, 3GPP as been working also with Presence, Group and Instant Messaging as well as for IMS Conferencing, which are considered as application level specifications and therefore potentially belonging to OMA mandate. The Internet Engineering Task Force (IETF) is the predominant body to create the protocol specifications for the Internet in general. Way of working in IETF is in some aspects quite different from business driven bodies such as 3GPP and OMA. The primary focus, naturally in IETF is in the integrity of the set of protocols intended for Internet, even though in many cases IETF has not achieved single solutions but instead there are several parallel protocol specifications for the very same purpose. Related to the work in 3GPP and in OMA the most critical protocols, which are still under development in IETF, include SIP and SDP. Standardization is often considered as work for the best of the mankind and therefore the performance of the service, applications and system should be the first concern of the bodies drafting the specifications.

5.4 Technology Proposed for Standardization

PoC standardization process is an exception to typical 3GPP and OMA standardization process [12]. The baseline technology is a synthesis of available proprietary technologies. Nokia has already launched products with PoC feature enabled. Ericsson and Motorola are using software application developers (Sonim and Magic4, respectively) to provide similar capability and Siemens is in the process of launching their first products supporting PoC. These companies however joined their effort in mid 2003 and created a specification, which is now the main contribution for the PoC standard in OMA. Other companies have commented and contributed supporting and improving ideas [12]. OMA define the characteristics of PoC which include:

- Wireless radio link, which is Always on and Always connected to the IMS Core, to all relevant application servers (AS) as well as to any other Internet access point. Naturally the physical radio is not active all the time

but is using the normal paging mechanisms to activate the always on virtual connection when needed.

- SIP based signaling used in 3GPP/IMS Core. This decision in 3GPP was made several years ago to emphasize the convergence as a goal for mobile and fixed communication domains.
- Half duplex voice over IP connection, which utilizes 3GPP AMR (see Appendix-II) voice codec as default. There is pressure to include other optional voice codecs in order to facilitate PoC as an universal application standard also for non-GSM system technologies.
- PoC Server is a crucial part of the system, which provides the establishment of the PoC sessions and brings the users together. PoC server also multiplies the speaker's bit stream to multiple streams for the listeners of the PoC session. PoC server is essential tool in opening current IP technology bottlenecks: Network Address Translation (NAT) and Firewalls, which isolate the sub-network hosts from the open Internet. Mobile devices connected through mobile network operator's packet data infrastructure is in practice always using virtual, local IP addresses.
- Performance enhancements for wireless friendly transmission are needed, IPv6 header compression as well as SIP signaling compression (see Appendix-I) are both quite important factors to bring acceptable level of service quality to PoC. PoC is not assuming Quality of Service classes, such as streaming class, to be implemented in the networks but it is able to utilize better than best effort. QoS when it is available networks in the future.

The main challenges in PoC include:

- Floor control must be agreed. Floor control has to provide high performance (low latency, high spectrum efficiency) and future proof solution (compatibility with floor control protocols in the Internet.
- Some dedicated support to both GSM/GPRS/ WCDMA and CDMA2000 radio access technologies PoC Server to Server interface for global service interoperability.
- General harmonization of approaches in order to provide seamless operation both in mobile and fixed environment. Critical item in

standardization and also in the future IMS based systems in general is the use of IPv6.Currently the IMS is specified fully to utilize the modern version of Internet Protocol but several MNOs are optimizing their plans for short term targets forcing vendors to provide dual stack IPv4/IPv6 products. This may cause legacy problems when PoC is used in multioperator environment.

5.5 OMA PoC Architecture

The PoC architecture is constructed by several small entities, each entity handling a different part of the system [13] . The architecture consists of the following central entities:

- PoC Client – Gives the user access to the PoC service.
- PoC Server – Contains the PoC service.
- SIP/IP Core – Handles sessions, SIP routing, authentication and authorization.
- GLMS (Group List Management Server) – Stores and manages groups and lists.
- Presence Server – Manages presence information.

The PoC architecture entities, and the interfaces between them, are shown in Figure 5.1. They are also described in detail further in the following sections.

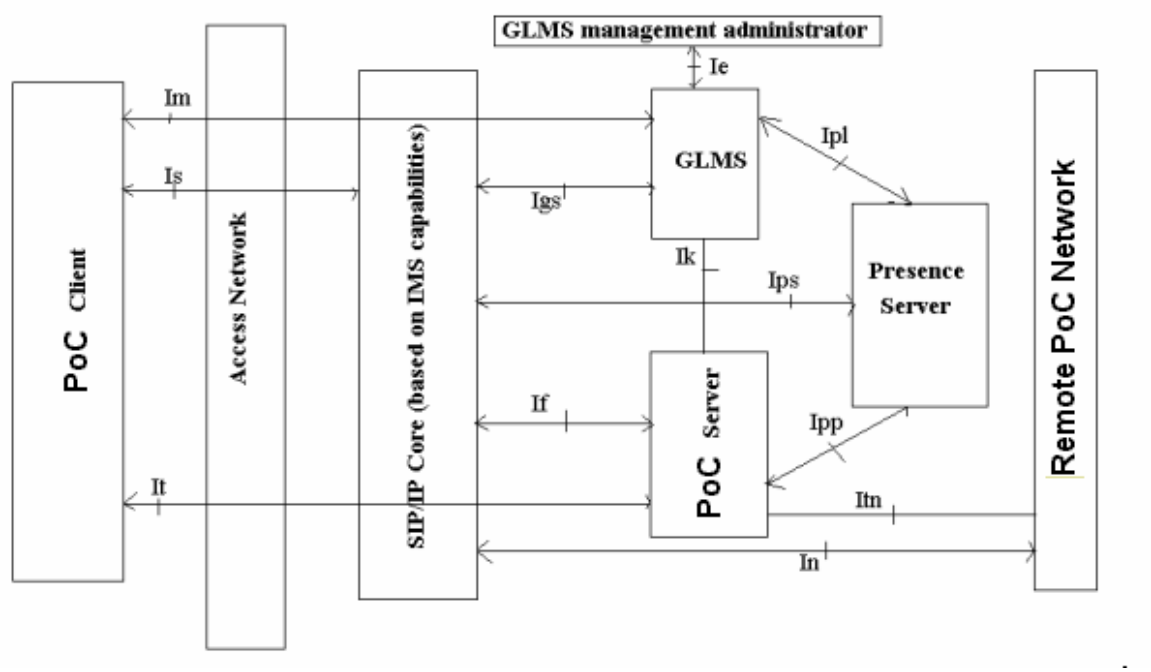

Figure-5.1 OMA based PoC architecture

5.5.1 Entities

The various entities present in the architecture are described below:

1) PoC Client

The PoC Client resides on the mobile terminal. It gives the user access to PoC services. The main purpose for the PoC Client is to send and receive messages via the PoC Server. It uses three different interfaces (Im, Is and It) to communicate with the PoC infrastructure [14]. The Im interface is used for list and group management, the Is interface for session and presence handling and the It interface for media transmissions. The PoC Client performs the following functions:

- PoC session initiation, participation and termination.
- Generate talk bursts for transmission and reproduce received talk bursts.
- Registration and authentication with the PoC Infrastructure.
- Provide access to PoC group lists.
- Support floor control procedures.
- Provide access to PoC subscriber for managing PoC group lists.
- Provide access to presence conditions of the PoC subscriber.

2) PoC Server

The PoC Server contains the PoC service [14]. The main goal for the PoC Server is to handle sessions and to distribute media from one user to all other users in the talk session. The PoC Server also handles the following functions:

- Access control
- Do Not Disturb
- Floor control
- Talker identification
- Participants information
- Quality feedback
- Charging reports

3) GLMS – Group List Management Server

The GLMS is used for storage and management of the groups and lists that are needed for the PoC service [14] . It handles the creation, modification, retrieval and deletion of groups and lists. There are three types of lists:

- Contact lists – stores contact entities in the GLMS.
- Group lists – defines PoC groups.
- Access lists – defines who's allowed to reach a specific user.

A contact list is a kind of address book that may be used by PoC users to establish an instant talk session with other PoC users or PoC Groups. A user may have one or several contact lists, containing identities of other PoC users or PoC Groups. A group list is a list of user defined PoC groups. The end user may select one group from the list to initiate an instant group talk session or chat groups talk session depending on the type of the group. An access list is used by the end user as means of controlling who is allowed to initiate instant talk sessions to the end user. An access list contains end user defined identities of other PoC end users or groups [14]. The end user may have one reject list and one accept list.

4) Presence Server

The Presence Server manages presence information. It is responsible for combining the presence-related information for a certain user from the information it receives from multiple sources into a single presence document. The presence server handles the publication, watching and fetching of Presence Information, it also handles the authorization for watching and fetching [14]. The authorization is done based on

authorization rules stored in the Presence Server. A user can have one of the following statuses:

- Reachable
- Do Not Disturb
- Busy
- Unavailable
- Offline

5) SIP/IP Core

The SIP/IP Core is the first point of contact for the PoC client. It is based on IMS and includes a number of SIP proxies and SIP registrars. The PoC client sends all of its SIP messages to the IP address of the outbound proxy, after resolving the SIP URI of the outbound proxy to an IP address [14]. The SIP/IP Core handles all routing of SIP signaling between the PoC Client and the PoC Server. The SIP/IP Core also performs the following functions that are needed in support of the PoC Service:

- Discovery and address resolution
- SIP compression
- Authentication and authorization of PoC Clients
- Maintains the registration state
- Charging information

5.5.2 Interfaces

1) Is interface

The Is interface supports the communication between the PoC Client and the SIP/IP Core [15]. The protocol for the Is interface is SIP (Session Initiation Protocol), transported with UDP. The Is interface supports:

- Session signaling between the PoC client and the PoC server
- Discovery and address resolution
- Authentication and authorization
- Registration
- Publishing of presence information

- Subscribing to presence information
- Receiving of presence notifications
- Subscription to modification by the GLMS of lists.
- Notification of modification by the GLMS of lists

2) It interface

The It interface is used for transporting media, floor control and link quality messages between the PoC Client and the PoC Server. It uses RTP and RTCP.

3) Itn interface

The Itn interface supports the communication between the PoC servers. It supports media transport and floor control procedures [15]. It uses RTP and RTCP.

4) Im interface

The Im interface is used for the communication between the PoC Client and the GLMS for the purpose of managing the groups, contact lists and access lists. The Im interface uses the XCAP protocol and gives the PoC Client the capability to create, modify, retrieve and delete groups and lists.

5) In interface

The In interface supports the communication and forwarding of SIP signaling messaging between SIP/IP Cores. The interface is based on SIP.

6) Ik interface

The Ik interface supports the communication between the PoC Server and the GLMS [15]. It enables the PoC Server to retrieve the groups and access lists from the GLMS. It is not yet specified which protocol it will use.

7) If interface

The If interface supports the communication between the SIP/IP Core and the PoC Server for session control [15]. The If interface is based on SIP. It supports session signaling, address resolution, charging information and publication, subscription and notification of Presence Information by the Presence Server to the PoC Server.

8) Ipl interface

The Ipl interface supports the communication between the GLMS and the Presence Server [15]. It enables transference of presence lists, group lists and subscription authorization policies to the Presence Server. It is not yet specified which protocol it will use.

9) Ips interface

The Ips interface supports the communication between the SIP/IP Core and the Presence Server. It enables uploading of the registration status from the SIP/IP Core to the Presence Server and the distribution of the presence information between the presence server and the PoC Client. Ips is based on SIP.

10) Igs interface

The Igs interface supports the communication between the GLMS and the SIP/IP Core [15]. It handles subscription and notification of the modification of lists. It is not yet specified which protocol it will use.

11) Ie interface

The Ie interface is between the GLMS and GLMS Management/Administration entity. This entity can act on behalf of end users and administrators subject to service providers access control policies [15]. Access may be provided via the intranet, internet or corporate networks. The Ie interface provides the capability to create, modify, retrieve and delete groups and lists.

5.6 Description of PoC client

The PoC client architecture used in the project is shown in the figure 5.2. The description of the client is discussed in the subsequent sections.

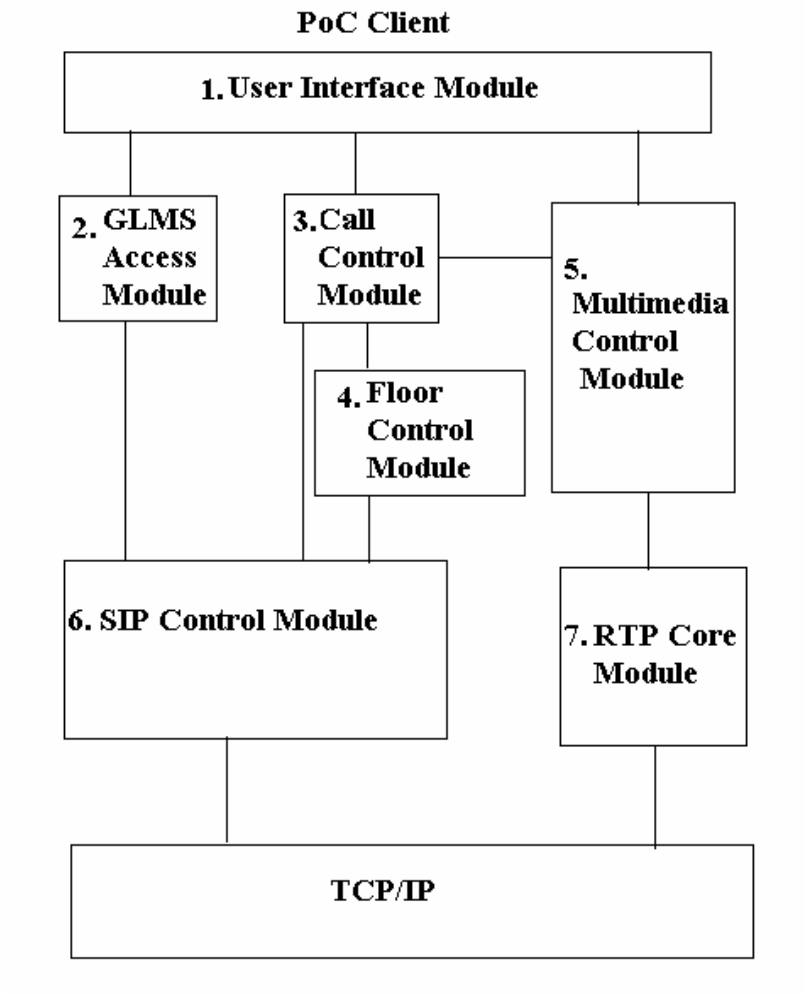

Figure- 5.2 The PoC client architecture

1) User Interface module:

A user interacts with the PoC system through the User Interface module. This module consists of four main window dialogs. The Login dialog is popped up after the PoC client program is executed [16]. It waits for the user to input the SIP URI (for the PoC client) and the password, and then executes the SIP registration procedure.

After the user is authenticated, the PoC client enters the standby mode, and the Phone dialog is activated. The Phone dialog alerts the user when an incoming call arrives. If the user misses the call, the Phone dialog shows the missed call information on the user interface. The user can change the presence status through the Phone dialog.

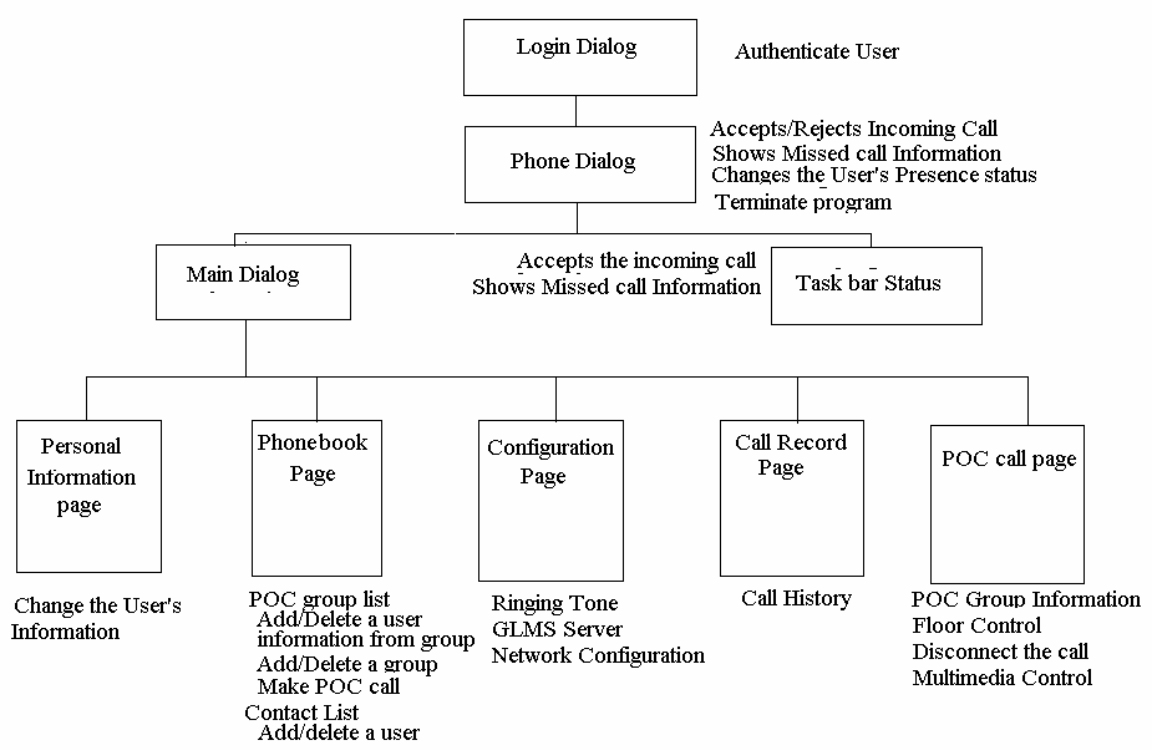

Figure-5.3 User Interface

After closing the Phone dialog, the user can select to open the Main dialog or the Taskbar Status Area icon. In the Taskbar Status Area icon mode, when a call arrives or a call is missed, a message window is popped up to notify the user. The Main dialog contains 5 pages [16]. The Personal Information page presents the user's personal information.

2) Call Control Module:

The Call Control module instructs other PoC client modules to handle the call related activities according to the presence status of the user and the preference types of other call parties [16]. Figure 5.4 illustrates the state diagram for the call control finite state machine (FSM) maintained by the Call Control module. The states are described below (where the term "user" represents this PoC client).

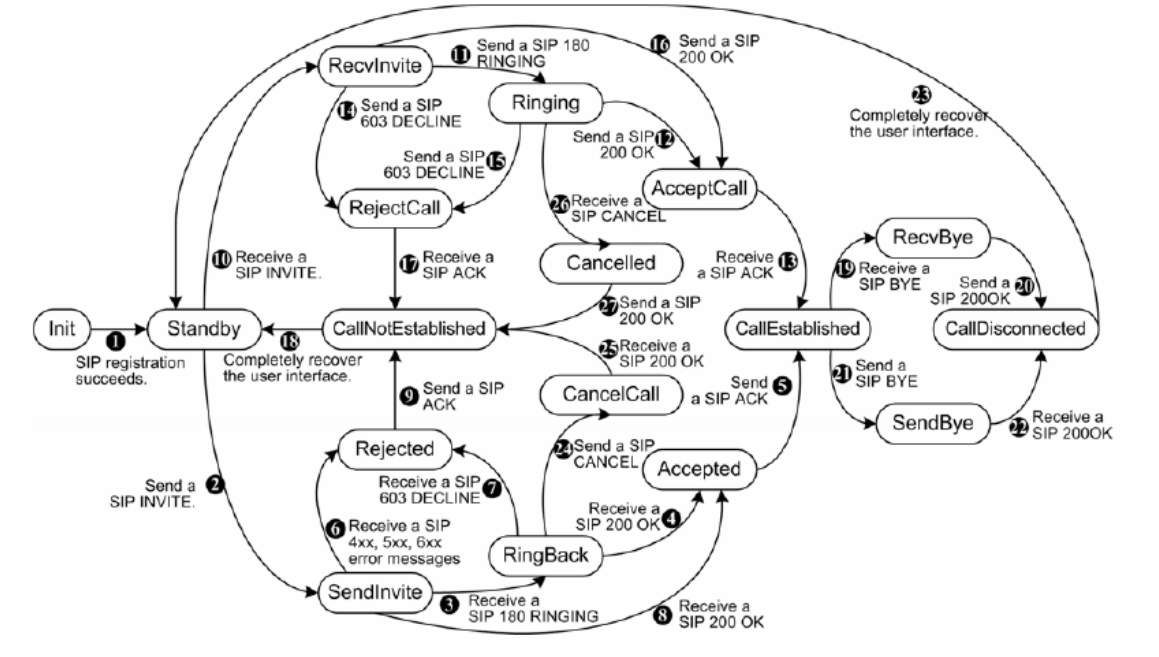

Figure-5.4 State diagram of the call control FSM.

Init: The FSM waits for SIP registration.

Standby: The FSM waits for an incoming/outgoing call.

SendInvite: The user requests an outgoing call.

RingBack: The other call party is ringing.

CancelCall: The user cancels the call.

Accepted: The outgoing call is accepted by the other call party.

Rejected: The outgoing call is rejected by the other call party.

RecvInvite: An incoming call arrives.

Ringing: The PoC client is playing the ringing tone to notify the user of the incoming call.

Cancelled: The incoming call is cancelled by the other call party.

AcceptCall: The user accepts the incoming call.

RejectCall: The user rejects the incoming call.

CallNotEstablished: The call is not established.

CallEstablished: The call is established, and the conversation begins.

SendBye: The user requests to disconnect the call.

RecvBye: The other call party requests to disconnect the call.

CallDisconnected: The call is disconnected.

Details of the FSM are discussed in message flow section.

3) Floor Control Module:

When a PoC call party obtains the “floor”, he/she has the right to speak at that moment. To obtain the floor, the PoC client needs to send a floor request to the PoC server and wait for a positive response [16]. In addition, the PoC server broadcasts the floor status to the call parties (e.g., someone has obtained the floor).

The floor-related functionalities are implemented in the Floor Control module. When a PoC call is established, the Call Control module issues a StartFloorReq command to activate the floor control FSM [17]. But, in our project only session set up is done therefore floor control module is not used.

4) Other POC client Modules:

The GLMS Access, the Multimedia Control, the SIP Core, and the RTP Core modules are described in this subsection [17]. The GLMS Access module is responsible for retrieving the user's information from the GLMS.

- The Multimedia Control module plays the ringing tone, the ringback tone or the busy tone to notify the user of various call states. After a call is established, this module plays the received voice data from other call parties and records the user's voice
- When the user is permitted to speak.
- The SIP Core module supports SIP communication with other network entities in the PoC system (e.g., GLMS and PoC servers). Three PoC client modules for SIP communication invoke this module.

(1) The GLMS Access module interacts with the GLMS through the SIP MESSAGE method.

(2) The Floor Control module exchanges the floor control signals with the PoC server by using the SIP INFO method [17].

(3) The Call Control module executes the call setup or disconnection procedures following the standard SIP protocol.

In our implementation, the ReSIProcate library is utilized for SIP protocol support. The RTP Core module builds a RTP session between the PoC client and the RTP proxy (for a PoC call), or another call party (for a VoIP call). The RTP Core module is

used for multimedia session. Since we have just implemented the call session between two clients therefore RTP core module is not used.

In the PoC client architecture, the GLMS Access module and the Floor Control module are specifically designed for PoC service. Other modules are used in both PoC and VoIP services.

5.7 Message Flow in a PoC Client

Based on the PoC client architecture described in the previous section, the message flow between the PoC client and other network entities in the PoC system, including Outgoing Call Setup, Incoming Call Setup, Floor Reservation, Floor Release, and Call Disconnection is discussed in this section [18] .

5.7.1 Outgoing Call Setup Procedure

When the user requests to make a PoC call, the Outgoing Call Setup procedure is executed as illustrated in Figure 5.5.

Steps 1-3: Based on the PoC group SIP URI specified by the user, the User Interface module requests the Call Control module to initiate a PoC call. The Call Control module instructs the SIP Core module to issue a SIP INVITE, and the call control FSM moves from **Standby** to **SendInvite.** The SIP INVITE is delivered to the PoC server where the PoC group's SIP URI is registered.

Steps 4-6: The PoC server queries the member data of the designated PoC group from the GLMS and dispatches the SIP INVITE to each of the group members. If an error occurs during the PoC call invitation, the PoC server returns a SIP 4xx, 5xx, or 6xx error message to the calling PoC client. Then the call control FSM of the calling PoC client moves from **SendInvite** to **Rejected**, and the calling PoC client replies a SIP ACK to the PoC server. Finally, the call control FSM moves to the **Standby** state, and the PoC client waits for next user instruction or incoming call [18]. Suppose that no error occurs. Step 7 and the subsequent steps are executed.

Steps 7-9: If a called PoC client receives the call invitation, this client plays the ringing tone and replies a SIP 180 RINGING to the calling PoC client through the PoC server. The Multimedia Control module of the calling PoC client plays the ringback tone to indicate the user that the Outgoing Call Setup procedure is in progress, and the call control FSM moves from **SendInvite** to **RingBack.**

Steps 10-12: If any of the called PoC group members picks up the phone (accepts the call invitation), the member replies a SIP 200 OK to the PoC Server. The PoC server chooses

the audio codec used in the RTP session between the calling PoC client and the RTP proxy. The PoC Server forwards the codec information to the RTP proxy, and also instructs the RTP proxy to reserve ports for the RTP session [18] .

Steps 13 and 14: The PoC server sends a SIP 200 OK to the calling PoC client, which includes the audio codec information, the IP address of the RTP proxy, and the reserved ports in the RTP proxy. These parameters are used in establishing the RTP session at Step 22. The calling PoC client call control FSM moves from **RingBack** to **Accepted.**

Steps 15-17: The SIP Core module responds a SIP ACK, and the call control FSM moves from **Accepted** to **CallEstablished.**The PoC server forwards the SIP ACK to the called PoC group members who have accepted the call.

Step 18: The Call Control module of the calling PoC client instructs the Floor Control module to enable the floor control function. The floor control FSM moves to **Init**.

Step 19: The User Interface module shows the PoC group information on the Call page of the Main dialog. Note that the user is only allowed to participate in one PoC or VoIP call.

Steps 20-22: The calling PoC client creates the RTP connection to the RTP proxy. Specifically, the Call Control module inquires the SIP Core module about the negotiated audio codec and the IP address/port number of the remote endpoint of RTP session (i.e., the RTP proxy), which are obtained from the PoC server at Step 13. The information is passed to the RTP Core module to create the RTP session following the standard RTP protocol.

Step 23: The Multimedia Control module activates the audio device and generates two processes for recording and playing the voice data [18] .

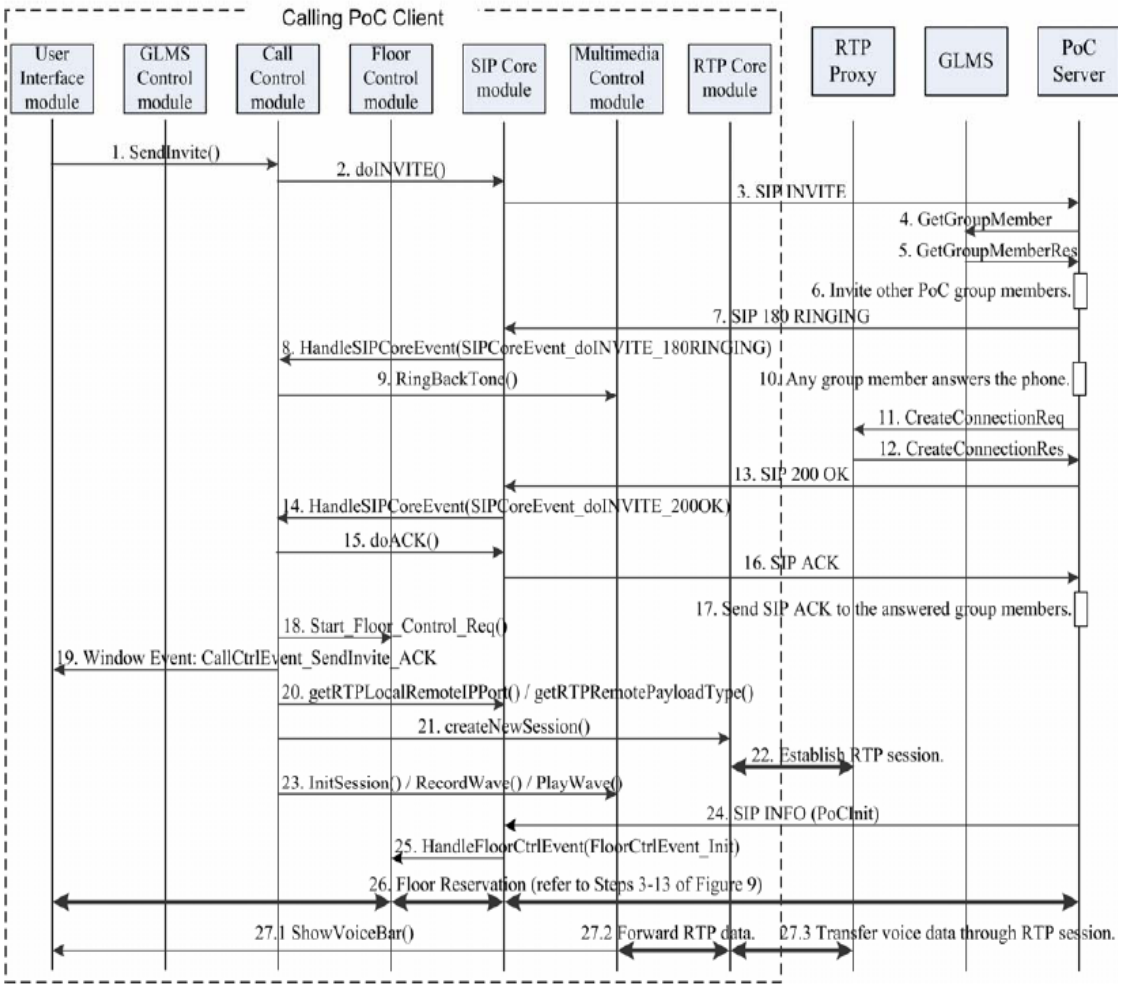

Figure- 5.5 Call setup Procedure

Steps 24-26: The calling PoC client is the first call party who is permitted to speak. The PoC server sends a PoC Init message carried by the SIP INFO method to the calling PoC client. The floor control FSM moves from **Init** to **ReqPending.** The Floor Reservation procedure is invoked.

Step 27: At this point, the conversion begins. The calling PoC client sends the voice to the RTP proxy through the Multimedia Control module and the RTP Core module (Step 27.2 and Step 27.3). During the call, the voices from other group members are forwarded to the Multimedia Control module (Step 27.3 and Step 27.2), and are played through the audio device. The volume of the currently played voice is reported to the User Interface module and shown on the Call page of the Main dialog (Step 27.1) [18].

Note that when other called PoC clients receive the call invitation at Step 6 of Figure 5.5, they may automatically accept the call invitation without playing the ringing tone. If so,

Steps 7-9 are skipped, and the PoC group members directly reply a SIP 200 OK to the calling PoC client through the PoC Server. Then the call control FSM of the calling PoC client moves from **SendInvite** to **Accepted.** When the called PoC clients receive the call invitation, and the ringing tone is played at Step 7 of Figure 5.5, two other situations may occur.

(1) All PoC group members reject the call invitation. The PoC server replies a SIP 603 DECLINE to the calling PoC client and the Outgoing Call Setup procedure exits. The call control FSM of the calling PoC client moves from **RingBack** to **Rejected.**

(2) The calling party presses the cancel button to cancel the outgoing call before any of the PoC group members replies a message. The call control FSM of the calling PoC client moves from **RingBack** to **CancelCall,** and waits for the PoC server to reply a SIP 200 OK. Upon receipt of the SIP 200 OK, the call control FSM moves from **CancelCall** to **CallNotEstablished** [18]**.**

5.7.2 Incoming Call Setup Procedure

For an incoming PoC call, the called PoC client is invited by the PoC server to join in the PoC call through the Incoming Call Setup procedure as illustrated in Figure 5.6, and the detailed steps are described as follows.

Steps 1-4: The PoC server receives a PoC call invitation from the calling party. It dispatches the PoC call invitation to each of the PoC group members.

Steps 5-9: After receiving the SIP INVITE, the call control FSM of the called PoC client moves from **Standby** to **RecvInvite.** The PoC client processes the incoming call according to the user's presence status (i.e., Online, Offline, Busy, or NoDisturb) and the preference type of the calling party (i.e., Auto-Answer, Manual-Answer, or Reject). Suppose that the user's presence status is not set as NoDisturb and the preference type of the calling party is set as Manual-Answer [19].

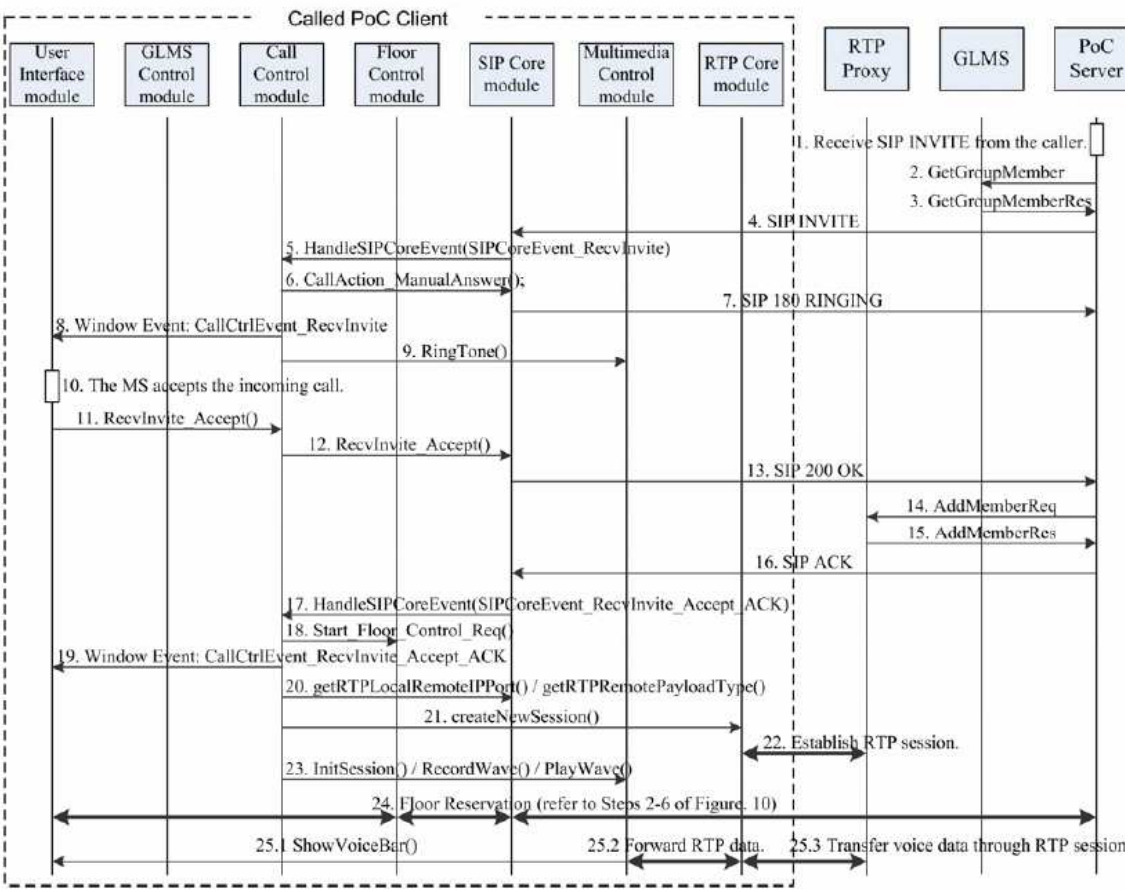

Figure-5.6 Incoming Call Procedure

The called PoC client sends a SIP 180 RINGING to the PoC server. Then the User Interface module shows the incoming call notification message, and the Multimedia Control module plays the ringing tone [19] . The called PoC clients call control FSM moves from **RecvInvite** to **Ringing.**

Steps 10-13: The called PoC client accepts the incoming call and replies a SIP 200 OK to the PoC server. The call control FSM moves from **Ringing** to **AcceptCall.**

Steps 14 and 15: The PoC server chooses the audio codec to be used in the RTP session between the called PoC client and the RTP proxy [19] . Then it forwards the codec information to the RTP proxy, and also instructs the RTP proxy to reserve ports for the RTP session.

Steps 16 and 17: The PoC server sends a SIP ACK to the called PoC client, which includes the audio codec information, the IP address of the RTP proxy, and the reserved ports in the RTP proxy [19] . These parameters are used in establishing the RTP session

at Step 22. When the called PoC client receives the SIP ACK, the call control FSM moves from **AcceptCall** to **CallEstablished.**

Steps 18-23: These steps are the same as Steps 18-23 in Figure 5.5.

Step 24: After the PoC call is established, the PoC server invokes the Floor Reservation procedure to inform the called PoC client of the current speaker. The detailed steps are described at Steps 2-6 in Figure 10. The called PoC client floor control FSM moves from **Init** to **Reserved** (transition 4 in Figure 6).

Step 25: This step is the same as Step 27 in Figure 5.5. After receiving the SIP INVITE at Step 4, two other scenarios may occur to the called PoC client [20] :

(1) If the user's presence status is set as NoDisturb or the preference type of the calling party is set as Reject, the called PoC client replies a SIP 603 DECLINE to reject the incoming call. The called PoC client call control FSM moves from **RecvInvite** to **RejectCall,** and the Incoming Call Setup procedure exits.

(2) If the user's presence status is not set as NoDisturb and the preference type of the calling party is set as Auto-Answer, Steps 6-11 in Figure 5.6 are skipped, and the called PoC client directly replies a SIP 200 OK to accept the incoming call. Then the call control FSM moves from **RecvInvite** to **AcceptCall.**

After the called PoC client plays the ringing tone at Step 9, other two scenarios may occur.

(1) The called PoC client rejects the incoming call. The call control FSM moves from **Ringing** to **RejectCall.**

(2) The calling PoC client cancels the call before the called PoC client makes the decision.

The called PoC client receives a SIP CANCEL, and the call control FSM moves from **Ringing** to **Cancelled.** Then the called PoC client replies a SIP 200 OK, and the call control FSM moves from **Cancelled** to **CallNotEstablished.**

In Step 24, the PoC server informs the called PoC client of the floor status. It is also possible that no PoC member attempts to talk while the called PoC client joins in the PoC call (i.e., the floor is idle). In this case, the PoC server sends a TokenFree message to the called PoC client through the SIP INFO method. The floor control FSM of the called PoC client moves from **Init** to **Free** [20]**.**

Equation 3

Chapter-6

IMPLEMENTATION OF AN API TO CHECK PoC FUNCTIONALITY ON MOBILE

To check the Push To Talk Over Cellular service on the test set 6401 provided by the client. The test sets are used to verify a particular service provided by a vendor on the handsets in the market. For example Nokia in the market offers PoC service on their handsets then these test sets are used to verify the service. So in this project we are implementing the API which can be used with test set 6401 to check functionality of mobile.

6.1 Software Used

Platform Used: Window 2000 professional.

Library Used: ReSIProcate in VC-7(dot net).

IMS Client : VC++.

Standards followed: OMA(Open Mobile Alliance) PoC message flow(see AppendixIII).

The prototype uses Windows 2000 professional platform. The library used is ReSIProcate which is used to implement SIP stack to support the PoC application. The IMS client is in VC++ on which this application runs. In this IMS client program, the messages are included which are to be sent between the two clients i.e., client 1 and client 2 which are representatives of two users. The prototype was tested on one machine with Windows XP. This test was mainly performed on two separate PoC clients installed on one machine only.

6.2 Design and Implementation

The two clients were implemented on one machine. The basic architecture is shown in the figure below. The communication takes place through the PoC server . Following steps take place:

1) Both the clients are registered with the PoC server.

2) Once the clients are registered now the signaling between the two clients can take place via PoC server. PoC server along with SIP core helps in signaling between the two clients.

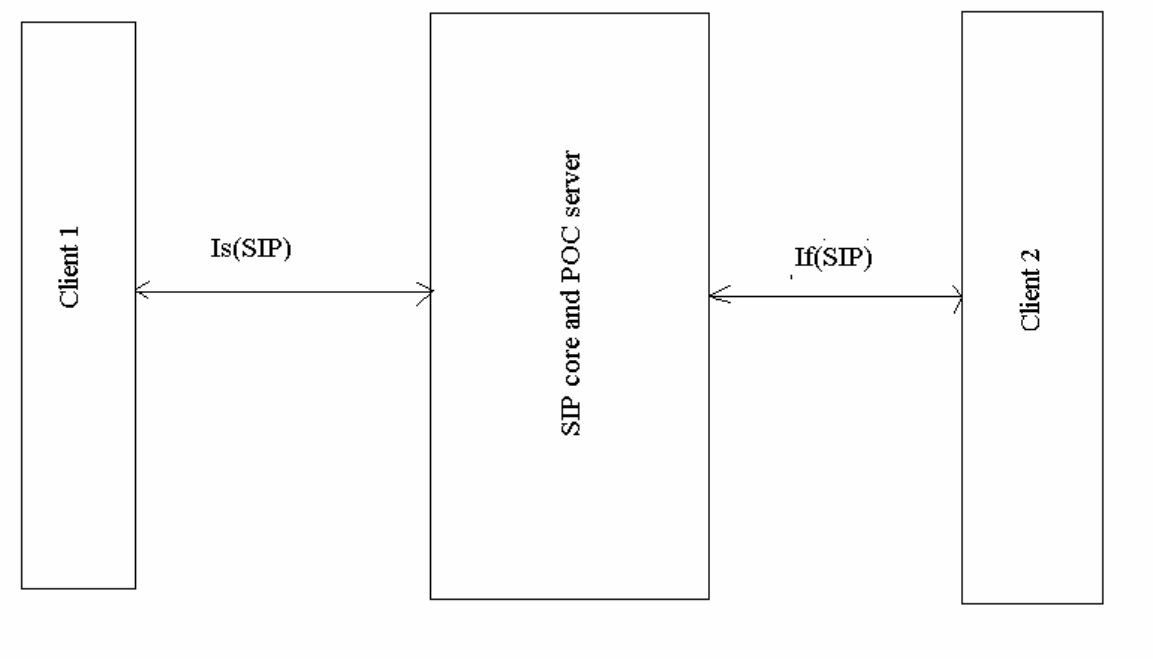

Figure-6.1 Implemented parts of OMA PoC architecture

PoC Client:

The main purpose for the client is to give the user access to the PoC service in a fast and easy way. It accomplishes this by combining a graphical user interface with the communication protocol SIP [21] . The client has to wait for user actions, SIP messages at once. This is accomplished by using threads. The client also handles sound recording and playback. All this combined makes it by far the most complex component in the system.

SIP core and PoC Server:

The SIP Core uses reSIProcate to communicate and basically just waits for incoming SIP-messages. Its main purpose is to keep track of who is registered and to which IP-address, and to forward the messages to the right IP-address. When it receives a register-message it will bind the clients SIP URI to its current IP address. All other messages are essentially just forwarded to the right address, a PoC server or another client[21].

The PoC Server utilizes SIP core to communicate over SIP. Its main purpose is to handle signaling sessions, talk sessions and forward sound streams to the users in the talk sessions[22]. It uses SIP for setting them up and taking them down.

6.3 Outputs

The testing resulted following output logs :

```
**************************************************************************
Test Name    : PoC-1.0-con-C-0047
Test Title   : On-Demand Session / Ad-hoc PoC Group Session setup / Unconfirmed
               Indication
GCF Priority : 1
SCR Reference: PoCCPSpec-CSI-C-011, PoCCPSpec-CSI-C-014
**************************************************************************
-------------------------Test Case Parameter Settings--------------------------
pc_Sup3GppIms = TRUE
pc_SupUnconfirmIndSignal = TRUE
pc_SupManualAnswerMode = TRUE
-------------------------------------------------------------------------------
TIMESTAMP    21:28:31:652
IMS APPLICATION :INFORMATION
LOG  :IMSProxyCSCF Constructed
FILE
:x:\trinity\source\application\applicationtester\imscomponents\imsapplication\imsproxycs
cf.cpp
LINE :53
TIMESTAMP    21:28:31:902
APPLICATION TESTER :POC Test Case PoC-1.0-con-C-0047 started
TIMESTAMP    21:28:31:933
APPLICATION TESTER :Originating Client Capability: Support for handling
                                  Unconfirmed Indication signalling.

TIMESTAMP    21:28:31:949
APPLICATION TESTER :PoC client does not have any active session
```

TIMESTAMP 21:28:31:949

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:36:386

APPLICATION TESTER :User Prompt - Please press OK and start the POC client to send the SIP REGISTER message

TIMESTAMP 21:28:38:839

****

IMS PDU :REGISTER

PDU Direction :From UE to Network

PDU Length :665 Octets

----------SIP MESSAGE----------

REGISTER sip:172.21.111.48:5070;transport=udp SIP/2.0To: <sip:rakesh@172.21.111.48:5070;transport=udp>From: <sip:rakesh@172.21.111.48:5090;transport=udp>;tag=f7162a4eVia: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-e07d3e1893584846-1--d87543-;rport=5090Call-ID: 3b560f3d940f8b01@dGNzMDU5MTk3LkFFUk9GTEVYCSeq: 1 REGISTERContact: <sip:rakesh@172.21.111.48:5090;transport=udp>;+g.poc.talkburst;+g.poc.groupadMax-Forwards: 70Reply-To: <sip::5090>Require: prefUser-Agent: PoC-client/OMA1.0Authorization: Digest username="PoC-UserA-private@networkA.net"Security-Client: ipsec-3gpp, alg=hmac-sha-1-96, spi-c=23456789Content-Length: 0

****

TIMESTAMP 21:28:39:011

APPLICATION TESTER : PoC Client sends SIP REGISTER request

TIMESTAMP 21:28:39:011

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:39:058

****

IMS PDU :200-OK

PDU Direction :From Network to UE

PDU Length :474 Octets

----------SIP MESSAGE----------

SIP/2.0 200 OK

To:<sip:rakesh@172.21.111.48:5070;transport=udp>;tag=23482900

From: <sip:rakesh@172.21.111.48:5090;transport=udp>;tag=f7162a4e

Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-e07d3e1893584846-1--d87543-;rport=5090Call-ID: 3b560f3d940f8b01@dGNzMDU5MTk3LkFFUk9GTEVY

CSeq: 1 REGISTER

Contact:<sip:rakesh@172.21.111.48:5090;transport=udp>;+g.poc.talkburst;+g.poc.groupadP-Associated-URI: <sip:rakesh@172.21.111.48:5070>Content-Length: 0

****

TIMESTAMP 21:28:39:167

****

IMS PDU :PUBLISH

PDU Direction :From UE to Network

PDU Length :513 Octets

----------SIP MESSAGE----------

PUBLISH sip:rakesh@172.21.111.48:5070;transport=udp SIP/2.0

To:<sip:rakesh@172.21.111.48:5070;transport=udp>

From:<sip:rakesh@172.21.111.48:5090;transport=udp>;tag=10561d56

Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-a0240e37e1683b10-1--d87543-;rport=5090Call-ID: 400fb428264e617e@dGNzMDU5MTk3LkFFUk9GTEVY

CSeq: 1 PUBLISH

Contact: <sip:rakesh@172.21.111.48:5090;transport=udp>Max-Forwards: 70

Content-Length:0

Request-URI: <sip:rakesh@172.21.111.48:5070;transport=udp>;tag=23482900

****

TIMESTAMP 21:28:39:214

IMS APPLICATION :INFORMATION

LOG :200 OK sent to Poc Client

FILE

:x:\trinity\source\application\applicationtester\imscomponents\imsapplication\imsinterfaceimpl.cpp

LINE :322

TIMESTAMP 21:28:39:214

APPLICATION TESTER :PoC Client is registered with the SIP/IP core successfully

TIMESTAMP 21:28:39:230

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:39:980

APPLICATION TESTER :User Prompt - Please initiate an Ad-hoc PoC Group Session to PoC Friend 1 and PoC Friend 2 and press OK

TIMESTAMP 21:28:40:495

****

IMS PDU :INVITE

PDU Direction :From UE to Network

PDU Length :1390 Octets

----------SIP MESSAGE----------

INVITE sip:rakesh@172.21.111.48:5070;transport=udp SIP/2.0

To:<sip:rakesh@172.21.111.48:5070;transport=udp>

From: <sip:rakesh@172.21.111.48:5090;transport=udp>;tag=b118c675

Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-106ba83d4b15125d-1--d87543-;rport=5090

Call-ID:195bd815bd23e749@dGNzMDU5MTk3LkFFUk9GTEVY

CSeq: 1 INVITE

Contact: <sip:rakesh_contact@172.21.111.48>;+g.poc.talkburstMax-Forwards: 70

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Content-Type: multipart/mixed;boundary=2d233e239b427e62Require: recipient-list-inviteUser-Agent: PoC-serv/OMA1.0Allow-Events: dialogP-Asserted-Identity: <sip:rakesh@172.21.111.48:5090;transport=udp>Accept-Contact: <sip:>;require;explicit;+g.poc.talkburst

Content-Length: 564Request-URI: <sip:rakesh@172.21.111.48:5070>--2d233e239b427e62

Content-Type: application/sdpv=0o=rakesh 1 1 IN IP4 172.21.111.158s=eyeBeamc=IN IP4 172.21.111.158t=0 0m=audio 50958 RTP/AVP 0m=video 2000 RTP/AVP 98a=rtpmap:0 PCMU/8000/1--2d233e239b427e62Content-Type: application/resource-lists+xml<?xml version="1.0" encoding="UTF-8"?>

<resource-lists xmlns="urn:ietf:params:xml:ns:resource-lists" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<list>

<entry uri="sip:bill@example.com"/>

<entry uri="sip:joe@example.org" />

</list>

</resource-lists>

--2d233e239b427e62--

****

TIMESTAMP 21:28:40:589

APPLICATION TESTER : PoC Client sends INVITE message to the test tool

TIMESTAMP 21:28:40:589

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:433

APPLICATION TESTER :The Accept-Contact header contains the PoC feature-tag "+g.poc.talkburst" with the parameters "require" and "Explicit"

TIMESTAMP 21:28:42:433

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:448

APPLICATION TESTER :The User-Agent header is set to PoC-serv/OMA1.0 which indicates the PoC release version

TIMESTAMP 21:28:42:448

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:464

APPLICATION TESTER :The PoC feature-tag "+g.poc.talkburst" is included in the Contact header

TIMESTAMP 21:28:42:464

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:479

APPLICATION TESTER :The Authenticated Originator's PoC Address is provided in the P-Asserted-Identity header set to the value rakesh@172.21.111.48:5090

TIMESTAMP 21:28:42:479

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:495

APPLICATION TESTER :The Request-URI is set to the Conference-factory-URI

TIMESTAMP 21:28:42:495

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:495

APPLICATION TESTER :The Content-Type header is set to multipart/mixed

TIMESTAMP 21:28:42:511

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:511

APPLICATION TESTER :The message includes a MIME SDP body as a SDP answer containing the ipaddress set to 172.21.111.158 and port of RTP session set to 50958

TIMESTAMP 21:28:42:511

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:526

APPLICATION TESTER :The media parameter offered by the PoC client is audio

TIMESTAMP 21:28:42:526

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:526

APPLICATION TESTER :The codecs parameter offered by the PoC client with media type audiois PCMU

TIMESTAMP 21:28:42:526

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:42:526

APPLICATION TESTER :The media parameter offered by the PoC client is video

TIMESTAMP 21:28:42:542

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:45:526

APPLICATION TESTER :In the message body ,there are two entries in the URI-list set to the value sip:joe@example.org and sip:bill@example.com and the XML document is valid and conforms with the schema.

TIMESTAMP 21:28:45:542

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:45:573

****

IMS PDU :100-TRYING

PDU Direction :From Network to UE

PDU Length :324 Octets

----------SIP MESSAGE----------

SIP/2.0 100 TryingTo: <sip:rakesh@172.21.111.48:5070;transport=udp>From: <sip:rakesh@172.21.111.48:5090;transport=udp>;tag=b118c675Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-106ba83d4b15125d-1--d87543-;rport=5090Call-ID: 195bd815bd23e749@dGNzMDU5MTk3LkFFUk9GTEVY

CSeq: 1 INVITE

Content-Length: 0

****

TIMESTAMP 21:28:45:839

****

IMS PDU :180-RINGING

PDU Direction :From Network to UE

PDU Length :375 Octets

----------SIP MESSAGE----------

SIP/2.0 180

Ringing To:<sip:rakesh@172.21.111.48:5070;transport=udp>;tag=6c3de14a

From: <sip:rakesh@172.21.111.48:5090;transport=udp>;tag=b118c675Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-106ba83d4b15125d-1--d87543-;rport=5090Call-ID: 195bd815bd23e749@dGNzMDU5MTk3LkFFUk9GTEVYCSeq: 1 INVITE

Contact: <sip:>Allow: Require: Content-Length: 0

****

TIMESTAMP 21:28:45:964

****

IMS PDU :200-OK

PDU Direction :From Network to UE

PDU Length :379 Octets

----------SIP MESSAGE----------

SIP/2.0 200 OK

To:<sip:rakesh@172.21.111.48:5070;transport=udp>;tag=ae72d62c

From: <sip:rakesh@172.21.111.48:5090;transport=udp>;tag=b118c675

Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-106ba83d4b15125d-1--d87543-;rport=5090

Call-ID:195bd815bd23e749@dGNzMDU5MTk3LkFFUk9GTEVY

CSeq: 1 INVITE

Contact: <sip:>

Content-Length: 0P-Answer-State: Unconfirmed

****

TIMESTAMP 21:28:46:073

****

IMS PDU :ACK

PDU Direction :From UE to Network

PDU Length :240 Octets

----------SIP MESSAGE----------

ACK sip: SIP/2.0

To: <sip:>

From: <sip:>

Via: SIP/2.0/UDP 172.21.111.48:5090;branch=z9hG4bK-d87543-e7320f0ba155a132-1--d87543-;rport=5090Call-ID:

CSeq: 1 ACKContact: <sip:172.21.111.48:5090>Max-Forwards: 70Content-Length: 0

****

TIMESTAMP 21:28:46:167

APPLICATION TESTER : Test Tool sends 180 Ringing response to PoC Client

TIMESTAMP 21:28:46:167

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:46:167

APPLICATION TESTER : Test Tool sends 200 OK response to PoC Client

TIMESTAMP 21:28:46:167

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:46:167

APPLICATION TESTER : PoC Client sends SIP ACK request in response to 200 OK

TIMESTAMP 21:28:46:182

APPLICATION TESTER :Partial Verdict:PASS

TIMESTAMP 21:28:46:229

APPLICATION TESTER :Final Verdict: PASS

TIMESTAMP 21:28:46:229

APPLICATION TESTER :POC Test CasePoC-1.0-con-C-0047 completed

****

6.4 Limitations

The main drawback in this project was that this project was not platform independent i.e., it runs only on Windows 2000 professional. Due to this reason the scope of this application is limited to those systems only, which support Windows 2000 professional.

While running the reciprocate libraries it was found that these libraries were not updated , so some more headers, to implement required functionalities, have to be included. Because of the size of the PoC specification, and the lack of information in it, some parts were dropped. The application was limited to only receiving and transmission of requests and responses. No voice data could be included successfully. Voice communication was dropped in a later stage.

Chapter-7

CONCLUSIONS AND FUTURE SCOPE

7.1 Conclusions:

The PoC service will provide benefits to all relevant players of the value system and hence has good likelihood to succeed .For the end user PoC is a new way to communicate, which supports all kinds of social groups, from sailing to hunting teams and from families.

Benefits to network operators and other operators are obvious. PoC is a low capital expenditure technology, which requires only low cost servers to be installed and operated. The server infrastructure even scales with the traffic. Operators can now finally utilize their existing data network capacity, which in the past has been somewhat difficult because of not so many driver applications. For operators PoC is clearly a way to differentiate, as Nextel has shown in the USA. PoC is one obvious way to segment the services. PoC can be seen on a contour, where the minimum value proposition is text (chat or instant) messaging, extending through multimedia messaging (especially simple audio messaging) to PoC and beyond to ordinary voice service and voice conference services. For mobile equipment vendors PoC is one additional feature, which will fuel the update cycle of the end user devices. For some models PoC will be available also as downloadable software. This will impact not only the sales of the mobile devices but have some impact to the competition for the winning application platform.

Following points have been observed in session establishment of PoC session:

1) Initiation latency for a PoC session is low: around 1 to 2 seconds: To set-up a PoC session is fairly quick, around 1 – 2 seconds if the client has been launched and if the terminal is in READY state. On the negative side terminals with established PDP contexts may after a certain time period be regarded as “inactive” on radio resource and, or, mobility management level. When this happens, the network will have to page the terminal before Push-to-talk speech frames can be delivered to a recipient, even if a Push-to-talk session already exists. This issue could be addressed by fine-tuning of timers that control the state transitions.

2) The application level signaling is fast for PoC: As SIP is used for signaling it is possible to use the SigComp compression technique to compress the SIP headers. This

makes the signaling overhead smaller and the signaling faster. This is one reason for the low call set-up times for PoC.

Table- 7.1 PoC Capacity & Latency comparison

PoC Capacity Dimensioning	
Average Duration	40secs
No.of bits per User	3
Session Initiation Latency in PoC	1-2 secs
Session Initiation Latency in GSM	3-5 secs

7.2 Future Scope:

The future scope of this work is that PoC service can be implemented using IMS and the service can be accessed by using the same mobile sets whose functionality is being checked. Advantages with PoC solutions based on the evolving OMA specifications are:

o Interoperability between terminals and networks

o Interoperability between operators

o Native PoC client support in terminals

o Synergies in terminals and networks with other future IMS based services

o The possibility to use performance boosters such as SIGCOMP for SIP signaling and Header Compression mechanisms for RTP frames carrying speech samples.

APPENDIX-I: A brief introduction to SIGCOMP

INTRODUCTION

Many application protocols used for multimedia communications are text-based and engineered for bandwidth rich links. As a result the messages have not been optimized in terms of size. For example, typical SIP messages range from a few hundred bytes up to two thousand bytes or more. With the planned usage of these protocols in wireless handsets as part of 2.5G and 3G cellular networks, the large message size is problematic.With low-rate IP connectivity the transmission delays are significant. Taking into account retransmissions, and the multiplicity of messages that are required in some flows, call setup and feature invocation are adversely affected. SigComp provides a means to eliminate this problem by offering robust, lossless compression of application messages.

SigComp is offered to applications as a layer between the application and an underlying transport. The service provided is that of the underlying transport plus compression. SigComp supports a wide range of transports including TCP, UDP and SCTP.

TERMINOLOGY

Application: Entity that invokes SigComp and performs the following tasks:

1. Supplying application messages to the compressor dispatcher.

2. Receiving decompressed messages from the decompressor dispatcher.

3. Determining the compartment identifier for a decompressed message.

Bytecode: Machine code that can be executed by a virtual machine.

Compressor: Entity that encodes application messages using a certain compression algorithm, and keeps track of state that can be used for compression. The compressor is responsible for ensuring that the messages it generates can be decompressed by the remote UDP.

Compressor Dispatcher: Entity that receives application messages, invokes a compressor, and forwards the resulting SigComp compressed messages to a remote endpoint.

UDVM Cycles: A measure of the amount of "CPU power" required to execute a UDVM instruction (the simplest UDVM instructions require a single UDVM cycle). An upper limit is placed on the number of UDVM cycles that can be used to decompress each bit in a SigComp message.

Decompressor Dispatcher: Entity that receives SigComp messages, invokes a UDVM, and forwards the resulting decompressed messages to the application.

Endpoint: One instance of an application, a SigComp layer, and a transport layer for sending and/or receiving SigComp messages.

Message-based Transport: A transport that carries data as a set of bounded messages.

Compartment: An application-specific grouping of messages that relate to a peer endpoint. Depending on the signaling protocol, this grouping may relate to application concepts such as "session", "dialog", "connection", or "association". The application allocates state memory on a per-compartment basis, and determines when a compartment should be created or closed.

Compartment Identifier: An identifier (in a locally chosen format) that uniquely references a compartment.

SigComp: The overall compression solution, comprising the compressor, UDVM, dispatchers and state handler.

SigComp Message: A message sent from the compressor dispatcher to the decompressor dispatcher. In case of a message-based transport such as UDP, a SigComp message corresponds to exactly one datagram. For a stream-based transport such as TCP, the SigComp messages are separated by reserved delimiters.

Stream-based transport: A transport that carries data as a continuous stream with no message boundaries.

Transport: Mechanism for passing data between two endpoints. SigComp is capable of sending messages over a wide range of transports including TCP, UDP and SCTP

Universal Decompressor Virtual Machine (UDVM):The machine architecture described in this document. The UDVM is used to decompress SigComp messages.

State: Data saved for retrieval by later SigComp messages.

State Handler: Entity responsible for accessing and storing state information once permission is granted by the application.

State Identifier: Reference used to access a previously created item of state.

ARCHITECTURE

In the SigComp architecture, compression and decompression is performed at two communicating endpoints. The layout of a single endpoint is illustrated in Figure :

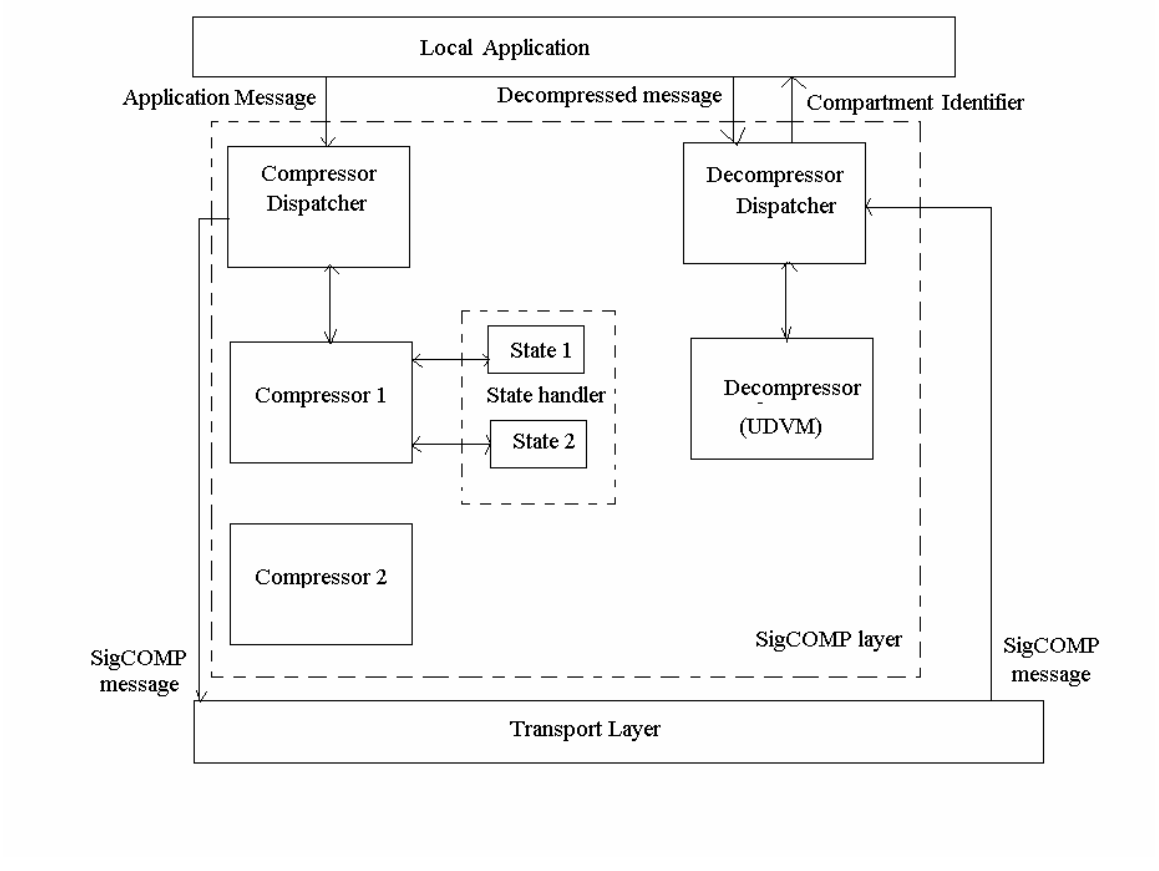

Figure-1 High-level architectural overview

The SigComp layer is further decomposed into the following entities:

1. Compressor dispatcher - the interface from the application. The application supplies the compressor dispatcher with an application message and a compartment identifier.

The compressor dispatcher invokes a particular compressor, which returns a SigComp message to be forwarded to the remote endpoint.

2. Decompressor dispatcher - the interface towards the application. The decompressor dispatcher receives a SigComp message and invokes an instance of the Universal Decompressor Virtual Machine (UDVM).It then forwards the resulting decompressed message to the application, which may return a compartment identifier if it wishes to allow state to be saved for the message.

3. One or more compressors - the entities that convert application messages into SigComp messages. Distinct compressors are invoked on a per-compartment basis, using the compartment identifiers supplied by the application. A compressor receives an application message from the compressor dispatcher, compresses the message, and returns a SigComp message to the compressor dispatcher. Each compressor chooses a certain algorithm to encode the data (e.g.,DEFLATE).

4. UDVM - the entity that decompresses SigComp messages. Note that since SigComp can run over an unsecured transport layer, a separate instance of the UDVM is invoked on a per-message basis. However, during the decompression process the UDVM may invoke the state handler to access existing state or create new state.

5. State handler - the entity that can store and retrieve state.State is information that is stored between SigComp messages, avoiding the need to upload the data on a per-message basis. For security purposes it is only possible to create new state with the permission of the application.

APPENDIX-II:AMR(Adaptive Multi Rate) Codec

INTRODUCTION

The transmission of speech from one point to another over GSM mobile phone network is something that most of us take for granted. The complexity is usually perceived to be associated with the network infrastructure and management required in order to create the end-to-end connection, and not with the transmission of the payload itself. The real complexity, however, lies in the codec scheme used to encode voice traffic for transmission.

The GSM standard supports four different but similar compression technologies to analyse and compress speech. These include full-rate, enhanced full-rate (EFR), adaptive multi-rate (AMR), and half-rate. Despite all being lossy (i.e. some data is lost during the compression), these codecs have been optimized to accurately regenerate speech at the output of a wireless link.

PRINCIPLE

The principle of the AMR codec is to use very similar computations for a set of codecs, to create outputs of different rates. In GSM, the quality of the received air-interface signal is monitored and the coding rate of speech can be modified. In this way, more protection is applied to poorer signal areas by reducing the coding rate and increasing the redundancy, and in areas of good signal quality, the quality of the speech is improved.

In terms of implementation, an ACELP(Algebraic coder excited linear prediction) is used. In fact, the 12.2 kbit/s AMR codec is computationally the same as the EFR codec. For rates lower than 12.2 kbit/s, the short-term analysis is performed only once per frame. For 5.15 kbit/s and lower, the open-loop pitch lag is estimated only once per frame. The result is that at lower output bit rates, there are a smaller number of parameters to transmit, and fewer bits are used to represent them.

The air transmission specification for GSM allows the splitting of a voice channel into two sub-channels that can maintain separate calls. A voice coder that uses half the channel capacity would allow the network operators to double the capacity on a cell for very little investment.

The half-rate codec is a vector sum excitation linear prediction (VSELP) codec that operates on an analysis-by-synthesis approach similar to the EFR and AMR codecs. The resulting output is 5.7 kb/s, which includes 100 b/s of mode indicator bits specifying whether the frames are thought to contain voice or no voice. The mode indicator allows the codec to operated slightly differently to obtain the best quality.

Half-rate speech coding was first introduced in the mid 1990's, but the public perception of speech quality was so poor that it is not generally used today. However, due to the variable bit-rate output, AMR lends itself nicely to transmission over a half-rate channel. By limiting the output to the lowest 6 coding rates (4.75 -- 7.95kbps), the user can still experience the quality benefits of adaptive speech coding, and the network operator benefits from increased capacity. It is thought that with the introduction of AMR, use of the half-rate air-channel will start to become much more widespread.

The Open Mobile Alliance (OMA) has published several new standards for mobile content services. OMA Enabler Releases, developed collaboratively by more than 380 OMA member companies around the world, enable interoperable wireless data services to be launched amongst operators and terminals worldwide. To date, OMA has published 26 Candidate and Approved Enabler Releases that have been incorporated into new products and increased market opportunities for the mobile industry.

By minimizing market fragmentation and enabling seamless interoperability, the Open Mobile Alliance (OMA) hopes to stimulate the growth of mobile services. Accordingly, it works to implement open and global standards in unified service platforms, thereby enabling vendors to implement their branded products while maintaining the interoperability of personalized services across markets and a broad range of mobile terminals. More specifically, the objectives of the OMA are

• to enable consumer access to interoperable and easy-to-use mobile services across geographies, operators and mobile terminals;

• to define an open standards-based framework for permitting services to be built, deployed, and managed efficiently and reliably in a multi-vendor environment;

• to establish a standards forum (the OMA) for the mobile industry to function as the driving force for creating service level interoperability; and

• to drive the implementation of open services and interface standards, using a user centric approach that guarantees rapid and broad adoption of mobile services.

OMA in the mobile platform and terminals

The OMA Mobile Applications Group is continuing to develop the Mobile Applications Environment, the heir to the WAP Forum Wireless Application Environment, which contains support for an address book, calendar, scripting language, and browser functions. The imminent affiliation of the Mobile Games Interoperability Forum, will put a function that depends heavily on standardizing terminals squarely on the OMA agenda. Obviously this will affect the work in the OMA and the direction it takes in the future.

Third-generation phones from Sony Ericsson and other manufacturers will greatly benefit from the specifications of the OMA, since they are based on open and interoperable standards and service enablers that provide the best possible quality end to- end, as implemented by Ericsson Mobile Platforms. For the sake of performance, it is still more efficient to perform many functions in the service layer of the fixed network. But with the addition of more technology in the mobile phone, the creation of entirely new end-user services is not far off. OMA in the (service) network.

The OMA does not define network technologies, since this lies outside of the scope set by its founders. The main task of the OMA is to provide enablers which simplify the development and deployment of enduser services that use mobile technologies. Ericsson's service network framework (SNF), for example, and the OMA architecture overlap, but not entirely.

By following the intent of the Ericsson SNF work and by capitalizing on select technology, Ericsson can make a strong contribution to the OMA standards (as well as make a noticeable impact on the industry). At best, by providing contributions that are based on ready-made Ericsson technology, Ericsson can stay one step ahead of the competition. Ericsson's customers will thus benefit from fast roll-out of OMA technology, which is based on a complete and feature rich SNF solution.

Since every stakeholder can benefit from the work produced by the OMA, it is paramount that end-users find it worthwhile to endeavor into a mobile experience for business and pleasure. Sony Ericsson is at the forefront with another generation of media-rich devices that create a mobile bridge to the entertainment industry. Technology from Ericsson's infrastructure business and Ericsson Mobile Platforms will make this possible.

Standards-development activities within the Ericsson infrastructure side with keen support from the Ericsson Mobile Platforms in Lund, Sweden, will play a great and important role in making the OMA a success for an entire industry. Ericsson Mobile Platforms will be committed to deliver the necessary technology and support to further enhance the end-user experience of advanced end to end mobile services.

REFRENCES

---

[1] Koukoulidis, V., Shah, M.,"The IP multimedia domain in wireless networks: concepts, architecture, protocols and applications", Multimedia Software Engineering, 2004. Proceedings. IEEE Sixth International Symposium, Page(s): 484 – 490, 13-15 Dec. 2004.

[2] Mani, M., Crespi, N., "Access to IP multimedia subsystem of UMTS via Packet Cable network", Wireless Communications and Networking Conference, 2005 IEEE, Volume: 4,Page(s): 2459-2465,13-17 March2005.

[3] Knightson, K., Morita, N., Towle, T, "NGN architecture: generic principles, functional architecture, and implementation", Communications Magazine, IEEE,
Volume: 43,Issue: 10,page(s): 49-56,Oct.2005.

[4] Jain, P., Kelkar, R., "Mobile IP: Enabling Mobility for the 3G Wireless Internet", Tata Consultancy Services Ltd., April 2003.

[5] Marsic, B., Borosa, T., Pocuca, S., "IMS to PSTN/CS Interworking", Telecommunications, 2003. 'ConTEL 2003'. Proceedings of the 7th International Conference, Volume: 2,Page(s): 701-704,11-13 June2003.

[6] Rahadian Dewantoro, Andreas Reifert, Michael Scharf, "IP Multimedia Subsystem (IMS) and Its Comparison with Different Systems", Seminar in High Performance Network Architecture (HPNA) Institute of Communication Networks and Computer Engineering (IKR), University of Stuttgart Germany 2005.

[7] Wei Zhuang, Yung Sze Gan, Kok Jeng Loh, Kee Chaing Chua, "Policy-based QoS architecture in the IP multimedia subsystem of UMTS", Network, IEEE,
Volume: 17,Issue: 3,Page(s): 51-57,May-June 2003.

[8] 3GPP TS 23228, "IP Multimedia Subsystem", stage 2,release 5.

[9] Blum, N. Magedanz, T., "PTT + IMS = PTM - towards community/presence-based IMS multimedia services", Multimedia, Seventh IEEE International Symposium, Page(s): 8, 12-14 Dec.2005.

[10] La Porta, T.F., "Security and IP-based 3G wireless networks", Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference, Page(s): 211,17-19 Oct.2005.

[11] Kim, P., Balazs,.A., van den Brock, E. , Kieselinann, G. , Bohm, W., "IMS-based push-to-talk over GPRS/UMTS", Wireless Communications and Networking Conference, 2005 IEEE, Volume: 4, Page(s): 2472 – 2477,13-17 March 2005.

[12] Parthasarathy, A. , "Push to talk over cellular (PoC) server", Networking, Sensing and Control, 2005, Proceedings 2005 IEEE, Page(s): 772-776, 19-22March2005.

[13] Raktale, S.K,"3 PoC: an architecture for enabling push to talk services in 3GPP networks", Personal Wireless Communications, 2005, ICPWC 2005, IEEE International Conference, Page(s): 202-206, 23-25 Jan. 2005.

[14] Bushmitch, D. Wanrong Lin Bieszczad, A. Kaplan, A. Papageorgiou, V. Pakstas, A., "A SIP-based device communication service for OSGi framework", Consumer Communications and Networking Conference, 2004, 'CCNC-2004',
Page(s): 453 – 458, 5-8 Jan. 2004.

[15] Plitsis, G. Keller, R. Sachs, J.,"Realization of a push service for Media Points based on SIP", Mobile and Wireless Communications Network, 2002, 4th International Workshop, Page(s): 256-260, 9-11 Sept.2002.

[16] Kolberg, M. Magill, E.H. , " Handling incompatibilities between services deployed on IP-based networks", Intelligent Network Workshop, 2001 IEEE, 2001,
Page(s): 360 – 370, 6-9 May 2001.

[17] Chih Yuan Hung, Chin Ping Tan, Li Chiung Chuang, Wei-Tsong Lee, "The implementation of the communication framework of SIP and MGCP in VoIP applications", ICON-2002, 10th IEEE International Conference on
Networks, Page(s): 449-454, 27-30 Aug 2002.

[18] Vlaovic, B. Brezocnik, Z.,"Packet based telephony", EUROCON '2001, Trends in Communications, International Conference, Volume:1, Page(s): 210 – 213, 4-7 July 2001.

[19] www.northstream.se.

[20] Eoin O'Regan, Dirk Pesch, "Performance Estimation of a SIP based Push-to-Talk Service for 3G Networks", Adaptive Wireless Systems Group Cork Institute of Technology Ireland.

[21] RFC 3667, " PoC architecture", Release 2.0.

[22] Raili Koivito, " Push To Talk Over Cellular: Still Searching the flow of success".

PUBLICATIONS

1. Hazel Saxena, Mishu Gupta,“ Direct to Home”, published in National Conference on Bio-Informatics Computing organized by Computer Science Engineering Department at Thapar Institute of Engineering and Technology, Patiala, Page(s): 566-571, held on 18th-19th March, 2005.
2. Hazel Saxena, Navjot Kaur, “Push To Talk over Cellular”, accepted in National Conference on Wireless Networks and Embedded Systems organized by Electronics and Communication Department at Chitkara Institute of Engineering and Technology, Rajpura to be held on 28th July 2006.