MIDDLEWARE ARCHITECTURE FOR SECURING AND IMPROVING IP MULTIMEDIA SUBSYSTEM (IMS) BASED NEXT GENERATION NETWORK MULTIMEDIA SERVICES

RESEARCHER: ZEESHAN SHAFI KHAN

REGISTRATION #: 19-FAS/PHDCS/S05

SUPERVISORS: PROF. DR. MUHAMMAD SHER
PROF. DR. KHALID RASHID

DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF BASIC AND APPLIED SCIENCES

INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD

PAKISTAN

2011

1. Internet protocol multimedia system
2. Computer software - Development

MIDDLEWARE ARCHITECTURE FOR SECURING AND IMPROVING IP MULTIMEDIA SUBSYSTEM (IMS) BASED NEXT GENERATION NETWORK MULTIMEDIA SERVICES

ZEESHAN SHAFI KHAN

19-FAS/PHDCS/S05

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science at the Faculty of Basic and Applied Sciences

International Islamic University,

Islamabad

Prof. Dr. Muhammad Sher

Prof. Dr. Khalid Rashid

September 2011

APPROVAL

Title of the Thesis:	Middleware Architecture for Securing and Improving IP Multimedia Subsystem (IMS) Based Next Generation Network Multimedia Services
Name of the Student:	Zeeshan Shafi Khan
Registration No.	19-FAS/PhDCS/S05

Accepted by the Department of Computer Science, INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD, in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science

Viva Voce Committee

Prof. Dr. Muhammad Irfan Khan
Dean, Faculty of Basic and Applied Sciences,
International Islamic University, Islamabad

Prof. Dr. Muhammad Sher (Supervisor)
Chairman, Department of Computer Science,
International Islamic University, Islamabad

Prof. Dr. Khalid Rashid (Supervisor)
Advisor, COMSATS Institute of Information Technology,
Islamabad

Dr. Muhammad Zubair (Internal Examiner)
Assistant Prof. Department of Computer Science,
International Islamic University, Islamabad

Prof. Dr. Sikandar Hayat Khiyal (External Examiner I)
Chairperson, Computer Sciences,
Fatima Jinnah Women University, Rawalpindi

Prof. Dr. Muhammad Younas Javed (External Examiner II)
Associate Dean/Head of Department.
Department of Computer Engineering,
College of EME (NUST), Rawalpindi

Thursday September 29, 2011

ABSTRACT

IP Multimedia Subsystem (IMS), an architectural framework for Next Generation Networks (NGN) planes to converge all the networks and services on one IP based platform. IMS application plane consists of various types of application servers those provides different types of services. These Services include Presence, Instant Messaging, Push to talk over cellular, multiparty conference etc. IMS application server and other servers are subject to various types of security threats including time dependent and time independent attacks. Moreover currently available service features are not enough to meet the needs of daily life communication. To secure the application plane we proposed a signature based role oriented Intrusion Detection and Prevention (IDP) system. An anomaly detection module is also added to increase the level of security. We also proposed few other solutions those add security in IMS application plane. These solutions include User preferences based instant messaging, presence based instant messaging, election based referring, location based deletion of malicious users etc. To enrich the IMS based multimedia services we developed different solutions for different services and these solutions include presence enabled call setup, media mixing through presence information, floor control mechanism, parameterized referring, election based right allocation mechanism etc. To test the developed solution we create an IMS testbed by using open source solutions. Prototypes of services are also developed. The results are obtained by implementing the proposed solution over the testbed. It is observed that the proposed solutions enhances the security of IMS based services, and include value added features to make them feasible for more daily life scenarios.

DECLERATION

I hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that I have conducted this research and have accomplished this thesis entirely on the basis of our personal efforts and under the sincere guidance of my supervisor Prof. Dr Muhammad Sher and Co-Supervisor Prof. Dr. Khalid Rashid. If any part of this project is proved to be copied out from any source or found to be reproduction of some other project, I shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

ZEESHAN SHAFI KHAN

19-FAS/PHDCS/S05

A Dissertation submitted to the

Department of Computer Science

International Islamic University Islamabad

As a partial fulfillment of requirements for the award of

The degree of

PhD in Computer Science

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time

ACKNOWLEDGEMENTS

All praise to Almighty Allah who has all the names, and who needs no name the most generous, considerate, and compassionate who has blessed mankind with this verdict to think, explore, to learn and discover the hidden secrets of this universe and helped me to broaden the veils of my thought and enabling me to get through the difficulties indulged during this project. Also admiration to our beloved Prophet Muhammad (PBUH) who is always a great source of inspiration of divine devotion and dedication to me.

I would cordially pay my special appreciations and whole heartedly considerations to my reverend supervisors Prof. Dr. Muhammad Sher and Prof. Dr. Khalid Rashid for their endless support, guidance and coordination while conducting this project. I owe them a great respect and honor and I am privileged to work under their supervision. It was their efforts, courage, moral support and endeavoring attitude that helped me to get through any problem or difficulty during each step of this project.

I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance and help. Thanking Dr. Sikandar Hayat, Dr, Afaq Hussain, Dr. Mureed Hussain, Dr. Nazir A. Sangi, for their views which helped me in improving the proposal, also Mr. Bilal Shah, Mr. Mehmood, and Mr. Saeed, Mr. Munawar Shah, Mr. Athar, and Mr. Saleem for providing the managerial and administrative support.

Thanking my friends for always being there for me whenever I needed them for their help, generosity and moral support. Special thanks to Mr. Rehan Shafi, Dr. Muhammad Zubair, Mr. Qutbuddin, Mr. Arman Shafi, Mr. Sagheer Ahmed, Mr. Usman Razzak, Mr. Muhammad Shoaib, Mr. Rashid Mehmood, Mr. Ajmal Bhatti, Mr. Naeem, Mr. Imran Tariq, Mr. Zia-ur-Rehman, Mr. Bashir Ahmed, Mr. Musharraf, Mr. Zubair Rafique, Mr. Irfan Nabi and Mr. Iftikhar Wattoo.

I would also like to thank my students who helped me to broaden my knowledge in different domains. Special thanks to Ms. Nabila Akram, Ms. Nazish Munawar, Mr. Bashir Ahmed, Ms. Isma Munir, Ms. Saira Shoukat, Mr. Zia-ur-rehman, Mr. Waheed

Ahmed, Ms. Rukhsana Kousar, Mr. Sharjeel Gellani, Mr. Saqlain Raza, Mr. Khalid Mehmood and Mr. Fraz Siddiqui.

I also owe a special thanks and gratitude to Dr. Thomas Magedanz and Technical University of Berlin, for supporting me in working on this idea and accompanying me with the material for study which I needed during this research. This work can not be completed without the support of Center of Excellence in Information Assurance, King Saud University, KSA. A special thanks to Dr. Khaled and Dr. Khurram who provides me opportunity to broaden my knowledge and vision in the field of networks and security. Acknowledgement section can not be completed without thanking the higher education commission of Pakistan which is the most encouraging body to promote research in Pakistan.

Finally my beloved parents and family who deserve the credit more than I could ever express for always being completely supportive to me. They have been a constant source of advice, love and devotion to me. From moral to financial they have been blessing me with all the support that I needed up till now in my life. A special thanks to my wife who was with me to get through thick and thin of my research.

I express my countless appreciation to all the people who have helped me during achieving this PhD degree and hope to have this honor that they would walk along me through out my life.

ZEESHAN SHAFI KHAN

19-FAS/PHDCS/S05

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
A-IMS	Advances in IP Multimedia Subsystem
AIN	Advanced Intelligent Network
AKA	Authentication and Key Agreement
ANSI	American National Standards Institute
AP	Authentication Proxy
APIs	Application Programming Interfaces
AS	Application Server
AuC	Authentication Centre
AUTN	Authentication Token
AV	Authentication Function
B2BUAs	Back To Back User Agents
BGCF	Border Gateway Control Function
BSF	Bootstrapping Server Function
B-TID	Bootstrapping Transaction Identifier
CA	Certification Authority
CAMEL	Customized Applications for Mobile Enhanced Logic

CAP	CAMEL Application Protocol
CBC	Cipher Block Code
CGI	Common Gateway Interface
CK	Cipher Key
COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
CPL	Call Programming Language
CPU	Central Processing Unit
CRLs	Certificate Revocation Lists
CS	Circuit Switched
CSCFs	Call State Control Functions
CSE	CAMEL Support Environment
DCA	Domain Certificate Authority
DDoS	Distributed Denial-of-Service Attacks
DES	Data Encryption Standard
DNS	Domain Name Server
DOM	Document Object Model
DoS	Denial of Service
DSS1	Digital Subscriber Signalling #1
EAI	Enterprise Application Integration
ESP	Encapsulating Security Payload
FMC	Fixed Mobile Convergence

FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GGSN	GPRS Serving Node
GPRS	General Packet Radio System
GSM	Global System for Mobile
GUSS	GBA User Security Settings
HE	Home Environment
HLR	Home Location Register
HMAC	Hash Message Authentication Code
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP – Secure (HTTP over TLS)
ICMP	Internet Control Message Protocol
I-CSCF	Interrogating Call State Control Function
ICV	Integrity Check Value
ID	Identity
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange

IM	Instant Messaging/IP Multimedia
IMPI IP	Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INAP	IN Application Protocol
IP	Internet Protocol
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISC	P Multimedia Service Control
ISG	Integrated Security Gateway
ISIM	IP Multimedia Services Identity Module
ISIM	IM Service Identity Module
ISPs	Internet Service Providers
ISUP	ISDN User Part
IT	Information Technology
ITU-T	International Telecommunications Union
Ks	Session Key
MAP	Mobile Application Protocol
MD	Message Digest
ME	Mobile Equipment

MG	Media Gate
MMD	Mobile Multimedia Domain
MRF	Media Resource Function
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
NAF	Network Authentication Function
NDS/AF	Network Domain Security / Authentication Framework
NDS/IP	Network Domain Security / Internet Protocol
NGN	Next Generation Network
NGNI	Next Generation Network Integration
OMA	Open Mobile Alliance
OSA	Open Service Access
OSE	Open Service Environment
P-CSCF	Proxy Call State Control Function
PDP	Packet Data Protocol
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PoC	Push to talk over Cellular
POTS	Plain Old Telephony Service
PS	Packet Switched
PSK	Pre-Shared Key

PTM	Push to Multimedia
PTT	Push To Talk
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RAND	Random number
RDDOS	Reflected Distributed Denial-of-Service
RES	Response
RFC	Request For Comments
RNC	Radio Network Controller
RPC	Remote Procedure Call
RTP	Real-time Transport Protocol
SA	Security Association
SAD	Security Associations Database
SBLP	Service Based Local Policy
SCPs	Service Control Points
S-CSCF	Serving Call State Control Function
SDP	Service Delivery Platform
SEG	Security Gateway
SER	SIP Express Router
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm

SIBs	Service Building Blocks
SIP S	Session Initiation Protocol
SIPSEE	SIP Servlet Execution Environment
SLEE	Service Logic Execution Environment
SOAP	Simple Object Access Protocol
SOC	Security Operation Centre
SPA	Service Provider Access
SPAN	Service Provider Access Networks
SPD	Security Policy Database
SPI S	ecurity Parameter Index
SS7	Signalling System Number 7
SSP	Secure Service Provisioning
TCP	Transmission Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
UAC	User Agent Client
UAs	User Agents
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment

UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication Standard
URI	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VHE	Virtual Home Environment
VLR	Visited Location Register
VoIP	Voice over Internet Protocol
WIN	Wireless Intelligent Networks
WLAN	Wireless Local Area Network
WSDL	Web Service Description Language
XCAP	XML Configuration Access Protocol
XDMS	XML Document Management Server
XML	eXtensible Markup Language
XRES	Expected Response

CHAPTER 1

1. NEXT GENERATION NETWORKS AND IP MULTIMEDIA SUBSYSTEM

A platform for integration of telecommunication and information technology (IT) and creation of new services ranges above the boundaries of network and technology is known as service delivery platform (SDP). SDP implementation makes possible the development of new multimedia services. A lot of improvements and enhancements are required in the existing technologies and infrastructure in order to implement SDP. Seamless connectivity between fixed and mobile networks is defined as fixed mobile convergence (FMC). We are living in an era of voice centric carrier with more relay on circuit switching. Frame Relay, ATM, and IP based services are also provided by few overlay networks. Main motive of next generation networks (NGN) is to integrate different type of networks on to one standardized platform that will be able to offer almost all the services (Nigel Seel, 2006). According to AT&T NGN is "*A packet based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables access to different service providers, independent of any access or transport technology*".

International telecom union-T described that in NGN packet based technology should be used to transfer the data. The call and service control functions should not be merged at one point, they should be separate. There should be transparency between the service and the network components. Since new services can be included in future so there should be open interfaces for service provisioning. End to end quality of service is another characteristic that needs to be considered. Internetworking is also required for network convergence. Mobile scenarios should also be considered so as fixed mobile convergence. Security and emergency communication like parameters are also important and should be considered.

1.1 Motivation

The foundation for this thesis stems from the future trends of Fixed-Mobile Convergence (FMC), All-IP networks and next generation Service Delivery Platform (SDP) is a result of merger of Internet and mobile communication, computer networks and Information Technology (IT). In the vision of All-IP Networks, the IP Multimedia Subsystem (IMS) has been developed by 3GPP and 3GPP2. The IMS is an overlay architecture for the provision of multimedia services such as Voice over IP (VoIP), video conferencing, presence, push-to-talk etc. on top of all IP networks and the future technology for the convergence of data, speech and mobile networks. The IMS integrates different value added services and seamless integration of legacy services. It enables consistent interactions with packet switched, circuit switched, and IP domains.

These emerging systems based on event oriented charging policies; i.e. to change specific events on the appropriate level. If two events have the same IP resources, the system may charge them differently for the same user in a single session. These characteristics make IMS as the future technology in a comprehensive service delivery and application oriented network environment. The IMS is based on the principles and protocols of the Internet defined by the IETF, which have been adapted by 3GPP and TISPAN for their use within a secure and scalable fixed-mobile communication. For establishing, controlling, modifying and terminating the session, session initiation protocol (SIP) is used as a standard signaling protocol. IMS core has different types of call state control functions (CSCF) servers which implement and manage the SIP functionalities. Home subscriber server (HSS) is used to provide authentication, authorization and accounting (AAA) related functionality based on the diameter protocol. Media Gateways and Media Server support potentially required adaptation of multimedia information for specific QoS requirements.

IMS specifies a comprehensive and service oriented architecture providing value added services and standardized interfaces for application service integration. With this technical revolution, the promising value added services support to change the entire communication environment, IMS Application Server (AS) is one of the proposed and developed service containers. The IMS is overlay architecture on top of TCP/IP protocol stack providing value added services. It is like other IP-based network having open and distributed architecture that can enable easy access to services, information, and resources. But on the other side the hackers can access open architecture to launch attacks on IMS networks. Therefore strong and complex security solution and mechanisms such as secure data transmission, confidentiality, authentication, data integrity, anti-replay protection and intrusion detection system are essential to implement independent and robust security framework for IMS. Moreover security measures need to be taken as AS to secure the services. Addition of new value added features to make IMS based services more enrich, secure and attractive is also a milestone that needs to be achieved.

1.2 Session Initiation Protocol (SIP)

To manage multimedia session IETF approved SIP as standard application layer protocol. SIP is capable of:

- Determination of user location
- Determination of availability of end users
- Determination of different types of parameters related to media
- Establishment of multimedia sessions
- Session management

SIP message is shown below.

```
INVITE sip:zee.khan@xyz.com SIP/2.0
Via: SIP/2.0/UDP cscf1.example.com:5060;branch=z9hG4bK8542.1
Via: SIP/2.0/UDP [5555::1:2:3:4]:5060;branch=z9hG4bK45a35h76
Max-Forwards: 69
From: abc <sip:alice@abc.com>;tag=312345
To: Zee Khan <sip: zee.khan@xyz.com>
Call-ID: 105637746
CSeq: 1 INVITE Contact: sip:abc@[5555::1:2:3:4]
Content-Type: application/sdp
Content-Length: 159
```

SIP responses can be classified into 6 broad domains those are:

- 1xx – Everything is ok and user should remain in-touch to continue the process
- 2xx – Target achieved. Request is accepted.
- 3xx – Few more actions are required to complete the request. It is re-direction

- 4xx – Syntax errors. Client side errors are sent with the starting code 4
- 5xx – Server side errors are sent through code 5
- 6xx – Not even a single server is able to response this request.

Last two digits "xx" represents the specific response.

1.2.1 SIP Extensions

RFC 3265 enhance the existing SIP functionalities by adding an event notification framework. A user who is interested in information of another entity can subscribe for it. Subscribe message is defined by the RFC 3265. After receiving a subscribe message it is responded through a notify message. Construction of notify message is also defined by the RFC. A user can get state information of another user by subscribing it. Response is sent through notify message. But before sending notification it must be assured that the required state information is published on the server about who is going to respond. If the information is not published then it is impossible to notify it. Thus to publish state information a publish method is introduced by RFC 3903.

A message method is added by RFC 3862 which supports the instant messaging. For reliability of responses RFC 3262 introduces a reliability framework. Session description can be updated by using the update method. Update request can be used only in session setup by any of the party. Caller and callee both are allowed to send update request. Refer request is introduced in RFC 3515 and it means transfer. One user may refer other users to become part of the session. Refer can also means call transfer. A junior can transfer call to a senior by using refer request.

1.3 Real Time Protocol (RTP)

For media transfer 3GPP approve the RTP as standard protocol. RTP provides monitoring of QoS using RTP control (RTCP) protocol (RFC3550). RTP header contains various fields namely:

- Version (V) – Its value is always 2.
- Padding (P) – for padding in case of fixed size blocks
- Extension (X) – RTP header extension.
- CSRC count (CC) – Source ID
- Marker (M) – its interpretation is defined by a profile.
- Payload type (PT) –codec
- Sequence number – increments by 1 for each RTP data packet.
- Timestamp – indicates the time when first octet in the payload was sampled.
- Synchronization source (SSRC) – RTP is not dependent on the underlying Internet Protocol (IP)
- Contributing source (CSRC) – this field carries a list of SSRCs indicating the sources that have contributed to a mixed media stream

RTCP packet types are:

- SR – Sender report
- RR – Receiver report
- SDES – Source description items
- BYE – End of participation.
- APP – application-specific functions

RTP requires few documents for particular multimedia application. It is sometime called as profile specification document.

1.4 Service Delivery Protocol

Service delivery protocol (SDP) is used for the description of multimedia session. An SDP message contains three levels of information:

- Session-level description – this includes the session identifier and other session-level parameters, such as IP address, subject, contact info about the session and/or creator.
- Timing description – start and stop times, repeat times, one or more media-level descriptions.

Media type and format – transport protocol and port number, other media-level parameters.

1.5 IP Multimedia Subsystem (IMS)

IMS is an architectural framework for the FMC that includes many protocols (3GPP TS 23.002). SIP, standardized by IETF, is the signaling protocol used by the IMS. In 1999 a forum known as 3G.IP launched the project of IMS. Currently 3GPP, 3GPP2 and telecoms & Internet converged services & protocols for advanced networks (TISPAN) are involved in standardization of the IMS (Telrad Networks, 2006).

In 2002 finally release 5 is announced and idea of IMS came into being. IMS was defined as IP based access independent network for fixed mobile convergence. Security issues, registration procedures, session setup details, charging architecture, roaming scenarios bearer control etc. are given more importance in release 5. IMS release 6 introduced many enhancements in the existing IMS architecture. Security is given more importance. In 2008 release 7 was introduced in which fixed mobile convergence was the focus point. IMS releases 4, 5 and 6 mainly focused on mobile scenarios, while release 7 integrates the fixed and mobile scenarios under one platform (3GPP TS 23.228).

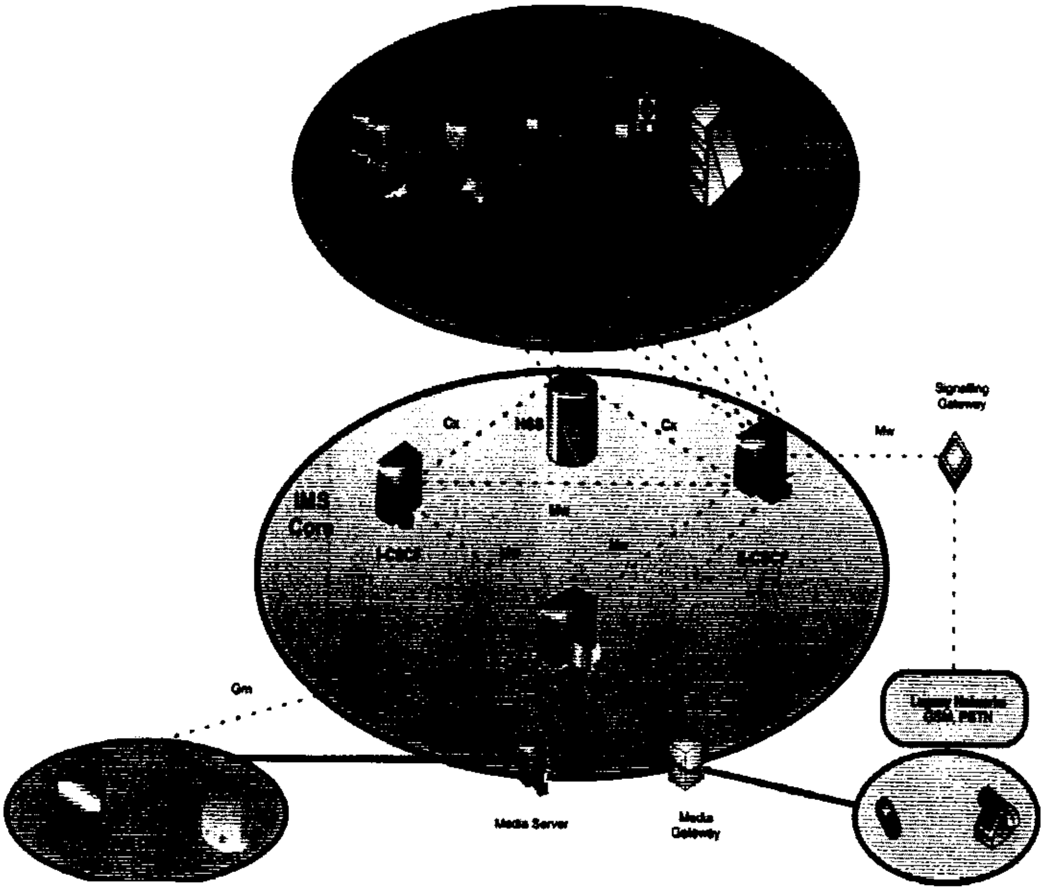


Figure 1.1: IMS Architecture and Components

1.5.1 IMS Components

Broadly IMS components can be classified into 6 main domains (3GPP TS 23.221). These 6 domains are described below:

1.5.1.1 Call Session Control Functions (CSCF)

IMS core consists of various types of CSCF. These CSCF are responsible for various types of tasks inside the IMS core and also provide interaction among upper and lower layers. IMS defined three CSCF, those are proxy-CSCF (P-CSCF), interrogating-CSCF (I-CSCF) and serving-CSCF (S-CSCF) (3GPP TS 23.003). Responsibilities of these three CSCF are described below.

P-CSCF

P-CSCF is the entry and exit point for a client. Whenever a client's request enters to IMS or it leaves the IMS, it goes through P-CSCF. Main responsibilities of P-CSCF are:

- First responsibility of P-CSCF is to compress the SIP header because due to text based nature of SIP it contains large amount of data and headers.
- Communication between a user and P-CSCF should be secure. For this purpose P-CSCF maintains security association with users. This is done at the time of registration and IPSec is the main protocol being used for security association.
- Various types of policy decision are enforced by policy decision function (PDF). P-CSCF interacts with the PDF to check the authorization. PDF also supports charging correlation information between IMS and GPRS.
- P-CSCF detects the emergency sessions and route them through circuit switched domains on priority. Since circuit switching is faster as compared to packet switching so emergency session should be routed through circuit switched domains.

I-CSCF

Whenever a request enters to an IMS network from another IMS network, I-CSCF acts as the entry point. Responsibilities of I-CSCF are:

- It checks that which S-CSCF will serve this user and also checks whether to route this request towards an application server or to S-CSCF. For this purpose I-CSCF consults the home subscriber server (HSS).
- I-CSCF allocates the appropriate S-CSCF to a user. Again it consults the HSS to check the capabilities of a user and assign S-CSCF.
- After assigning the S-CSCF, I-CSCF routes the incoming requests towards that S-CSCF.

S-CSCF

S-CSCF is considered as the heart of IMS core. Its responsibilities include authentication of users, downloading user's profile, registration of users, routing decisions, session setup, etc. For authentication of users S-CSCF receives the first register request and prepares a challenge for the user. User after answering the challenge waits for the completion of authentication and registration procedure.

S-CSF also decides that where to route this incoming packet. It can contact some application server or to breakout IMS network. Request may also flow steadily from one IMS network to another IMS network. Details of routing decision are shown in Figure 1.2.

1.5.1.2 Databases

IMS contains two databases namely subscription locater function (SLF) and HSS. When I-CSCF receives a request it needs to contact for HSS to get the address of next hop. The question is that from where I-CSCF will get the address of HSS.

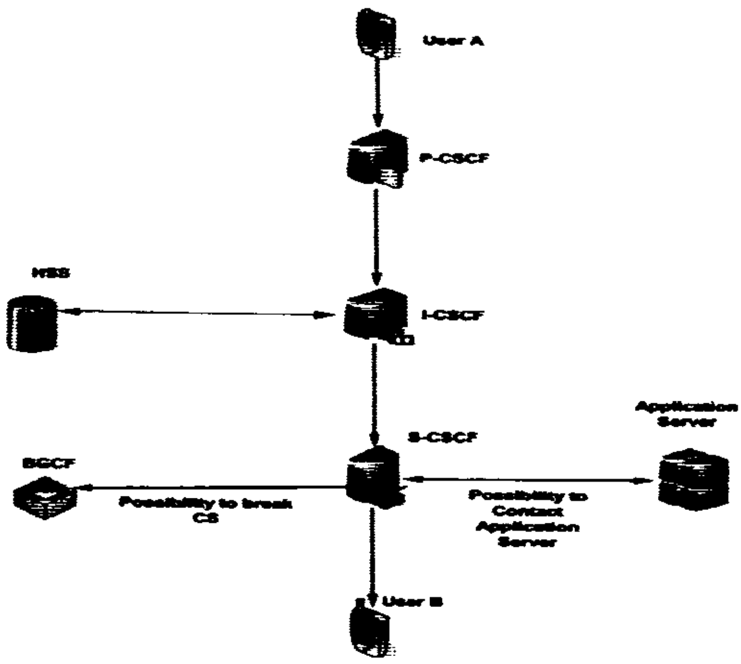


Figure 1.2: Routing from S-CSCF

SLF contains address of HSS. HSS contains all the user related data. It contains public and private identities of users. Public identities are used for call routing and service subscription while the private identities are used for authentication and registration purposes. Access parameters and service triggering information is also stored in HSS.

1.5.1.3 Service functions

IMS contains three main service functions. First one is known as multimedia resource function controller (MRFC) that handles the communication between S-CSCF and other entities and control the multimedia resource function processor MRFP. MRFP provides the requested resources to MRFC. Third one is application server (AS) that links the IMS core to the application plane and provides different types of services (3GPP TS 22.101).

1.5.1.4 Internetworking functions

To enable SIP and real time protocol (RTP) to share information between IMS and CS-CN four internetworking functions are defined by 3GPP. If S-CSCF finds that it needs to breakout the IMS to CS-CN, it forwards the request towards breakout gateway control function (BGCF). BGCF decides whether to breakout in the existing network or to some other network. If it needs to breakout in existing network it forwards the packet towards media gateway control function (MGCF) for further processing. If it needs to breakout in another network then BGCF forwards the packet towards another BGCF (3GPP TS 23.228). Protocol conversion is necessary when a breakout happens. Signallling gateway performs the duties of protocol conversion. For example, it converts the SS7 request to SIP and vice versa. Resources are reserved by the interaction of MGCF with IMS-media gateway (MGW) (3GPP TR 23.981).

1.5.1.5 Support functions

PDF takes different types of information like session related or media related and makes a policy decision based on this information. It issues an authorization token to user equipment (UE) by using P-CSCF as intermediate hop. Control plane traffic among different security domains is protected by security gateway (SEG).

1.5.1.6 Charging Function

Different types of charging functions work together to make an efficient charging framework for IMS. These functions include charging triggering function (CTF), charging data function (CDF) and charging gateway function (CGF) (3GPP TR 23.815). Different types of attacks that can be launched on IMS are shown in Figure 1.3.

1.5.2 IMS Layered Architecture

3GPP has decided to use a layered approach to architectural design. This means that transport and bearer services are separated from the IMS signalling network and session management services. Further services are run on top of the IMS signaling network. In some cases it may be impossible to distinguish between functionality at the upper and lower layers. The layered approach aims at a minimum dependence between layers. A benefit is that it facilitates the addition of newaccess networks to the system later on. Wireless Local Area Network (WLAN) access to the IMS was added in 3GPP Release 6 and fixed broadband access to the IMS is being standardized in Release 7. The layered approach increases the importance of the application layer as services are designed to work independent of the access network and the IMS is equipped to bridge the gap between them. Whether the subscriber is using a mobile phone or a PC client to communicate, the same presence and group list functions in IMS will be used.

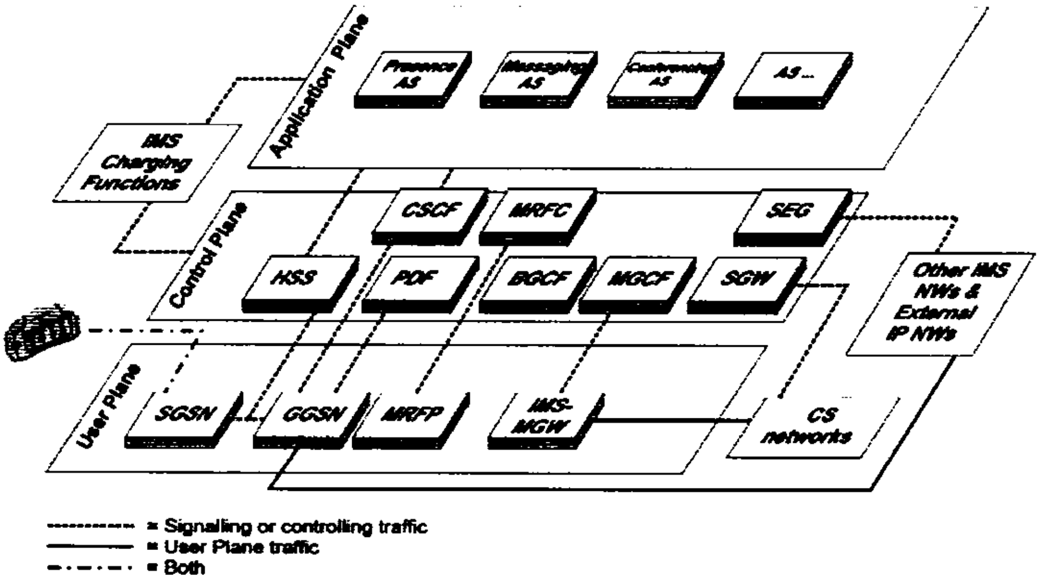


Figure 1.3: IMS Layered Architecture (Miikka Poikselka et al. 2006)

1.5.3 NGN and IMS Security

X.805 security architecture is defined by ITU to secure the NGN. Non Repudiation, Authentication, Confidentiality, and Availability are given special attention along with access control, communication security, privacy and integrity (3GPP TS 33.102) (3GPP TS 33.120).

1.5.3.1 IMS core Security

IMS core, as we have discussed, consists of CSCF and databases. In this section we describe the security requirements for IMS core.

Mutual Authentication of User and Network

S-CSCF performs the authentication of user and user authenticates the network through challenge response based mechanism. This mutual authentication is performed at the time of registration.

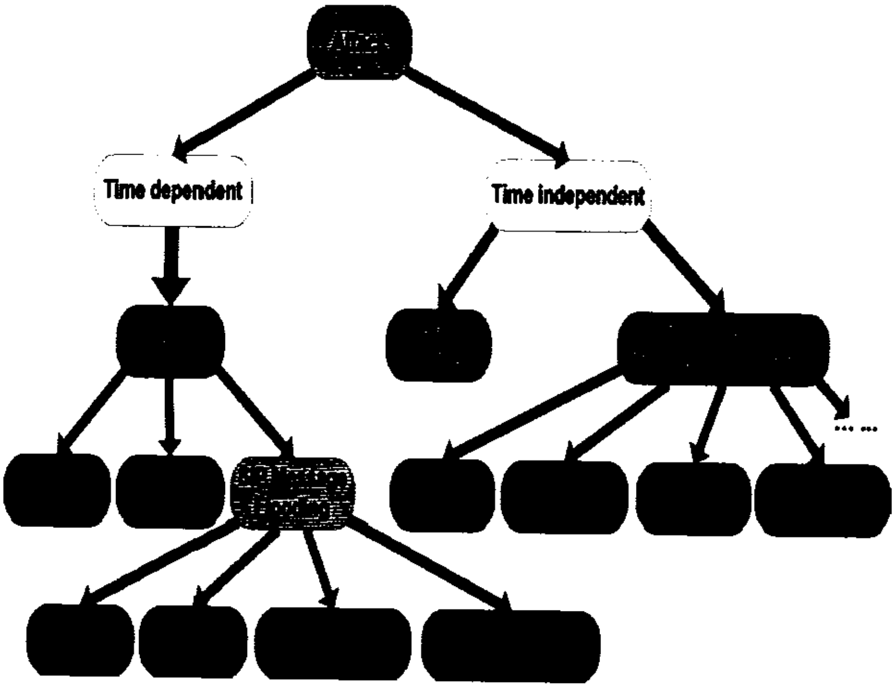


Figure 1.4: Possible Attacks on IMS (M.Sher et al. 2007)

First of all to become a user of IMS a device needs to have registration. In order to get registered the user initiates a registration process by sending a 'Reg' request. A flood can be generated by sending enormous number of 'Reg' request within a small period of time. Enormous numbers of invite requests can occupy a major share of network and results in degradation or DoS. In order to use a service like presence a user first needs to subscribe for it. The subscribe request is received by the specific server. A user with malicious intentions can send a bulk of subscribe request to a particular server so that the server becomes busy and the legitimate users will not be able to get service from that particular server. Presence service deals with publish requests. Whenever a user wants to share its own status information with other users it publishes them over the presence server. Flood of publish request can block the presence service. In most of the cases a session is required among the IMS users to carry communication. An attacker can launch session modification attack by sending a 'Re-Invite' request. Session modification can change the current communication parameters and results in disturbance at the user's side. A CANCEL attack can be launched to end a half established IMS session. Session teardown attack terminates a running session and hence stops the communication. Session teardown attack can be launched through 'Bye' request. SQL injection can also be injected inside the SIP request.

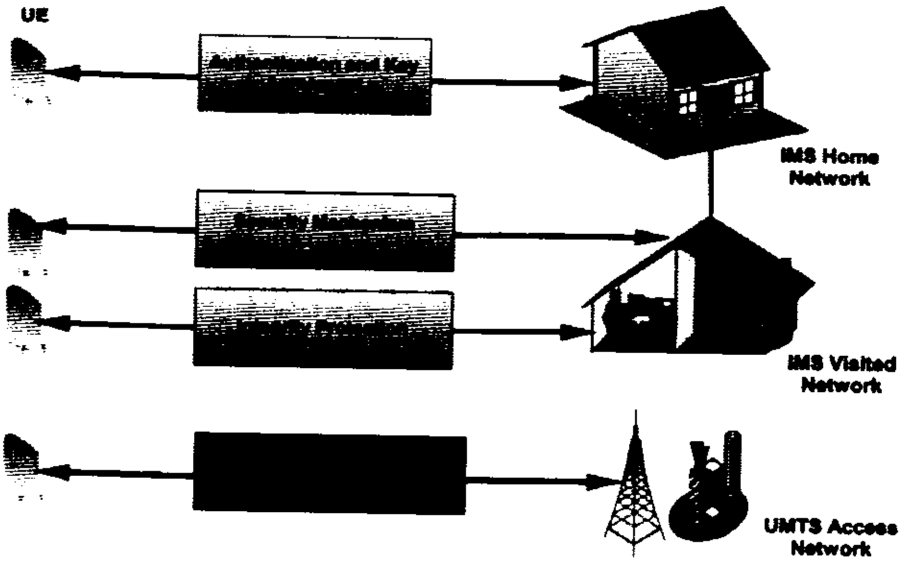


Figure 1.5: IMS Security Mechanisms (M. Sher et al. 2007)

1.5.3.2 IMS Application Platform Security

- To secure the HTTP based traffic Ut interface is equipped with authentication and key agreement (AKA) algorithm. Generic bootstrapping architecture (GBA) with generic authentication architecture (GAA) provides pre service access authentication. Transport layer security is also deployed on Ut interface (3GPP TS 33.220) (3GPP TS 33.222).

1.6 IMS BASED MULTIMEDIA SERVICES

Some times IMS is considered as a service while it is not true. IMS is an architectural framework that is able to integrate set of services on one platform. On top of the IMS plane there is an application plane that contains different types of servers to provide various services. In this thesis since our focus is only on presence, instant messaging, push to talk and multiparty conference so we will provide a detailed introduction of these services. Figure 1.6 shows the IMS service architecture, Figure 1.7 shows the

IMS layered architecture along with application plane and Figure 1.8 shows the IMS multimedia enabler architecture.

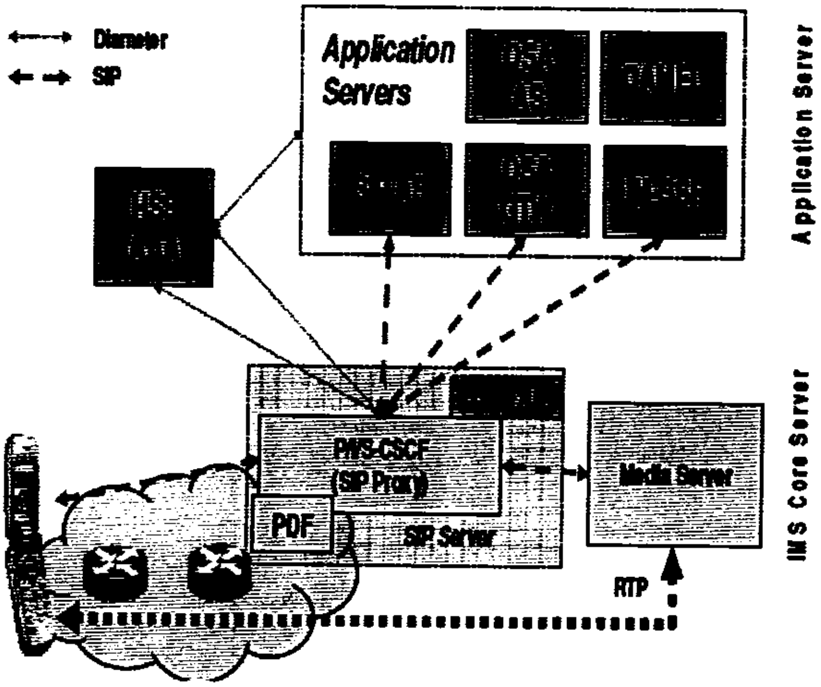


Figure 1.6: IMS Service Architecture (M. Sher et al. 2007)

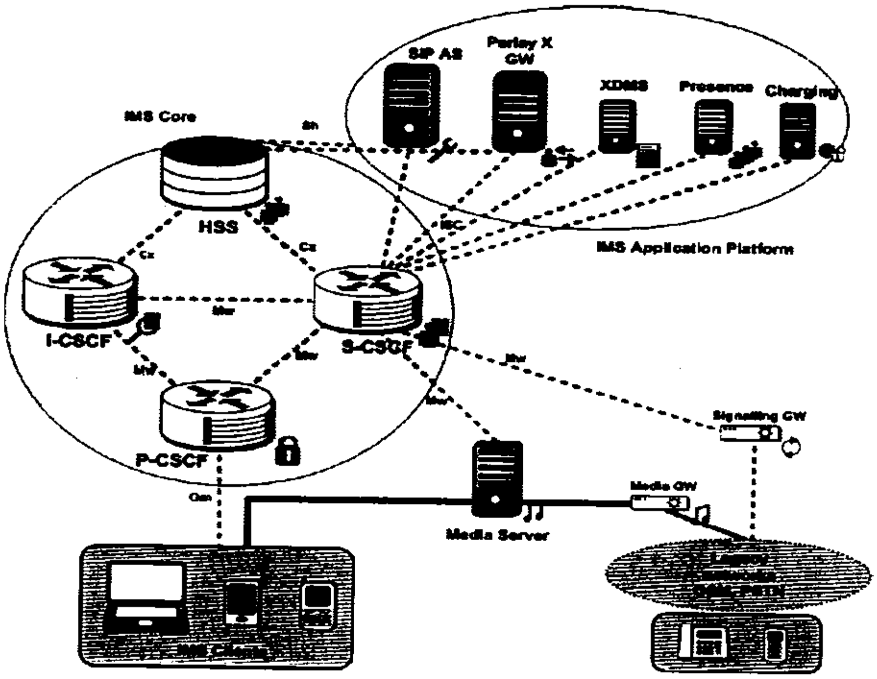


Figure 1.7: IMS Layered Architecture (M. Sher et al. 2007)

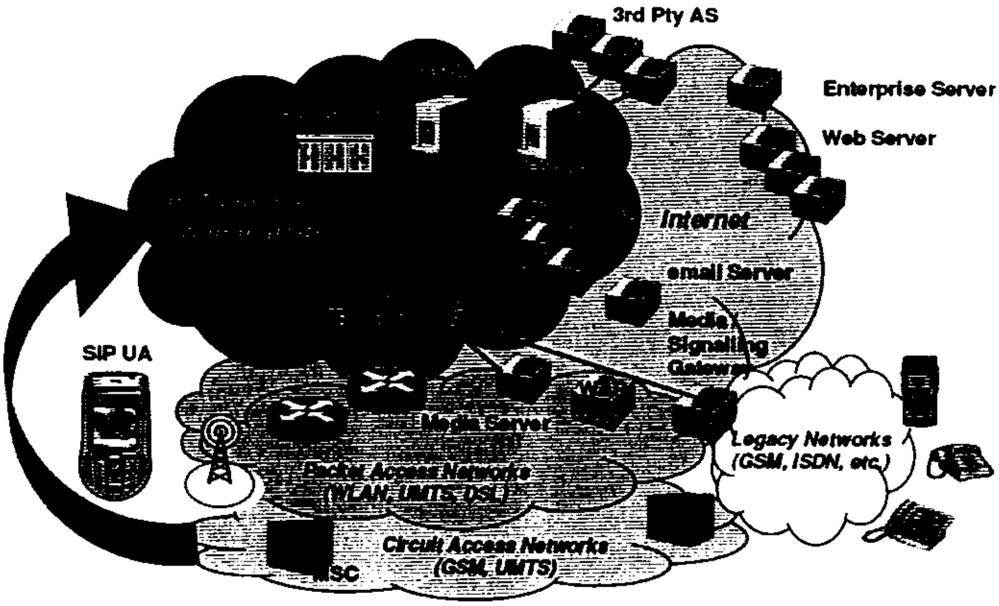

3rd Pty AS
Enterprise Server
Web Server
Internet
email Server
Media Signaling Gateway
SIP UA
Media Server
Packet Access Networks (WLAN, UMTS, DSL)
Circuit Access Networks (GSM, UMTS)
MSC
Legacy Networks (GSM, ISDN, etc.)

Figure 1.8: IMS as Multimedia Service Enabler (M. Sher et al. 2007)

1.6.1 Presence

Presence is a service that provides current status of a user to other authorized users. Status may include:

- Location
- Current activity
- Person and terminal availability
- Terminal capabilities
- Currently available services
- Communication preferences
- Others

First it was considered that Presence can only be used along with instant messaging but later on it is concluded that Presence is the main driving force for all the services. It can be used along with other services. If a person, before creating a push to talk session, wants to know how many fixed members are available at this time, it can be checked through presence and can help to decide that whether to create a push to talk session or not. Presence and instant messaging are changing the personal and corporate communications paradigm. In future presence service will become heart of the communication and will be used in almost all the services.

Security becomes the major concern in sharing of personal Presence information. SIP is used to provide security of Presence information. Proper authorization rules are configured by the owner of the information. These authorization rules specify that who can access what type of information at what time. Presence information can be available at different levels and different scopes to different watchers. This means that different watchers may be authorized to view different parts of the presence information of presentity. The choice of who sees what belongs to the presentity. The presentity can set such authorization levels using an XCAP-defined solution in the form of permission statements. [Draft-ietf-geopriv-common-policy], [Draft-ietf-simple-presence-rules], [Draft-ietf-simple-common-policy-caps] and [Draft-ietf-simple-pres-policy-caps] define the XML schema along with its semantics. Presence can benefit from business sector, cooperate group to children. Presence includes some new terminologies those are defined below (3GPP TS 22.940).

- Presentity – It represents the person who wants to publish its presence information

- Watcher – It is the entity who wants to view the published Presence information of presentity.
- Presence Agent (PA) – It stores the presence subscription details and sends notification messages.
- Presence User Agent (PUA) – publish and manipulates presence information
- Presence server – manages presence information uploaded by PUAs and handles presence subscription requests.
- Watcher presence proxy – identifies the target network for a presentity and resolves its address.
- Presentity presence proxy – identifies the presence server assigned to a certain presentity.

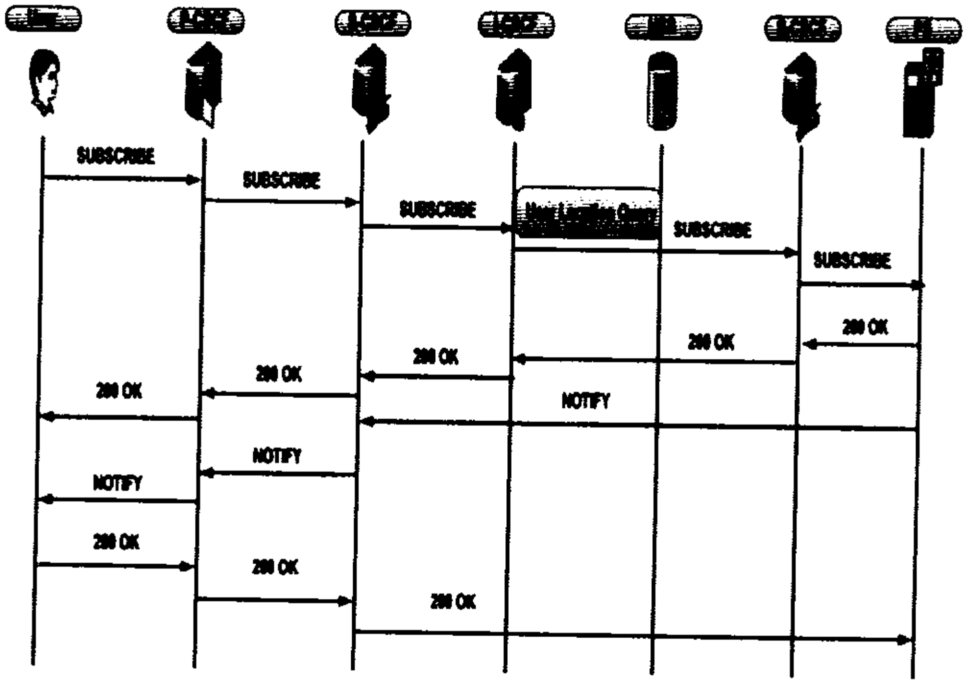


Figure 1.9: Presence Subscription

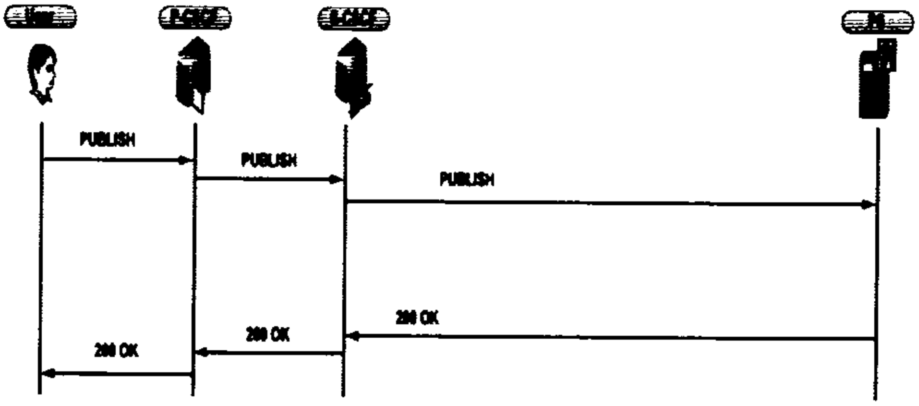


Figure 1.10: Presence Publication

1.6.2 Instant Messaging

Messaging service allows a user to send messages to another user. Message contents can carry text or multimedia data. Immediate messaging and session based messaging are two main types of NGN messaging service. In immediate messaging the sender prepares a message, selects the destination and forwards the message towards the destination. If the receiver device is not active message is stored at application server and delivers to the receiver as soon as it becomes alive. A single message can be sent to multiple receivers.

Session based messaging is like Internet Relay Chat (IRC). Before exchanging messages, both the parties establish a session. After the session establishment users are allowed to exchange messages and at the end session is terminated through BYE request. Figures 1.11 and 1.12 represent the immediate messaging flow and the session based messaging (3GPP TS 22.940).

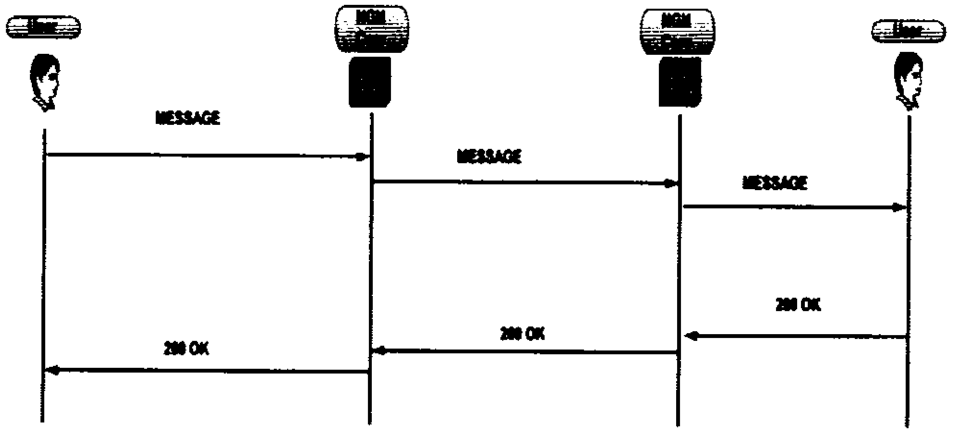


Figure 1.11: Immediate Messaging

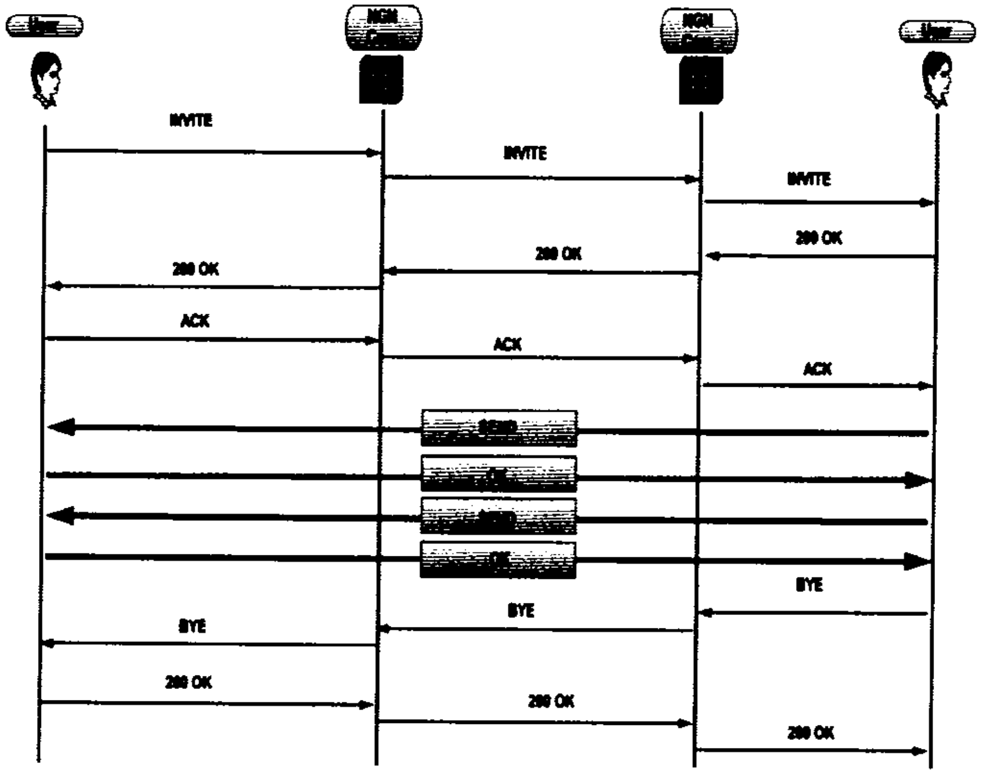


Figure 1.12: Session Based Messaging Flow

1.6.3 Multiparty Conferencing

A conversation among multiple users is known as conference. Conference can be classified into three types:

- Loosely coupled conferences

- Fully distributed multiparty conferences
- Tightly coupled conferences

Our focus is on tightly coupled multiparty conference. Conference scope is not restricted to audio only, a conference can be video as well as text based. In tightly coupled conference all the users have a connection with a central point known as "focus". This focus is responsible for transcoding, media mixing and participant list notifications. A conference is identified by a universal resource locator (URI). A signaling dialogue is set by the focus among the participants. Different conference rules are configured to conference policy that includes:

- Directives on the lifespan of the conference
- Who can and who cannot join the conference (membership policy)
- Definitions of roles available in the conference and the responsibilities associated with those roles
- Who is allowed to request which roles.

Conference can be created from different ways and the most popular is SIP based method. A conference factory UR can be allocated and globally published in order to automatically create an ad hoc conference, using SIP call control means (INVITE request): a conference factory URI is globally routable.

Changes in the conference state are notified through a conference state notification event package that uses SIP event framework. This event package informs the participants that who has left the conference and who has joined as a new user.

A SIP subscribe request is routed by users to subscribe a conference. Subscribe request moves towards the conference server "focus" via different call session control functions. Conference server subscribes it and sends notification to the subscriber.

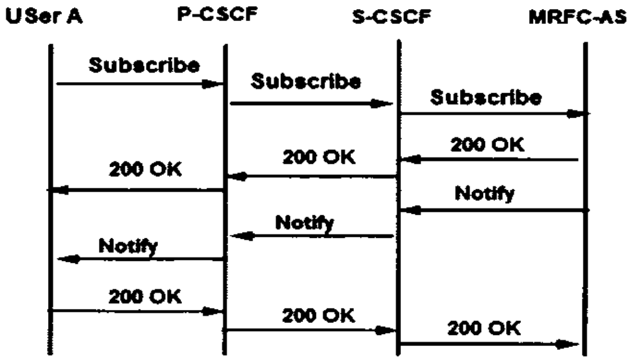


Figure 1.13: Subscription to Conference State

When creating a conference with a conference factory URI the conference participant generates an initial INVITE request. The conference server creates a focus for the newly created conference, assigns it a conference URI and returns the conference URI in the Contact header of the 200 OK response.

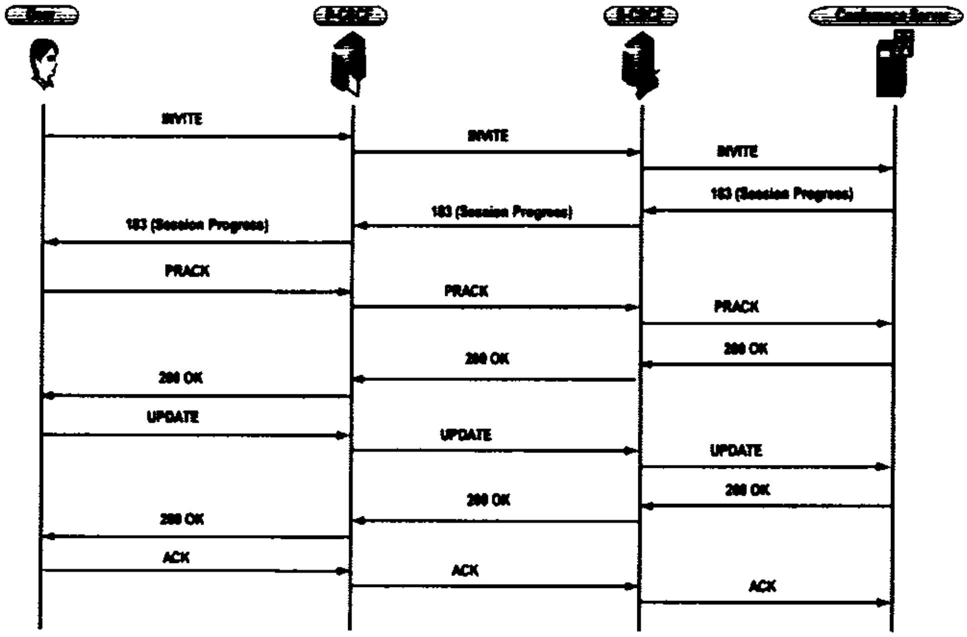


Figure 1.14: Conference Creation

In order to invite a new user into the conference a refer request is sent. If it is accepted a notify message is sent to the initial sender who acknowledge it by sending 200(OK) response. The process is shown in Figure 1.15.

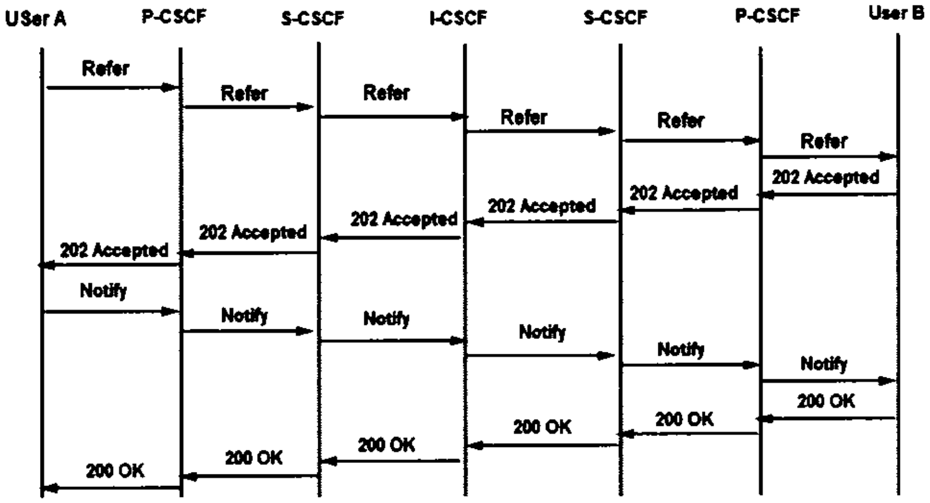


Figure 1.15: Referring a User to Conference

1.6.4 Push to talk over Cellular (PoC)

A service that provides, one way, one to one and one to many voice communication is known as PoC. PoC is a half duplex service means that at a time only one can speak while all others will listen. Each user sends data to an application server that forwards it to all other participants. This service is more resource friendly as compared to circuit switched network because it includes only the time for which the communication actually takes place.

PoC uses multi-unicasting. A sender sends media burst towards the PoC server, and PoC server forwards the duplicate copies to all the participants of that session. Signaling information is controlled by SIP and data is managed and sent by using RTP/RTCP. PoC server can be of two types. All the signaling information flows through participating PoC server and data traffic is controlled and managed by controlling PoC server.

PoC features are:

- PoC communication: PoC sessions can be of different types
    - Dial-out group: In dial-out group initiator selects that who will participate in this session
        - Pre-defined dial-out group: A list is pre-configured. As soon as the session is established, all the members are invited to join session
        - Temporary dial-out group: There is no pre-defined list, participants are selected on run time by the initiator
    - Join-in group: Users are allowed to join group themselves, no invitation is required
        - Open join-in group: Any one can join this group
        - Close join-in group: Only a specific group of users can join the session
- A user can simultaneously participate in multiple PoC sessions
    - The user can lock herself into a single group. Only traffic from that group will be delivered to the user
    - The user can set one of the sessions as a primary PoC session. Traffic in the primary session is delivered to the user

    - Among secondary PoC sessions, the traffic of ongoing conversation is delivered as long as the conversation remains active. After a silent period the PoC server selects active media from another session.

- A session can be created through different ways:
    - Pre-established: Users already have session with the controlling server
    - Controlling server just join them to one session
    - On-demand: Session is created from scratch
- Incoming session can be treated through different ways:
    - Auto: As soon as user equipment get the invitation, an automatic acceptance is sent to the server
    - Manual: User manually answers whether to join this session or not
- Instant personal alerts allows the users to get different types of information through messages
- Barring features allows to configure rules about acceptance and rejection of different PoC sessions

A talk burst is simply a single burst of media flowing from a participant to the controlling PoC server. The controlling PoC server distributes the talk burst to all of the participants of the session. For floor control, the PoC specifications define the Talk Burst Control Protocol (TBCP) as part of the user-plane specifications. TBCP is used to request, grant, deny and release the PoC session floor (Alam et al. 2008). The floor moderator, or the TBCP server, is always located in the controlling PoC function. TBCP includes the following messages:

- TBCP Talk Burst Request (TB_Request)
- TBCP Talk Burst Granted (TB_Granted)
- TBCP Talk Burst Deny (TB_Deny)
- TBCP Talk Burst Release (TB_Release)
- TBCP Talk Burst Taken (TB_Taken)
- TBCP Talk Burst Revoke (TB_Revoke)
- TBCP Talk Burst Idle (TB_Idle)
- TBCP Talk Burst Acknowledgement (TB_Ack)
- TBCP Talk Burst Queue Status Response (TB_Queued)
- TBCP Talk Burst Queue Status Request (TB_Position)
- TBCP Connect (Connect)
- TBCP Disconnect (Disconnect)

1.6.5 Push to Multimedia

PTT in a cellular network is extended by using media capabilities like Instant Messaging (IM), real-time video transfer and file transfer and is known as Push To Multimedia (PTM). PTM introduces Packet switched functionality in a cellular network that brings good opportunity for business. The basic principle of communication is very simple - just push a button and communicate to users from your list. Radio resources are used more efficiently in PTM. Network resources are reserved one-way for the duration of media bursts, rather than two-way for an entire session. Multimedia conversation systems and their importance are also discussed. In

PTM there is a central server known as controlling PTM server. Active Queue management can also be applied on PTM server to reduce the congestion.

1.7 Problem Statement

IMS is among one of the emerging technologies and becoming an industry standard for NGN. We in this thesis addressed various problems related to IMS based Multimedia Services. We considered 4 most important services including Presence, Instant Messaging, Multiparty Conference and Push to Talk over Cellular (PoC). Each of the service has its own problems. At the end of the thesis we also tried to solve few security risks those can be faced by all these services. Now in the following paragraphs we are going to discuss problems of each service one by one.

Presence is a dynamic countineous service and it puts a heavy load on the air interface of the network. Since capacity of the air interface is very small as compared to wired networks so this dynamic service results in heavy load at the air interface of the network. This heavy load may also results in degradation or denial of service. Secondly Presence service can not be used as a triggering condition within the SIP request. This limitation results in overall delay in call setup as well as also results in wastage of valueable resources.

Instant messaging first of all subject to targeted attacks. By sending enromous number of immediate messages a flood can be created at the end of a particular receiver. Session based messaging is subject to session based attacks like Invite flooding, seesion teardown attack, session termination attack etc.

PoC has several other problems associated with the service provisiong mechanism of PoC. First problem is regarding rights allocation since in PoC all the users have same rights so it can not be utilized in many real life scenarios. Since it is a half duplex service so the scalibility is another issue. Few dozen users in one PoC session may results in a very higher waiting time. Within a session there is no privacy control mechansin exists. The current architecture of PoC also faces problems like disturbance at the end of irrelevant users, wastage of valueable resouces through blind delivery of media, internal threats etc.

Multiparty confernce allows single participant to refer any number of participants. It allows the attackers to create a cluster and invite more attackers. Refeering is also fully authorized so it also creats scalibilty problem.

Overall IMS application plane is subject to Invite flooding attack, Register flooding attack, session teradown attack, cancel atack, invite to death attack. All these attacks still can be launched on IMS application plane so secure solutions are needed against these attacks.

1.8 Research Objectives

This thesis deals with security and enrichment of IMS based multimedia services. Main objectives to carry this resaerch include securing the IMS application plane from different types of security attacks launched from the underlying networks and users. Securing the IMS based specific multimedia services from different types of security attacks launched from the underlying networks and users is one of the objectives to carry this research. Attacks like invite flooding, session modification attacks, password guessing etc. can be launched and it is necessary to secure the application plane and the specific 60services from these types of attacks. Addition of new value added features in IMS based multimedia services to make these services more attractive and enrich is another objective of this research. These value added features on one hand will result in reducing the network load and on the other hand will enhance the scalbility and use of these services in real life scenarios.

1.9 Contribution

In this thesis our contribution is of enriching and securing the IMS based multimedia services. We started from presence service and we find that our proposed solution reduces the overall time required for call setup. The proposed solution also results in reducing the load from the air interface of the networks. We showed the statistics in the form of graphs in chapter 5. We also provide a framework for automatic presence based call setup to reduce the wastage of valuable resources.

In instant messaging our focus was to mitigate the targeted attacks. We developed three different frameworks and we find that these frameworks results in mitigating the chances of targeted attacks as well as session based attacks.

Multiparty conference is secured against internal threats by introducing election based referring. Restricted referring also makes this service available in more real life scenarios.

In PoC and PTM we solved various problems. First different rights are allocated to different users that help to apply this service in more real life scenarios. Scalability problem is addressed by adding more users with restricted rights. Privacy and disturbance problems are addressed via media mixing algorithms. Next achievement is to reduce the average waiting time. It is achieved through dynamic floor control time and media mixing.

At the end an Intrusion Detection and Prevention (IDP) framework is developed and performance of non evolutionary algorithms is tested for the first time in IMS. Results show that in different scenarios different algorithms perform differently.

Main motive of the thesis is to secure and enrich the multimedia services as well as the application server that is the only connection point between different servers and underlying networks. Details are shown in figure 1.16.

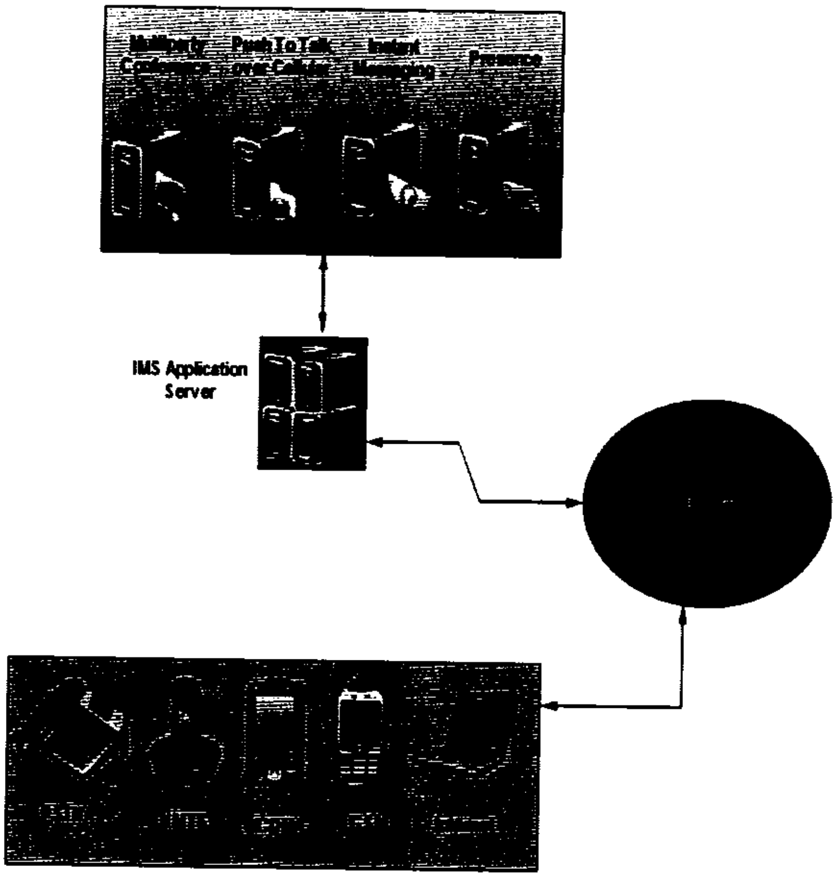


Figure 1.16: IMS Architecture with Thesis Modules

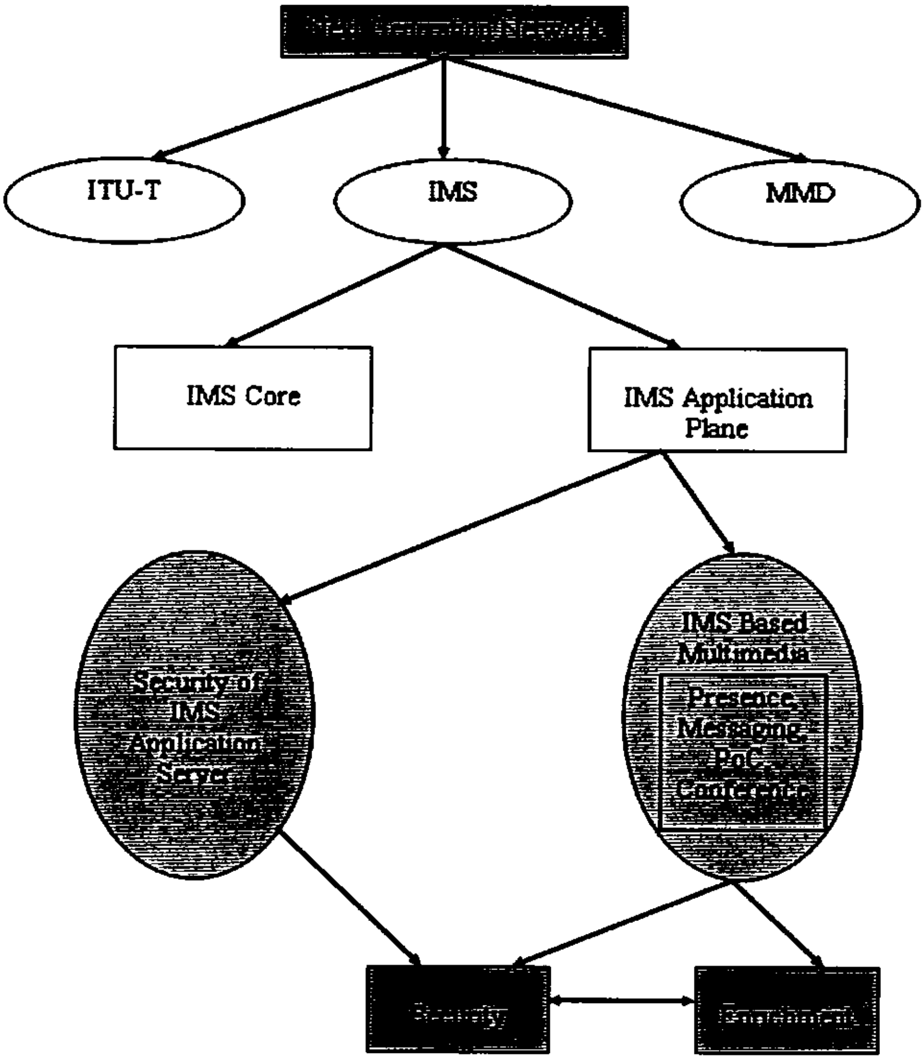


Figure1.17: Flowchart of the Modules of the Thesis

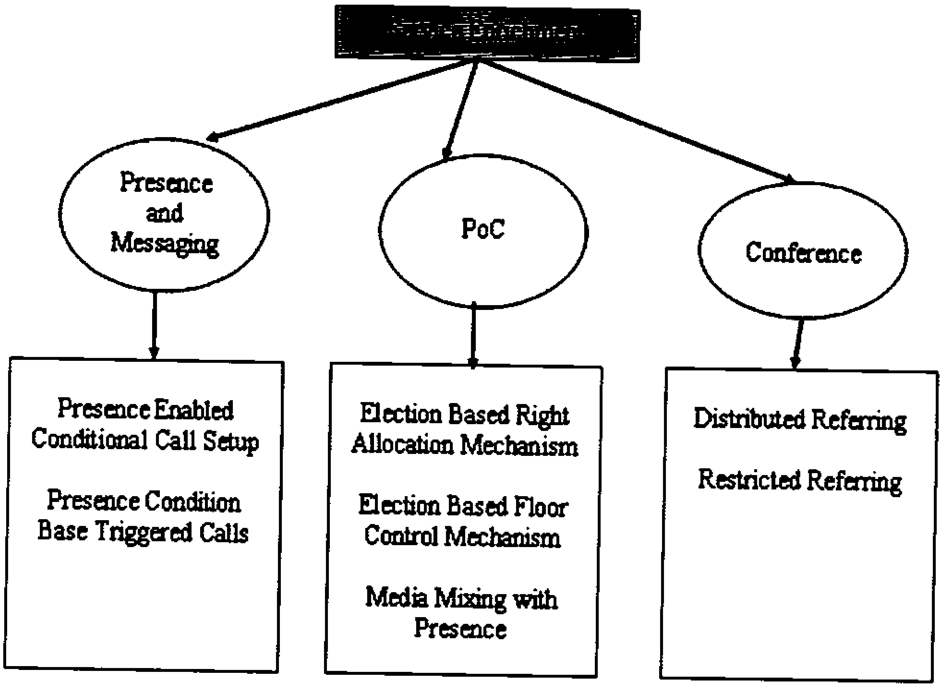

Presence and Messaging
PoC
Conference
Presence Enabled Conditional Call Setup
Presence Condition Base Triggered Calls
Election Based Right Allocation Mechanism
Election Based Floor Control Mechanism
Media Mixing with Presence
Distributed Referring
Restricted Referring

Figure 1.18: Service Enrichment Module

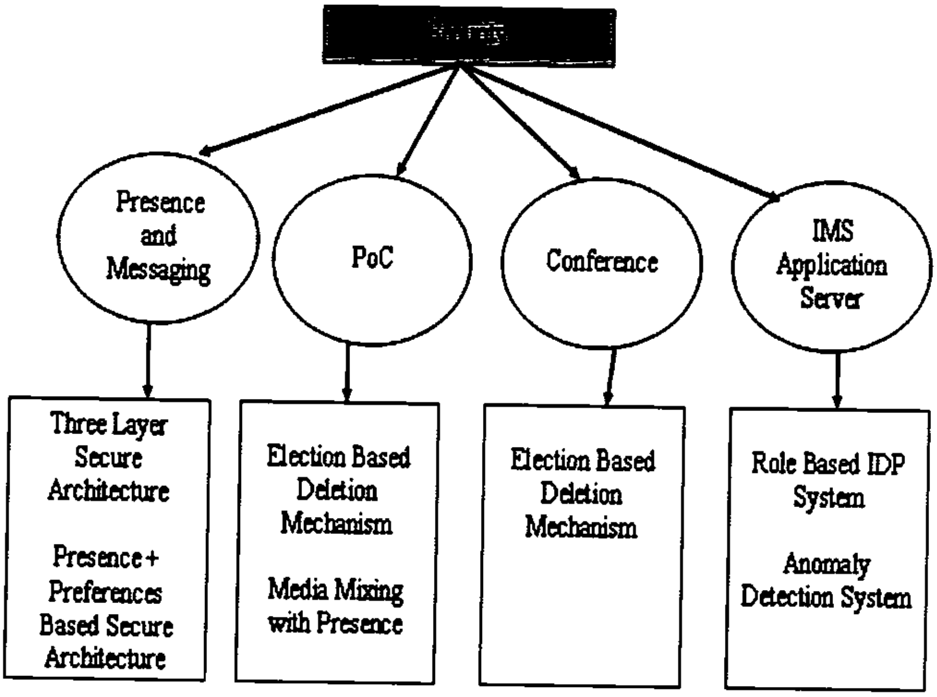

Presence and Messaging
PoC
Conference
IMS Application Server
Three Layer Secure Architecture
Presence+ Preferences Based Secure Architecture
Election Based Deletion Mechanism
Media Mixing with Presence
Election Based Deletion Mechanism
Role Based IDP System
Anomaly Detection System

Figure 1.19: Security Module

1.10 Thesis Layout

Chapter 1 starts with introduction of IMS. Various components of IMS are described in detail. After that SIP is described in detail. Various fields, structure of the header is also provided. Next section of chapter 1 includes details about RTP. SDP is also discussed in later half of chapter 1. After discussing these protocols introduction of IMS based multimedia services is provided. First presence service is discussed. After that detail about instant messaging is provided. Multiparty conference is at the third place and at the end PoC and PTM are discussed. After discussing the services, problem statement related to each service is provided. Objectives are discussed after discussing the problem definition. A little description of the solution is also provided at the end of the chapter 1.

Chapter 2 consists of related work and literature review. Since this chapter is little lengthy so we divided it into three parts. First part highlights the literature related to presence and messaging service. At the end of this part we provided critical analysis of the literature discussed. Second part consists of literature related to PoC and multiparty conference. Critical review is also provided at the end of the section. Last part includes the work related to overall security of IMS and NGN.

Chapter 3 elaborates the problems related to each service in more detail. First problems related to presence service are described. After that problems related to messaging, PoC and multiparty conference are discussed. At the end of the chapter overall security risks are discussed.

Chapter 4 consists of methodology and framework. For each type of problem different framework is developed and methodology is discussed. Since this thesis focus four different service and inside each service different problems are addressed so different frameworks are developed for each type of problem.

Chapter 5 consists of different types of scenarios (Case studies), their testing and results. This chapter explains how our proposed frameworks are better as compared to existing work. Chapter 6 consists of conclusion and future work.

CHAPTER 2

2. LITERATURE SURVEY

This chapter highlights the existing work performed in domain of multimedia services and NGN. We divided this chapter into three parts. The first part consists of the literature related to Presence and Messaging. Second part highlights the related work regarding PoC and multiparty conference. Third part discusses the overall security issues of IMS. Within each part we again make groups of relevant research articles. In part one first group of articles is about definition and standard about presence and messaging. Second group combines the articles related to effect of presence and instant messaging on network performance. Third group highlights the articles those emphasize on using presence service inside the other services. Last group consists of research articles written on security of presence and messaging service.

2.1 Part 1: Presence and Instant Messaging

Day et al. defined the terminologies used in presence and messaging. Watcher, Presentity, etc. are first time defined in this RFC 2778 (Day et al. 2000). They also described that independent protocols should be developed for instant messaging and presence. In RFC 2779 they defined the minimum requirements for a protocol designed for presence and messaging (Day et al. 2000). Milewski et al. had presented the idea of live address book. According to them this service will facilitate the users by reducing the disturbance rate (Milewski et al. 2000). Zarri discussed that services provided by IMS are not new but in IMS these services are presented in more attractive way and one service can be used as an enabler in another service. The author also discussed the availability of these services. Since IMS can be accessed from any underlying network therefore these services will be available to more and more users (Zarri, 2002). 3GPP TS 22.940 defines the issues and terminologies of messaging service. Conlan et al. discussed the current modeling and personalization techniques available in user specific services. Application of context aware services in different scenarios is also discussed by the authors (Conlan et al. 2003).

According to Pailer since Parlay APIs and SIP are declared standard by 3GPP so mapping of SIP over Parlay is a necessary step. Pailer also proposed a frame work for service creation and management in different types of networks. Mobility aspects are also considered by the author by using Parlay user status service API (Pailer, 2004). Rosenberg tested the SIP for presence and messaging. Event packages are defined for both presence and instant messaging (Rosenberg, 2004). Saint et al. described the main features of extensible messaging and presence protocol. Extensible markup language is used for the exchange of messages (Saint et al. 2004).

Rahman et al. described the architecture and protocols of the mobile multimedia instant messaging and presence service (Rahman et al. 2004). The author emphasized on the relationship between SIP and wireless village framework. The major focus was on analyzing the protocol standards for Instant Messaging and Presence Service (IMPS). Jin et al. proposed the use of SIMPLE for instant messaging and presence and highlighted the advantages of using SIP for presence (Jin et al. 2004). They also analyzed the IM&P architecture. Huh et al. discussed the different design considerations related to the presence service. They explained the design consideration of presence agent, supporting multiple presence packages and user authentication function (Huh et al. 2005).

Buford described that Instant Messaging and presence service supports different protocols but do not provide dynamic roaming. First they emphasized on the need of client and server dependent roaming aware mechanism and then to enable roaming they described and analyzed a technique for handoff (Buford, 2005). Huh et al. described the basic call flow for interoperability in the presence service based on SIP (Huh et al. 2006). SIP is classified into registration function and subscription & notification function. Author also presented the detailed explanation of each of the message exchanged during the registration, subscription and notification procedure. Reichl et al. designed an experimental testbed for IMS. They included call session control functions, DNS, home subscriber server, support for GPRS, EDGE, UMTS, WLAN, IPv4 and IPv6 support etc. They deployed location based presence service over this testbed and evaluate the cost and benefit (Reichl et al. 2006). This paper presented the results of two research projects namely CAMPARI and SIMS. Rashid et al. discussed the emergence of IMS in mobile industry. They elaborated the role of rich presence and localization services in mobile entertainment applications (Rashid et al. 2006).

Saghir et al. studied different types of terminal capabilities for IMS and selected UAPROF technology as the most valuable. After that presence specification are used to check the compatibility (Saghir et al. 2006). Ribeiro et al. tried to solve terminal network heterogeneity problem by using IMS and P2P based middleware. Interest based P2P communities are developed by using this layered architecture. Open IMS core is used to implement the architecture. They concluded that it is feasible to use their proposed solution for service creation and deployment (Ribeiro et al. 2007). Jiang et al. proposed a three layer for presence service. Layer one provides network services, layer two is responsible for basic services to all users and layer three contains the policies related to personalization service. The authors proposed to add location, line status, role and availability in the presence information. To extend Call Processing Language (CPL) for presence authors defined four top level actions, five operations and a presence switch. The major focus of the authors was on presence service and call control (Jiang et al. 2007). Jae et al. described the technologies that have been developed or being developed by IETF IMPP WG and SIMPLE WG. The purpose of the author was to update the readers about presence and instant messaging (Jae et al. 2007). 3GPP TS 22.141 define the requirements and issues of presence service in details.

Sabta et al. described convergence of IMS and web 2.0 services. Authors analyzed and compared similar solutions being developed earlier. At the end they presented their convergence protocol and named it TEWCOP. TEWCOP focuses on maximum convergence without affecting the compatibility of services with traditional networks (Sabta et al. 2009). Bailly et al. worked on convergence of web and IMS applications. How IMS-web gateway will work to achieve this convergence is also discussed by the authors (Bailly et al. 2009). Islama et al. described how third party offered services can be subscribed and session can be made. To make the things clear they explained their solution through the two use cases. The focus was on user centric service provisioning (Islama et al. in 2009).

Femminella et al. described the implementation of media server controller. Since media server controller has important role on provisioning of third party services to IMS so its implementation technicalities were important to discuss. Platform developed by FOKUS is used to implement this media server (Femminella et al. 2009). Bormann et al. worked on testing complex service architectures. For the test case presence service was used. Focus was on requirement, design and implementation of currently available complex service architecture (Bormann et al. 2009). Lishoy et al. used the location based services for authenticating the mobile phones (Lishoy et al. 2010). Syed et al. presented the enhanced architecture of location based services (Syed et al. 2010). Christian et al. in 2011 discusses the different new applications of services (Christian et al. 2011). Chung-Wei et al. presented that how to select the trustworthy service (Chung-Wei. et al. 2011).

2.1.1 Effect of Presence and Instant Messaging on Network

Pous et al. evaluated the presence and instant messaging application in UMTS network. According to authors since presence is dynamic live information so it puts heavy load over the network. For instant messaging they found that average delay is 16.6 seconds and 70% of total delay is due to the core network (Pous et al. 2002). Miladinovic et al. studied the presence event notification in UMTS. According to the authors subscription of presence information puts heavy load on air interface of user's network. Authors proposed that instead of subscribing presence information for short period of time, a watcher should subscribe the presence with an intermediate server for a very long period of time. The intermediate server is responsible for the subscription of presence at presence server for short period of time. Since this intermediate server is proposed inside the core network so it reduces the load on the air interface (Miladinovic et al. 2005).

Rishi et al. analyzed the effect of presence service over network. PULL and PUSH based communication mechanisms for presence service are discussed and compared. The authors pointed out that since the presence service is not point to point service so it adds a significant load of traffic over the network because every change in the presence information of a presentity is communicated to all of its subscribers. Privacy issues are also discussed by the authors (Rishi et al. 2005). Alam et al. analyzed the cost of presence service. According to them, it is essential to reduce the load of the traffic in order to make the presence service more attractive. In the paper they provided an analytical framework to measure the performance of the IMS presence service (Alam et al. 2005).

Yang in 2006 presented distributed presence service middleware architecture to cope with the problems like service provisioning, Quality of Service (QoS), bandwidth provisioning (Yang, 2006). Florian et al. described that instead of subscribing to presence service individually, subscription should be allowed to a Resource List Server (RLS). RLS collects the information and sends it in bundles. It reduced the number of messages resulting in efficient utilization of resources. Author also proposed that instead of providing information to subscriber after every change, the RLS should collect the information and provide it to the watcher only on demand (Florian et al. 2006). Pailer et al. proposed architecture for location service enablers in IMS. They proposed that trigger information and notification should be processed in the terminal. They claimed better efficiency compared with other solutions (Pailer et al. 2006).

Nisha et al. analyzed the IMS network by considering SIP delay as main parameter. Authors formulate a queuing model for IMS and studied work load on SIP server (Nisha et al. 2006). Alam et al. proposed Weighted Class Based Queuing (WCBQ) in order to reduce the load at presence server. According to the authors a watcher who is subscribed for a list of 100 presentities will receive a notification message after every change in any of the 100 presentities. It will result in consumption of resources at client side that is equipped with low processing devices. The WCBQ drop the low priority pre existing messages in order to reduce the load. The results showed that during the heavy traffic load this mechanism works well (Alam et al. 2007).

Salinas described the advantages and disadvantages of using presence service. Author described that on one side presence service facilitates many other services, makes the communication easy, reduces the unnecessary traffic etc. and on the other side it has privacy concerns. An intelligent user can guess the routine of other users by viewing their presence history. According to the author presence service also involves the end user so it requires that the end user must be aware that how to use presence service (Salinas, 2007). Sedlar et al. proposed the use of presence information in an enterprise environment. According to the authors if the presence information is collected from different sources and provide to the subscribers after aggregation then it can help the employees to organize themselves more efficiently (Sedlar et al. 2007). Loreto et al. used the idea of presence network agent to improve the performance of the presence service by minimizing the load from radio access network. The author discussed few open issues which needed to be resolved in order to improve the performance of the presence service (Loreto et al. 2008).

Mckeon et al. studied the effect of presence service over the latency and throughput of the network. The authors analyzed that the presence service can put a large load over the network due to much traffic (Mckeon et al. 2008). Beltern et al. presented the fully distributed platform to deploy presence service. They proposed middleware architecture consisting of two layers. First layers takes the intelligent decision to process and manage the presence information and the second layer is responsible for sending and receiving messages like subscribe and notify. The major emphasize is on the management of the presence information in order to make it more efficient. RA rules, defined by the authors, restrict a user to communicate with other users (Beltern et al. 2008).

Chen et al. argued that presence notifications put an extra load on network as well as on watcher. Therefore to reduce the load of presence notifications they worked on introducing a new notification method called as weakly consistent scheme. In this scheme notifications are delayed up to a specific period of time and resulted in reducing network load (Chen et al. 2009). Paolo et al. worked on enhancing the location based services. Among the location based services authors focused on presence service. According to authors, implementation of presence service requires two main issues to be resolved. Firstly they focused on load balancing and secondly automatic activation and de-activation of presence service was considered (Paolo et al. 2009). Paolo et al. argued that the major issue in the success of presence service is scalability. Since presence is a dynamic continuous service so due to heavy load a question on scalability arises. To solve this issue authors proposed three extensions to the presence service. First they optimized the inter-domain distribution of notified messages, secondly they proposed a framework for differentiated quality and thirdly client side buffering was proposed (Paolo et al. 2009).

2.1.2 Use of Presence in Other Services

Akkawi et al. presented a gaming platform for IMS. Reasons described by Akkawi et al. to develop this platform for IMS include availability of services like presence and messaging. Presence information firstly publishes the game requirements through well known protocols and secondly it grouped the users who have same interests. Messaging services provides a co-ordination among the players. Players can share their views with each other by using the messaging service (Akkawi et al. 2004). Dinoff et al. worked on user's context. Intuitive Network application framework was use by the authors to profile user's preferences. Then it was studied that how these preferences could be used to measure the user's context. It used both intelligent and user feedback techniques to achieve the target (Dinoff et al. 2006).

Kranz et al. worked on instant messaging. They modified current instant messaging to ubiquitous presence system. How arbitrary devices can be connected to presence system was also discussed. Design space of ubiquitous presence system is another achievement of authors. At the end they developed a fully functional prototype for the ubiquitous presence system (Kranz et al. 2006). Paivi et al. analyzed the role of instant messaging through iTV among the children age from 9 to 11. They wanted to study social interaction among the children. Moderator can be used to initiate and coordinate a topic however it was optional. People, rules technology and purpose were considered as four pillars of iTV learning. In this solution children were the people, rules are developed by the children themselves and purpose was the active participation of children in the program (Paivi et al. 2007). Amirnate et al. presented a distributed conference solution over centralized conference clouds and the discovery was made through presence. Authors also proposed mechanisms for distribution of conference related information and management of distributed conference (Amirnate et al. in 2007).

Wang et al. presented the idea of PoC session setup using rich presence information. All the group members are invited without telling the presence information. The server retrieved and compared the presence information and only those users were invited whose presence information matched with the request. It decreased the session setup delay and reduced the presence related SIP signaling traffic (Wang et al. in 2007). Petemel et al. described the mechanism for enterprises to collect presence information from multiple presentities and distribute among the consumers. The author focused on the basic and extended system of the presence service (Petemel et al. 2008).

Zhu et al. developed a new lookup service enabler for the presence service offered by IMS. This enabler has the capacity to identify different types of groups based on their presence information. Since the current presence information data format did not support this enabler so it was also modified to make this enabler successful (Zhu et al. 2009). Zheng et al. presented a new mechanism to formulate instant messaging group based on their presence information. Since presence information was changing very quickly so the formed groups were purely dynamic. The solution took the presence information as input and formed the group on the basis of presence information (Zheng et al. 2009).

2.1.3 Security Issues in Presence and Instant Messaging

Magedanz et al. proposed an "Open IMS Playground" a test bed for IMS. This testbed included almost all the major components of IMS core. This open source was used to test academic and industrial research on IMS. Open IMS Playground included functionality of all call session control functions, home subscriber server, media or streaming server, application server, different types of SIP application servers etc. Application layer was designed with different types of applications like presence etc (Magedanz et al. in 2005).

William Enck et al. identified the vulnerabilities and risk originated from the interface of cellular network with Internet. The authors demonstrated the ability of depriving bandwidth capacity of cellular network by sending enormous malicious SMS traffic originated from Internet resulting in denial of voice as well as legitimate SMS service. They have investigated the feasibility of exploiting the vulnerability by an adversary even equipped with limited resources. They have discussed NPA/NXX, Web scraping, web interface interaction and other techniques of creating hit lists for effective attack. They quantified that it required about 165 and 240 SMS per second to jam to voice & SMS service of the cities Manhattan and Washington D.C respectively, which was translated into dialup modem bandwidth requirement for successful attack on the cities. The authors estimate 325,525 messages per second to set the entire USA's cellular networks non-responsive. The suggested solution to the problem included separation of voice and data, rate limitation and resource provisioning. However major achievement of the research was identification of the problem that emphasized on finding a better and complete solution for the problem (William Enck et al. 2005).

William Enck et al. proposed a compound solution to the problem discussed above. They suggested separation of voice from SMS traffic by implementing weighted fair queue that assure reserve bandwidth quota for voice and SMS thus confining the effect of attack on SMS service ensuring minimum effect on the voice traffic. Their mechanism mitigated the attack and lessens its effect on the voice traffic. However the protection of the legitimate SMS and other traffic needed to be addressed. The application of the proposed mechanism resulted in under utilization of available bandwidth during non-attack time (William Enck et al. 2006).

Vishal et al. presented a survey on security issues in presence and proposed few solutions to solve these security issues. Authors emphasized on authentication of the watcher and presentity, authorization and access control over presence information and the integrity and confidentiality of the presence information. For authentication author proposed asserted identity, cryptographically verified identity and certificate based authentication. For data integrity and confidentiality of the presence information the authors proposed the use of private and public keys (Vishal et al. 2006). M. Sher et al. proposed a Transport Layer security (TLS) along with the intrusion detection system to secure the IMS application server against various types of time dependent and time independent attacks (M.sher et al. 2006). M. Sher et al. presented the trust domain relationship based inter domain security model for IMS. Keys are managed using public key infrastructure. For confidentiality and integrity IPSec is used (M.sher et al. 2006). Rosenberg described that proper authorization should be implemented in presence service. For this purpose they developed the authorization rules. These authorization rules define that at what time what information should be delivered to how many watchers (Rosenberg, 2007).

Sher et al. developed an Intrusion Detection and Prevention (IDP) system to secure the IMS application server. This IDP system compared all the incoming and outgoing requests and responses with the defined rules and decided whether to forward it or not. It was very difficult to maintain a comprehensive list of rules. In this paper the main focus of the authors was on misuse detection only (M.sher et al. 2007). Sher et al. in 2007 described a security model to secure the IMS application layer from time independent attacks like SQL injection. To attain this purpose authors developed an intrusion detection and prevention system. Transport layer security is also provided in the paper (M.sher et al. 2007). Rebahi et al. described that IMS is subject to various types of denial of service attack. In order to make the IMS successful authors emphasized to secure it from these attacks. Solutions to mitigate the denial of service attack were presented in the paper (Rebahi et al. 2008).

2.1.4 Limitations in Survey-Presence and Instant Messaging

XCAP is a protocol that defines the authorization rules to protect the personal presence information. Security against un-authorized access is presented through this XCAP but other security concerns are also required a lot of attention to be solved. Vishal et al. in 2008 presented different security measures against unauthorized accessed, worked on adding confidentiality in presence (Vishal et al. 2008). For confidentiality they proposed private and public key infrastructure. Availability is a major security service which is ignored by many authors. Various types of denial of service and degradation of service attacks can be launched on presence service. These attacks include subscribe flooding attacks and publish flooding attacks.

Messaging service security issues become more critical because it is subjected to more security attacks as compared to presence service. William et al. discussed that how message flood can affect the availability of other cellular services. They argued that cellular traffic of a city size of Manhattan can be blocked by generating 165 messages per second. In case of converged networks when an Internet connected client sends a burst of messages to air interface, an automatic denial of service attack takes place (William et al. 2005). It is very important to secure the networks against message flooding attacks. Currently a very little work has been done in this direction.

Messaging service also faces other security threats which are not being addressed by the researchers till now. In case of session based messaging different types of session based flooding attacks can be launched including invite flooding attack. Targeted attacks make the things more difficult. Network based intrusion detection and prevention systems can be used to secure the network based attacks but for targeted attacks in which a single user is chosen as victim it is very difficult to design a solution. Targeted attacks are still among the open problems in NGN and IMS.

In 2002 presence and messaging services are tested on UMTS network and a heavy delay was found. In 2005 it was argued that the major load that is created by presence service is due to its subscription and notification mechanism. In 2005 it was reported by many researchers that presence increase the network load with a high ratio. Scalability issues in presence are also discussed by a large number of research based organizations and individuals.

Different solutions are proposed to minimize the network load created by the presence. Some argued that presence subscription should be for a longer period of time and a few said that presence notifications can be reduced through proper access control and utilization rules. It was also suggested that instead of an individual subscription, the subscriber should be allowed to subscribe a resource list. Different queuing models have been also proposed to reduce the network load.

All the above mentioned solutions work well to minimize the network load but the percentage of reduction is so small that scalability of presence service is still an open problem. Currently researchers are again working on reducing the network load created by presence. Major studies related to presence based network load focuses on securing the radio interface from denial of service. Inside the IMS core, scalability is not a major issue but when the traffic generated by core network enters into the radio channel a heavy load create the chances of denial of service or at least degradation of services. It still requires a comprehensive solution to reduce the network load from the air interface.

Presence is the service that can be used along with almost all the services for context awareness. Work has been done to use the presence service to establish push to talk (PTT) groups, to play computer games, to create multi party conferences etc. Presence can also be used in many other services to make them more comprehensive. It is ignored by researchers that how presence can be used inside the IMS session setup process. Use of presence service to secure the network communication is not considered by many researchers. It can be used as a good security tool to protect various types of services from different types of attacks. These attacks may also include flooding and targeted attacks.

A service that provides one way, one to one and one to many voice communication is known as push to talk over cellular (PoC). PoC is a half duplex service means at a time only one user can speak while all others will listen. Each user sends data to an application server who forwards it to all other participants. This service is more resource friendly as compared to circuit switched network because it includes only the time for which the communication actually takes place. Real time protocol (RTP) and session initiation protocol (SIP) are two main protocols used in PoC. A conference is a service that allows multiple users to communicate at a time. A conference can be a loosely coupled conference, fully distributed multiparty conference or tightly coupled conference. The conference does not only mean an audio conference. It can be video conference or text conference (chatting).

2.2 Part 2: Related Work- Push to talk and Conference

Tosi introduced enhanced push services and provided architectural solutions for them. The author combined the location based presence and instant messaging service with push services. The author argued that challenging services by Infotainment and Infocommercial can be made more enriched by using this mixture. The solution is prepared to fit in IMS architecture (Tosi, 2004). Niklas et al. presented the idea of Push to Multimedia (PTM) and created a PTM application based on IMS architecture. According to authors, simple voice based services are not enough to meet the demands of the users of current communication era. Push technology should provide exchange of multimedia contents. For this purpose they extended the simple push to talk service towards push to multimedia. Open service access (OSA)/Parlay interfaces are used to develop this new application. Community based services are made available through different communication channels. According to author PTM provides new communication features to the users (Niklas et al. 2005).

Peng et al. presented a priority based new call control scheme for push to talk services. According to the authors proposed scheme decreased the call delay to 600 ms. They proposed to encapsulate the signaling messages and voice in a single packet (Peng et al. 2006). Imen et al. described what the service is? Service has different meanings in different domains. The authors summarize the literature on the meanings of the service. After that NGN service definition is also summarized. At the end final obtained service definition is applied on presence service. Concept of service profile and service components is used in summarizing this definition (Imen et al. 2006).

Alam et al. purpose the idea of narrowcasting. According to them instead of sending media burst to all the participants of the conference, it should be delivered according to the preferences of the sender and receivers. Each participant can configure the preferences that to whom voice should be sent. (Alam et al. 2006). Anh et al. analyzed the group behavior modeling and traffic modeling for PoC. One to one invitation and batch invitation methods are compared and the results showed that there is more floor blocking in batch invitation as compared to one to one invitation (Anh et al. 2006). Gan et al. described distributed Push To Talk (PTT) mechanism. According to them permission to speak is automatically determined by the users in distributed manners instead of using central arbitrator (Gan et al. 2007).

Niklas et al. discussed that how small and medium enterprises can create new services without having deep knowledge. This research work was the part of Multi Access Modular Service Framework, a funded research project. Main goal of the project is to develop an open service delivery platform for NGN (Niklas et al. 2007). Roman et al. described that how to access IMS attached services from different IMS based platforms. The proposed mechanism increases the availability of services (Roman et al. 2007). Doolin et al. presented Daidalos approach to add context awareness in IMS services. How context awareness can be used in sensor networks is also demonstrated by the authors (Doolin et al. 2007).

Amirnate et al. presented a distributed conference solution over centralized conference clouds and the discovery is made through presence. Authors also proposed mechanisms for distribution of conference related information and management of distributed conference (Amirnate et al. 2007). Wang et al. investigated session setup procedure for the PoC group communications by using presence service. Shared XML document management server (XDMS) can provide presence information to PoC server and users can be invited according to their presence information. They tested their solution for pre-arranged groups and found that session setup delay was reduced up to 20%. Authors claimed that their proposed method significantly decreased the SIP signaling traffic as well as reduced the session setup delay (Wang et al. 2007).

Alam et al. described that on demand PoC session should have priority over pre established sessions. An optimal timer should be used to terminate a PoC session. Author presented the two state markov models to derive the maximum number of allowable simultaneous sessions (Alam et al. 2008). Meng et al. analyzed the talk burst control of the PoC by using queues and without using queues. The authors perform simulation in order to justify the comparative results. They conclude that this paper provides gaudiness to setup the PoC parameters (Meng et al. 2008). Jenq et al. described that PTT service can filter context information and establish an applicable PTT session in terms of current contexts of PTT users (Jenq et al. 2008). They combined the features of PTT and context awareness to achieve an enriched set of services. SIP INFO method is used for floor control. For context awareness 3GPP IMS and open mobile alliance (OMA) PoC architecture is used.

Jani et al. proposed an interconnection between peer to peer SIP (P2PSIP) and IMS. On one side an application server and on the other side a peer is required to make this interconnection successful. At the end prototype architecture is developed. This interconnection allows users of different applications to communicate with each other. The focus is only on signaling protocol (Jani et al. 2008). Mikcozy et al. discussed the efforts made by different standardization bodies to shift the simple IPTV technology to NGN based IPTV solutions. The authors divided the whole standardization process in three steps. First step is focused on NGN no IMS IPTV solutions, second step focused on IMS based IPTV and the last step about converged IPTV solution (Mikcozy et al. 2008).

Vehmas et al. discussed different issues in PoC service. Firstly their focus was on standard system architecture of PoC. Vendor's product strategies, regulation and service provisioning were some other issues described by the authors. Service diffusion functions were also analyzed in this paper (Vehmas et al. 2008). Mittal et al. presented a new framework to develop telecom applications by hiding the lower layer complexities. They name their framework as SewNet. First an abstraction model was developed and it was called as T-Rec Proxy model. Two use case scenarios were used to demonstrate the effectiveness of proposed framework (Mittal et al. 2008). Wang et al. proposed a service invocation mechanism for integrated services as well as for initial filter criteria. Main contribution of authors included definition of core and auxiliary service capability and a new modified definition of initial filter criteria. Multimedia message integrated service was used to elaborate and demonstrate the results (Wang et al. 2008). Wang et al. proposed interaction among different sessions established by one user. Session feature comparison module was added to achieve the target. This module contains description list of session and processing logic to service broker. For every service, the solution matched the triggering request (SIP) with the rules defined in the processing logic (Wang et al. 2008).

Hezmi et al. described the technologies and overview of FOKUS media interoperability lab that was developed by Fraunhofer institute FOKUS as a part of open IMS playground. Validation was performed by implementing different enablers. Authors concluded that IPTV is no more a fiction. It will be available for commercial use in all over the world in near future (Hezmi et al. 2008). Mehdi et al. discussed that how cable networks can be connected to IMS. Since cable networks are the major component of fixed networks therefore connecting them with IMS will move us one step forward towards fixed mobile convergence. Review presented in the article described different issues and solution related to convergence of cable networks and IMS. Leung et al. in 2008 discussed the use of service oriented architecture (SOA) architecture over IMS. The authors reviewed the work that was done in this domain (Mehdi et al. 2008). Alberto et al. analyzed the requirements and described the architecture of Multimedia Open Internet Services and Telecommunication Environment (MONSTER), a framework for mobile multimedia clients currently developed at the Fraunhofer Institute for Open Communication Systems (FOKUS) (Alberto et al. 2008). Lalanne et al. tested that whether the PoC service obey the standard requirements of IMS or not. Most relevant properties were tested by applying two phase testing strategy. In the first phase invariants were verified. More properties could be tested by just adding them in the proposed framework of authors (Lalanne et al. 2009). Weinberg presented the contextual push to talk. According to authors this contextual push to talk will reduce the duration of the voice dialogue (Weinberg, 2009).

Luo et al. implemented the PTT service on WinCE PDA. Authors argued that since PTT claims as 4G service so it should be tested on latest devices. Routed protocols were also ported to WinCE platform to make the implementation successful (Luo et al. 2009). Cho et al. deployed the PoC service on IMS platform. Focus of the author was just to test whether this push to talk service can really perform as it was claimed (Cho et al. 2009). Xing et al. measured the performance of PTT service over wireless networks. They tested different scheduling policies to reduce the delay. Moreover call setup procedures were also tested by the authors over different types of wireless networks (Xing et al. 2009). Pillai et al. described that currently PTT service does not suit the wireless networks. Call setup load and other requirements make this service infeasible for wireless network. They optimized the current PTT service so that it should become more cost effective when implemented on wireless networks (Pillai et al. 2009). Cruz et al. tested the push to talk service in IMS mobile scenarios. They concluded that the service was very flexible and could be used with different types of networks. Different features can be used in different environments (Cruz et al. 2009). Cho et al. tested and improved the PTT service by implementing it over IMS. They introduced the OMA PoC 2.0 architecture and after that simulation is performed to get the results (Cho et al. 2009).

3GPP standard document 3GPP TS 22.948 defined requirements for IMS convergent multimedia conferencing (CMMC) service in IMS. Main objective was to identify features of IMS multimedia conferencing which included a framework, session setup, media control, floor control, policy enforcement, standardization, adoption etc. 3GPP standard document 3GPP TS 22.174 defined Push Service and its requirements. It focused on core requirements for the service, operators and initiators.

Transfer of push data from a Push Initiator to a Push Recipient, Latency and Priority classes, were also described in the document. Nazish et al. in 2010 presented an election based algorithm for right allocation in PTM. In the dissertation they also described a media mixing algorithm (Nazish et al. 2010). Nikos et al. discussed call conference room interception attacks and also provided mechanism to detect those (Nikos et al. 2010).

2.2.1 Limitations in Literature-Push to talk and Conference

From the literature it can be concluded easily that use of presence information is recommended at the time of PoC session setup. But since presence information is the dynamic information and may change with the clock tick so it should be considered throughout the session. In literature we have not found any solution that recommends the use of up to date presence information in data or media dissemination. PTM server does not count the presence information while sending the media toward receivers. Ignoring the presence information at the time of media distribution results in wastage of valuable resources. So for as PTM service is concerned, very little work has been done on this topic. Niklas Blum is the main author who writes about PTM server architecture. A lot of work is needed to be done on PTM. Talk burst control protocol is introduced by 3GPP to handle different issues related to PoC. Maximum floor control time is introduced as the maximum time that a user can take to send media in one turn. Maximum floor control time is same for all the participants of the session. No one has proposed that how different maximum floor control time can be allocated dynamically to different users.

Who can send what type of media is another question that needs an answer. Current literature is silent in this domain. A user who becomes the member of the session can send and receive any type of media as fully authorized member. Privacy is another problem that exists in PoC server and no work to answer it. Within a PoC session a user can not share private information with few members of the session. A media burst that is sent towards PoC server will be received by all the members of the session. Security of PoC and conference service is another issue that is discussed by many researchers of the world. Different solutions are proposed to secure the PoC and conference server but still there is a need to improve those solutions. Conference and PoC services are still subject to various types of security threats including invite flooding attacks, SQL injection, refer flooding attacks etc. A comprehensive solution is needed to handle these attacks.

An authenticated user may act maliciously inside a PoC session or multiparty conference. In the literature we found nothing that can solve this problem. Internal threats are discussed by a number of researchers and it was proposed that the session initiator should take a step to eliminate an authenticated malicious user. Single participation based elimination may results in further dispute among the members of the session. So a distributed solution is required to handle the internal threats. Constant rights throughout the session add more inflexibility in PoC session. A user who joined the session with particular rights can not request for more rights during the session. This inflexibility reduces the application of PoC and conference services in real life scenarios.

IMS consists of layered architecture. At the bottom lies access network layer which contains various types of IP and legacy networks and users. On the top of access layer

IMS core layer is established that consists of call session control functions, databases, etc. On the top of IMS core there exists an application plane consisting of various types of application servers. IMS application server is the main server that connects the IMS core with application plane through ISC interface. In this chapter we present the literature on security of IMS and related protocols and after that we identify the security threats which still can be launched on application plane. We propose a secure IDP system to mitigate the effect of identified attacks.

2.3 Part 3: Literature Survey- IMS and NGN Security

Schafer et al. discussed different types of security challenges for NGN. Major focus was on DoS and location privacy (Schafer, 2004). Sun et al. explained the XML configuration Access Protocol (XCAP). XCAP usage for representing resource list and authorization is discussed in detail. At the end the authors showed communication procedure between IMPP client and server in the presence of XCAP (Sun et al. 2005). Magedanz et al. proposed an "Open IMS Playground" a test bed for IMS. This testbed includes almost all the major components of IMS core. This open source can be used to test academic and industrial research on IMS. Open IMS Playground includes functionality of all call session control functions, home subscriber server, media or streaming server, application server, different types of SIP application servers etc. Application layer is designed with different types of applications like presence etc. (Magedanz et al. in 2005). Sawda et al. described that besides the good security of SIP, it is still not subject to non repudiation and they proposed some changes in the SIP header in order to allow non repudiation service (Sawda et al. 2005).

William Enck et al. identified the vulnerabilities and risk originated from the interface of cellular network with Internet. The authors have demonstrated the ability of depriving bandwidth capacity of cellular network by sending enormous malicious SMS traffic originated from Internet resulting in denial of voice as well as legitimate SMS service. They have investigated the feasibility of exploiting the vulnerability by an adversary even equipped with limited resources. They have discussed NPA/NXX, Web scraping, web interface interaction and other techniques of creating hit lists for effective attack. They have quantified that it requires about 165 and 240 SMS per second to jam to voice & SMS service of the cities Manhattan and Washington D.C respectively, which translates into dialup modem bandwidth requirement for successful attack on the cities. The authors estimate 325,525 messages per second to set the entire USA's cellular networks non-responsive. Their suggested solutions to the problem include separation of voice and data, rate limitation and resource provisioning. However, major achievement of the research is identification of the problem that emphasizes on finding a better and complete solution for the problem (William Enck et al. 2005).

William Enck et al. proposed a compound solution to the problem discussed above. They suggested separation of voice from SMS traffic by implementing weighted fair queue that assure reserve bandwidth quota for voice and SMS thus confining the effect of attack on SMS service ensuring minimum effect on the voice traffic. Their mechanism mitigates the attack and lessens its effect on the voice traffic. However the protection of the legitimate SMS and other traffic needs to be addressed. The application of the proposed mechanism results in under utilization of available bandwidth during non-attack time (William Enck et al. 2006).

Imen et al. described the definition of service in detail. The authors first define the service from IT, Business and Telecom point of view and after that they focused on service definition from NGN point of view. They described that a service is a set of components where each component has some capabilities to serve. At the end they applied this definition over the presence service (Imen et al. 2006). M. Sher et al. proposed a Transport Layer security (TLS) along with the IDP system to secure the IMS application server against various types of time dependent and time independent attacks (M. Sher et al. 2006). M. Sher et al. presents the trust domain relationship based inter domain security model for IMS. Keys are managed using public key infrastructure. For confidentiality and integrity IPSec is used (M. Sher et al. 2006).

Vishal et al. presented a survey on security issues in presence and proposed a few solutions to solve these security issues. Authors emphasized on authentication of the watcher and presentity, authorization and access control over presence information, and the integrity and confidentiality of the presence information. For authentication author proposed asserted identity, cryptographically verified identity, and certificate based authentication. For data integrity and confidentiality of the presence information authors proposed the use of private and public key (Vishal et al. 2006). M. Sher et al. introduced a generic bootstrapping architecture to secure IMS and 3G networks. Authentication procedures are defined for IMS. Results are tested on IMS testbed developed by FOKUS. They developed an IDP system to secure the IMS application server. This IDP system compares all the incoming and outgoing requests and responses with the defined rules and decides whether to forward it or not. It is very difficult to maintain a comprehensive list of rules. In this paper the main focus of the authors is on misuse detection only (M. Sher et al. 2007).

Roman et al. proposed an attachment of non IMS enabled platform with the IMS platform in order to provide access to different services (Roman et al. 2007). M.

Sher et al. described a security model to secure the IMS application layer from time independent attacks like SQL injection. To attain this purpose authors developed an IDP system. Transport layer security is also provided in the study (M. Sher et al. 2007). Jan worked on security of SIP. He discussed various number of security threats faced by SIP. First the author addressed the call hijacking. Tampering of message body is another threat that is dealt by the researchers. Session teardown attacks are also considered as a threat. Author declared DoS as the biggest threat to SIP. Eavesdropping and spam are some of the other attacks discussed in this paper. Author analyzes the SIP based authentication and identified that current SIP based authentication is also subject to few security gaps. Security of terminals and servers is also deeply investigated by the author. At the end the author apply the proposed security threat on SIP based peer to peer network and validate that whether the identified threats really exists or not. It was found that SIP based peer to peer network is subject to all the identified threats. Author further proposed that secure routing, intrusion detection, lawful interception, identity enforcement etc. are the few areas which can be improved to secure the SIP based communication (Jan, 2007).

Hunter et al. discussed different security issues faced by IMS. General security issues discussed by authors include mutual authentication between UE and IMS, security association between user and P-CSCF, security between HSS and S-CSCF, domain level security etc. Security issues for network providers include toll fraud, IPv4 vs IPv6, authentication, use of IPsec, gateway attacks, Dos etc. Security issues for users contain DoS, identity and presence consideration, personal data and privacy (Hunter et al. 2007). Anzaloni et al. studied the performance of SIP based authentication in IMS. Authors described various types of mobility scenarios. Role of mobile IP is also discussed and different service levels are devised to check the performance. First focus of the authors was on SIP security and secondly they worked on security of mobile IP. At the end author mentioned the delay caused by the authentication procedure (Anzaloni et al. 2007).

Rebahi et al. described that IMS is subject to various types of DoS attack. In order to make the IMS successful author emphasize to secure it from these attacks. Solutions to mitigate the DoS attack are presented in the paper (Rebahi et al. 2008). Yufei et al. discussed the idea of cache based session setup. According to the authors the proposed scheme reduces the session setup delay and saves the network resources (Yufei et al. 2008). Aliya et al. worked on attack analysis in IMS. Attacks discussed by authors include ICMP flooding, UDP flooding, TCP flooding, SIP based flooding attacks etc. After that they devised security framework for IMS. Security framework proposed by authors consists of a lightweight IDP system. They worked on bio inspired solution to secure the IMS (Aliya et al. 2008).

Gouda et al. described that currently user needs multi-pass AKA procedure for authentication in IMS. According to the authors this multi-pass mechanism not only increases the load on AAA server but also results in increasing authentication delay. Author proposed a modified authentication procedure for IMS by eliminating the unnecessary steps. Instead of using multi-pass, authors preferred to use one pass authentication scheme. This scheme also reduced the chances of DoS attack on IMS. An analytical method was used to study the performance of the proposed authentication mechanism (Gouda et al. 2009). Zubair et al. discussed the robustness and reliability of SIP servers against different types of DoS attacks (Zubair et al. 2009). Hecht et al. implemented an anomaly based IDP system for IMS. They argued that since it is one of the best IDP so it will give better results in IMS as well (Hecht et al. 2009).

Ehlert et al. devised a specification based IDP to address different types of SIP based attacks. Authors implemented the proposed IDP and concluded that it is capable of handling many threats. Major focus of the authors was on DoS attack (Ehlert et al. 2009). Luo et al. analyzed the impact and cost of different security solutions designed for IMS. The performance matrix was based on quality of protection and performance. The authors devised seven level of IMS security introduced by 3GPP. QPN model was used to evaluate the performance (Luo et al. 2009). Wahl et al. worked on securing IMS against different types of security threats. They proposed an autonomous and self sufficient protection system to secure the IMS. The focus was on signature less detection of attacks (Wahl et al. 2009). Abdelnur et al. described few new attacks those can be launched on SIP based authentication procedure. Authors argued that SIP has given so much importance but still it is subject to various types of security threats (Abdelnur et al. 2009). To preserve privacy in SIP Giorgos et al presented a framework (Giorgos et al. 2010). Subharthi et al. presented the architecture for NGN and also discussed few issues related to security (Subharthi et al. 2011). M. Sayyad et al. wrote a review about IMS and discussed different security threats faced by IMS in the current communication age (M. Sayyed et al. 2011). Cristina-Elena presented an authentication solution for the 4G networks (Cristina-Elena et al. 2011). Barbara et al. define the attack defense tree for NGN in detail (Barbara et al. 2011). Thierry provided a SIP firewall for IMS core (Thierry et al. 2011).

2.3.1 Critical Analysis of Literature Survey-IMS and NGN Security

Secure solutions related to IMS and application plane are mainly focused on two issues. First part consists of authentication and key agreement procedure and second part focuses on flooding attacks. As far as authentication and key agreement is concerned, it is still subject to various types of security threats. Authentication takes place inside the registration procedure of IMS. A user sends registration request and receives a challenge, after answering the challenge, waits for successful registration message. The first register request contains the public and private IDs of the users. Private ID of the user is used in authentication process and it must remain private. Sending in SIP based register request makes it insecure because SIP is a text based protocol and the first register request is not encrypted. Sending private key in an un-encrypted plain text makes it highly vulnerable against various types of security threats. Second issue that is discussed in the literature is on flooding attack. To mitigate the effect of flooding attacks IDP system is proposed. No doubt IDP system works well to provide security against flooding attacks but certain parameters are ignored while designing the IDP system. First of all signatures are defined against every type of attack, so it places all the users into one domain. A request that is considered an attack for a very low priority user is also considered as an attack for a high priority user. While in reality it is not the case, high priority users have much more rights as compared to low priority user. User's role is ignored by the proposed IDP system. Secondly blacklists are used to penalize the attackers. How long an attacker will remain in blacklist is another issue that is not answered by the literature. Literature proposed a fixed time blacklist mechanism. Fixed time makes the solution inflexible and does not fit into many real life scenarios.

2.4 Chapter Summary

In this chapter we present the existing work done by the researchers in the area of NGN and IMS. The literature is divided into three sub sections. First section discusses the work related to presence and messaging. At the end of this section critics are also provided. Second section consists of literature about push to talk, and multiparty conference and the third section talk about the literature related to security of IMS and NGN.

CHAPTER 3

3. PROBLEM DEFINITION AND ANALYSIS

IMS is among one of the emerging technologies and becoming an industry standard for NGN. We in this chapter addressed various problems related to IMS based Multimedia Services. We considered 4 most important services including Presence, Instant Messaging, Multiparty Conference and Push to talk over Cellular (PoC). Each of the service has its own problems. At the end of the chapter we also discussed few security risks those can be faced by all these services. Now in the following paragraphs we are going to discuss problems of each service one by one.

3.1 Presence

Subscription of presence service requires exchange of 4 messages on air interface. If a user wants to get presence information of 100 presentities at different times then all of them are subscribed individually. It will result in exchange of 400 messages per subscriber over the radio interface and if there are 100,000 subscribers, it results in exchange of 40, 000,000 messages over the radio interface. When a user does not require the presence information of presentity, unsubscription is must (Day et al. 2000).

In the un-subscription process the subscriber sets zero as expiry time. The presence server notifies the subscriber that the presence service, of a particular presentity, is un-subscribed. It can easily be concluded that un-subscription of presence service also requires exchange of four messages over the air interface. Now if a user needs the presence information for a short period of time or for connecting only one call then exchange of four subscription and four un-subscription messages will put a heavy load on the air interface (Florian et al. 2006, Mckon et al. 2008). Moreover it will also delay the overall process. Therefore it requires a solution that reduces the number of exchanged messages over the air interface when a user needs presence information for a very short period of time.

For example Receiver can deny calls by not answering or by making the status busy or unavailable. But from caller point of view no such mechanism exists that can provide the opportunity to make a conditional call. An employee who wants to call to boss only if the boss is in office must require subscribing the presence information of the boss. There is no mechanism which allows the users to send a conditional 'Invite' request (based on receiver's presence information) without subscribing the presence information of the receiver. Conditional call means that the call from caller will only be connected if a particular condition becomes true else the call will be dropped. If a user wants to call another user only if the receiver is in Washington D.C. then first presence information of the receiver is subscribed and after that it will be decide whether to make a call or not. Subscription to presence service requires exchange of subscribe and notify messages

If user A needs to call another user B provided the status of the user B is according to the expectation of the user A then it must need to subscribe the presence information before establishing the call if presence information of B is not already subscribed. Exchange of the 4 messages of the subscription causes a significant delay in the call establishment and also increases the load on the radio access network. If user A wants to call user B occasionally or once in a month then the user A does not require the presence information of user B all the time. Therefore if user A subscribe for the presence information of the user B only to decide that whether to establish a call or not then user A has to unsubscribe the presence information immediately after making the call in order to avoid the unnecessary notification messages. Un-subscription also puts load on the network. Since no mechanism exists which allow the user to make a call on the basis of the receiver's presence status without subscribing the presence information.

3.2 Immediate Messaging

Sending enormous number of messages to a targeted member is possible through immediate messaging because it does not require any session establishment (Enck et al. 2006). So immediate messaging is also vulnerable to a security threat known as immediate messaging flood (Khan et al. 2009). Since immediate messaging does not require any session establishment so a sender can send enormous messages to deny the services to legitimate users. Attacker can have one of the two intentions while launching an immediate message flood attack. First an attacker wants to overload the server in order to deny services to all the other users. Secondly an attacker can launch an attack to disturb a targeted single user, so in this case all the messages will be destined to a single user. This type of attack is easier to launch for the attacker.

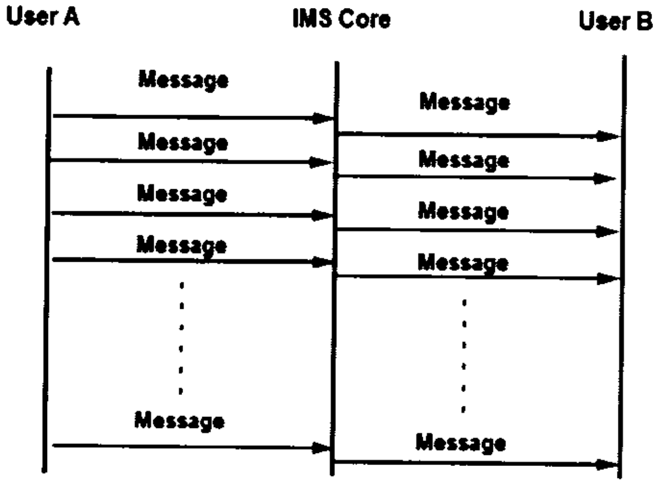


Figure 3.1: Immediate Message Flooding on Targeted User

3.3 Session Based Messaging

Session based messaging is subject to various types of flooding attacks:

3.3.1 Invite Flooding

Whenever a user wants to establish a session to exchange session based instant messaging, an invite request is routed towards the receiver. Sending too many invite requests may results in flooding and can cause denial of service (M. Sher et al. 2007). Figure 3.2 elaborate the problem to make it clearer.

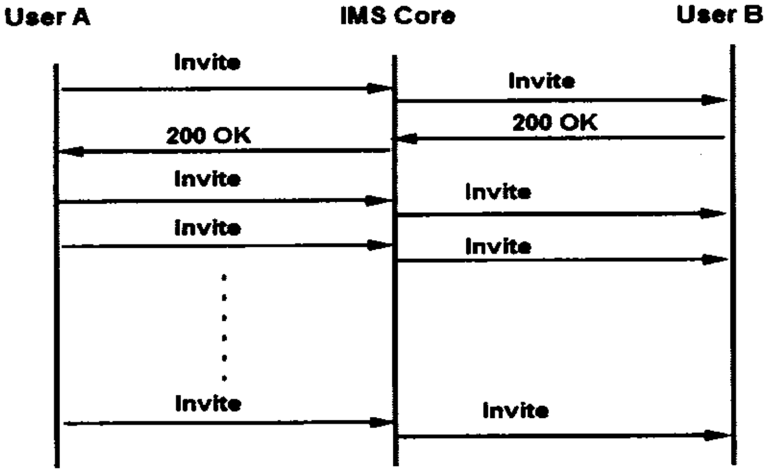


Figure 3.2: Invite Message Flooding on Targeted User

3.3.2 Session-Based Attacks

Different types of session based attacks can also be launched to create an effect of denial of service or degradation of service. These attacks include:

3.3.2.1 Session Modification Attacks

In most of the cases a session is required among the IMS users to carry communication. An attacker can launch session modification attack by sending a 'Re-

Invite' request. Session modification can change the current communication parameters and results in disturbance at the user's side (M. Sher et al. 2007).

3.3.2.2 Cancel Attack

A CANCEL attack can be launched to end a half established IMS session (M. Sher et al. 2007).

3.3.2.3 Session Teardown Attack

Session teardown attack terminates a running session and hence stops the communication. Session teardown attack can be launched through 'Bye' request (M. Sher et al. 2007).

3.4 Push to talk over Cellular and Push To Multimedia

From the literature we identified various types of problems and vulnerabilities in the current service mechanism of PoC and PTM. These problems are discussed in detail:

3.4.1 Rights Allocation Problem

PTM service allows a group of users to share multimedia data with each other. It should be decided who can send what type of data to how many member of the PTM group (Miikka et al. 2006). Current architecture of PTM is silent in this regard. Anyone who becomes a member of PTM session has the right to send any type of media to all the participants of the PTM session. Granting full rights to all the users of the PTM session reduces its applicability in many of the real life scenarios (Alam et al. 2006). For example in a university a PTM session is established among president, deans, chairmen and they want to invite students to the PTM session but as a listener only. Current PTM architecture does not allow inviting students as listeners only. Any member who becomes the PTM session has the full rights and can send any type of media. Allowing full rights to each and every member reduces the applicability of PTM in many real life scenarios as described in the above mentioned example.

3.4.2 Scalability Problem

Since PTM is a half duplex service therefore only one member can communicate at a particular time. All the other members have to wait for their turn to send media (Miikka et al. 2006). Turn to send media is controlled by the controlling PTM server. Now if the size of the PTM group is bigger average waiting time to get turn for sending media will be very high and results in unsatisfied users and at the end failure of PTM service. For example if on average a user takes 1 minute to send media then for 20 members of the session a user will get back turn to send after 20 minutes on round robin basis. Higher the number of participant higher the average delay. This scenario limits the PoC and PTM service to become more scalable. Details are shown in Figures 3.3 and 3.4.

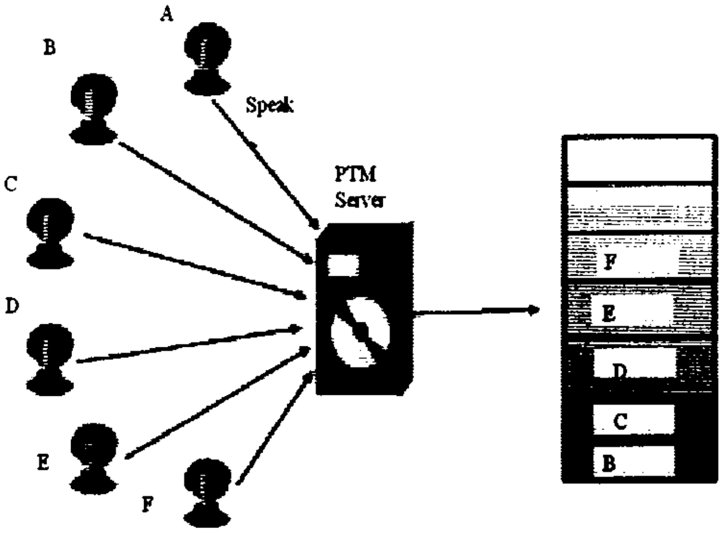


Figure 3.3: Waiting Queue with 6 Users

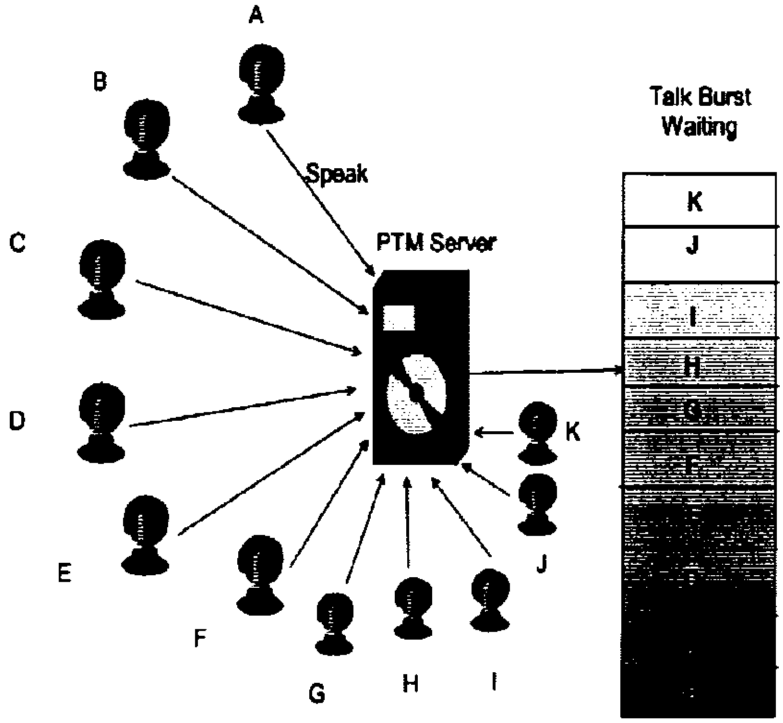


Figure 3.4: Waiting Queue With 11 Users

3.4.3 Privacy Problem

In a PTM session a user is not allowed to share media with few selected members of that PTM session. Media forwarded towards controlling PTM server is sent towards all the members of the PTM session (Miikka et al. 2006). Users can not share their private information with selected members of the group. Figure 3.3 shows that user A wants to send data to user B, C, H, and I because they are close friends of A. A does not want that its information be delivered to user D, E, F and G but in PTM it is not possible.

3.4.4 Resource Utilization Problem

In PTM when media burst reaches to controlling PTM server, it forwards that media to each and every user of that PTM session (3GPP TS, 2009). Data might not be required by all the members. Sending media to the members who do not require it results in wastage of valuable resources. These resources include processing at the end of PTM server, processing at the end of user and battery consumption of user equipment. All these resources are consumed in delivering a message that is not required by the receiver. For example in Figure 3.5 if user A's message is relevant to users B, C, H and I then sending it to users D, E, F and G will results in wastage of resources.

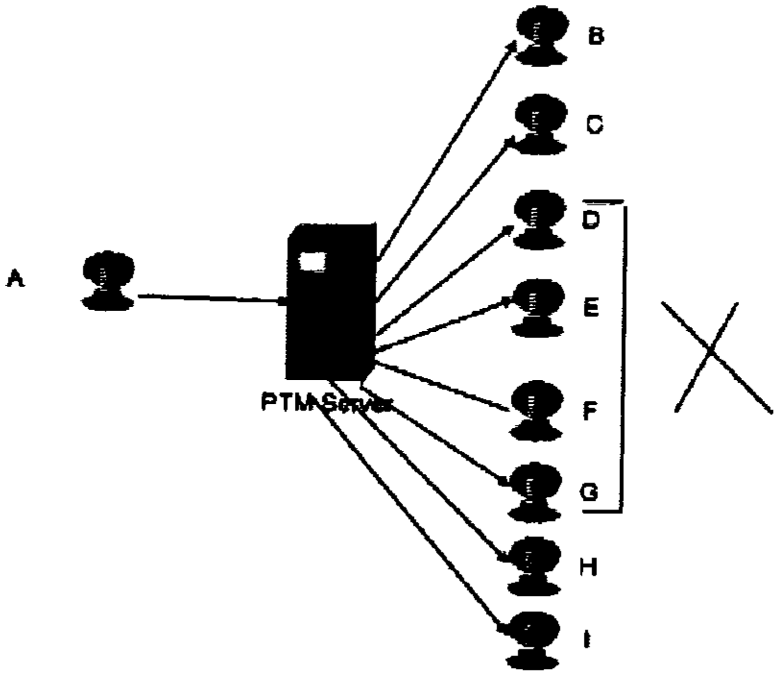


Figure 3.5: Privacy Problem in PTM

3.4.5 Membership Problem

Since in open PTM session anyone can be invited therefore it may results in conflict. Inviting a new member without taking consent from the existing members can results in conflict. For example, if a new user N is invited to the PTM session and there are some personal clashes of N with user O, P, Q and R (existing members of the PTM session) then it can result in conflict. Inviting one new member may results in four angry members (3GPP TS, 2009).

3.4.6 Disturbance Problem

In PTM when media burst reaches to controlling PTM server it forwards that media to each and every user of that PTM session. Data might not be required by all the members. Sending media to the members who do not require it results in disturbing those members. Again if we give a look to Figure 3.5 we can see that if A's message is not relevant to user D, E, F and G then it will create disturbance for them (3GPP TS, 2009).

3.4.7 Internal Threat

When a user becomes a member of Push to Talk (PTT) PTT or PTM session, sending and receiving of media is allowed to that user. Since PTT and PTM use the uni-multicasting so a single sent packet is received by all the members of that session. The session initiator has the right to delete any user from the ongoing PTT or PTM session. Single authority based deletion of authenticated user may results in dispute among the existing members of that session. But in some cases deletion of a user is necessary. For example, a user after getting authentication and becoming part of a PTT and PTM session may act maliciously. In PTT and PTM there is no mechanism that successfully deletes a user from the session as well as eliminates chances of dispute among the existing members of the session. Secondly when a user gets the turn to send media on the session it can be used for a very long time that may results in starvation (maximum floor time) to send useless traffic.

3.4.8 Maximum Floor Time

Maximum floor time is the maximum time that a user can consume to send media. After maximum floor time the resources are revoked from that user and allocated to the next user who wants to send media. Maximum floor time is defined for session. Within a session all the users have the same maximum floor time. Allocating same maximum floor time to all the users again reduces the applicability of PTT and PTM in many real life scenarios. In a session users can have different designations, priorities and roles. For example in a university based PTM session participant can be president of the university, deans, chairmen, faculty members, staff, students etc. Assigning same maximum floor time to a president and to a peon is not a good solution. Secondly theme of the session is also important. If the theme is to get awareness about student's problems then students should be allowed more floor time as compared to others (3GPP TS, 2009).

3.4.9 Joining with Full Rights

A user who wants to become member of a PTM session is bound to request for joining the session with full rights. A user who just want to listen the PTM session and does not want the video can not do so. A user is not allowed to join the session with limited rights according to the needs (3GPP TS, 2009).

3.4.10 Blind Delivery of Media

As soon as PTM or PTT server receives media from a user, it sends copies to all other members of the session without knowing the current status of receivers. Few receivers may not be available to receive that media, or user equipment (UE) of receivers may not be compatible with some codec etc. Multicasting the media without knowing the current status of the receivers results in wastage of valuable resources (3GPP TS, 2009).

3.4.11 Constant Rights Throughout the Session

In PTM no mechanism exists that can provide different rights to a user during different periods of time within a session. Rights allocated at the start of the session remain constant till the end (3GPP TS, 2009).

3.5 Multiparty Conference

There are many problems with the existing working mechanism of the conference service. These problems are described in detail.

3.5.1 Invite Flooding Attack

A SIP based flood can be launched over the conference service by sending enormous number of invite requests. Since every invite request results in creation of a conference which require considerable amount of resources at the conference server so large number of invite requests may results in denial of service. Figure 3.6 shows the invite flooding attack.

3.5.2 Single Participant based Referring Mechanism

Conference allows a single participant to invite anyone to the conference through refer request. Therefore an existing participant of the conference can invite such a person who is not acceptable by the other existing participants of that conference.

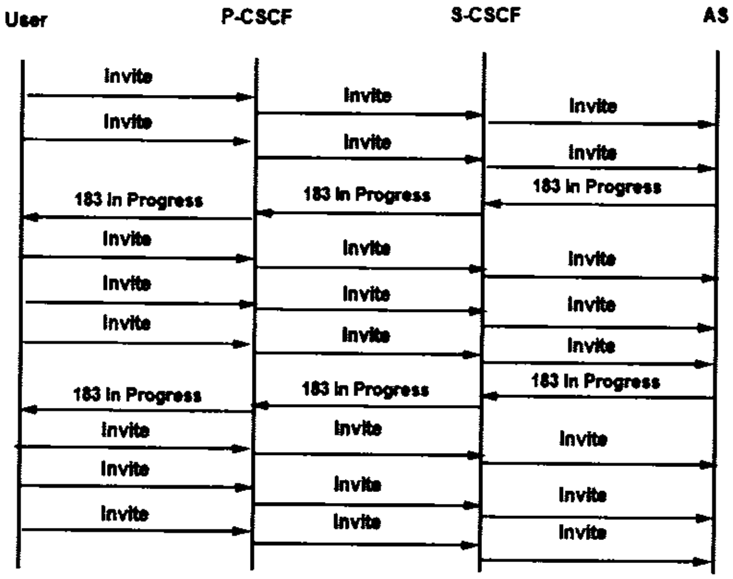


Figure 3.6: Multiparty conference based invite flooding attack

Therefore the other participant may leave the conference due to the inclusion of a new member. In short single participant based authority may results in conflict and dissatisfaction among the existing participants of the conference. Figure 3.7 shows the referring mechanism.

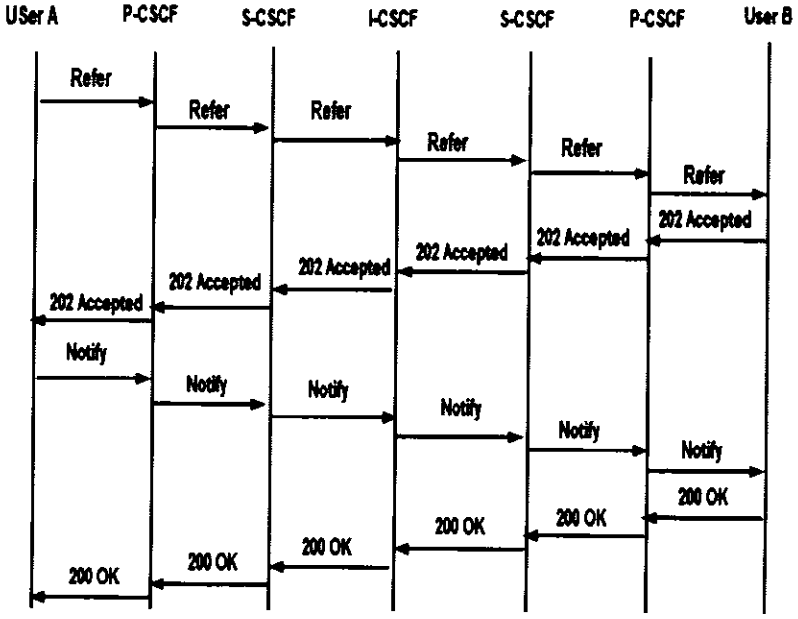


Figure 3.7: Multiparty conference based referring mechanism

3.5.3 Fully Authorized Referring

Whenever a person is referred into the conference it becomes a fully authorized participant of that particular conference. Fully authorized means that if it is a video conference then that participant has the full authority to watch, listen and speak. We can not restrict it to only watch or speak. In real life there are many scenarios where we need passive participants. Passive means that the authority of those participants is limited. So this fully authorized mechanism reduces the applicability of the conference service in real life.

3.6 IMS and NGN

Application plane of the IMS consists of number of application servers. Application servers may include presence server, messaging server, conference server, PoC server, SIP application server, charging server etc. whenever a request arrives at IMS core, S-CSCF decides whether this request requires to contact with some application server or not.

If the request needs to contact with some application server, S-CSCF forwards it towards the application plane. The request may contain an attack which can results in destruction at application plane. Problem or destruction at application servers will automatically results in degradation of quality of service or DoS. Therefore sending the requests blindly towards the application plane allows the attacker to attack easily over application server. We divided the attacks into different categories, Time dependent and Time Independent attacks.

From Intrusion Detection point of view, all attacks those can be detected after the particular duration of attack instead of being detected immediately belong to time dependent attack. The primary feature of this category is that an attack is composed of a large amount of data packets. We describe only the SIP flooding attacks because they are the most serious threat for IMS. In flooding the attacker sends lot of fake messages to victim machine or network to produce traffic workload. In case of IMS core, the P-CSCF can be overwhelmed by SIP REGISTER flooding attacks. As a result, the resources could become congested and produce bottleneck. In case of AS, the SIP Servlet server can be overwhelmed by the flooding attacks. There will be no available resources to handle the legitimate SIP messages. Time-independent attacks are serious threat to IMS like VoIP networks. The fake message cloud that is on behalf of an attack can immediately cause damage on the victim's node if it is not detected and blocked immediately. Time dependent and Time independent attacks are shown in Figure 3.8. Here our focus is on time dependent attacks only.

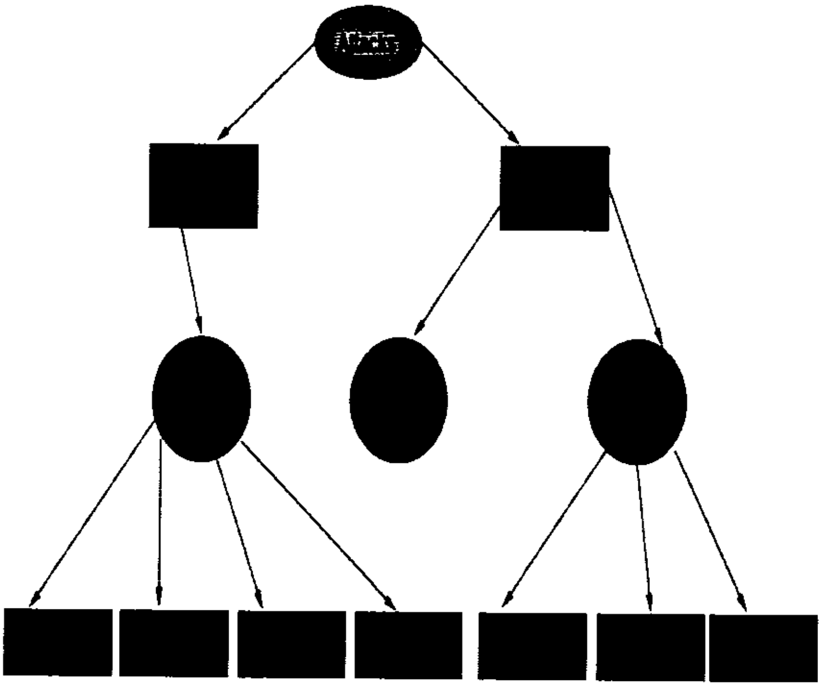


Figure 3.8: Time Dependent and Time Independent Attacks

3.6.1 Register Flooding Attacks

First of all to become a user of IMS a device needs to have registration. In order to get registered the user initiates a registration process by sending a 'Reg' request. A flood can be generated by sending enormous number of 'Reg' request within a small period of time.

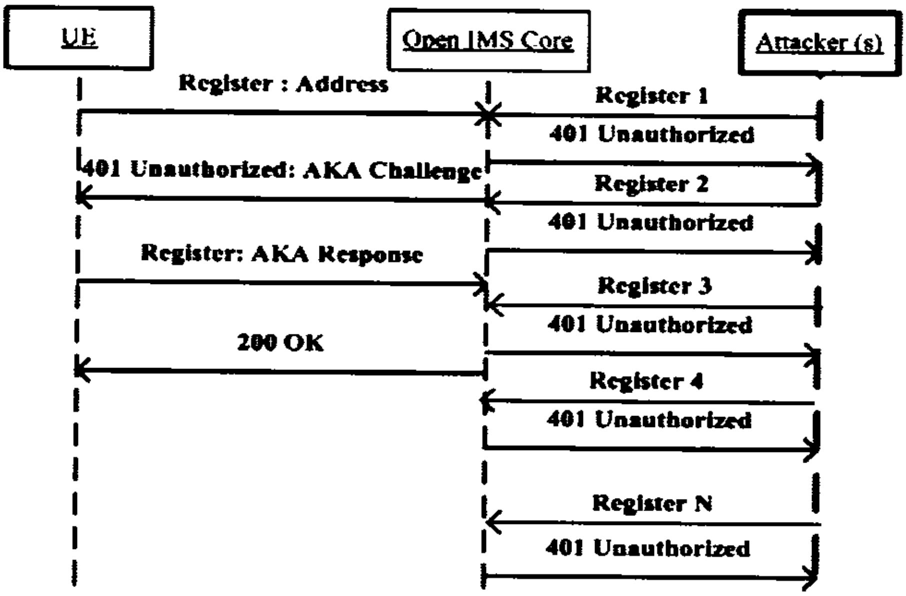


Figure 3.9: Register Flooding Attack (M. Sher et al. 2007)

3.6.2 Invite Flooding Attacks

In IMS session is established through 'INVITE' request. Whenever a user wants to call another user an 'Invite' request is routed from caller to receiver. Enormous numbers of invite requests can occupy a major share of network and results in degradation or DoS. Structure of an invite request is given below:

```
INVITE sip:zee@ims-test.com SIP/2.0
Via: SIP/2.0/UDP soft.phone123.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Zee <sip:zee@ims.tets.com>
From: Shan <sip:shan@phone123.com>;tag=1928201547
```

Call ID: a84b4c76e66710@soft.phone123.com

CSeq: 345612 INVITE

Contact: <sip:shan@soft.phone123.com>

Content-Type: application/sdp

Content-Length : 143

Invite flooding attack is shown in Figure 3.10

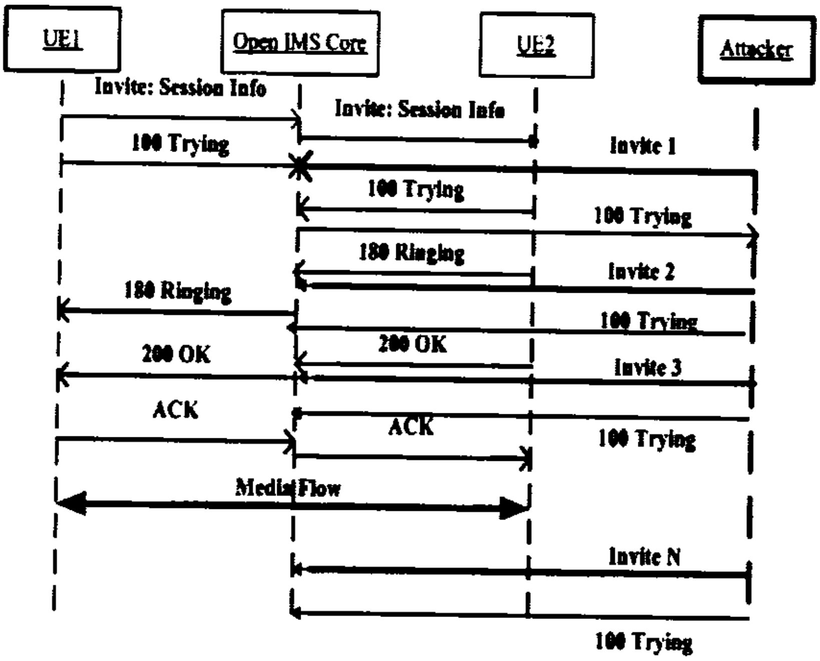


Figure 3.10: Invite Flooding Attack (M. Sher et al. 2007)

3.6.3 Subscribe Flooding Attacks

In order to use a service like presence a user first needs to subscribe for it. The subscribe request is received by the specific server. A user with malicious intentions can send a bulk of subscribe request to a particular server so that the server becomes busy and the legitimate users will not be able to get service from that particular server.

3.6.4 Publish Flooding Attacks

Presence service deals with publish requests. Whenever a user wants to share its own status information with other users it publishes them over the presence server. Flood of publish request can block the presence service. Publish flooding attacks are shown in Figure 3.11.

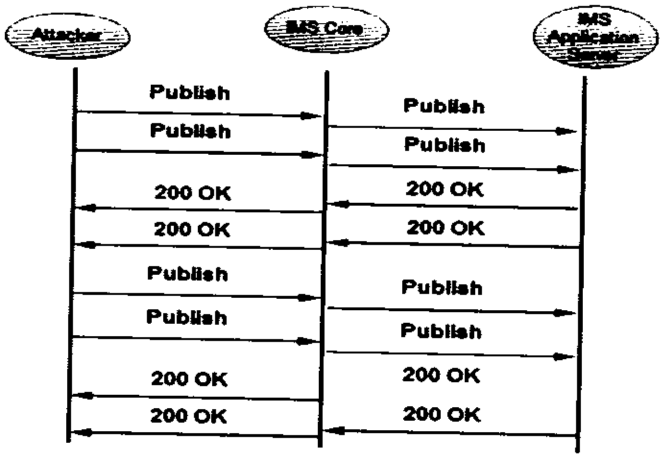


Figure 3.11: Publish Flooding Attack (M. Sher et al. 2007)

3.6.5 Session Modification Attacks

In most of the cases a session is required among the IMS users to carry communication. An attacker can launch session modification attack by sending a 'Re-Invite' request. Session modification can change the current communication parameters and results in disturbance at the user's side.

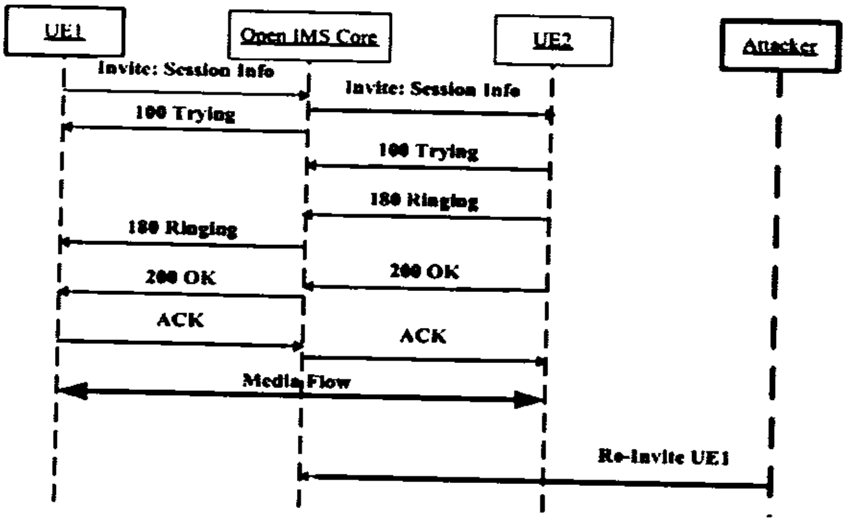


Figure 3.12: Session Modification Attack (M. Sher et al. 2007)

3.6.6 Cancel Attack

A CANCEL attack can be launched to end a half established IMS session.

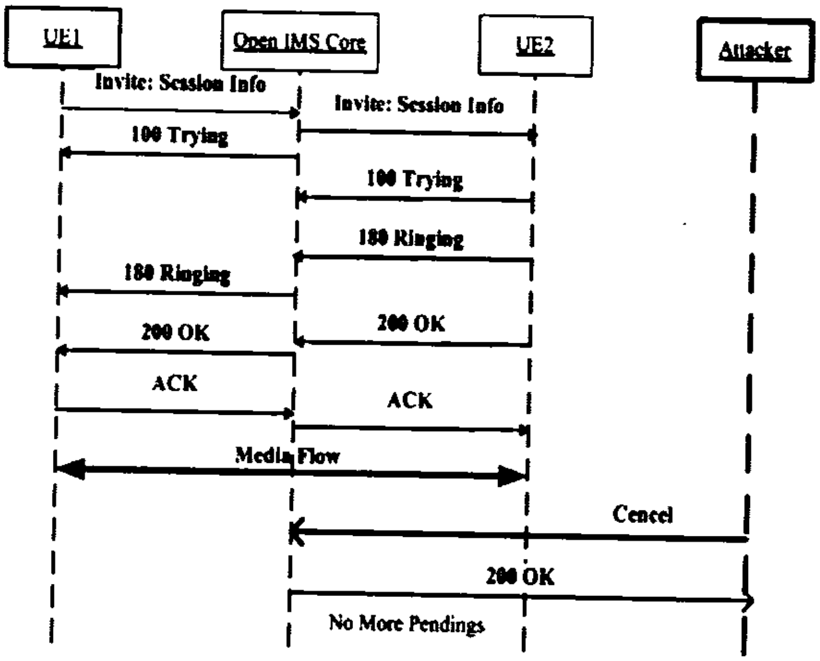


Figure 3.13: Cancel Attack (M. Sher et al. 2007)

3.6.7 Session Teardown Attack

Session teardown attack terminates a running session and hence stops the communication. Session teardown attack can be launched through 'Bye' request.

Moreover S-CSCF does not distinguish among the request initiators, and the requests themselves. All the requests are treated equally so as the request initiators. No priority or higher preference is provided to any of the users or any of the requests.

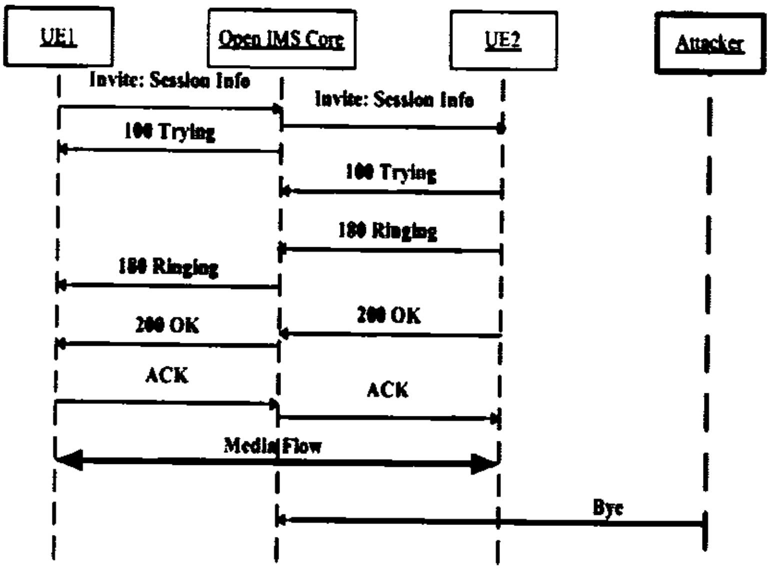


Figure 3.14: Session Teardown Attack (M. Sher et al. 2007)

3.7 Chapter Summary

In this chapter problems related to IMS and IMS based multimedia services are discussed in detail. In the first section of the chapter problems related to presence service are discussed. It is found that since presence is continuous dynamic service so it puts a great load on the air interface. Moreover it is also finds that presence information must needs subscription even if caller requires that information for a very little period of time. Subscription and un-subscription on one hand requires a significant amount of time and on the other hand it also consumes a good part of the bandwidth at air interface. Second section consists of problems related to messaging. We find that in immediate messaging since user is allowed to send any number of messages without creating any session so it creates a security risk a the receiver end. In session based messaging all types of session based attacks like cancel and session modification attacks are possible. In the third section problems related to PoC and PTM are discussed. The first problem is about the scalability of PTM. Since PTM is a half duplex service so increase in number of participants also increasing the average waiting time of getting turn to speak. Second problem is about delivering data to irrelevant users that creates privacy problem as well as disturbance problem. Maximum floor control time is also fixed and equal for all the participants. It is not allocated on the basis of the user's requirement or on user's role in that session. Fourth section talks about problems related to multiparty conference and it includes single participant based referring and fully authorized referring. Fifth section consists about security threats to IMS and NGN. Register flooding attack can be launched by sending enormous number of register requests. In the same way invite flooding attack can also be launched. Other attacks those are discussed in this section includes session based attacks, publish flooding attack, etc.

CHAPTER 4

4. SOLUTION, METHODOLOGY AND FRAMEWORK

To solve the problems discussed in chapter 3 we designed different frameworks. Since focus is on different services and with in each service objective is to solve multiple problems so different frameworks were needed for each type of problem. This chapter discusses these frameworks and their internal working and methodology.

4.1 Presence Enabled Conditional Call Setup

Our proposed presence enabled conditional call setup allows the caller to send a conditional invite request to the receiver without subscribing the presence information of the receiver. The presence information is verified during the call setup. A user inserts condition inside the 'Invite' request of the call. When this invite request arrives at the S-CSCF, it checks whether it contains some condition or not. If no condition exists the call is routed according to the normal procedures. If it contains a presence based condition the S-CSCF extract that condition and forward it to the presence server. The presence server verifies whether this caller is authorized to view this information or not. If the caller is not authorized on that specific presence information then the presence server returns an error message and upon receiving the error message the S-CSCF immediately dropped the call. The scenario is described in Figure 4.1.

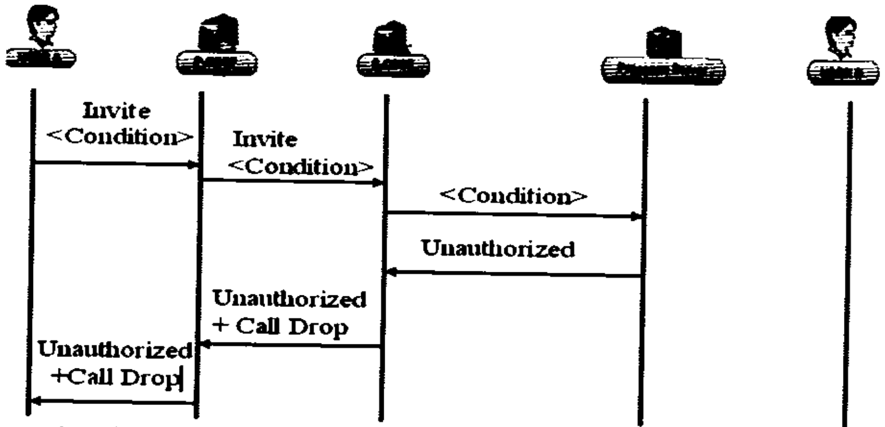


Figure 4.1: Conditional Call Scenario When Condition Contain Unauthorized Presence Attribute

If the user is authorized for that presence information then presence server retrieve that attribute of the presence information and returns it to the S-CSCF. Upon receiving that presence information, S-CSCF matches it with the condition. If it does not match with the condition then S-CSCF drops the call and returns the current presence information to the caller. The details are shown in Figure 4.2.

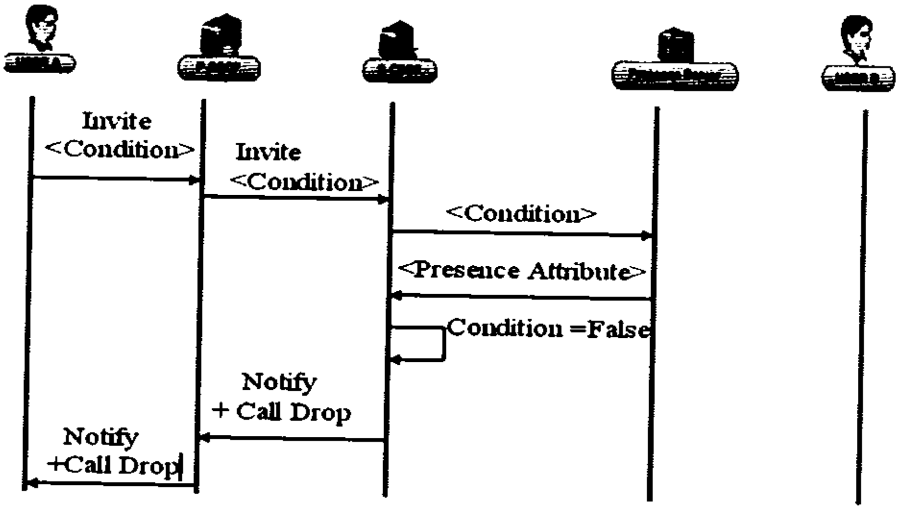


Figure 4.2: Conditional Call Scenario When Condition Becomes False

If the condition becomes true then S-CSCF removes the presence condition from the Invite request and forwards it to the receiver and the remaining procedure of call setup works according to the standard procedures. In this scenario there is no need to return the presence information to the caller because if the call is established then it can automatically be concluded and the value of the presence information is the same as the condition specifies. Figure 4.3 specifies the details.

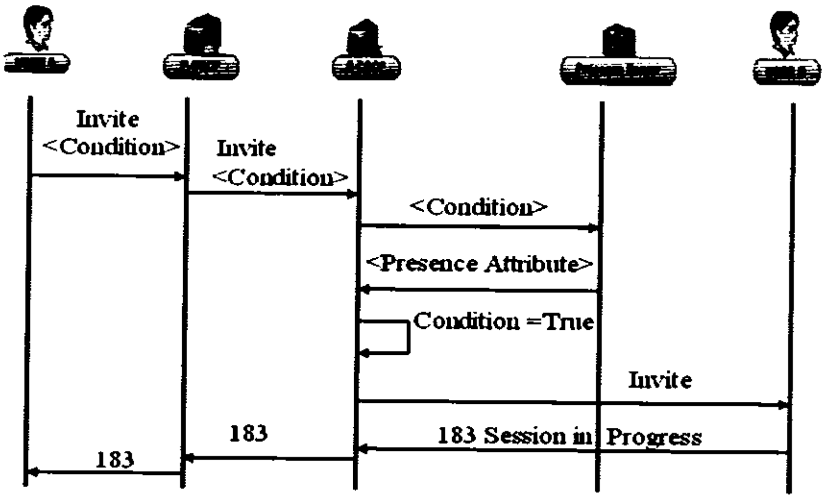


Figure 4.3: Conditional Call Scenario When Condition Becomes True

4.2 Security Solutions for Instant Messaging

Three solutions are proposed to mitigate the effect of flooding attacks launched through instant messaging. These three solutions are described below.

4.2.1 Three Layer Secure Architecture

To mitigate the effects of above mentioned security threats, we propose a secure architecture that consists of three layers. Layer one, sender's authorization, reduces the misuse of sender's resources. A priority based IDP system is layer two that secures the application server as well as the receiver. The third layer consists of receiver's preferences. Details of each layer are described below:

4.2.1.1 Layer One: Sender's Authorization

Since most attacks are launched through spoofed addresses, it is quite possible that an attacker can use considerable resources or identity of other users at any time. To reduce the chances of this misuse, the sender applies some authorization rules at S-CSCF; those are filtered whenever any request or message is received by the S-CSCF with the identity of that sender. These rules are the preferences of the sender and are configured by the sender after registration. If a sender thinks that someone can generate a burst of messages by misusing the identity, the sender can configure a rule that allows only a limited number of messages per hour, for example, 60. Since the rule does not allow more than 60 messages per hour, an attacker who spoofed the identity of this user can send only 60 messages per hour. In this way misuse of the sender's resources can be minimized. Also, the sender can block himself to establish any session between 3:00 pm to 5:00 pm because sender is busy with family during this time. Similarly, a sender can restrict herself to send any message to another user during 4:00 pm to 7:00 pm.

These rules can be configured as:

```
<?XML version=”1.0” encoding= “UTF-8”>

<Rules>

<Rule type=Sender_Authorization>

<User> 192.168.10.1 </User>

<Rule1>

<Name> Message Flood </Name>
```

```
<Number> 61 </Number>

<Interval> 60 </Interval>

<Alert> Message Flood </Alert>

</Rule1>

<Rule2>

<Name> Session establishment </Name>

<time_start> 3:00 pm </Time_start>

<Time_end> 5:00 pm </Time_end>

<Action> Invite </Action>

<Alert> Not Allowed </Alert>

</Rule2>

<Rule3>

<Name> Session establishment </Name>

<time_start> 4:00 pm </Time_start>

<Time_end> 7:00 pm </Time_end>

<Action> Invite </action>

<Destination> 192.168.10.10 </Destination>

<Alert> Not Allowed </Alert>

</Rule3>

</Rules>
```

Whenever any request or message with the identity of that particular sender is received by the S-CSCF, it is first matched with authorization rules. If the request contradicts with any of the authorization rules, it will be discarded immediately else it will be forwarded for further processing. Figure 4.4 shows the interaction among the objects of this layer.

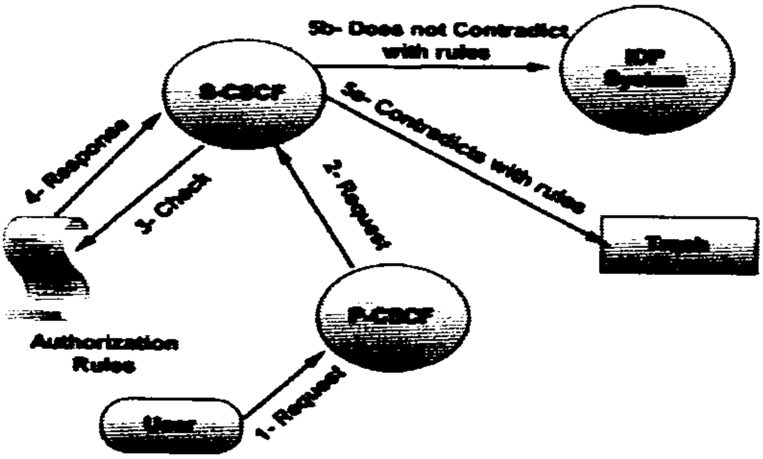


Figure 4.4: Object Interaction Diagram of Sender's Authorization Rules

4.2.1.2 Intrusion Detection System

In order to secure the messaging server, we propose a middleware between IMS application server and messaging server. This priority-based IDP system consists of various components, including:

(a) **Misuse detection:** It is one of the important components that receives the request from S-CSCF and decides whether it contains an attack or not.

(b) **Priority Table:** This component stores the priority of every user. These priorities are assigned at the time of registration.

(c) **Blacklist:** Blacklist consists of list of attackers who tried to attack on the network. An attacker remains into the blacklist for a specific period of time.

(d) Rules: It is a priority wise comprehensive list of rules to identify the attack.

When S-CSCF finds that the sender is authorized to send the request, it forwards the request to the application server who forwards it towards misuse detection component of the intrusion detection system. Misuse detection first checks the blacklist to find whether the sender is legitimate or not. If the sender is found in the blacklist, the request is discarded; if the sender is not in the blacklist, the misuse detection component retrieves the priority of the sender from the priority table. The request then is matched with the attack rules by the misuse detection component. If a user with priority 3 is allowed to send only three “invite” requests per five minutes (300 seconds), then the attack rule will look like:

```
<?XML version=”1.0” encoding= “UTF-8”>
<Rules>
<Rule type=Flood>
< priority > 3 </priority>
<Name> INVITE </Name>
<Method> INVITE </Method>
<Number> 3 </Number>
<Interval> 300 </Interval>
<Alert> INVITE FLOOD </Alert>
</Rule>
```

If the request matches any of the attack rules, it is considered as an attack and discarded immediately. The sender is put into the blacklist. If the request does not match any of the attack rules, then it is forwarded to the application server. An object interaction diagram of the IDP system is shown in Figure 4.5.

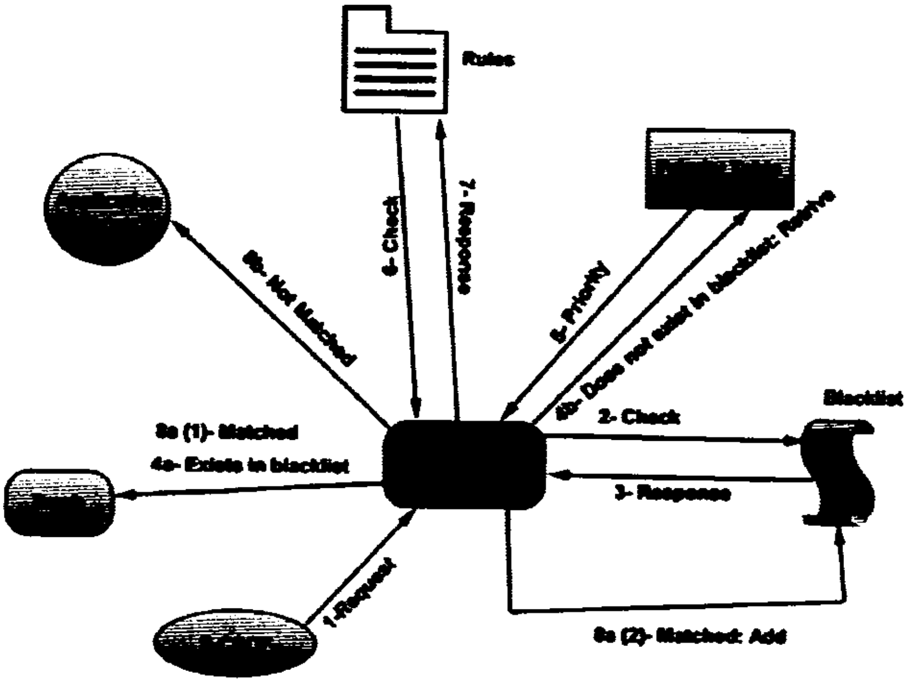


Figure 4.5: Object Interaction Diagram of IDP System

4.2.1.3 Receiver's Preferences

Layer three consists of receiver's personalization rules. The receiver registers the personalization rules over the layer three of the security architecture (Beltran & Paradells, 2008). These rules are specifically related to the messaging service only. As soon as a message arrives at module three, it compares the message with the rules specified by the user and takes action accordingly. Layer three is deployed over the application server. Examples of the user personalization rules can be:

```
<?XML version="1.0" encoding= "UTF-8">
<Rules>
<Rule type=Sender_Authorization>
<User> 192.168.10.1 </User>
```

```
<Rule1>
<Name> User X </Name>
<time_start> 7:00 pm </Time_start>
<Time_end> 9:00 pm </Time_end>
<Action> Invite </Action>
<Alert> Not Allowed </Alert>
</Rule1>
<Rule2>
....
</Rule2>
..........
<Rule_n>
........
<Rule_n>
</Rules>
```

The receiver will receive urgent messages, and the attacker's messages will be dropped either at layer one, or layer two, or layer three. Figure 4.6 explains the object interaction diagram of the security architecture in detail.

4.2.2 Presence Enabled Secure Architecture

In this section we describe our proposed presence enabled secure architecture. Presence service is proved as a good service provisioning mechanism when it is used with other services. We also propose to use presence service inside the messaging service. To use presence service users have to subscribe for it. Subscription and notification of presence service put an extra load on air interface of the network since it requires exchange of messages. In our proposed solution there is no need to subscribe for the presence service. Presence service is checked and verified during the transit of instant message.

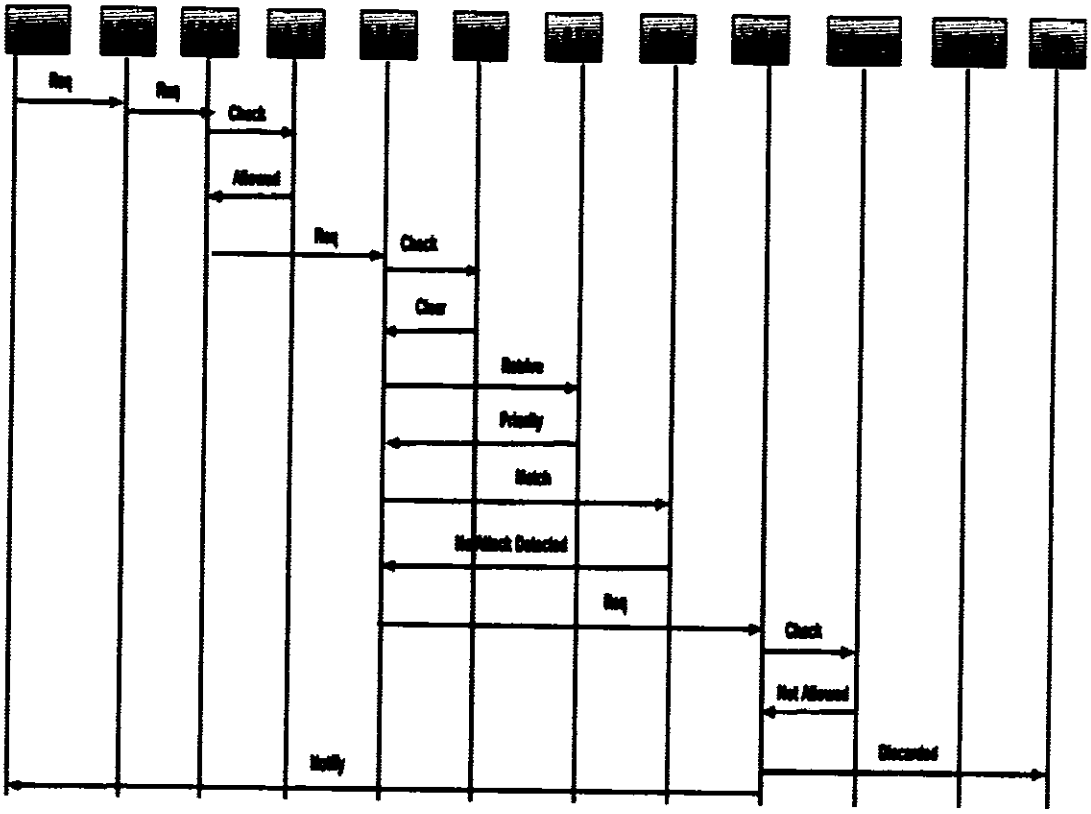


Figure 4.6: Three Layer Secure Architecture

Whenever a user sends an immediate message or tries to initiate a session with particular user, the message or request is received by P-CSCF. P-CSCF after receiving the request forwards it to S-CSCF. In the normal scenarios S-CSCF after performing necessary actions forwards the message or request towards the receiver's P-CSCF. But in our proposed solution S-CSCF, before forwarding message or request towards receiver, checks the presence information of sender as well as receiver. Checking the presence information of a sender is necessary because if someone is misusing (spoofing) the identity of the sender it can be traced out from presence information of the sender. If the presence information of the sender contradicts with the sent request or message it means that the identity of the sender is misused by someone else. In that case message or request is discarded and sender is notified about the situation.

If the message or request does not contradict with the presence information of the sender then it is matched with the presence information of receiver. Presence information of receiver may state that currently incoming sms may create disturbance so receiver is not willing to receive sms at that particular time. In this case forwarding the request or message towards receiver not only results in disturbance at receiver's end but also results in wastage of valuable resources. In the proposed solution if the message or request contradicts with the receiver's presence information it is discarded immediately. Figures 4.7 and 4.8 describe the situation in more detail.

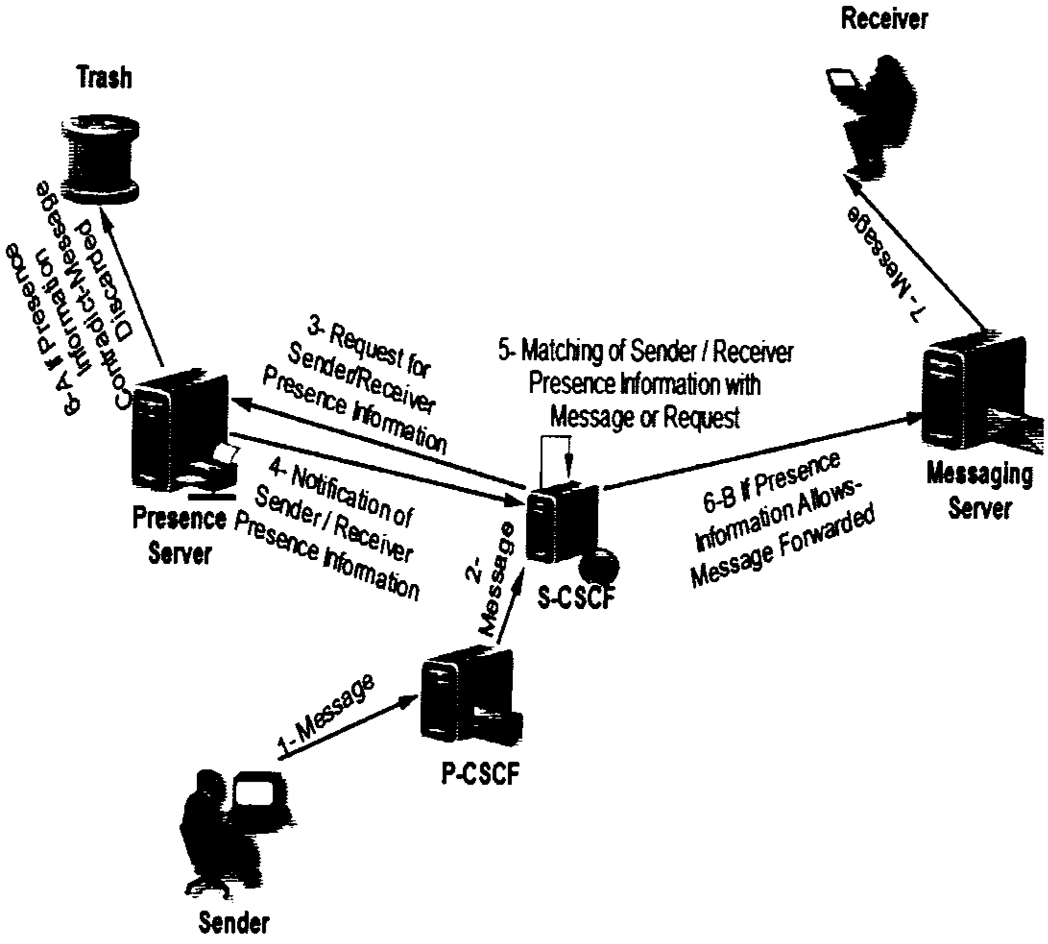

Receiver
Trash
8-A If Presence Information Contradict-Message Discarded
7- Message
3- Request for Sender/Receiver Presence Information
5- Matching of Sender / Receiver Presence Information with Message or Request
Presence Server
4- Notification of Sender/ Receiver Presence Information
2- Message
S-CSCF
6-B If Presence Information Allows- Message Forwarded
Messaging Server
1-Message
P-CSCF
Sender

Figure 4.7: Presence Enabled Instant Messaging Architecture

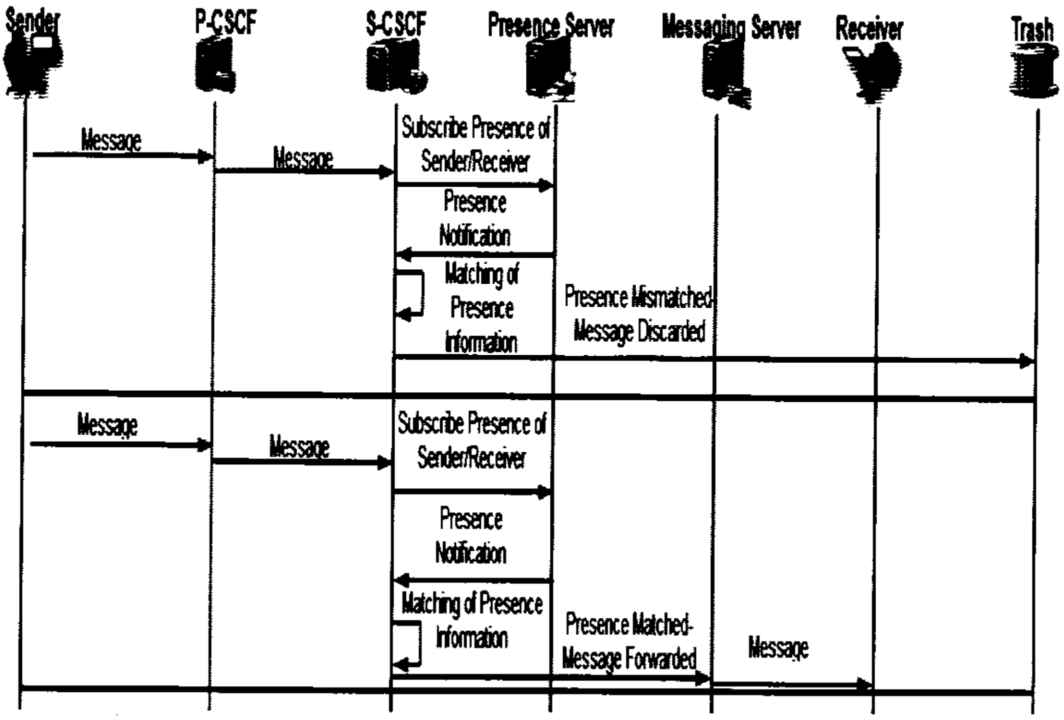

Sender
P-CSCF
S-CSCF
Presence Server
Messaging Server
Receiver
Trash
Message
Message
Subscribe Presence of Sender/Receiver
Presence Notification
Matching of Presence Information
Presence Mismatched-Message Discarded
Message
Message
Subscribe Presence of Sender/Receiver
Presence Notification
Matching of Presence Information
Presence Matched-Message Forwarded
Message

Figure 4.8: Presence Enabled Instant Messaging Flow

4.2.3 Presence and Preferences Based Secure Architecture

Checking the presence information of sender and receiver reduces the misuse of network resources and prevent the network from various types of attacks. But since presence information cannot describe all the current requirements of the users so blocking the attacker by using presence information only is not enough. Something more should be added to it to make the solution more secure.

We added authorization rules along with the presence information. Receiver specifies the authorization rules those are stored at messaging application server. Sender sends a message, S-CSCF first verifies the presence information of the sender to make it sure that the identity of the sender is not misuses. After that presence information of the receiver is checked to verify the current status of the receiver. If the request or message does not contradict with the presence information of sender and receiver then it is forwarded towards messaging server. At messaging server user specify the receiving rules. These rules are more comprehensive compared to presence information. Few examples of rules can be:

```
<?XML version=”1.0” encoding= “UTF-8”>
<Rules>
<Rule type=Sender_Authorization>
<User> 192.168.10.1 </User>
<Rule1>
<Name> User X </Name>
<time_start> 7:00 pm </Time_start>
<Time_end> 9:00 pm </Time_end>
<Action> Invite </Action>
<Alert> Not Allowed </Alert>
</Rule1>
<Rule2>
</Rule2>
<Rule_n>
<Rule_n>
</Rules>
```

These rules are compared with the incoming request or message and if any contradiction is found the request or message is discarded and the sender is notified. Figure 4.9 and 4.10 describe the scenario in detail.

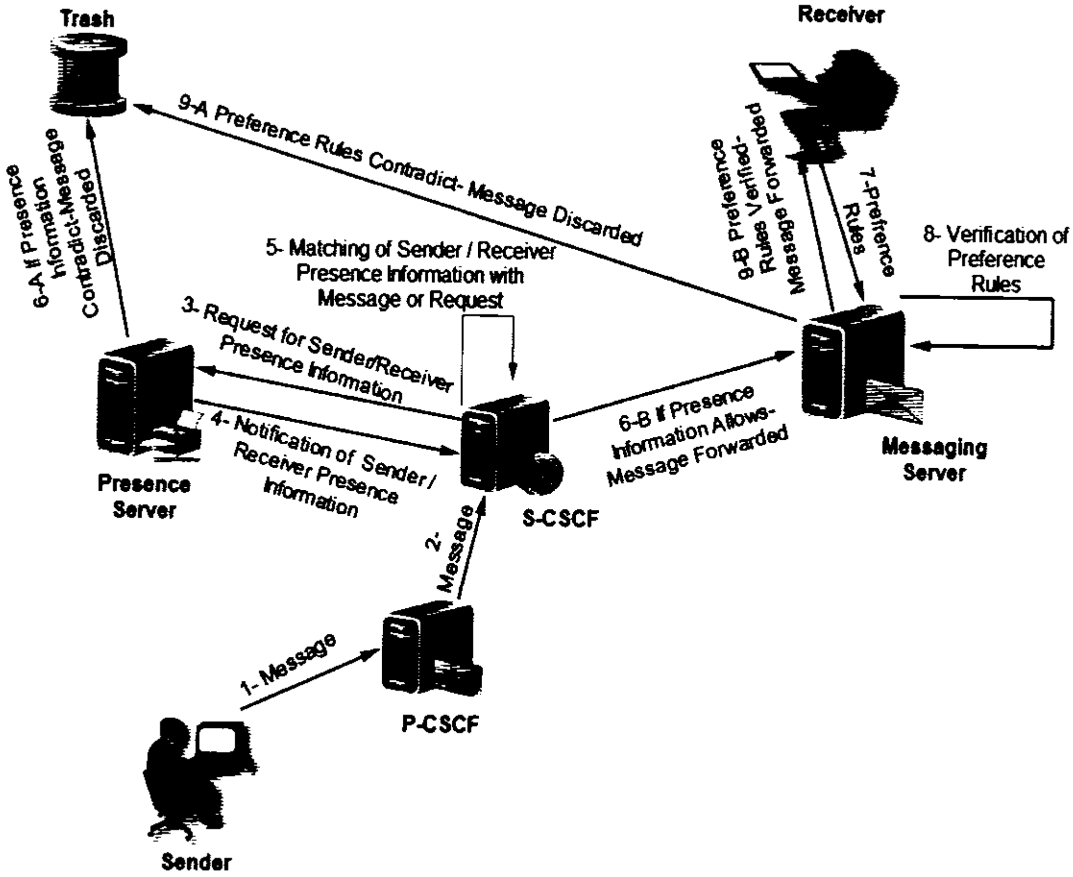

Trash
Receiver
9-A Preference Rules Contradict- Message Discarded
6-A If Presence Information Contradict-Message Discarded
9-B Preference Rules Verified- Message Forwarded
7- Preference Rules
8- Verification of Preference Rules
5- Matching of Sender / Receiver Presence Information with Message or Request
3- Request for Sender/Receiver Presence Information
4- Notification of Sender/ Receiver Presence Information
Presence Server
S-CSCF
6-B If Presence Information Allows- Message Forwarded
Messaging Server
2- Message
1- Message
P-CSCF
Sender

Figure 4.9: Presence and Preference Based Instant Messaging Architecture

4.3 Election Based Mechanism for Membership and Rights Allocation

If a user applies for full rights then existing members of the session decide what rights should be allocated to that user. For this purpose we proposed an election based rights allocation mechanism. Whenever a user is invited in a PTM session or a user sends a join request, an election is started among the existing members of that PTM session. Each of the existing members is notified by the PTM controlling server that a new user with SIP URI <ZZZ> wants to join this PTM session. Each of the existing members cast their vote to allow the new user to become part of the PTM session or not.

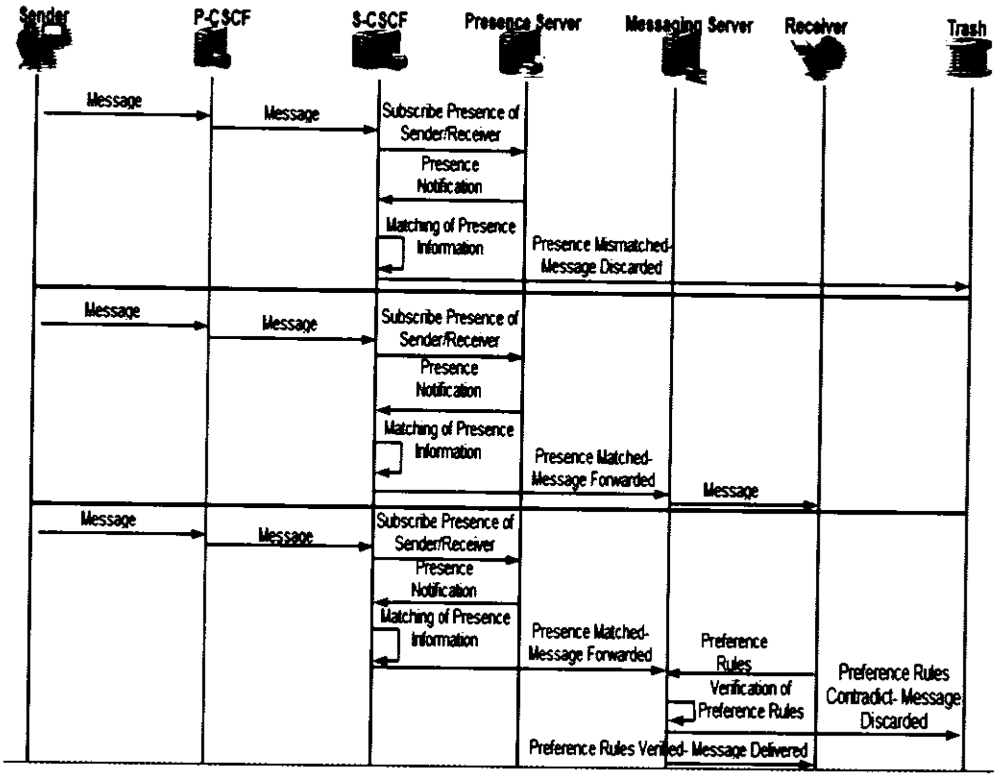

Sender
P-CSCF
S-CSCF
Presence Server
Messaging Server
Receiver
Trash
Message
Message
Subscribe Presence of Sender/Receiver
Presence Notification
Matching of Presence Information
Presence Mismatched-Message Discarded
Message
Message
Subscribe Presence of Sender/Receiver
Presence Notification
Matching of Presence Information
Presence Matched-Message Forwarded
Message
Message
Message
Subscribe Presence of Sender/Receiver
Presence Notification
Matching of Presence Information
Presence Matched-Message Forwarded
Preference Rules
Verification of Preference Rules
Preference Rules Contradict-Message Discarded
Preference Rules Verified-Message Delivered

Figure 4.10: Presence and Preference Based Instant Messaging Flow

If the new user is allowed to become member of the session, what rights should be allowed. In our proposed mechanism all the users do not have full rights. Few users can have full rights and few can have limited rights. For example a user can have full rights <Speaker, Listener, Watcher>, another user can have limited rights <Watcher, Listener>. Voting power of each of the user is same in order to avoid the monopoly of few users.

4.3.1 Voting Option

Whenever a user casts the vote, one from the 6 available options is selected. Each of the picked option has different weight as compared to the other options. Available options and their weights are shown in Table 4.1.

Table 4.1: Available Options to Cast Vote and Their Weights

Available Options	Weight
Full Rights	4
Speaking and Listening	3
Speaking Only	2.5
Watching and Listening	2
Listening only	1
Not Allowed	0

Each participant has to cast the vote within a specified period of time. After timeout a user who does not cast the vote will not be counted in election process.

4.3.2 Polling Algorithm

PTM server after receiving the request sends it to all the members of the session and asks them to cast their vote for the new user. Votes are first cast on the basis of joining request. If the new user requests for limited rights the votes are cast accordingly. Rights are allocated by PTM controlling server after receiving votes from all the users or at timeout. Obtained votes are calculated by using the formula:

$$\text{Votes Obtained} = \sum_{i=0}^{n} (4\ (\text{Voting power of each user is same}) * \text{Selected option by user } i) \rightarrow \quad (1)$$

n is the total number of users who are casting their votes.

After that total votes are calculated by using the formula:

$$\text{Total Votes} = \sum_{i=0}^{n} (4 * \text{value of the rights requested by new user}) \rightarrow \quad (2)$$

At the end percentage of obtained votes is calculated by using the equation:

Percentage of obtained votes = (Votes obtained / Total votes) * 100 → (3)

4.3.3 Decision Making

After calculating votes and percentage, PTM controlling server decides whether to allow this user to become member of the PTM session or not. If the user is allowed to become member then what rights should be allocated. For this purpose threshold values are configured and rights are allocated according to the threshold values. Threshold values that we have used in our experiments are listed in Table 4.2.

Table 4.2- Votes and Decisions

Percentage of obtained votes	Decision
< 20%	Not allowed
> 20%	Listener Only
> 35%	Listener and Watcher
> 50%	Speaker only
> 60%	Speaker and Listener
> 70%	Full rights

Since all the users are not allowed to send media so it first reduces the media contention. Reducing the media contention solves the scalability problem. More and more users can be added as listener and watcher only.

4.4 Media Mixing with Presence

We take 10 members all with full rights. These 10 members include Alice, Bob, Carel, Duminy, Ellen, Freddy, Gllen, Quetra, Paul, and Shan. We assumed that Alice has some secretes to share with Carel, Dumminy, Freddy, Paul and Shan therefore it does not want to send media to Bob, Ellen, Gllen and Quetra. However Alice is willing to receive media from all the members of the session. Similarly other members also have some conflict with one another and want to share some information only with selected members of the session. Table 4.3 shows the detail who wants to send and receive media to whom.

Table 4.3: Preference Rules

User	Send To	Receive From
Alice	Carel, Duminy, Freddy, Paul, and Shan.	Bob, Carel, Duminy, Ellen, Freddy, Gllen, Quetra, Paul, and Shan.
Bob	Alice, Carel, Paul, and Shan.	Alice, Carel, Paul, and Shan.
Carel	Alice, Bob, Duminy, Freddy, Paul, and Shan.	Alice, Bob, Duminy, Ellen, Freddy, Gllen, Quetra, Paul, and Shan.
Duminy	Alice, Bob, Carel, Ellen, Freddy, Gllen, Quetra, Paul, and Shan.	Alice, Bob, Carel, Freddy, and Shan.
Ellen	Alice, Bob, Gllen, Paul, and Shan.	Alice, Bob, Gllen, Paul, and Shan.
Freddy	Bob, Carel, Duminy, Gllen and Quetra,	Alice, Bob, Duminy, Ellen, Gllen and Quetra
Gllen	Alice, Bob, Carel, Duminy, Ellen, Freddy, Quetra, Paul, and Shan.	Alice, Bob, Carel, Duminy, Ellen, Freddy, Quetra, Paul, and Shan.
Quetra	Alice, Bob, Carel, Duminy, Ellen, Freddy, Gllen, Paul, and Shan.	Alice, Bob, Carel and Duminy
Paul	Bob, Carel, Duminy, Freddy and Gllen	Bob, Carel, Duminy, Freddy, Gllen and Quetra
Shan	Alice, Bob, Carel, Duminy, Ellen, Freddy, Gllen, Quetra, and Paul	Carel, Freddy, Gllen and Quetra

Table 4.4: List of Senders and Receivers After Media Mixing (Nazish et al. 2010)

User	Send To	Receive From
Alice	Carel, Duminy, Freddy	Bob, Carel, Duminy, Ellen, Gllen, Quetra, Shan.
Bob	Alice, Carel, Paul	Carel, Paul, Shan.
Carel	Alice, Bob, Duminy, Paul, Shan.	Alice, Bob, Duminy, Freddy, Gllen, Quetra, Paul, Shan.
Duminy	Alice, Carel, Freddy, Gllen, Quetra, Paul	Alice, Carel, Freddy, and Shan.
Ellen	Alice, Gllen	Gllen
Freddy	Carel, Duminy, Gllen	Alice, Duminy, Gllen, Quetra
Gllen	Alice, Carel, Ellen, Freddy, Paul, Shan.	Ellen, Freddy, Quetra, Paul, Shan.
Quetra	Alice, Carel, Freddy, Gllen, Paul, Shan.	Duminy
Paul	Bob, Carel,Gllen	Bob, Carel, Duminy, Gllen, Quetra
Shan	Alice, Bob, Carel, Duminy, Ellen, Gllen	Carel, Gllen, Quetra

Now when all the users have specified their rules, Controlling PTM server mix these rules and devise a new table consisting of the exact entries that what information should be delivered.

Instead of sending the media blindly to all the members of the session we proposed a presence based media mixing solution. At the start of the PTM session the PTM server subscribes the presence information of all the members of the session. If a new user is added to the session then first of all its presence is subscribed by the PTM server. After receiving the media from a user, PTM server first matches it with the send/receive rules. After deciding that this media will be forwarded to how many users PTM server checks the presence information of the intended receivers. If the presence information states that a particular receiver is not available then media is not forwarded to that user. It results in more efficient utilization of resources. Only those users will receive the media whose presence information show that they are willing to receive it. Details are shown in Figure 4.11.

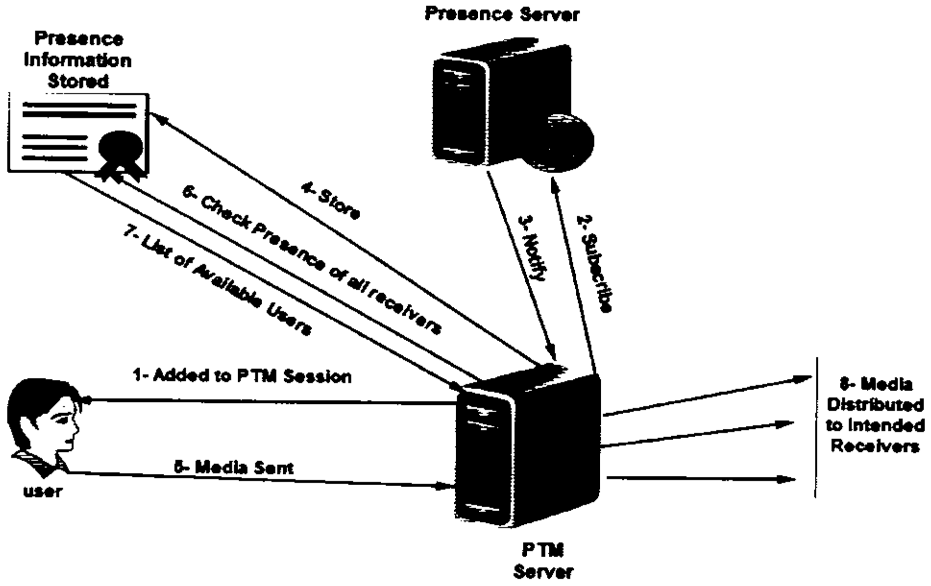

Presence Server
Presence Information Stored
4- Store
6- Check Presence of all receivers
7- List of Available Users
3- Notify
2- Subscribe
1- Added to PTM Session
5- Media Sent
user
8- Media Distributed to Intended Receivers
PTM Server

Figure 4.11: Media mixing with presence

We described the scenario by adding a "presence" and "list of final receivers" column in the Table 4.5. "Presence" column shows the availability of the users listed in "send to" column. Final list is prepared by applying "and" operation on "send to" and "presence" column. If a user is listed in "send to" column and its presence information is also available only then it can be added in list of final receivers. In the Presence information column of the Table 4.5 "Y" shows that user is available to receive the media and "N" shows that user is not available to receive media.

4.5 Election Based Distributed Deletion Mechanism

To successfully delete a malicious user from an on-going PTT and PTM session an Election Based Distributed Authority mechanism is designed. In this mechanism whenever an authenticated user finds that one of the other users is acting as a malicious user, it sends a request to delete that user from the session.

Table 4.5: Media Mixing With Presence

User	Send To	Receive From	Presence Information	Final List of Receivers
Alice	Carel, Duminy, Freddy	Bob, Carel, Duminy, Ellen, Gllen, Quetra, Shan.	Y, Y, N	Carel, Duminy
Bob	Alice, Carel, Paul	Carel, Paul, Shan.	Y, N,Y	Alice, Paul
Carel	Alice, Bob, Duminy, Paul, Shan.	Alice, Bob, Duminy, Freddy, Gllen, Quetra, Paul, Shan.	Y, N, Y, Y, Y	Alice, Duminy, Paul, Shan.
Duminy	Alice, Carel, Freddy, Gllen, Quetra, Paul	Alice, Carel, Freddy, and Shan.	Y, Y, Y, Y, Y, N	Alice, Carel, Freddy, Gllen, Quetra
Ellen	Alice, Gllen	Gllen	Y, Y	Alice, Gllen
Freddy	Carel, Duminy, Gllen	Alice, Duminy, Gllen, Quetra	Y, N, N	Carel
Gllen	Alice, Carel, Ellen, Freddy, Paul, Shan	Ellen, Freddy, Quetra, Paul, Shan.	Y, Y, Y, N, N, Y	Alice, Carel, Ellen, Shan
Quetra	Alice, Carel, Freddy, Gllen, Paul, Shan	Duminy	Y, N, Y, N, Y, N	Alice, Freddy, Paul
Paul	Bob, Carel, Gllen	Bob, Carel, Duminy, Gllen, Quetra	Y, Y, N	Bob, Carel
Shan	Alice, Bob, Carel, Duminy, Ellen, Gllen	Carel, Gllen, Quetra	Y, Y, N, N, Y, Y	Alice, Bob, Ellen, Gllen

The controlling server receives the deletion request and starts an election among the members of the session by sending a "cast_vote" message. All the members are required to cast their votes as either agree or disagree. The user against whom the election is conducted is not allowed to cast the vote. If user does not cast the vote until timeout then that user is not considered in overall result calculation. The timeout value is predefined by the session imitator. After getting response from all the users or at timeout the controlling server calculates the votes. If the votes to delete that user from the session exceed more than a predefined threshold value (i.e. 75%) the controlling server deletes that user from the session.

If it does not exceed the threshold value then the user remains a part of the session. This feature can be misused by an attacker to waste the network resources by sending too many deletion complaints. To handle this situation whenever controlling server finds that the deletion requester is not correct (the election votes do not exceed the threshold value), it issues a warning to election initiator. If election initiator repeats that mistake and sends another deletion request and again the request fails to get the required vote, the controlling server deletes the requester from the session. In this way a user can send maximum two wrong deletion requests. Figure 4.12 shows the scenario in detail.

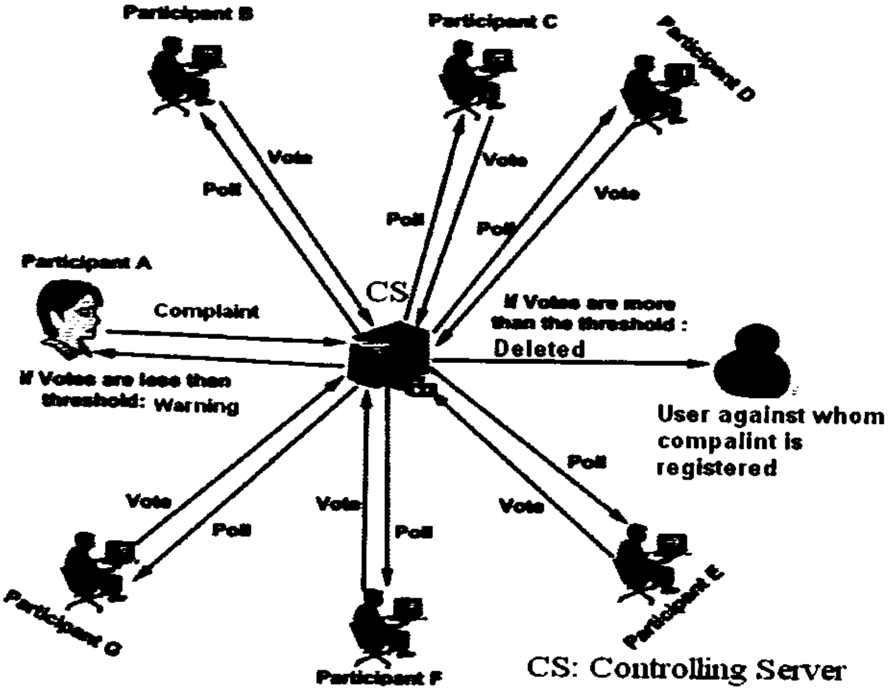


Figure 4.12: Election Based Distributed Deletion Mechanism

4.6 Allocation of Maximum Floor Control Time

Talk burst control protocol (TBCP) is introduced to communicate various types of information between users and controlling servers. When controlling server finds that the current user is using the floor for a very long period of time it can revoke the floor by using TBCP_Revoke command.

But deciding it at the run time that when to revoke the floor requires continuous monitoring and run time decision by the controlling server. Secondly controlling server uses the same revocation time for all the users. We introduce a technique in which the session initiator defines the maximum floor time for all the users. The session initiator can set this time on per user basis. It means different time can be set for every user. For example if the session initiator thinks that a user A has more important data to share it can allow user A to keep the floor for a long period of time as compared to other users. Now there can be a situation in which a user may need floor for longer period of time while the session initiator allows to keep the floor for small period of time. User is allowed to send a request to controlling server for keeping the floor for longer period of time. The controlling server after getting the request again use the election base technique to decide whether to allow the user to keep the floor for longer period of time or not. If once a user is disallowed to use the floor for longer period of time, re-request is not allowed. It means in a session a user is allowed only once to request for longer floor control time.

4.7 Solutions to Problems Related to Multiparty Conference

In order to handle different types of flooding attacks and internal threats we developed an Intrusion Detection System. To reduce the chances of conflict among the existing participants of the conference service, we offer an election based distributed referring authority mechanism and to maximize the scope of the conference service in real life we introduce the concept of parameterized referring. Details of each solution are described below:

4.7.1 Intrusion Detection System

To mitigate the effect of invite flooding attacks and others we propose an intrusion detection system based on misuse detection component. Misuse detection detects the attack and penalizes the attacker before serving the request. Attack rules consist of comprehensive list of the rules related to every type of possible attack. Rules are defined with respect to the role. Blacklist contains the list of the users who try to attack over the network. These users are blocked for a particular period of time.

Rules can be called as signature. To formulate the signatures we obtain two dataset of signatures. First data set is obtained from The Cooperative Association for Internet Data Analysis (CAIDA) and the second data set is obtained from defense advance research project agency (DARPA) known as KDDCUP. Different quality attributes are configured to shortlist the most relevant signatures. We select 79 signatures from CAIDA and 39 signatures from KDDCUP. Signatures are selected on the basis of different quality attributes those are explained below.

- False Positive
- False Negative
- Completeness
- Breadth
- Precision
- Recall

- Collision

When an application server receives a request for conference server then instead of forwarding it directly to conference server the application server sends it to a middleware based intrusion detection system. This intrusion detection system is equipped with the set of rules about each type of attack. This module after receiving the request first matches it with the blacklist. If that user's ID exists in the blacklist the request is discarded. If the user does not exist in the blacklist then the misuse detection module matches it with the attack rules. If the request matches with any of the attack rules it is considered as an attack and is discarded immediately. After discarding the requests the attacker is put into the blacklist for certain period of time. Here we also describe the mechanism for the blacklist timings. The blacklist timings depend upon the attacker. If it is particular user's first attempt to attack, it is blacklisted for few minutes but if user again tries to attack after getting out from the blacklist then its blacklist timings are doubled from the previous timings. For this purpose a counter is initialized for every attacker whenever it makes first attempt to attack. With every subsequent attack request the counter is incremented by one and the blacklist timings are doubled from the previous timings. If the request does not match with any of the attack rules it is considered a legitimate request and forwards to the conference server. Conference server serves the request.

4.7.2 Election Based Distributed Referring Authority

Conference service allows a single participant to refer anyone to the conference. Therefore a participant may refer a person who is not acceptable by other participants of the conference. This situation can result into conflict. In order to prevent the conference service from these types of conflicts and to create friendly environment among the conference participants we develop an election based distributed referring authority mechanism. Whenever a participant wants to refer a person it initiates an election by sending a refer request to the conference server. Conference server starts polling by sending a Poll request to all the existing participants of the conference. The participants are required to cast their vote either with "yes" or "no". Yes for allowing the refer request and no to reject it. If a participant does not reply within the specified period of time it is automatically considered as "yes". After receiving responses from all the participants or at the end of the specified time, the conference server counts the votes. If a certain percentage (i.e. 60%) of the members replied in "yes" the refer request is entertained else it is discarded and the initiator is notified. Initiator's response is always counted as "yes". Figure 4.13 explains the scenario in detail.

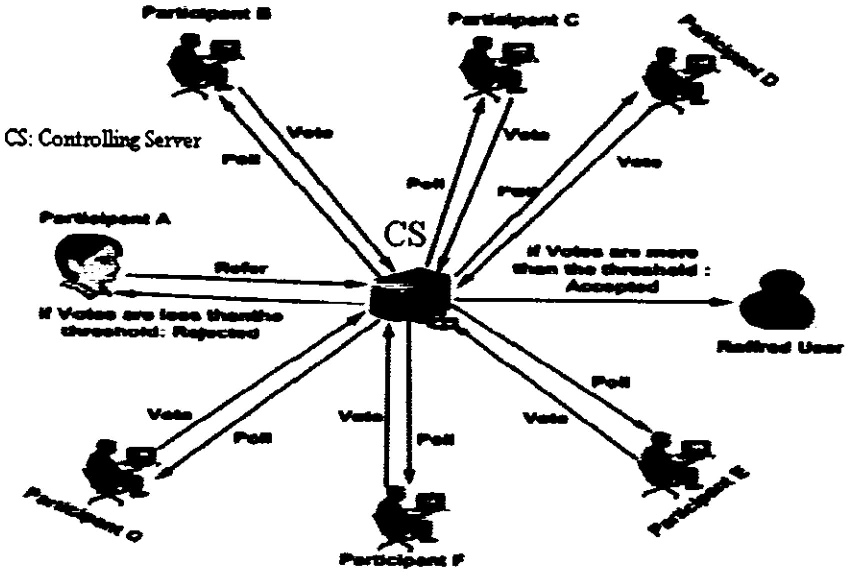


Figure 4.13: Election Based Referring Mechanism

Whenever a participant refers to some other person into the IMS conference, it becomes fully authorized member of the conference. There are many scenarios where we want to invite few persons as a passive member of the conference. Here passive means that the participant is not fully authorized for all types of action. The authority of the participant is limited i.e. only to watch the conference (Listening and speaking is not allowed). To accommodate these types of scenarios in the IMS conference we propose a parameterized refer request mechanism. Whenever a participant launches a refer request it also specifies the authority of the referred user along with the refer request. Authority represents actions that referred participant can take (watching, listening, speaking etc.). The details are shown in Figure 4.14. This mechanism reduces the load from the network by allowing only few users to send the media. Scalability that is the major problem with the conference server can be achieved through this mechanism by adding more and more passive users. If all the participants are allowed to speak in a conference then the decision about turn to speak may results in conflict. Since this mechanism can also reduce the number of users allowed to talk so this problem can be solved up to great extent.

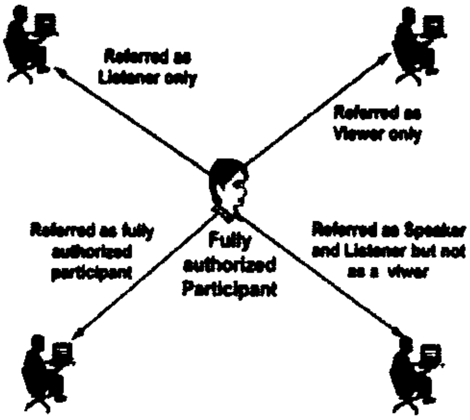

Referred as Listener only
Referred as Viewer only
Referred as fully authorized participant
Fully authorized Participant
Referred as Speaker and Listener but not as a viwer

Figure 4.14: Parameterized Referring

4.8 IMS and NGN Security

To improve the security of the IMS application servers and to make them more resilient against different types of attacks we propose a role based IDP that acts as a middleware between IMS core and application plane. S-CSCF has the authority to route the request towards the IMS application plane. When a request arrives at S-CSCF, it decides whether to route it towards application plane or in some other direction. Initial filter criteria are used to support the decision of S-CSCF. Top level view of proposed IDP is shown in Figure 4.15.

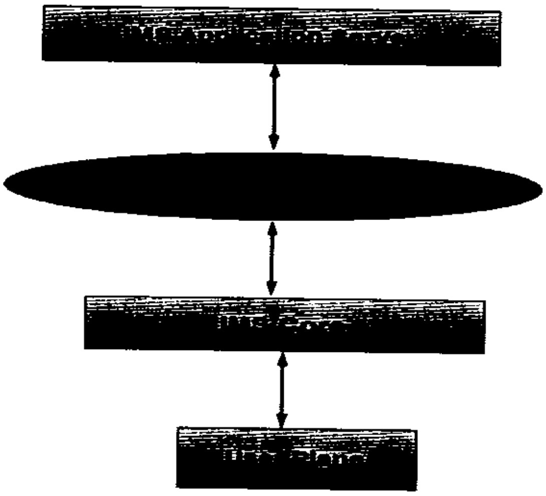


Figure 4.15: Top Level View and Placement of IDP System

The objective of IDP system is to protect IMS Application Servers (ASs) and secure SIP signaling on IP Multimedia Service Control (ISC) interface. The ISC interface connects AS with IMS core. The 3GPP has not standardized specific security solution to secure this ISC. We concentrate the security threats that IMS ASs have challenged, especially the SIP signaling attacks on this interface and general on the whole. The lower level attacks could be prevented by using low-level security mechanisms, e.g., Transport Layer Security (TLS) and IP security (IPsec) to secure the communication channel by encryption. The higher level attacks like SQL injections at application level are not mitigated by low-level security mechanisms. Hence, the task of IDP-AS is to detect and block such higher level attacks.

Since our IDP stands in-between IMS core and application plane so whenever S-CSCF route a request towards any application server first it is received by the IDP. Different components of our proposed IDP system are described in details as:

4.8.1 SIP Stack

It is the first component that receives the request and delivers the response. As soon as S-CSCF decides that it needs to route this request towards application plane, it forwards the request towards the SIP stack. We can say SIP stack entry works as an entry and exit point of our IDP.

4.8.2 Blacklist Configuration

As soon as an attack is identified the attacker is put into the blacklist. SIP stack after receiving request first checks the blacklist in order to ensure that sender is not in the blacklist. If sender is found in the blacklist, request is discarded immediately. Now the question is whether this blacklist will be fixed or dynamic. Fixed list means that it will be configured at the time of creation of network and after that it will remain static. But this solution is not flexible. How long an attacker will remain blacklisted is another question. We developed an adaptive algorithm for blacklist timings. As soon as an attack is detected, blacklist history is consulted and it is checked whether the user was in the blacklist earlier. If it is found from the history that this user has already blacklisted one or more times before launching this attack then it is put into the blacklist and its blacklist timings are increased on the basis of level of current attack and number of times for which that user was put into the blacklist. If the current request is the first time attack from that particular user then on the basis of level of attack it is decided whether to put this attacker into blacklist or just to give a warning. If it is decided that attacker will be put into the blacklist then the blacklist timings are again decided on the basis of level of attack.

4.8.3 Level of Attack

Attacks can be categorized into different levels based on severity. We define a number of signatures for different types of attacks and each signature has a particular level of severity that is assigned at the time of formulation and verification of that signature. When a request matches with a signature, it is checked what is the level of attack associated with that particular signature.

4.8.4 Role Formulation

There exists no network where all the users have same rights and preferences. Rights and preferences of the users vary according to their requirements. We assigned different roles to different users on the basis of rights allocated to the users. These roles are defined at the time of registration and can be changed through re-register procedure. Whenever S-CSCF receives a register request it issues a challenge to the users, upon receiving a challenge it downloads the user's profile from HSS. At the time of downloading user profile and adding user's registration its role is defined on the basis of different packages subscribed etc. To store the user's roles a table is added to the HSS. This table can be copied by the IDP system or IDP system can get direct access to HSS. Direct access to HSS is not a good solution so we prefer that whenever there is change in the role table it is copied to the IDP through S-CSCF. IMS users are divided into three priority roles.

- High Priority Role: A user with more privileges is ranked as high priority user
- Medium Priority Role: A user with average privileges ranked as medium priority user
- Low Priority Role: A user with low privileges is ranked as low priority user

4.8.5 Signature Formulation

Attack signatures are defined to detect the attacks. All the well known attacks have some patterns and those patterns are defined and listed by many of the research organizations and many of the IDP systems. We collected two data sets of signatures and shortlist few signatures from those data sets. The first data set is known as KDDCUP and it is obtained from DARPA. It contains about 14000 pages on which thousands of signatures are listed. Second data set is obtained from Cooperative Association for Internet Data Analysis. After getting the data set we short list few of the rules related to SIP based DoS attacks. In order to short list the rules first we collect all the rules related to SIP and DoS attacks. After that we identify the attack signatures on the basis of time, severity, and lower level protocols. We only selected the attack signatures which were defined after 2004 and whose severity level is more than 5. Since SIP mostly works with UDP so we take only UDP based signatures. After getting the signatures we verify them through various tests. These tests include header analysis, payload analysis and state base analysis. At the end of signature verification 286 rules are selected from KDDCUP and 521 rules from Cooperative Association for Internet Data Analysis. We also define few new signatures according to our test case requirements. Signatures are also divided into two more categories on the basis of time dependency.

To start our IDP first S-CSCF sends a request towards SIP stack, SIP stack checks the blacklist and if a user is found in the blacklist the request is discarded. If user is not found in blacklist then the user is added to partner list and its role is extracted from the table. Signatures are divided into three categories depending upon the type of roles. Every role has different list of signatures and within a list signatures are sorted on the basis of severity. Signatures of major attacks are put on top and signatures of minor threats are placed at the bottom of the list. After retrieving the role the request is matched with the signatures. If request is matched with any of the signature, it is discarded immediately and level of attack is checked. We define 10 levels of attacks and all the signatures are divided into these 10 levels. Higher level represents more severe attack. So when an attack is detected the user is put into the blacklist and it remains into the blacklist for the number of minutes equal to the level of attack. After getting out from the blacklist if the same user retry to attack then it will again put into the blacklist and this time blacklist timing will be equal to level of this attack multiply by sum of previous blacklist timings. If the request does not match with any of the signatures, it is considered as legitimate request and an "OK" response is forwarded towards S-CSCF who forwards the request towards application server. Detail architecture of IDP is given in Figure 4.16.

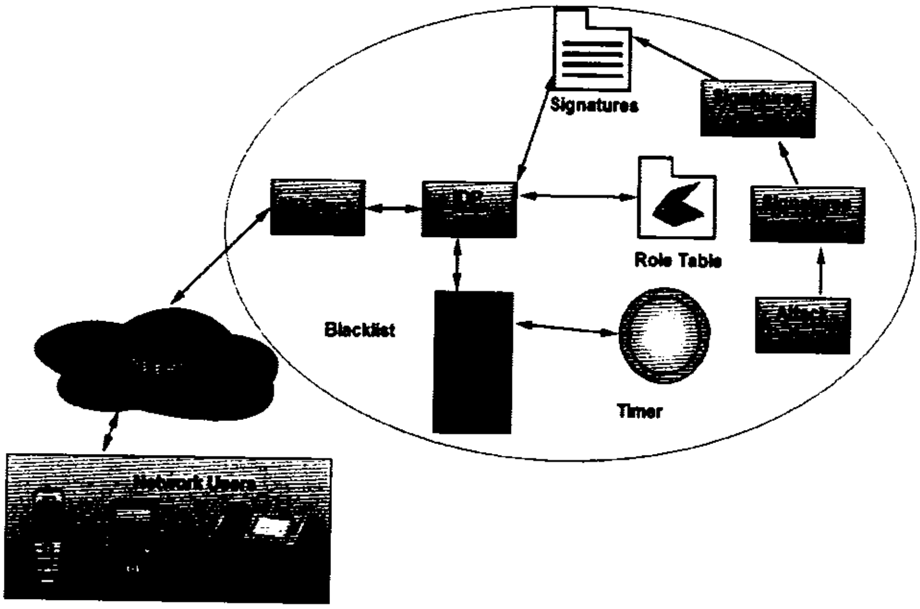


Figure 4.16: Architecture of the IDP System

To detect time-independent (TI) attack, the IDP-AS compares the message with defined attack rules, if matches, it turns the procedure attack detected, and announces the detection and block the message, otherwise the message is regarded as secure and is forwarded to the SIP Server.

To detect time-dependent (TD) attacks, the partner has a timer to perform periodic checking the state of user. As timer is triggered, a comparison between the current state of partner & the defined attack rules will be carried out: if matches, the procedure attack detected takes over the control. The further messages to or from the UE will be blocked.

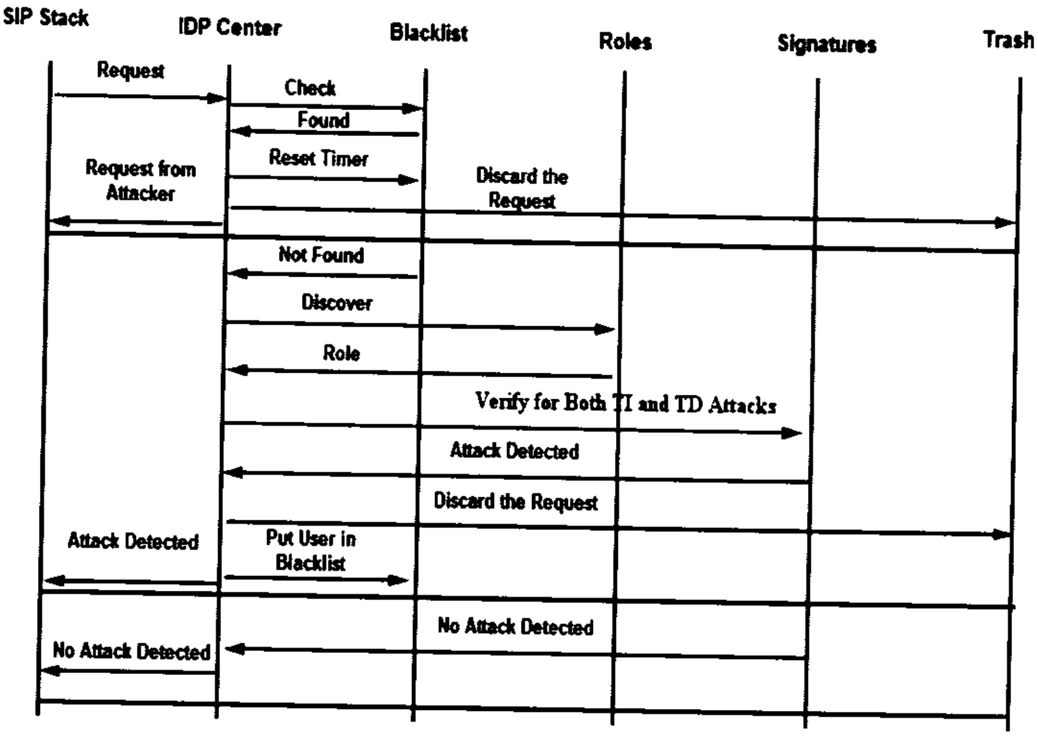


Figure 4.17: Sequence Diagram of Proposed IDP System

4.9 Testing of Non-Evolutionary Algorithms

In anomaly detection module we started the implementation of the testbed with the deployment of IMS core. IMS core consists of four main components. First P-CSCF, entry point for the users, is configured with support of security association and Session Initiation Protocol (SIP) compression features. For the whole core network we use IMS open core. I-CSCF is also configured to find out the appropriate S-CSCF. Finally S-CSCF is configured with routing and registration support. Boarder gateway control function is deployed to exit from the IMS network. Signaling gateway is also configured for the non-IMS users. ISC interface is used to create a contact between S-CSCF and the application server. Mw interface connects the CSCF with each other. Last step in IMS core deployment is the configuration of HSS. It was Cx interface that is used for interaction between HSS and CSCF.

Next step is to configure the client. To configure the client we use SIP-P. SIP-P is a tool that can generate IMS clients with full functionality. We divide the clients into three different groups. First group of client is named as Legitimate group and all the clients in this group act normally and communicate by following the standard communication procedures. Second group of clients is named as Flooding clients. In this group all the clients send bulk of SIP requests towards the core network to create effect of denial of service. Third group is named as Malformed clients and the nodes of this group sends attack packets (excluding flooding attacks) towards the core network. These attacks mainly include invite to death and SQL injection. To create malformed attacks we use two different tools. First tool is known as Codenomicon and second tool is SIP security evaluation tool.

Third step was to create dataset. To create dataset we deployed two sniffers. The first sniffer is deployed on Gm interface between the Legitimate client group and the P-CSCF and the second sniffer is deployed on the Gm interface between other two groups and P-CSCF. Wireshark is used to sniff the packets. Both the sniffer after sniffing the packets sent them to an offline analysis machine. Now the offline analysis machine consists of two datasets. First that is obtained from legitimate clients and the second that is obtained from malicious users. After that 10 fold cross validation technique is deployed to train and test the data. In the training phase the system learns the rule and behavior and on completion of the training phase those rules are tested on real time packets. Feature extraction module after extracting the features forwards it to classifier. Detail of feature extraction module is given below. Classifier ends with different types of rule those can be used as an anomaly detection tool. It is classifier's responsibility to decide whether the packet contains an attack or not. If a packet contains an attack it will be considered as malicious packet otherwise it will be accepted as legitimate packet. Figure 4.18 is explaining the structure of the testbed in detail.

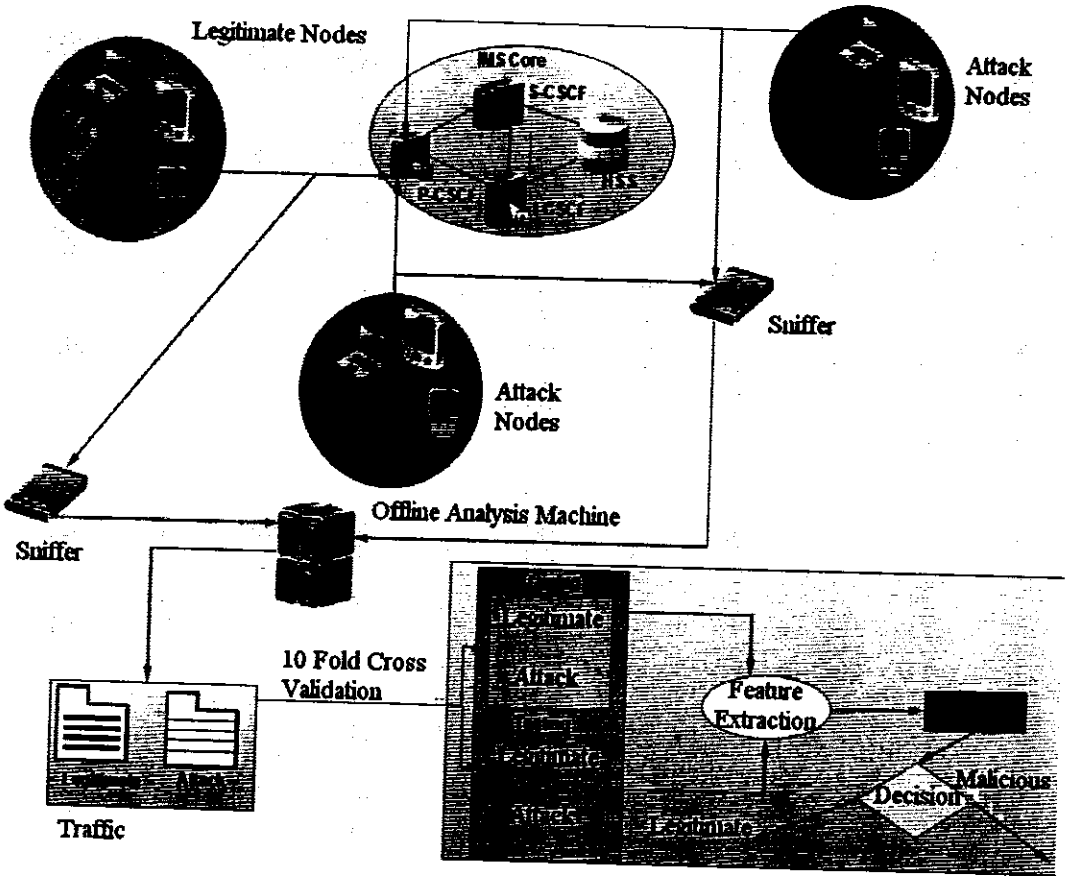


Figure 4.18: Testbed for Anomaly Detection

4.9.1 Feature Extraction

As SIP is request/response based protocol so features are extracted from both types. So far as flooding is concerned the first feature is the quantity (Zubair et al. 2009). Here quantity refers to the number of SIP request and response messages generated. These SIP messages include Register, Invite, Subscribe, 200 Ok, Bye, Cancel, Re-Invite, 100, 481, etc. Errors are also counted including the client and server errors. Time duration is another feature that needs to be extracted, in how much time how many requests are arrived from particular source gives us a good idea to predict a flooding attack. User's role is another feature without which it is not possible to get high success rate. Users are classified into three different groups and each group has different preferences. Group one with higher priority can send more SIP requests as compared to users of group three who are low priority users.

Feature in malformed packets are ranked on the basis of statistics and information theory measures. The most popular parameter is the information gain. Through information gain uncertainty is reduced by having prior knowledge (Cover et al. 2006). Entropies H(C) and H(F) defines the uncertainty with class attribute C and feature F. Mathematically the information gain of F with respect to C is shown in the equation below:

$$IG(C; F) = H(C) - H(C|F) \qquad (1)$$

Y is considered as value of legitimate dataset and z is for the malicious dataset. For a given probability p(θsi), IG can be computed by:

$$IG(y; z) = -(\frac{y}{y+z}).log_2(\frac{y}{y+z}) - (\frac{z}{z+y}).log_2(\frac{z}{z+y}) \qquad (2)$$

4.9.2 Classifier

In this paper our focus is on non-evolutionary classifiers. We have selected four well known non-evolutionary classifiers. Reason of selecting these classifiers is there goodwill in the available literature (Akbar et al. 2009). Now we will provide a little detail of each of the four selected classifier.

A. **Support Vector Machine :** In this classifier Instances of different classes are differentiated by creating decision boundaries (hyper plane). It is commonly used for two class problem (Lewicki et al. 2006).

B. **C4.5 Algorithm :** Feature set is mapped over a specific class and from training data a decision tree is generated. This decision tree is applied recursively on the subset of the features. Only those attributes are considered the part of the final classification which gain largest set of information (Quinlan et al. 1996).

C. **Naîve Bays Algorithm :** In this probabilistic classifier it is assumed that there is no statistical relation between presence/absence of an attribute. This algorithm has shown good results in many real life scenarios (Rish et al. 2001).

D. **Inductive Rule Learner :** By using greedy induction this algorithm creates rule-set. It is also known as Repeated Incremental Pruning to Produce Error Reduction (RIPPER). Postpass optimization is performed over the rule-set to achieve the fitness. Cross validation techniques are also used to mitigate the chances of over fitting (Han et al. 2006).

4.9.3 Legitimate Dataset

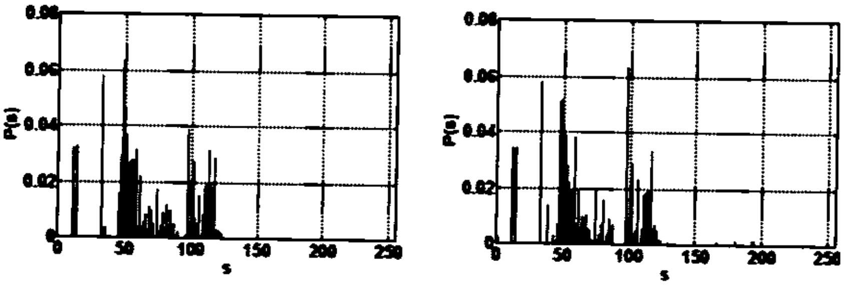
The original SIP traces are very important for our study as it help us to perform accurate analysis of IMS traffic. Therefore, the real world benign dataset for out study has been collected from an operational IMS service provider in our region. The service provider provides services to a large number of users and to several enterprise entities. We developed a SIP traffic logger and deployed it on the P-CSCF of IMS core in order to sniff a real world SIP traffic of more than 30 days. The log contains traces of various SIP dialogues from multiple users in form of SIP request and response messages.

4.9.4 Malicious Dataset

We have created a testbed to generate malicious SIP requests targeting the IMS architecture. Our testbed consists of Open IMS Core (FOKUS, 2006): an open source implementation of IMS Call Session Control Functions (CSCFs) and a lightweight Home Subscriber Server (HSS). We launch attacks on the IMS core by using our customized SIP Security Evaluation Tool. The tool is capable of launching several thousand malicious SIP requests to the server on a pre defined attack rate. We also use the security testing tool by Codenomicon Defenses to produce anomalous SIP messages containing syntactical anomalies, format string and input validation vulnerabilities. While collecting datasets from variety of tools, we ensure that no evident artifacts are commenced in malicious dataset that makes the detection instinctively undemanding. This makes our dataset diverse containing wide set of malicious messages and real world exploitation test cases. We sniffed the malicious requests at P-CSCF of an IMS core to perform our analysis.

4.9.5 Analysis of Dataset

As discussed earlier, SIP is a text-based protocol therefore we start our analysis with the byte-level(character) distribution of IMS traffic to detect malicious packets. Figure 4.19(a) and 4.19(b) show the byte-level distribution of benign and malicious dataset. It can be clearly seen that the occurrence probabilities of tokens, characters and other syntactical attributes in benign and malicious packets do not show large variance. Therefore, it can be intuitively argued that byte-level distribution of malicious packets do not change because the malicious content is averaged out by the whole packet size. This strategy of entrenching small malicious content is frequently adopted to make them fit inside buffer overflows/unused fields to evade detection of malicious packets.



a) Legitimate Data b) Malicious Data

Figure 4.19: Byte Level Distribution

4.9.6 Modeling of Byte-Level Distributions

We present the SIP packet S as sequence of bytes S = {s0, s1, s2.......sl} , where l is the length of the SIP message. With no loss of generality, we can also treat every successive n bytes in S as our input attributes to classification module. This is commonly referred as n – gram feature space, where the frequency of n bytes in S acts as a measure of its importance in S. The right choice of the value of n plays a critical role in such systems: if n is too small, the probability of false detection increases; otherwise if we choose large value for n, it significantly increases the processing overhead making the framework infeasible for real time systems. For real-time detection of malicious packets, we need a model that not only extracts the relevant underlying information but it should be efficient in term of throughput of the system. We therefore modeled the byte-level distribution of S in k states i.e . $\Theta s = \{ \Theta s_0, \Theta s_1, \Theta s_2, ... \Theta s_k\}$. The transaction function ψ operates on the byte level distribution of each incoming packet S and embeds the spatial information in the form of probability of state transitions. With each byte value si, such that si→ Θsi, we computed the transition of byte si+1 followed by the byte si as $t_{\{\Theta i,\ \Theta i+1\}}$ and the probability of state transition as p{Θi, Θi+1}. The transition probabilities of k states are represented in Probability matrix P(Θs), with dimensions kxk (k = 2^8 in case of byte level distribution). Mathematically the entrenching function ψ is represented as:

$$\psi(S) \rightarrow (P(\theta_s))_{\theta_s \in S} \quad (1)$$

with each row $0 \leq i \leq k$ of $P(\theta_s)$ satisfies the condition

$$\sum_{\theta_{si}=1}^{\theta_{si}=k} p(\theta_{si},\theta_{si+1}) = 1 \quad (2)$$

We computed the probability transition matrix during the training phase from the benign packets. While computing the P(Θs) we assume that the transition between byte values follows the Markov property. We consider each probably in P(Θs) as a potential attribute for our classification module. However, there can be few states that do not contain valuable information for classification module. For example, Figure 4.20 depicts that the occurrence probability of certain byte values is zero in benign traffic making the corresponding state transition probabilities p(Θsi) = 0. Therefore, it makes perfect sense to remove redundant features – having low classification potential – from P(Θs) and it should not degrade the false alarm rate. The removal of redundant features will also reduce the dimensionality of probability transition matrix: as a result better through put can be achieved.

The IG value near to 1 depicts higher classification potential of transition probabilities.

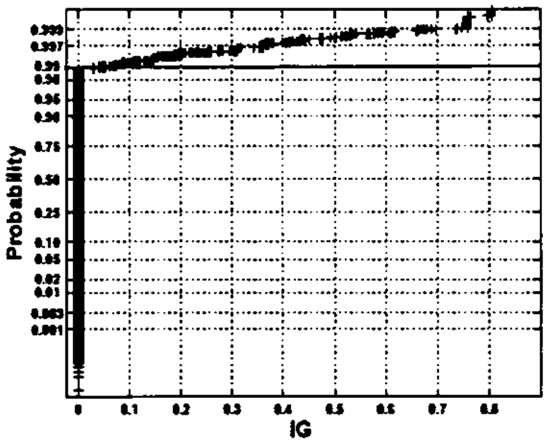


Figure 4.20: Normal Probability Graph of IG Values

4.10 Chapter Summary

In this chapter we discussed different frameworks and the methodology to solve the problems related to IMS based multimedia services. So far as presence is concerned we presented presence enabled conditional call setup mechanism and presence triggered automatic call mechanism. In presence enable conditional call setup we proposed that for occasional calls user is not needed to subscribe the presence service. Presence is used during the call setup process. On one hand this solution educes the load from the air interface and on the other hand it reduces the overall delay. In presence triggered call setup we proposed that presence condition will be stored and upon getting the correct response from presence server, the S-CSCF automatically generates a call. For instant messaging, security solutions like three layer secure architecture, presence and preference based secure solutions are presented. In three layers secure architecture layer one takes the preferences from sender and hence reduces chances of misuse and spoofing. Layer consists of an IDP system that tries to detect an attack and the third layer takes the receiver preferences and minimizes the disturbance problem and targeted attacks. In other solutions presence service is used to reduce the chances of message flooding attack on targeted users. Election based rights allocation, deletion and floor control mechanisms, media mixing with presence are the solutions proposed for PoC and PTM. In election based rights allocation a user gets the rights on which all the other participants agree. Maximum floor control time is also allocated to the users on the basis of their role in the session. Media mixing algorithm takes the preferences of all the users and deliver the media according to those preferences. Distributed and Limited rights referring solutions are developed for multiparty conference. IDP system based on misuse detection and anomaly detection modules is developed to secure the application servers from different types of flooding and other attacks. In misuse system first time we introduced the role of the user in attack detection. Secondly we also consider the severity of the attack. A new blacklist algorithm is also proposed to penalize the attacker in case of attack detection. In anomaly detection module we tested four non evolutionary algorithms. Till now, according to our best knowledge, non evolutionary algorithms are never used in IMS for increasing the security.

CHAPTER 5

5. RESULTS AND DISCUSSION

In this chapter we discussed the testing platform, test scenarios and results. After that results are elaborated in detail.

5.1 Testbed Environment

To obtain the results of the proposed scenario we tested it on an IMS testbed. The testbed consists of IP phones (Soft Phones), IMS core and IMS application server. First we download an open source IP phone and modify its working to enable it to work with our testbed. After that IMS core open source is downloaded and configured accordingly. The IMS core that we configure consists of 4 major components. First we configure the P-CSCF and all its relevant features like PDF, IPSec association etc. After that I-CSCF is configured. S-CSCF is also configured with routing protocols, registration and AKA mechanism, initial filter criteria etc. HSS is prepared with all the relevant tables to store user and network specific data. On the top of the IMS core we develop a prototype of IMS application server that can be accessible through ISC interface. Layout of the testbed is shown in Figure 5.1.

A prototype of presence service is developed and configured in order to obtain the results.

5.2 Case 1: Presence Based Conditional Call

In order to evaluate presence based conditional call setup mechanism we developed a case consisting of four scenarios. In first scenario we routed call from one soft phone to another soft phone those are placed at long distance.

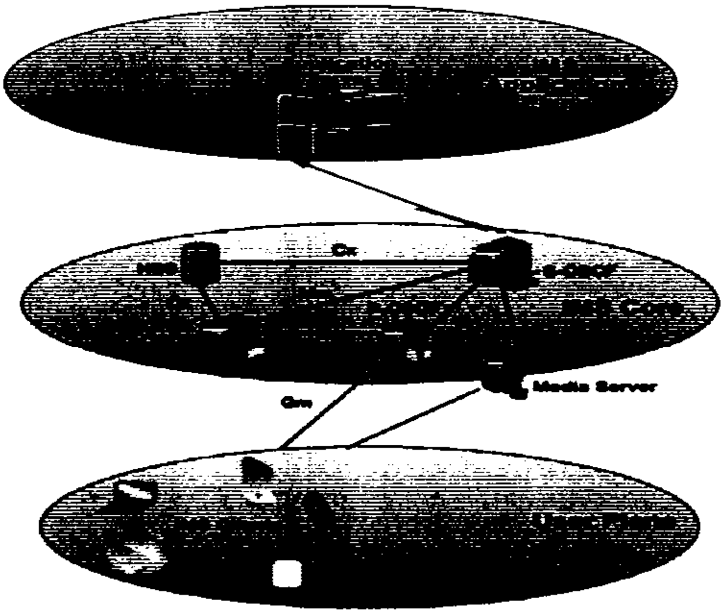


Figure 5.1: Testbed Scenario

900 Kilometers are considered as a long distance. By generating a lot of useless traffic over the network we determined the results at different traffic loads. The first scenario is the one in which two communicating parties exist at long distance and the load on the network is normal. We take 25% to 30% load as normal. In the 2nd scenario we routed a call from one soft phone to another soft phone those were placed in one building. This experiment is also conducted at normal load. In 3rd scenario users are placed at long distance and results are measured at heavy load. 70% to 75% load is treated as heavy load. In 4th scenario users are placed in same building and results are measured at heavy load. In the last set of experiments we checked average number of messages exchanged over the air interface.

5.2.1 Results of Scenario 1

In the first set of experiments we calculate the average delay in normal call setup. It is almost the same as described in ITU E.721 recommendations. These delays are also verified by many research articles (Mahmood et al. 2009). We also calculate the presence subscription and un-subscription delay including notifications. At the end we calculate the overall delay in conditional call setup. We find that in conditional call setup, delay is very much lower as compared to total delay of presence subscription, call setup and presence un-subscription.

We find that call setup delay in normal scenario is 8 seconds. After that we calculate the delay of presence subscription and presence un-subscription. Collective delay of presence subscription and call setup is found as 10.5 seconds. Collective delay of presence subscription, presence un-subscription and call setup is 12.9 seconds. Call setup delay of our proposed conditional call setup model is calculated and delay of 8.9 seconds is found. We plot the graph of total delay by generating 120 calls. Figure 5.2 explains the results in more detail.

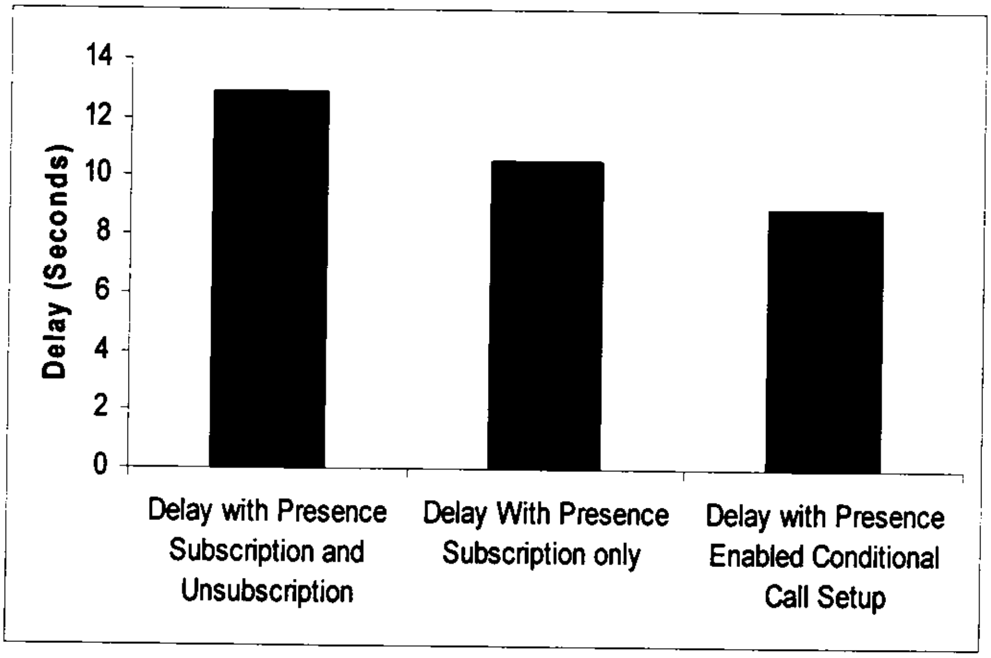


Figure 5.2: Delay of Long Distance Calls With Normal Load

5.2.2 Results of Scenario II

In the second experiment we check the overall delay in local call setup. We find that call setup delay in normal scenario is 3 seconds. After that we calculate the delay of presence subscription and presence un-subscription. Collective delay of presence subscription and call setup is found as 5.1 seconds. Collective delay of presence subscription, presence un-subscription and call setup is 7 seconds. Call setup delay of our proposed conditional call setup model is calculated and delay of 3.8 seconds is found. We plot the graph of total delay by generating different number of calls.

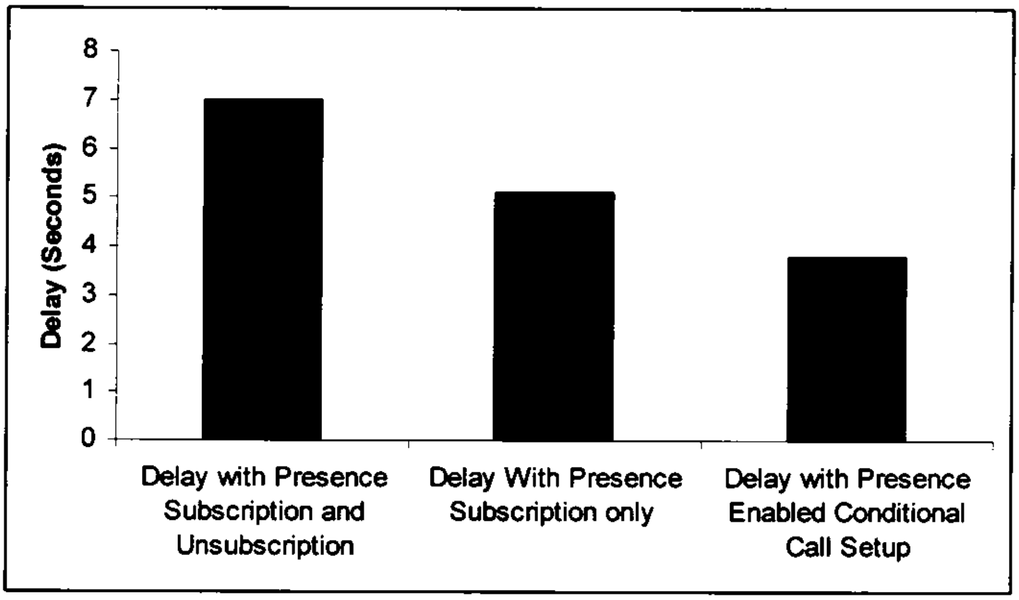


Figure 5.3: Delay of Local Calls With Normal Load

5.2.3 Results of Scenario III

In the third experiment we check the overall delay in long distance call setup under heavy network load. We find that call setup delay in existing scenario is 12 seconds. After that we calculate the delay of presence subscription and presence un-subscription. Collective delay of presence subscription and call setup is found as 15.7

seconds. Collective delay of presence subscription, presence un-subscription and call setup is 19.1 seconds. Call setup delay of our proposed conditional call setup model is calculated and delay of 13.2 seconds is found. We plot the graph of total delay by generating different number of calls.

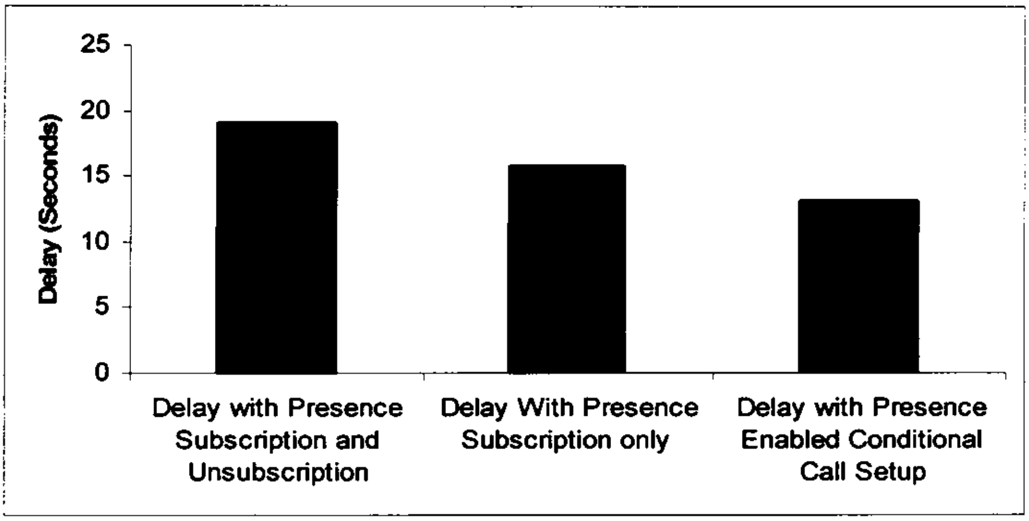


Figure 5.4: Delay of International Calls With Heavy Load

5.2.4 Results of Scenario 1V

In the fourth experiment we check the overall delay in local call setup under heavy network load. We find that call setup delay in existing scenario is 4.5 seconds. After that we calculate the delay of presence subscription and presence un-subscription. Collective delay of presence subscription and call setup is found as 7.8 seconds. Collective delay of presence subscription, presence un-subscription and call setup is 10.6 seconds. Call setup delay of the proposed conditional call setup model is calculated and delay of 5.6 seconds is found. We plot the graph of total delay by generating different number of calls.

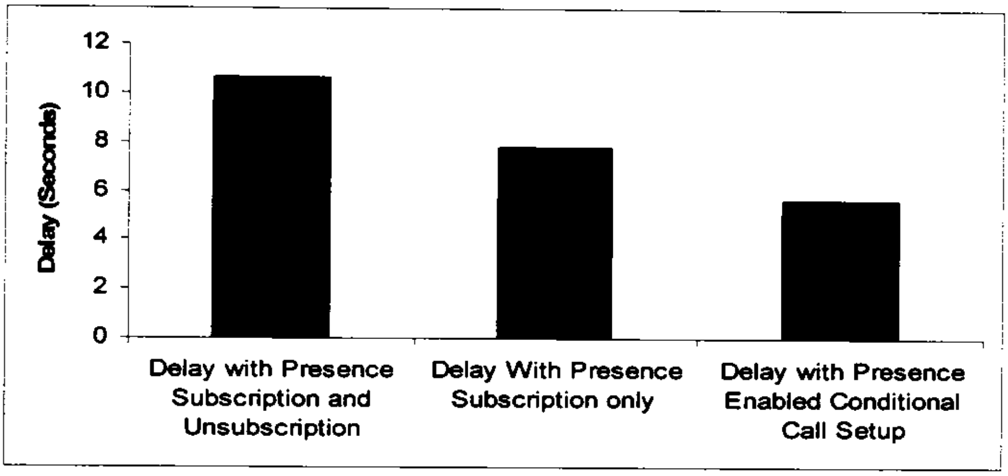


Figure 5.5: Delay of Local Calls With Heavy Load

5.2.5 Results of Scenario V

In case of subscribe before call the number of messages exchanged for presence service subscription are not required for conditional call. Figure 5.6 shows that the number of messages exchanged for different number of calls require far more messages in the traditional mechanism as compared to our conditional call mechanism. The presence subscription process requires exchange of 4 messages. Therefore the traditional subscribe before call mechanism requires total exchange of 5 messages to send a presence based call setup request 'Invite' (4 messages for presence subscription and one for SIP Invite request). While in our presence enabled conditional call mechanism only one request is exchanged at the air interface of the watcher. (Presence condition enabled SIP Invite request).

The procedure of Un-subscribing the presence service is very much similar to the subscription procedure. The only difference is that instead of sending the 'Subscribe' request, a watcher sends a 'Subscribe' request with expiry time equals to zero. Since presence notifications are generated after every change in the presence information of the subscribed attributes so it puts high load on the network as well as on watcher's device.

If the only purpose of the watcher is to get presence information to route a call then in traditional process first it needs to subscribe for the presence information and after making the call it needs to unsubscribe the presence information in order to avoid unnecessary notifications. In our presence enabled conditional call mechanism a watcher neither need to subscribe for the presence information nor does it require unsubscribing it.

The presence subscription process requires exchange of 4 messages and un-subscription also requires exchange of 4 messages. Therefore in this case the traditional subscribe before call mechanism requires total exchange of 9 messages (4 messages for presence subscription, 1 for SIP Invite request and 4 for presence un-subscription) to send a presence based call setup request 'Invite' if the caller does not require presence information after the call. In our presence enabled conditional call mechanism since there is no presence subscription so un-subscription is also not required. Therefore only one message is exchanged between caller and P-CSCF (presence condition enabled SIP Invite request).

5.3 Case 2: Three Layer Secure Architecture

To test the validity of the three layer secure architecture, we take four users. Two users with IP addresses 92.168.10.1 and 192.168.10.2, respectively, play the role of senders. We named them as "user A" and "user B," respectively. A's priority is set as 3 and B's priority is set to 1 (higher number shows the higher priority). Both users configure the same set of authorization rules at the S-CSCF. The list of those rules is given in simple text format as:

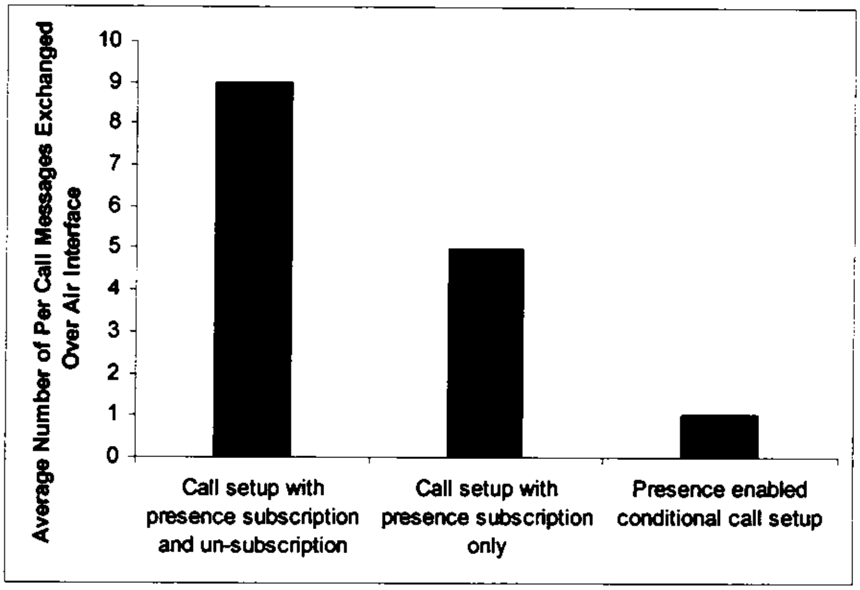


Figure 5.6: Performance of Presence Enabled Conditional Call

- Only forward 100 messages per hour
- Do not create any session between 3:00 pm to 5:00 pm
- Create session with user Y only between 6:00 pm to 6:00 am

Attack rules configured at the IDP system are:

- A user with priority 3 can send three Invite requests per five minutes
- A user with priority 2 can send two Invite requests per five minutes
- A user with priority 1 can send one Invite request per five minutes

Two receivers are configured with the IP addresses 192.168.10.3 and 192.168.10.4. We called them "user Y" and "user Z" respectively. Preferences of user Y are given below in the simple text.

- Do not establish any session from 9:00 pm to 11:00 pm
- Receive only 20 messages per hour
- Give priority to A's messages

In the first experiment, user A sends an invite request to create a session with user Y at 4:00 pm. Since A's authorization rule number 2 does not allow to establish session with user Y at 4:00 pm, the request is discarded at S-CSCF. In the second experiment, user B tries to establish a session with user Y at 7:00 pm. Since rule 3 of the authorization layer allows the establishment of a session with Y at 7:00 pm, the request is forwarded to the IDP system. Since it was user B's first invite request, the IDP system finds no attack and the request is forwarded to the application server. The application server finds no contradiction with Y's preferences, and the request is forwarded to Y. Figure 5.7 shows the sequence diagram of the experiment (in the figures, A.R stands for authorization rules; M.D, misuse detection; P.T priority table; and AS, application server).

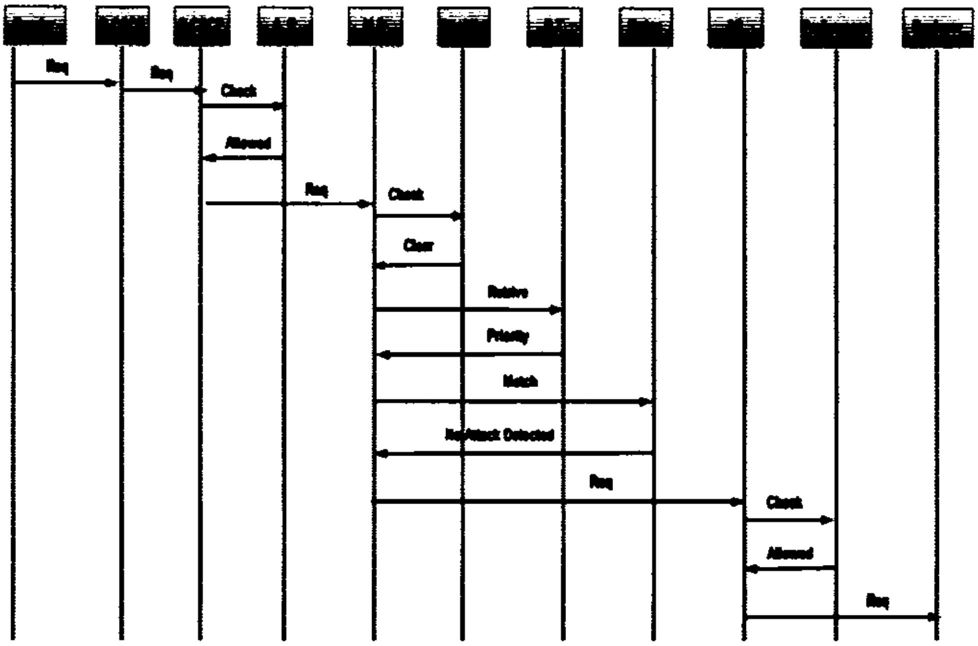


Figure 5.7: Result and Flow of Second Experiment

In the third experiment, user B immediately after sending the invite request to user Y launched the same request for user Z. The authorization layer finds no contradiction with the rules, and the request is forwarded to the IDP system. The IDP system checks for user B in the blacklist and, after getting the negative response, retrieves the priority of user B. After that it matches the request with the attack rules. Since user B's priority was 1 so only one session per five minutes is allowed to establish, the request is discarded because it was the second invite request received from user B within five minutes. User B is added into the blacklist. Figure 5.8 shows the sequence diagram of the experiment.

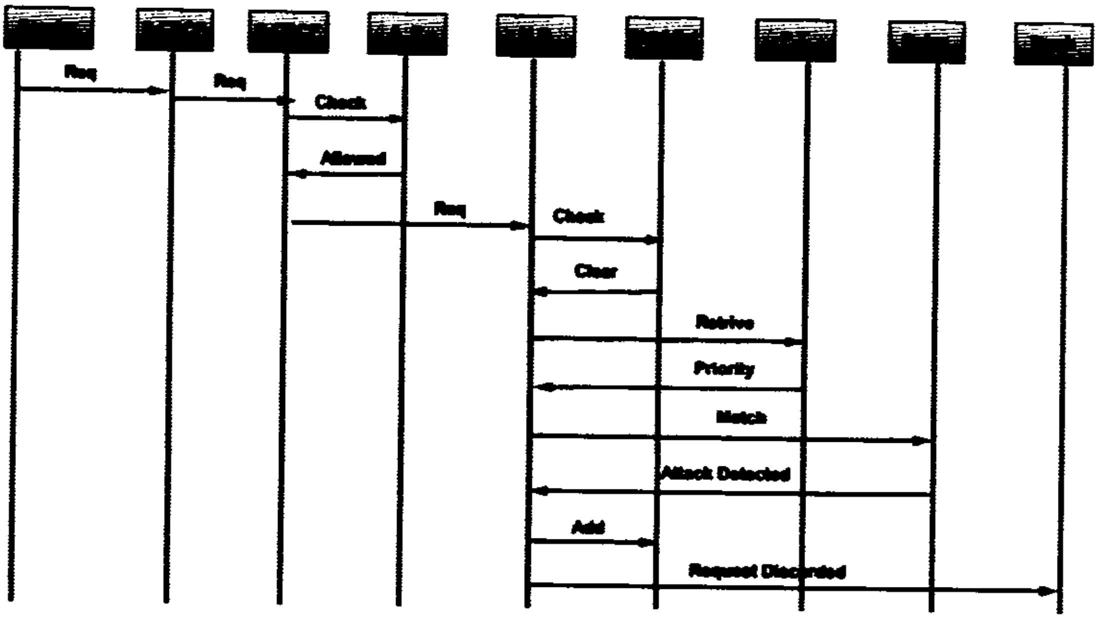


Figure 5.8: Result and Flow of Third Experiment

In the fourth experiment, user A, who has already sent an invite request to user Z, sends an invite request to create a session with user Y after 1 minute of the first invite request at 10:00 pm. The first layer finds no contradiction with the rules, so the request is forwarded to the IDP system. The IDP system, after checking the blacklist and retrieving the priority from the priority table, matches it with the attack rules. Since the priority of user A is 3 so A is allowed to send three invite requests per five minutes, the IDP system considers it as legitimate request and forwards it to the application server. User Y's preferences does not allow user A to establish a connection at 10:00 pm, so the request is discarded and the sender is notified. Figure 5.9 shows the sequence diagram of the experiment.

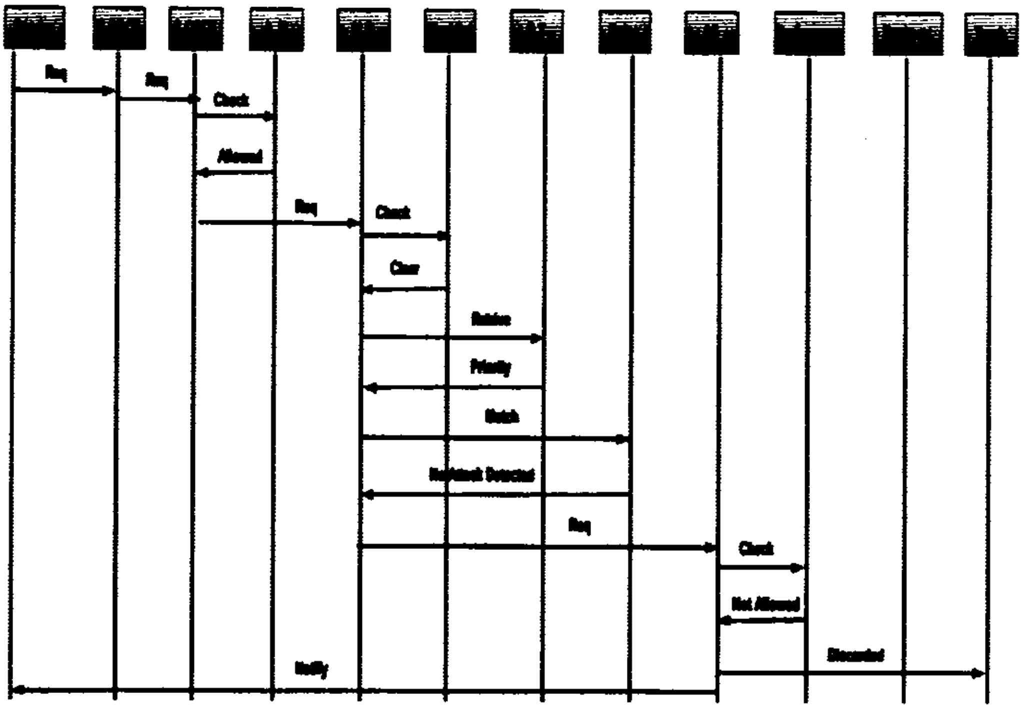


Figure 5.9: Result and Flow of Fourth Experiment at 10:00 pm

We repeat the fourth experiment at 12:00 am and, at this time session, the connection is established successfully. After that we measure the performance of layer one security (no rules are defined for layers two and three). The sender (user A) applies three rules regarding authorization:

- Only 60 messages are allowed per hour, and no more than one message can be sent during a single minute.
- Do not forward any message to user Y.
- Do not forward any message from 1:00 am to 9:00 am.

After specifying these rules, we develop a spoofed program with the IP of user A and launch an immediate message flood for one hour (10:00–11:00 am). During that one hour the spoofed user sends 500 messages. Of these 500 messages, 20 are destined for user Y. The results are shown in Table 5.1.

Table 5.1: Performance of Layer One Only

Total messages	No. of messages delivered	No of messages discarded at sender's end
500	59	441

The results show that only 59 messages are served and 441 messages are discarded. Of those discarded, 440 messages are discarded due to rule I because only one message is allowed per minute, and one message is discarded due to rule II because during the 24th minute three messages arrived and all three were destined for user Y. So no message is forwarded during the 24th minute. In the next experiment, the performance of level two is measured. Only one attack rule is defined: if a sender sends more than eight messages per minute consider it an attacker and block it for 10 minutes. After that we send zero to seven messages for the first five minutes, and the IDP system forwarded all the messages to the application system. In the 6th minute of the experiment, nine messages are generated. As soon as the ninth message reached at the IDP, it detects the flooding attack, puts the sender into blacklist, and discards the message.

In the next experiment, immediate messaging flood is launched over the third layer of security mechanism. Only three preference rules are defined:

- Give maximum priority to user A's messages.
- Block the messages of user B.
- Only send 10 messages per hour and a message after every six minutes.

To implement the scenario, we send seven messages from user A, 25 messages from user B, and 10 messages from user X. The experiment is conducted for one hour. Table 5.2 describes the results in detail.

Table 5.2: Performance of Layer Three Only

	Messages delivered		
Scenario	User A	User B	User X
All the messages are forwarded during the first 5 minutes	7 (First)	0	3 (Last)
User X and B forwarded the messages in first 5 minutes while the user A forwarded the messages after 20th minute	7 (Last)	0	3 (First)
User X and B forwarded the messages in first 5 minutes while the user A forwarded the messages after 30th minute	5 (Last)	0	5 (First)
User B forwarded the messages in first 5 minutes while the user X forwarded the messages after 30th minute and User A after 55th minute	1 (Last)	0	4 (First)
User B forwarded the messages in first 5 minutes while the user A and X forwarded the messages after 30th minute	5 (First)	0	0
User B forwarded the messages in first 5 minutes while the user A and X forwarded the messages after 55th minute	1 (First)	0	0

In the next experiment we calculated the delay in session setup for session based messaging. We divide the delay into three categories namely delay of layer one of secure architecture (D1), delay of layer two of secure architecture (D2), and delay of layer three of secure architecture (D3). We find that D1 is 1.8 mille seconds (ms), D2 is 2.3 ms in normal scenario but when numbers of session requests come in bulk it increases up to 7.2 ms and D3 is 1.5 ms per message. In the graph below we presented the total delay of different number of sessions established.

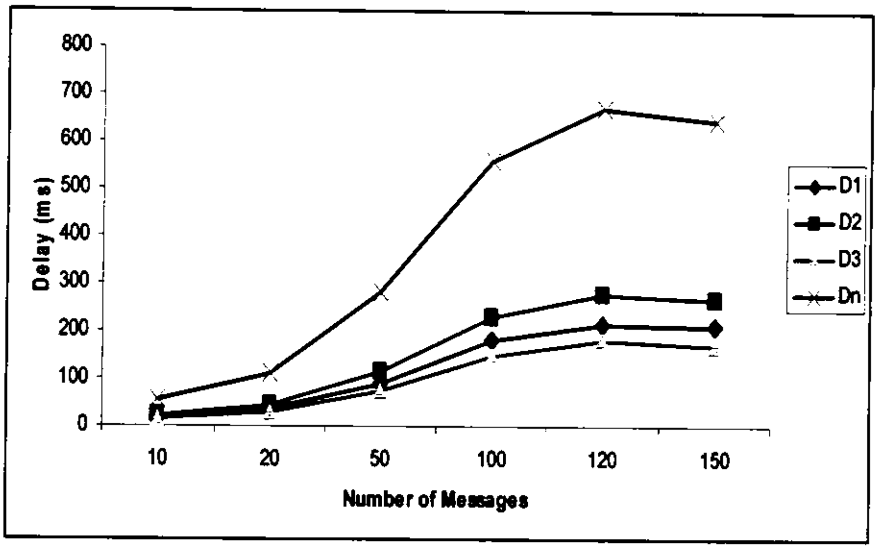


Figure 5.10: Delay in Three Layer Secure Architecture

5.4 Case 3: Presence Enabled Secure Architecture

Subscription and notification of presence information requires exchange of 4 messages over the air interface. Since our proposed solution checks the presence information during the transit so it is not necessary to subscribe for it. It saves the 4 messages per subscription that results in saving the valuable resources and reduces to the load on air interface. To test the validity of the presence and preferences based proposed solution, we take four users. Three users with IP addresses 192.168.10.1 and 192.168.10.2, 192.168.10.3 respectively, play the role of senders. We named them as "user A" and "user B," and "Z" respectively. One receiver is configured with the IP addresses 192.168.10.4 and named as "Y". Preferences of user Y are given below in the simple text.

- Receive only 20 messages per hour and a message after every three minutes.

- Give priority to A's messages
- B is allowed to send only 6 messages per hour and it has priority after A
- Z is allowed to send 4 messages only.

In the first experiment we tested validity of checking sender's presence. For this purpose we set the presence information of user A as busy and do not want to send and receive any instant message. Then we send an immediate message from user B by spoofing the identity of user A. We find that S-CSCF discards that message and a notification is received by user A that its ID is misused by some person. In the 2nd experiment we verify the presence information of receiver. User Y sets that currently it is not possible to receive any message. After that user A sends a message and it is discarded by S-CSCF after checking the presence information of user Y.

In the third experiment we checked the validity of receiver's rules. User A sends 25 messages and user B sends 12 messages to Y. It is found that Y receives only 20 messages from user A. All other messages are discarded. This is because of rule 1 and rule 2. After that we send 10 messages from user A and 6 from user B and 4 messages from user Z. We find that all the messages are received by user Y.

In the 4th experiment 14 messages are sent from user A, 25 messages from user B, and 10 messages from user Z. The experiment is conducted for one hour. Various scenarios are tested and Table 5.3 describes the results in detail.

Table 5.3: Results of 4th Experiment

Scenario	User A's delivered messages	User B's delivered messages	User Z's delivered messages
All the messages are forwarded during the first 2 minutes	14 (First)	6 (Last)	0
User Z and B forwarded the messages in first 2 minutes while the user A forwarded the messages after 20th minute	14 (Last)	6 (First)	0
User Z and B forwarded the messages in first 2 minutes while the user A forwarded the messages after 30th minute	10 (Last)	6 (First)	4 (Second)
User B forwarded the messages in first 2 minutes while the user Z forwarded the messages after 30th minute and User A after 55th minute	2 (Last)	6 (First)	4 (Second)
User B forwarded the messages in first 2 minutes while the user A and Z forwarded the messages after 30th minute	10 (Last)	6 (First)	0
User B forwarded the messages in first 5 minutes while the user A and X forwarded the messages after 55th minute	2 (Last)	6 (First)	0

5.5 Case 4: Results of Election Based Rights Allocation Mechanism for PTM

In this scenario Alice (a user) initiates a PTM session. After a while Bob sends a join request, an election is initiated and Alice allow Bob to join with full rights. Carel was the third who wants to become member of this PTM session, the election results also allowed Carel with full rights. Duminy is the fourth to request and it is allowed as watcher and listener only. After 10 minutes of session establishment 50 users are allowed to become member of the PTM session with different rights. 10 members are allowed with full rights including the session initiator, 6 members as speaker and listener, 2 as speaker only, 12 members join the PTM session as listener and watcher and 20 members are the listener only.

In the first experiment we calculate the average waiting time for media burst control. Every user is allowed to speak maximum for 1 minute in one turn. We run this experiment for 3 hours. First we take the results on the current delivery mechanism. We find that when all the users are allowed to speak the average waiting time per user is about 37 minutes. We repeat the same experiment by activating our election based right allocation mechanism where all the users are not allowed to request for media burst control. Only 18 from the 50 members are allowed to send media. We find that at this time average waiting time per user for media burst control is only 13 minutes. Even though total members of the session are still 50 but since all of them are not allowed to send media so the contention and average waiting time per user reduce significantly. We repeat the same experiments with different number of users and the results are shown in Figure 5.11.

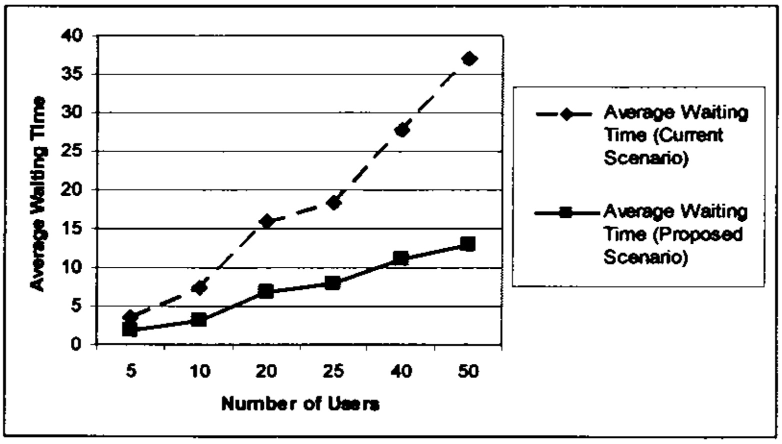


Figure 5.11: Average Waiting Time

In Figure 5.11, it is shown that average waiting time increases with increasing the number of users. But the ratio of increasing in our proposed scenario is far lower as compared to existing scenario. If there are 100 users in a PTM session average waiting time is 62 minutes in case of current scenario while it is 34 minutes in case of proposed scenario. So this solution makes the PTM service more scalable and a large PTM group can be established with different rights to different users.

5.6 Case 5: Results of Media Mixing With Presence

After testing the number of messages forwarded by PTM server in case of configured send/receive rules, we tested the scenario of presence based send/receive rules. We found that the number of messages exchanged in case of presence based send/receive rules are lesser as compared to send/receive rules only. Results are found by implementing the scenario described in Table 4.5.

We can conclude that due to specified rules and presence information each user's sent media is forwarded to selected members only. So if user A sends a message it will be forwarded to only 2 users as shown in Table 4.5. So if every user sent 50 messages then total numbers of messages sent by controlling server in case of presence based send/receive rules are 1350.

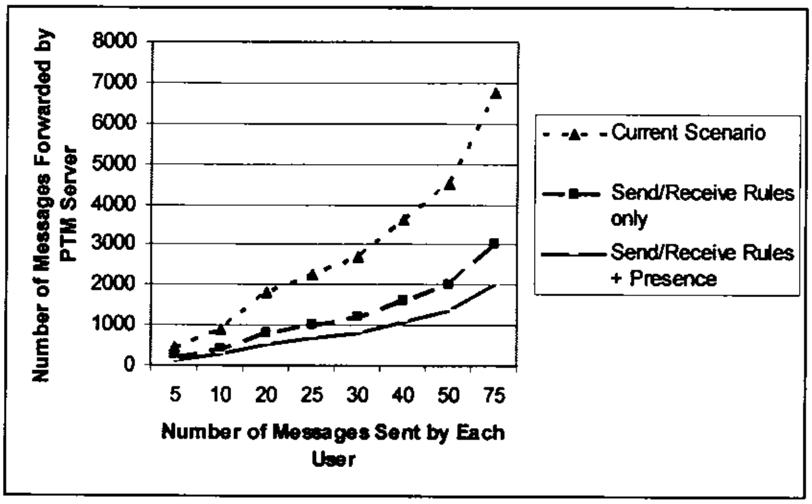


Figure 5.12: Number of Messages Forwarded by Controlling PTM Server in Presence + Send/Receive Rules Scenario

5.7Case 6: Results of Election Based Deletion Mechanism

To validate the above mentioned solutions we applied them into real PTT and PTM scenarios by using the IMS testbed. We run the election based deletion mechanism in two scenarios.

In the first experiment we take an example of university friends. One user named as user A initiates a PTT session and invites 9 friends (B,C,D,E,F,G,H,I,J) to join that session. The session remains active for 45 minutes. During the 16th minute of the session user J complaints that user F is acting as malicious user so the controlling server starts an election. The threshold value was 60%. At the end of the election controlling server finds that only 55% votes are cast in the favor of the complaint. So it issues a warning to user J.

In 20th minute user D launches a complaint against user E. The results showed 77% votes so the controlling server deletes the user E from the session. At the start of 31st minute user J again launches a complaint but this time against user B. This time the complaint got only 39% votes. So J is also deleted from the session. These statistics and actions are summarized in Table 5.4.

In the above mentioned scenario all the users have the same voting power. It means vote of every user has value equal to 1. But in the second experiment we change the scenario. We establish a PTM session among the stakeholders of the university. The Chancellor, President, 3 Deans, 3 Faculty Members and 3 Students participated in the session.

Table 5.4: Summary of Results of First Experiment

Time (Minute)	Activity	Value/Users	Votes in Favor	Votes Against	Result
0	Session Setup	A	-	-	-
0	Invitation	B,C,D,E,F,G,H,I,J	-	-	-
0	Setting of threshold value	60%	-	-	-
16	J complaints against F	A,B,C,D,E,F,G,H,I,J	55%	45%	A warning is issued to J
20	D complaints against E	A,B,C,D,F,G,H,I,J	77%	33%	E is deleted from the session
31	J complaints against B	A,B,C,D,F,G,H,I	39%	61%	J is deleted from the session

The chancellor, President and Deans vote is considered 3 times than that of students. Faculty member's one vote is considered as 2 votes of student. Again the session lasts for 45 minutes. In the 5th minute one of the student complaints to delete one of the Dean from the session.

The threshold value was 50%. One of the Dean, 2 of the faculty members and the other 2 students agreed to delete that Dean from the session. But the Chancellor, President, one of the Dean and One faculty member cast their vote against the complaint. So 10 votes are cast in the favor of the complaint while 11 votes are cast against the complaint so the Dean remains the part of the session and a warning is generated to the student who launches the complaint. During 21st minute the Chancellor launches a complaint to delete one of the faculty members from the session. Two of the Deans and two faculty members cast their vote against the chancellor's request while president one of the Deans and students cast their vote in favor of chancellor's request. So 10 votes are cast against the chancellor's request and 12 votes are caste in favor. Therefore faculty member is deleted from the session. These statistics and actions are summarized in Table.

Table 5.5: Summary of Results of Second Experiment

Time (Minute)	Activity	Value/Users	Votes in Favor	Votes Against	Result
0	Session Setup	Chancellor	-	-	-
0	Invitation	1 President 3 Deans 3 Faculty Members 3 Students	-	-	-
0	Setting of threshold value	50%	-	-	-
0	Setting of Vote-Value	Chancellor=3 President =3 Deans=3 Faculty Members=2 Students=1			
5	one of the student complaints to delete one of the Dean	1 Chancellor 1 President 3 Deans 3 Faculty Members 3 Students	10	11	A warning is issued to the student
21	Chancellor launches a complaint to delete one of the faculty members	1 Chancellor 1 President 3 Deans 2 Faculty Members 3 Students	12	10	One of the faculty member is deleted from the session

5.8 Case 7: Results of Election Based Floor Allocation Mechanism

We also apply our proposed maximum floor control time algorithm in the above mentioned campus based PTM session. The session initiator sets that the Chancellor and President can use the floor maximum for 5 minutes, Deans and Faculty members for 3 minutes and students for 2 minutes. During the session one of the Dean requests for the floor for 5 minutes. An election is started by the controlling server. Threshold value was 50%. The request gets 75% votes and the Dean is allowed to use the floor for 5 minutes.

5.9 Case 8: Results of Election Based Distributed Referring

In the next experiment we evaluate our election based distributed referring authority mechanism. For this experiment the threshold value is set to 75%. We launched 5 refer requests in a conference of 10 participants. Out of these 5 refer requests 3 got more than 75% votes so they became the member of the conference and the 2 requests fail to gain 75% vote so they are discarded by the conference server.

We repeat this experiment with different values and Table 4.11 shows the results. In the last we identify few scenarios for the applicability of the parameterized refer request and validates the proposed mechanism in those scenarios. We take the Campus example where administration and the faculty members start a video conference to discuss few important issues. Latter on the president of the university referred few students into the conference but they were only allowed to watch and listen the conference. They were not allowed to speak in the conference. This feature is obtained through the parameterized refer request.

Table 5.6: Results of Election Based Referring Mechanism

EXP.#	REFER REQUESTS	ALLOWED (75% OR MORE VOTES)	DISCARDED (LESS THAN 75% VOTES)
1	5	3	2
2	12	6	6
3	16	7	9
4	20	7	13

5.10 Case 9: IDP System

In order to validate our solutions we conduct number of experiments over the IMS testbed. First we configure the set of rules for different types of attacks. Rules not only vary from attack to attack but also from role to role. Description and XML script of different attacks is shown below.

Table 5.7: Description of Invite Flooding Attack for High Priority User

	Value	Description
Type	Flood	It is time dependent flooding attack
Name	Invite Flooding	The rule is called Invite flooding
Method	INVITE	The attack is launched through SIP INVITE request
Status	-	Status is Null because Invite request itself is used to launch the attack
Role	High Priority	This rule is only for high priority user
Number	300	300 Invite request is allowed to user
Interval	60	60 seconds is the time interval in which a user can send 300 Invite requests
Alert	Invite Message Flood	If attack is detected then this message will be displayed by the IDP

Table 5.8: Description of Invite Flooding Attack for Low Priority User

	Value	Description
Type	Flood	It is time dependent flooding attack
Name	Invite Flooding	The rule is called Invite flooding
Method	INVITE	The attack is launched through SIP INVITE request
Status	-	Status is Null because Invite request itself is used to launch the attack
Role	Low Priority	This rule is only for low priority user
Number	100	100 Invite request is allowed to user
Interval	60	60 seconds is the time interval in which a user can send 300 Invite requests

Alert	Invite Message Flood	If attack is detected then this message will be displayed by the IDP

```
<?XML version=”1.0” encoding= “UTF-8”>
<Rules>
<Rule type=Flood>
<Role> 3 (High Priority) </Role>
<Name> INVITE </Name>
<Method> INVITE </Method>
<Number> 300 </Number>
<Interval> 60 </Interval>
<Alert> INVITE FLOOD </Alert>
</Rule>
<Rule type=Flood>
<Role> 1 (Low Priority) </Role>
<Name> INVITE </Name>
<Method> INVITE </Method>
<Number> 100 </Number>
<Interval> 60 </Interval>
<Alert> INVITE FLOOD </Alert>
</Rule>
<Rule type="sqlinject">
<Role> 4 Any </Role>
<Name>Drop statement</Name>
<Statement>drop</Statement>
<Alert>a drop injection attack launched</Alert>
</Rule>
<Rule type="sqlinject">
<Role> 4 Any </Role>
<Name>Delete statement</Name>
<Statement>delete</Statement>
<Alert>a delete injection attack launched</Alert>
</Rule>
```

After configuring the rules we launched different experiments to check the validity of the role based IDP. In the first experiment we allowed a user with high priority role to send 300 INVITE requests within 60 seconds. Since the user is allowed to send 300 requests within 60 seconds so these requests are considered secure by the role based IDP system and forwarded to the Application Server (AS).

In the second experiment we take the same scenario as in the first experiment but this time the user's role was of low priority so it is only authorized to send 100 requests within 60 seconds. We analyze the request number 101 that is sent within 60 seconds. We find that the role based IDP system considered it as an attack, discarded the request immediately, and put the user into the blacklist.

In the last experiment we measured the delay caused by our proposed IDP. Delay is calculated from the time when request enters into SIP stack and when the decision comes back to S-CSCF. Average delay is calculated and results are shown in Figure 5.13.

From Figure 5.13 it can easily be concluded that at the peak average delay of our proposed system and average delay of existing systems is almost same. However at different stages delay of our proposed system is slightly higher as compared to existing systems. This high delay is because of two reasons. First reason of delay is due to few extra steps added into our proposed system like execution of blacklist algorithm, role discovery etc. The second reason that increases the delay is the number of signatures we used. We take 827 signatures and all these signatures are checked every time that increases the delay.

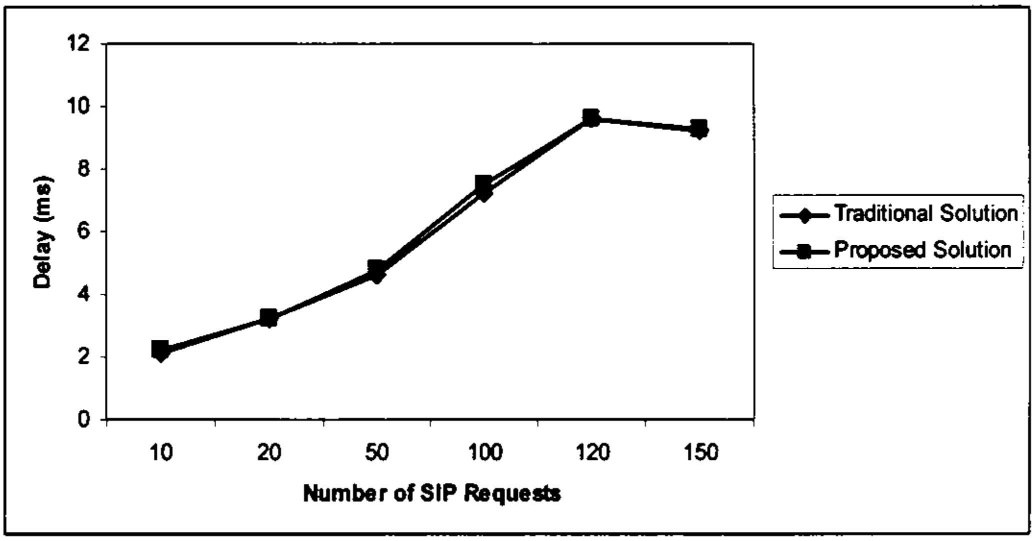


Figure 5.13: Average Delay of IDP System

5.11 Case 10: Results of Anomaly Detection Algorithms

Next question is about the results. How we can measure the performance of any classifier or feature extraction module. We have selected few parameters those will determine the performance results.

A. **Accuracy:** Accuracy mainly includes False Negative, False Positive, Precision, Breadth etc. If these values are up to the satisfaction level the solution can be considered as accurate.

B. **Training Time:** How much time the training process takes is another issue that largely affects the performance of the solution. It is our second parameter to consider.

C. **Rule-Set** : Size of the rule-set and its completeness is another performance parameter that can not be ignored.

D. **Testing Time:** Another important parameter to consider is the testing time. It is one of the most important parameter because it results in real time delay in packet.

5.11.1 Results and Discussion

In this section, we explain our experimental setup and results. As discussed earlier, our proposed methodology generates an attributive input by modeling the byte level distributions of IMS traffic. We create the training sample by randomly collected 50 benign and 50 malicious messages respectively from IMS traffic. The training samples are used in selecting the discriminative features for our analysis. For testing, we use stratified 10 fold cross validation technique to evaluate the performance of different machine learning algorithms. In this strategy we divide the complete dataset into 10 equal parts, where 9 parts are used to train the classifier and left over part is used for testing. The procedure is repeated on all parts and average results are reported. We use standard definitions of detection accuracy and false alarm rate with the help of four parameters: 1. Correct classification of malicious SIP message, True Positive (TP). 2. Correct classification of benign message, False Positive (FP). 3. In-correct classification of a malicious SIP message, False Negative (FN). 4. In-correct classification of a benign message, True Negative (TN). We define Detection Rate (DR) as: DR = (TP/TP+FN) and False Alarm Rate (FAR) as: FAR = (FP/FP+TN). The standard Receiver Operating Characteristic (ROC) (Cover et al. 2006) analysis is adopted to evaluate the accuracy of our system. ROC curves are extensively used in machine learning and data mining to depict the trade-off between the detection rate and the false alarm rate of a given classifier. We reported the detection accuracy of each algorithm by using the area under ROC curve (AUC) $0 \leq \text{AUC} \leq 1$. Figure 5.16 shows the ROC plot of different machine learning classifiers used in our study to classify anomalous IMS traffic. Figures 5.14, 5.15 and 5.16 summarize the results of our experiments. The first interesting insight is that the difference in the relative detection accuracies, by operating on byte-level distributions on SIP packet, of all classification algorithms show large variance in some cases. C4.5 gives the best detection accuracy of 0.99 on the selected feature set. It is closely followed by RIPPER which provides the detection accuracy of 0.98. On the contrary, NB and C-SVM provide relatively low accuracies of 0.94 and 0.81, respectively. Note that while providing the low accuracy on selected features both NB and C-SVM have lowest training time of 1.64 and 1.73 seconds. It is also interesting to note that all machine learning algorithms used in our experimentation are efficient in terms of testing an individual SIP request. (Note that for real world scenarios, delay in testing the SIP requests can severely degrade the QoS of IMS services.) Figure 4.18 shows the testing time per packet of all the machine learning algorithms we have use. Note that C4.5 only takes 152 micro seconds to classify the SIP message. The testing time of NB and C-SVM takes 270 and 280 micro seconds respectively. RIPPER is being slowest and takes 391 micro seconds in classifying the anomalous message.

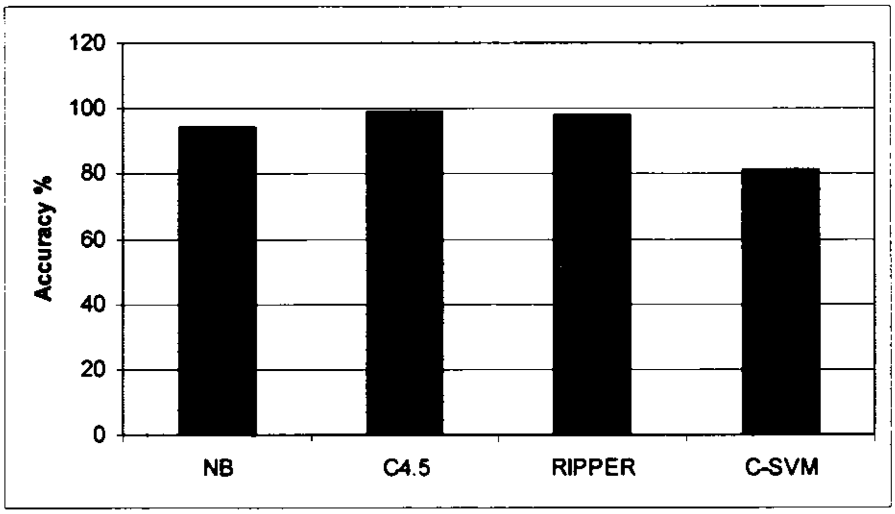


Figure 5.14: Accuracy

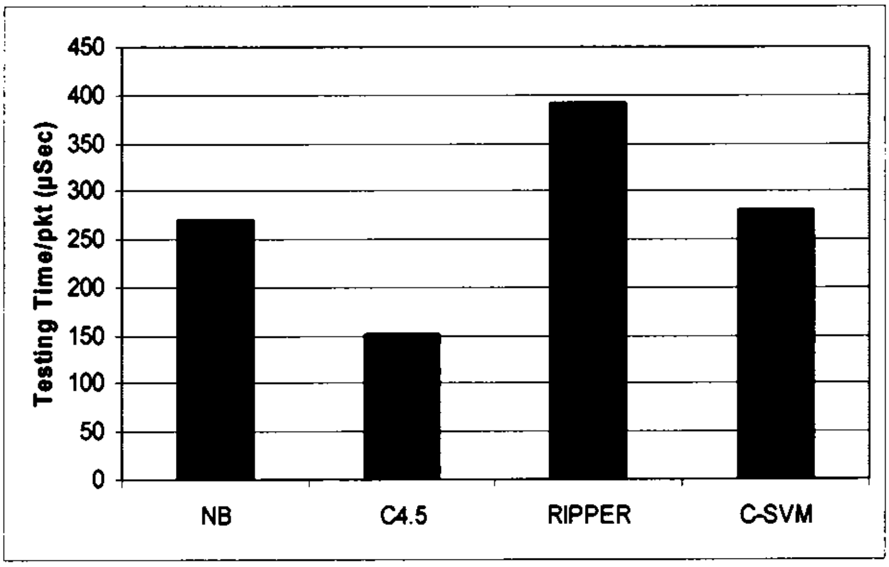


Figure 5.15: Training Time

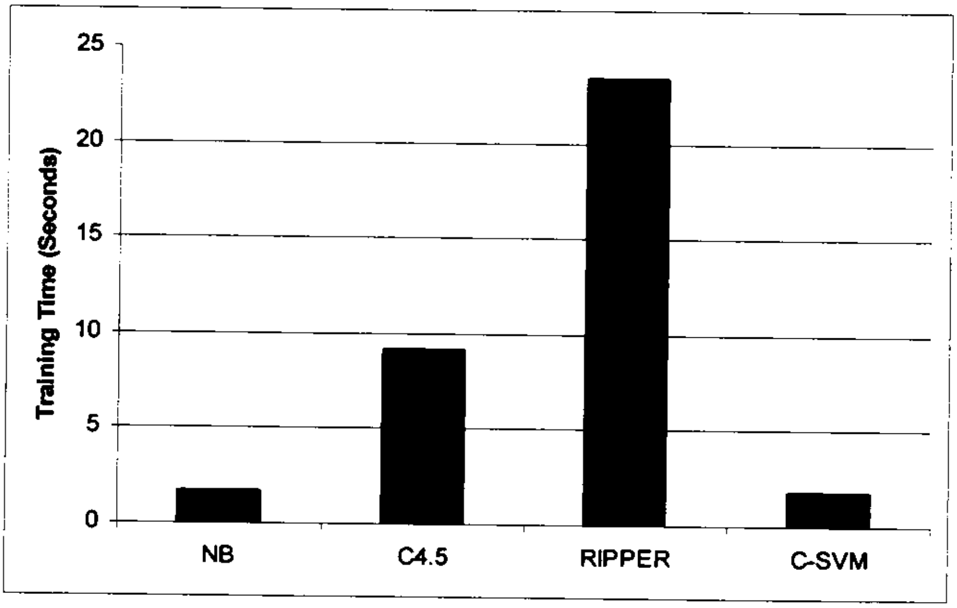


Figure 5.16: Testing Time

5.2 Chapter Summary

In this chapter results are discussed. To obtain the results we tested them on IMS testbed. Different set of experiments are conducted to evaluate each of the proposed framework. Services prototype are prepared for testing purpose. Results are shown in the forms of graphs and tables. After each graph it is discussed that what is the reason behind these results and why the difference between different solutions exist. First we test the performance of presence enabled conditional call setup. We test it in 4 scenarios to calculate the overall delay and compare the results in different graphs. We also tested the load on the air interface by applying and without applying presence enabled conditional call setup. In 2nd set of experiments we obtained the results from three layer secure architecture. The main performance matrix consists of delay and efficiency in terms of blocking the attack or un-wanted packets. Results of election based right allocation are also obtained and scalability of the PTM service is checked by comparing the average waiting time. Media mixing algorithm provides the results that how many total packets are received by each of the participant of the session and out of those received packets how many packets user really wants to receive. Experiments are also conducted to obtain the results of maximum floor control time, distributed referring etc. Second last set of experiments is conducted to check the performance of misuse system. Results are obtained and compared with existing IDP system. In last set of experiments we measure the performance of four non evolutionary algorithms inside the IMS. The performance matrix consists of testing time, training time, and accuracy.

CHAPTER 6

CONCLUSION AND FUTURE WORK

In future it is planned to route all the traffic through IP. Moreover convergence at network and service level also helps the users to get all the services from any underlying network. The architectural framework that is developed to implement the NGN is known as IMS. 3GPP has the leading role in developing standards related to IMS. We, in this thesis, worked on security and enrichment of IMS based multimedia services. The services those are the main focus of this thesis include presence, instant messaging, push to talk over cellular and multiparty conference.

Presence service provides the dynamic up to date information of other users and it can be used inside many other services. We developed a presence based conditional call setup mechanism in which it is not required to subscribe the presence information. Presence information of the receiver is checked during the call setup procedure and then decides whether to establish this session or not. On one hand this solution results in reducing the load on air interface of access network and on the other side it saves the valuable time.

Instant messaging is subject to various types of threats like immediate message flooding, invite flooding, session based attacks, etc. We proposed two different solutions to avoid these threats. In the first solution we proposed a three layer secure architecture. These three layers include sender's authorization rules, IDP system and receiver's preferences. Together these three layers secure the messaging server as well as the end users. In the second solution we used presence information of the users to decide whether to convey this message or not. Authorization rules and receiver's preferences are also used along with the presence information.

Push to talk over cellular and push to multimedia service is subject to various types of problems including privacy problem, rights allocation problem, disturbance problem, scalability problem, resource utilization problem, membership problem, floor control problem etc.

It is found that since presence is continuous dynamic service so it puts a great load on the air interface. Moreover it is also finds that presence information must needs subscription even if caller requires that information for a very little period of time. Subscription and un-subscription on one hand requires a significant amount of time and on the other hand it also consumes a good part of the bandwidth at air interface. Second section consists of problems related to messaging. We find that in immediate messaging since user is allowed to send any number of messages without creating any session so it creates a security risk a the receiver end. In session based messaging all types of session based attacks like cancel and session modification attacks are possible. The first problem of PoC and PTM is about the scalability of PTM. Since PTM is a half duplex service so increase in number of participants also increasing the average waiting time of getting turn to speak. Second problem is about delivering data to irrelevant users that creates privacy problem as well as disturbance problem. Maximum floor control time is also fixed and equal for all the participants. It is not allocated on the basis of the user's requirement or on user's role in that session. Problems related to multiparty conference include single participant based referring and fully authorized referring. Register flooding attack can be launched by sending enormous number of register requests. In the same way invite flooding attack can also be launched. Other attacks those are discussed in this section includes session based attacks, publish flooding attack, etc.

After discussing the problems we discussed different frameworks and the methodology to solve the problems related to IMS based multimedia services. So far as presence is concerned we presented presence enabled conditional call setup mechanism and presence triggered automatic call mechanism. In presence enable conditional call setup we proposed that for occasional calls user is not needed to subscribe the presence service. Presence is used during the call setup process. On one hand this solution reduces the load from the air interface and on the other hand it reduces the overall delay. In presence triggered call setup we proposed that presence condition will be stored and upon getting the correct response from presence server, the S-CSCF automatically generates a call. For instant messaging, security solutions like three layer secure architecture, presence and preference based secure solutions are presented. In three layers secure architecture layer one takes the preferences from sender and hence reduces chances of misuse and spoofing. Layer consists of an IDP system that tries to detect an attack and the third layer takes the receiver preferences and minimizes the disturbance problem and targeted attacks. In other solutions presence service is used to reduce the chances of message flooding attack on targeted users. Election based rights allocation, deletion and floor control mechanisms, media mixing with presence are the solutions proposed for PoC and PTM. In election based rights allocation a user gets the rights on which all the other participants agree. Maximum floor control time is also allocated to the users on the basis of their role in the session. Media mixing algorithm takes the preferences of all the users and deliver the media according to those preferences. Distributed and Limited rights referring solutions are developed for multiparty conference. IDP system based on misuse detection and anomaly detection modules is developed to secure the application servers from different types of flooding and other attacks. In misuse system first time we introduced the role of the user in attack detection. Secondly we also consider the severity of the attack. A new blacklist algorithm is also proposed to penalize the attacker in case of attack detection. In anomaly detection module we tested four non evolutionary algorithms. Till now, according to our best knowledge, non evolutionary algorithms are never used in IMS for increasing the security.

To obtain the results we tested them on IMS testbed. Different set of experiments are conducted to evaluate each of the proposed framework. Services prototype are prepared for testing purpose. Results are shown in the forms of graphs and tables. After each graph it is discussed that what is the reason behind these results and why the difference between different solutions exist. First we test the performance of presence enabled conditional call setup. We test it in 4 scenarios to calculate the overall delay and compare the results in different graphs. We also tested the load on the air interface by applying and without applying presence enabled conditional call setup. In 2nd set of experiments we obtained the results from three layer secure architecture. The main performance matrix consists of delay and efficiency in terms of blocking the attack or un-wanted packets. Results of election based right allocation are also obtained and scalability of the PTM service is checked by comparing the average waiting time. Media mixing algorithm provides the results that how many total packets are received by each of the participant of the session and out of those received packets how many packets user really wants to receive. Experiments are also conducted to obtain the results of maximum floor control time, distributed referring etc. Second last set of experiments is conducted to check the performance of misuse system. Results are obtained and compared with existing IDP system. In last set of experiments we measure the performance of four non evolutionary algorithms inside the IMS. The performance matrix consists of testing time, training time, and accuracy. At the end we are mentioning the major achievements of the thesis.

- 8 Messages per Invite request are reduced from the air interface for occasional calls
- Overall call setup delay is reduced from 7.1 to 3.8 seconds in case of local calls at normal load
- Invite request is enriched by adding presence based condition
- Targeted attacks are mitigated through receiver preferences
- Scalability is achieved by adding different types of users with different roles
- Average waiting time is reduced almost 3 times from the original waiting time
- Reduction in number of received messages results in solving privacy as well as solves the disturbance problem
- Different signatures are defined for different service levels
- Adaptive nature of blacklist algorithm punishes the attacker more severely
- 98.5% accuracy is achieved by utilizing non evolutionary algorithms
- Testing time of non evolutionary algorithm is acceptable for real time services
- IMS based multimedia services are provided with more value added features
- Make it feasible to use IMS based multimedia services in most of real life scenarios

6.1 Future Work

In future this work can be extended in many different directions. These directions include:

6.1.1 Anomaly Detection Algorithm

We in this thesis presented an anomaly detection module by introducing existing non-evolutionary algorithms inside the IMS. In future we are planning to introduce new algorithms and neural network techniques for the anomaly detection in IMS. The basic purpose is to minimize the training and testing time and to maximize the accuracy.

6.1.2 Handling of Load on S-CSCF

Few of our solutions involve S-CSCF and put some extra work on this entity. Since this is the main entry inside the core network so our focus in future is to enhance our solutions to minimize the load from the S-CSCF.

6.1.3 Automatic Presence Updation

Currently whenever presence information of an entity changes it is communicated to the subscribers. There are few attributes those may change in a predetermined sequence. So in that case instead of sending presence notification, the subscriber can calculate the presence information on the basis of certain patterns by using different fuzzy and neural network techniques. It will reduce the load from the network as well as will results in efficient resource utilization.

6.1.4 Testing on TISPAN

TISPAN is another release by 3GPP and it not only includes mobile networks but also include fixed network. We are very confident that our developed solutions will work as efficiently in TISPAN as they are working in IMS but in future we have plan to test them over TISPAN.

6.1.5 Retransmission of Packets

If a packet is dropped due to congestion or buffer overflow that packet will be retransmitted. In case of retransmission that message will again be calculated in order to count the packets for time dependent attacks. Double counting of packets can cause inefficiency in IDP system so for this purpose retransmitted packets can be identified at P-CSCF and they should not be counted two times. P-CSCF needs a mechanism to pin point the retransmitted packets.

BIBLIOGRAPHY

3rd Generation Partnership Project, Technical Report, 3GPP TR 22.940 "IP Multimedia Subsystem (IMS) messaging; Stage 1", 2009.

3rd Generation Partnership Project, Technical Specifications, 3GPP TS 22.141, "Presence Service Stage 1" 2009.

3rd Generation Partnership Project, Technical Specifications, 3GPP TS 22.174 "Push services, service aspects stage 1", 2009.

3rd Generation Partnership Project, Technical Specifications, 3GPP TS 22.948 "Study of requirements of IP-Multimedia Subsystem (IMS) convergent multimedia conferencing", 2009.

A. Amirante, T. Castaldi, L. Miniero and S.P. Romano, "Improving the scalability of an IMS-compliant conferencing framework through presence and event notification", Proceedings of IPTCOMM '07, New York USA 2007.

A. Anzaloni, M. Listanti, I. Petrilli, D. Magri, "Performance Study of IMS Authentication Procedures in Mobile 3G Networks", IWCMC'07, August 12–16, 2007.

A. Ghavam, R. Liscano, M. Barbeau, T. Gray, N. D. Georganas , "Secure Presence-based Services", http://www.scs.carleton.ca/~barbeau/Publications/2002/liscano.pdf.

A. Niemi, J. Arkko, V. Torvinen, "HTTP Digest Authentication Using AKA", IETF RFC 3310, 2002.

Adel Al-Hezm, Stefan Arbanowski, Thomas Magedanz, "Interactive Multimedia Services over Open NGN Testbed", Tridentcom 2008 March 18–20, 2008.

Adel Al-Hezmi, Fabricio Carvalho de Gouveia, Thomas Magedanz, "Provisioning of Multimedia Services over Open NGN Testbed" Ambi-sys, 2008.

Alberto Diez Albaladejo, Alin Murarasu, Thomas Magedanz, "Design of a Coherent Mobile Multimedia Framework for Convergent Services", Proceedings of MoMM2008, Austria, 2008.

Aliya Awais , Muddassar Farooq ,M Younus Javed, "Attack Analysis & Bio-Inspired Security Framework for IP Multimedia Subsystem", GECCO '08 July 12–16, 2008.

Allen E. Milewski and Thomas M. Smith, "Providing Presence Cues to Telephone Users" CSCW'00, December 2-6, Philadelphia, 2000.

Amirante, T. Castaldi, L. Miniero, S.P. Romano, "Improving the scalability of an IMS-compliant Conference framework through presence and event notification", ACM IPTCOMM '07, 2007.

Amjad Akkawi, Sibylle Schaller, Oliver Wellnitz, Lars Wolf, "A Mobile Gaming Platform for the IMS", SIGCOMM'04 Workshops, Aug. 30 & Sept. 3, Portland, 2004.

An'an Luo, Chuang Lin, Kai Wang, Lei Lei, Chanfang Liu, " Quality of protection analysis and performance modeling in IP multimedia subsystem", Computer Communications, Volume 32 , Issue 11, July 2009.

Andras Balazs, "Push-to-talk Performance over GPRS", ACM MSWiM'04, 2004.

Andreas Bachmann, Alice Motanga, Thomas Magedanz, "Requirements for an Extendible IMS Client Framework" *Mobilware'08*, February 12-15, 2008.

Anis Zouari, Karine Guillouard, Jean-Marie Bonnin, "A Performance Analysis of Distributed QoS Negotiation During Establishment Sessio", ACM Q2SWinet'07, 2007.

Arturo Salinas, "Advantages and Disadvantages of Using Presence Service", www.tml.tkk.fi/Publications/C/21/salinas_ready.pdf.

ATIS Next Generation Network (NGN) Framework Part I: NGN Definitions, Requirements, and Architecture, November 2004.

ATIS Next Generation Network (NGN) Framework Part II: NGN Roadmap 2005, August, 2005.

Barbara Kordy, Sjouke Mauw, Saša Radomirović, Patrick Schweitzer, "Foundations of attack-defense trees", FAST'10 Proceedings of the 7th International conference on Formal aspects of security and trust Springer-Verlag Berlin, Heidelberg ©2011.

Bassam El Saghir,Noel Crespi, "A New Framework for Indicating Terminal Capabilities in the IP Multimedia Subsystem", IEEE Global Telecommunications Conference, 2006.

C. Faure, "Presence Service in 3G Networks", IEE conference on 3G mobile technologies, 2002.

C. Kaufman, Ed. "Internet Key Exchange (IKEv2) Protocol, IETF, RFC 4306", December 2005.

C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865, June 2000.

Cao Peng, Yang Xiangmin, Zhang Lei, "A new call control scheme for push to talk system", ACM Mobility 06, 2006.

Carlo Alberto Licciardi1, Paolo Falcarin, "Technologies and Guidelines for Service Creation in NGN", http://www.cercom.polito.it/Publication/Pdf/210.pdf.

Chai-Hien Gan, Yi-Bing Lin, "Push-to-Talk Service for Intelligent Transportation Systems", IEEE transactions on intelligent transportation systems, vol. 8, no. 3, september 2007.

Chen, E.Y., "Detecting DoS attacks on SIP systems," IEEE Workshop on VoIP Management and Security, Page(s):53 – 58, April 2006.

Christian Kloch, Jens Enevold Kristensen, Bent Bilstrup, "Future Scenarios: What are the Future Services and Applications?", Wireless Personal Communications: An International Journal Volume 53 Issue 3, May 2010.

Christoph Hecht, Peter Reichl, Andreas Berger, Oliver Jung, Ivan Gojmerac, "Intrusion Detection in IMS: Experiences with a Hellinger Distance-Based Flooding

Detector",Proceedings of the 2009 First International Conference on Evolving Internet, 2009.

Christopher J Pavlovski, Quentin Staes-Polet, "Digital Media and Entertainment Service Delivery Platform" ACM MSC'05, 2005.

Chung-Wei Hang, Munindar P. Singh, "Trustworthy Service Selection and Composition", ACM Transactions on Autonomous and Adaptive Systems (TAAS) TAAS, Volume 6 Issue 1, February 2011.

Cristina-Elena Vintilă, Victor-Valeriu Patriciu, Ion Bica, "A J-PAKE based solution for secure authentication in a 4G network", NEHIPISIC'11 Proceeding of 10th WSEAS international conference on electronics, hardware, wireless and optical communications, Stevens Point, Wisconsin, USA ©2011.

D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol", IEEE Communication Surveys Volume 8, No.3 ISBN 1553-877X, pp 68-81, 2006.

D. Maughan, M. Schertler, M. Schneider, J. Turner, IETF, RFC 2408, "ISAKMP: Internet Security Associations and Key Management Protocol" 2002.

D. Piper, IETF RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP" November 1998.

David Soldani, Renaud Cuny, "On the Deployment of Multimedia Services in Wireless Networks: Radio Dimensioning Aspects for UTRAN FDD", Proceedings of the First International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QSHINE'04), 2004.

Davide Tosi, "An Advanced Architecture for Push Services", Proceedings of the Fourth International Conference on Web Information Systems Engineering Workshops (WISEW'03), 2004.

Dongmei Jiang, Tet Hin Yeap, Liscano, R., Logrippo, L, "Two Approaches for advanced presence services in SIP communications", IEEE 7th Malaysia International Conference on Communication, 2005.

Dongmei Jiang, Tet Hin Yeap, Luigi Logrippo, Ramiro Liscano, "Personalization for SIP Multimedia Communications with Presence", http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.63.8748.

El Sawda, R., Urien, P., Hajjeh, I, " Non Repudiation for SIP Protocol; SIP Sign", 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2005.

Eduardo Ribeiro, Rui J. Lopes, "An architecture for the provision of Content Networks based on IMS, Metadata, Presence and P2P technologies", Proceedings of MNCNA'07, Newport Beach - CA, USA, November 26, 2007.

Eugen Mikoczy, "Next Generation of Multimedia Services – NGN based IPTV architecture", 15th International Conference on Systems, Signals and Image Processing, 2008. IWSSIP 2008.

Fatna Belqasmi, Chunyan Fu, Mohammed Alrubaye, Roch Glitho, "Design and implementation of advanced multimedia conferencing applications in the 3GPP IP multimedia subsystem", IEEE Communications Magazine Volume 47 , Issue 11, November 2009.

Felipe Lalanne, Stephane Maag, Edgardo Montes de Oca, "An Automated Passive Testing Approach for the IMS PoC Service", 2009 IEEE/ACM International Conference on Automated Software Engineering, 2009.

Giorgos Karopoulos, Georgios Kambourakis, Stefanos Gritzalis, Elisavet Konstantinou, "A framework for identity privacy in SIP", Journal of Network and Computer Applications Volume 33 Issue 1, January, 2010 Academic Press Ltd. London, UK.

G. Kormentzas, T. Andrade, A. (Hamid) Asgari, C. Skianis, "Service management enhancements to IMS architecture", International journal of network management, 2007.

Garrett Weinberg, "Contextual Push-to-Talk: A New Technique for Reducing Voice Dialog Duration", MobileHCI'09, Bonn, Germany, September 15 - 18, 2009.

Gonzalo Camarillo, Miguel A. Garcia-Martin, "The 3G IP Multimedia Subsystem (IMS) – Merging the Internet and the Cellular Worlds", 2nd Edition, John Wiley & Sons Ltd. ISBN-13: 978-0-470-01818-7, The Atrium, Southern Gate, Chichester, West Sussex, England, 2006.

Günter Schäfer, "Research Challenges in Security for Next Generation Mobile Networks", www.pampas.eu.org/Position_Papers/UnivofBerlin.pdf.

H. Khartabil, Telio, E. Leppanen, M. Lonnfors, J. Costa-Requena "An Extensible Markup Language (XML)-Based Format for Event Notification Filtering" Request For Comments 4661, September 2006.

H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RFC 3550 RTP -A Transport Protocol for Real-Time Applications", July 2003.

H.Yeganeh,A.H.Darvishan,M.Dindoost,H.Sabaei, "A Proposed Structure for Application Server in NGN", The Third International Conference on Internet and Web Applications and Services, 2008.

Hanhua Lu, Yong Zheng, Yanfei Sun, "The Next Generation SDP Architecture: Based on SOA and Integrated with IMS", Proceedings of the 2008 IEEE Second International Symposium on Intelligent Information Technology Application, December 2008.

Humberto Abdelnur, Tigran Avanesov, Michael Rusinowitch and Radu State, "Abusing SIP authentication", Journal of Information Assurance and Security, 4, 2009.

Hung Nguyen Chan, "Research and Development of an integrated multimedia conferencing system", First International Conference on Communications and Electronics, 2006.

Hyun Wook, Miyoung Huh, ShinGak KangHyun Wook, Miyoung Huh, ShinGak Kang, "Design of presence agent server for SIP-based presence services", The 7th International Conference on Advanced Communication Technology, 2005.

Igor Miladinovic, "Presence and Event Notification in UMTS IP Multimedia Subsystem", Fifth IEE International Conference on 3G Mobile Communication Technologies (3G 2004) The Premier Technical Conference for 3G and Beyond (CP503) London, UK, 18-20 Oct. 2004.

Imen Grida, Ben Yahia, Emmanuel Bertin, Jean Pierre, Deschrevel Noel, Crespi, "Service Definition for Next Generation Networks", Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06), 2006.

I. Rish. An empirical study of the naive Bayes classifier. In Proc. IJCAI-01 Workshop on Empirical Methods in AI, volume 335, 2001.

J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", IETF RFC 3329, January 2003.

J. Fiedler, T. Kupka, S. Ehlert, T. Magedanz, D. Sisalem, "VoIP Defender: Highly Scalable SIP-based Security Architecture", IPComm, New York, USA, 2007.

J. Klensin, Ed., "Simple Mail Transfer Protocol, IETF RFC 2821", April 2001.

J. Rosenberg, "A Presence Event Package for the Session Initiation Protocol (SIP)", Request for Comments: 3856, 2004.

J. Rosenberg, "Presence Authorization Rules", Request for Comments: 5025, 2007.

Jae Cheon Han, Sun Ok Park, Shin Gak Kang, Hyoung Ho Lee , "A Study on SIP-based Instant Message and Presence", The 9th International Conference on Advanced Communication Technology, 2007.

Jae-Hyung Cho, Jae-Oh Lee, "IMS Based PoC Service Deployment", Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC, 2009.

Jae-Hyung Cho, Je-Hyun Lee, Bi-Feng Yu, Jae-Oh Lee, "Push-to-Talk Service Investigation and Improvement", Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing - Volume 02, 2009.

Jan Seedorf, "SIP Security Status Quo and Future Issues", events.ccc.de/congress/.../1116-22c3_SIPsecurity_JanSeedorf.pdf.

Jani Hautakorpi, Arturo Salinas, Erkki Harjula, and Mika Ylianttila, "Interconnecting P2PSIP and IMS", The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 2008.

Jenq-Muh Hsu, Wei-Bin Lain, Jui-Chih Liang, " A Context-Aware Push-to-Talk Service ", International Conference on Multimedia and Ubiquitous Engineering, 2008.

John Buford, Alan Kaplan, Vipul Bhasin, "Transparent Roaming Between Instant Messaging and Presence Service Providers in Wireless Networks", IEEE CCNC, 2006.

Juan, "A survey of IMS clients for NGN service delivery", Proceedings of the 9th international conference on Communications and information technologies, 2009.

Judy van Biljon, Paula Kotzé, "Modelling the Factors that Influence Mobile Phone Adoption", ACM SAICSIT 2007.

Juniper Networks, " Solution Brief – How Juniper Networks Enables Intelligent, Secure, and Open IMS-FMC Networks", September 2006.

K. Knuettel, T. Magedanz, L. Xie, "SIP Servlet Execution Environment (SIPSEE) – An MS / NGN SIP AS for Converged Applications", ICIN07 Conference, Bordeaux, France, 2006.

K. Knuttel, T. Magedanz, L. Xie, "SIP Servlet Execution Environment (SIPSEE) – An IMS / NGN SIP AS for Converged Application", International Conference on Intelligence in Networks, ICIN, Bordeaux, France, 2006.

Karim Sbata, Houda Khrouf, Sabine Zander, Monique Becker, "Converging Web and IMS services: stakes and solution proposals", Proceedings of MEDES 2009, France, October 27-30, 2009.

Kerry Jean, Kun Yang, Alex Galis, "A Policy Based Context-aware Service for Next Generation Networks", Department of Electronic & Electrical Engineering, University College London, Torrington Place, London WC1E 7JE, UK, 2009.

Kevin Doolin, Andreas Pashalidis, Andreas Kassler, "Context-Aware Multimedia Services in a Pervasive Environment- The Daidalos Approach", Software Organization & MonITоring of Ambient Systems Workshop.Canada, February 11-14, 2008.

Krish Pillai, Haseeb Akhtar, "Optimizations for Push-to-Talk in Wireless Networks", Proceedings of the 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies, 2009.

Lan Wang, Daqing Gu, "A Study on Session Setup for Group Communications in Push-to-talk over Cellular Using Rich Presence", ieeexplore.ieee.org/iel5/4391971/4391972/04392055.pdf?arnumber=4392055.

László Bokor, Zoltán Faigl, Sándor Imre, "Flat Architectures: Towards Scalable Future Internet Mobility", The future internet Springer-Verlag Berlin, Heidelberg ©2011.

Lishoy Francis, Keith Mayes, Gerhard Hancke, Konstantinos Markantonakis, "A location based security framework for authenticating mobile phones", M-MPAC '10 Proceedings of the 2nd International Workshop on Middleware for Pervasive Mobile and Embedded Computing ACM New York, NY, USA ©2010.

Loreto, S. Eriksson, G.A., "Presence Network Agent: A Simple Way to Improve the Presence Service", Communications Magazine, IEEE, 2008.

Luca Monacelli, Including Overload Control in Existing IMS Compliant Networks by Using Traffic Shapers", Mobimedia'09, September 7–9, 2009.

M. Ali Akbar, Muddassar Farooq, “Application of Evolutionary Algorithms in Detection of SIP based Flooding Attacks”, Genetic and Evolutionary Computation Conference (GECCO), ACM Press, Montreal, Canada, 2009.

M. Day, S. Aggarwal, G. Mohr, J. Vincent, “A Model for Presence and Instant Messaging” Request for Comments: 2778, 2000.

M. Day, S. Aggarwal, G. Mohr, J. Vincent, “Instant Messaging / Presence Protocol Requirements” Request for Comments: 2779, 2000.

M. Femminella, R. Francescangeli, F. Giacinti, E. Maccherani, A. Parisi, G. Reali, “Implementation of Third Party Media Server Controller for IMS Networks”, Proceedings of Mobimedia’09, London, UK, September 7–9, 2009.

Miikka Poikselka, Georg Mayer, Hisham Khartabil, Aki Niemi, ”IP multimedia concepts and services” 2nd Edition, Jhon Wiley & Sons Ltd. 2006.

M. Pous, D. Pesch, G. Foster, A. Sesmun, “Performance Evaluation of a SIP Based Presence and Instant Messaging Service for UMTS” 4th International Conference on 3G Mobile Communication Technologies, 2003. 3G 2003.

M. Sayyad, N. Ansari, S. Burli, H. Shah, A. Khatanhar, “Review of IP multimedia subsystem”, ICWET '11 Proceedings of the International Conference & Workshop on Emerging Trends in Technology ACM New York, NY, USA ©2011.

M. Sher, T. Magedanz, “Developing Network Domain Security (NDS) Model for IP Multimedia Subsystem (IMS)”, Journal of Networks, Vol.1, No.6, November/December 2006, pp.10-17, ISSN: 1796-2056 © Academy Publisher, Oulu, Finland, 2006.

M. Sher, T. Magedanz, “Development of IMS Privacy & Security Management Framework for FOKUS Open IMS Testbed”, Journal of Mobile Multimedia, Vol. 2, No.3, 225-258, ISSN: 1550-4646 © Rinton Press, 2006.

M. Sher, T. Magedanz, W.T. Walter, "Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)", IEEE 1st Int. Conference on Availability, Reliability & Security, Vienna, Austria, 20th-22nd April 2006. IEEE/ARES2006 Proceeding ISBN 978-0-7695-2567-9, pp. 502-509, April 2006.

M. T. Alam, and Z. D. Wu, “Dimensioning and optimization of push-to-talk over cellular server”, International journal of network management, 2008.

M. Zarri , “Future Service capabilities Offered by the 3gpp system”, 4th International Conference on 3G Mobile Communication Technologies, 2003. 3G 2003.

M. Zhang, Y. Fang, “Security Analysis and Enhancement of 3GPP Authentication and Key Agreement Protocol”, IEEE Transactions on Wireless Communication Vol. 4, No. 2, ISBN 1536-1276, March 2005.

M. Zubair Rafique, M. Ali Akbar and Muddassar Farooq, “Evaluating DoS Attacks Against SIP-Based VoIP Systems”, IEEE-GLOBECOM 2009.

MA Bihina Bella, JHP Eloff, MS Olivier, “USING the internet protocol detail record standard for next-generation network billing and fraud detection”, Information and Computer Security Architectures (ICSA) Research Group Department of Computer Science University of Pretoria Pretoria South Africa, 2008.

Magedanz, T., Popescu-Zeletin, R., "Intelligent Networks - Basic Technology, Standards and Evolution", International Thomson Computer Press, ISBN: 1-85032-293-7, London, UK, June 1996.

Mamdouh Gouda, Mohamed Haggag, "Enhanced Authentication Mechanism for Next Generation Networks", Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, 2009.

Marc Bailly, Philippe Menard, "Connecting mobile IMS services With Web applications", http://dx.doi.org/10.4108/ICST.MOBIMEDIA2009.7504.

Marek Natkaniec, Katarzyna Kosek-Szott, Szymon Szott, Janusz Gozdecki, Andrzej Głowacz, Susana Sargento, "Supporting QoS in Integrated Ad-Hoc Networks", Wireless Personal Communications: An International Journal, Volume 56 Issue 2, January 2011.

Martin Strohbach, Martin Bauer, Ernoe Kovacs, Claudia Villalonga, Nils Richter, " Context Sessions – A Novel Approach for Scalable Context Management in NGN Networks",MNCNA '07, November 26, 2007.

Matthias Bormann, Diederich Wermser, Ralf Patz, "Conformance Testing of Complex Services Exemplified with the IMS' Presence Service", Proceedings of the 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies, 2009.

Matthias Kranz, Paul Holleis, Albrecht Schmidt, "Ubiquitous Presence Systems", Proceedings of SAC'06 Dijon, France, April 23-27, 2006.

McKeon, F., "A study of SIP based instant messaging focusing on the effects of network traffic generated due to presence", IEEE International Symposium on Consumer Electronics, 2008.

Meng-hsun Tsai, Yi-bing Lin, " Talk burst control for push-to-talk over cellular", IEEE Transactions on Wireless Communications, 2008.

Michael T. Hunter, Russell J. Clark, Frank S. Park, "Security Issues with the IP Multimedia Subsystem (IMS)", MNCNA '07, November 26, 2007.

Miikka Poikselka, Georg Mayer, Hisham Khartabil, Aki Niemi, "IP multimedia concepts and services" 2nd Edition, Jhon Wiley & Sons Ltd. 2006.

MiYoung Huh, SunOk Park, Wook Hyun, JaeChon Han, IlJin Lee, ShinGak Kang, "Basic call flow for interoperability test in the presence services based on SIP", The 8th International Conference on Advanced Communication Technology, 2006.

MiYoung Huh, Wook Hyun, JaeChon Han, IlJin Lee, ShinGak Kang , "Design considerations for user authorization in the presence services based on SIP", The 7th International Conference on Advanced Communication Technology, 2005.

Mohammad Sabbir Alam, Michael Cohen, Ashir Ahmed , "Design for Controlling Media Privacy in SIP Conferencing Systems", International Conference on Digital Telecommunications, 2006.

Mohsin Iftikar, Tejeshwar Singh, Bjorn Landfeldt, Mine Caglar, " Multiclass G/M/1 queueing system with self-similar input and non-preemptive priority", Computer Communications, 2008.

Muhammad Sher, Shaoke Wu, Thomas Magedanz, “Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)”, IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation, 2006.

Muhammad Sher, Thomas Magedanz , “Developing Intrusion Detection and Prevention (IDP) System for IP Multimedia Subsystem (IMS) Application Servers (AS)”, Journal of information assurance and security, 2007.

Muhammad Sher, Thomas Magedanz , “Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks”, Third International Symposium on Information Assurance and Security, 2007.

Muhammad Sher, Thomas Magedanz, “Developing Network Domain Security (NDS) Model for IP Multimedia Subsystem (IMS)”, Journal of networks, 2006.

Muhammad T. Alam, Zheng da Wu, “Admission control approaches in the IMS presence service”, International Journal of Computer Science, Volume 1, Issue 4, 2007.

Muhammad T. Alam, Zheng da Wu, “Cost Analysis of the IMS Presence Service”, 1st Australian Confrence on Wireless Broadband and Ultra Wideband Communication, 2006.

N. Blum, T. Magedanz: “'Push-To-Video as a platform for NGN Services”, 11th European Wireless 2005 - "Next Generation Wireless and Mobile Communications and Services", Nicosia, Cyprus, April 10-13, 2005.

N. Subramanian, Sachin Narayanan, Mohammed Misbahuddin, “RUDRAA – an intRUsion Detection & pRevention signature formulAtion process”, International Conference on Advances in Computing, Communication and Control (ICAC3’09), 2009.

Natalia Kryvinska, Christine Strauss, Lukas Auer, Peter Zinterhof, “Conceptual framework for services creation/development environment in telecom domain”, proceedings of the 10th ACM International Conference on Information Integration and Web-based Applications & Services, November 2008.

Nigel Seel, “Chapter 2: The Next-Generation Network and IMS”, From: Business Strategies for the Next-Generation Network, Auerbach Publications, 2006.

Niklas Blum, Thomas Magedanz, “PTT + IMS = PTM - Towards Community/Presence-based IMS Multimedia Services ” Proceedings of the Seventh IEEE International Symposium on Multimedia (ISM’05), 2005.

Niklas Blum, Thomas Magedanz, Horst Stein, “Service Creation & Delivery for SME based on SOA / IMS”, Proceedings of MNCNA ’07, November 26, 2007.

Nikos Vrakas, Dimitris Geneiatakis, Costas Lambrinoudakis, “A call conference room interception attack and its detection”, TrustBus'10 Proceedings of the 7th international conference on Trust, privacy and security in digital business Springer-Verlag Berlin, Heidelberg ©2010.

Nisha Rajagopal and Michael Devetsikiotis, “Modeling and Optimization for the Design of IMS Networks”, Proceedings of the 39th Annual Simulation Symposium, 2006.

Noëmie SIMONI, Chunyang YIN, Rhéa BERBERI, Ghislain DU CHENE, "An NGN middleware based on an enhanced IMS", ACM MNCNA '07, 2007.

Noëmie SIMONI, Chunyang YIN, Rhéa BERBERI, Ghislain DU CHENE, "An NGN middleware based on an enhanced IMS", MNCNA '07, November 26, 2007.

Nokia Siemens Networks, "IMS Technical Description and Information" A50016-D3605-X20-1-7618, Id: 0900d80580129f8e, 2007.

O.Rashid, P.Coulton and R.Edwards, "Implications of IMS and SIP on the Evolution of Mobile Applications", IEEE Tenth International Symposium on Consumer Electronics, 2006. ISCE '06. 2006.

Otso Kassinen, Erkki Harjula, Petri Pohjanen, Timo Koskela, Jussi Ala-Kurikka, Mika Ylianttila, "Group-based content push with dynamic session startup", Proceedings of the 4th international conference on Mobile and ubiquitous multimedia, 2005.

Owen Conlan, Ruaidhrí Power, Keara Barrett, "Next Generation Context Aware Adaptive Services" Proceedings of the 1st international symposium on Information and communication technologies, Dublin, Ireland, 2003.

P. Karn, P. Metzger, W. Simpson, "The ESP Triple DES (3DES) Transform, IETF, RFC 1851", 1995.

P. Lewicki et al. Statistics: Methods and Applications. StatSoft, Inc., 2006.

P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core", Request for Comments: 3920, 2004.

Päivi Aarreniemi-Jokipelto, "Instant Messaging in Informal Learning via Interactive Television – Online Communities Among Children in a "Get Along" Program", ACM Computers in Entertainment, Vol. 5, No. 2. August 2007.

Paolo Bellavista, Antonio Corradi, Luca Foschini, "Enhancing the Scalability of IMS-Based Presence Service for LBS Applications", Proceedings of the 2009 33rd Annual IEEE International Computer Software and Applications, 2009.

Paolo Bellavista, Antonio Corradi, Luca Foschini, "IMS-based presence service with enhanced scalability and guaranteed QoS for interdomain enterprise mobility", IEEE Wireless Communications, Volume 16 , Issue 3, 2009.

Parthasarathy, A., "Push to talk over cellular (PoC) server", IEEE Networking, Sensing and Control, 2005. Proceedings. 2005.

Peter Reichl, Sandford Bessler, Joachim Fabini2, Rudolf Pailer, Joachim Zeiss, "Implementing a Native IMS Location Service Enabler over a Prototypical IMS Core Network Testbed" Proceedings of the 8th IEEE International Conference on E-Commerce Technology and the 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), 2006.

Peternel, K., Zebec, L., Kos, A., "Using presence information for an effective collaboration", 6th International Symposium on Communication Systems, Networks and Digital Signal Processing, 2008.

Prof. Dr. Ing. habil. Thomas Magedanz, "IMS vs. P2P and Web 2.0 - Understanding the Role of the IP Multimedia System (IMS) in Face of a Converging Telco and Internet Service World", Eighth International Workshop on Applications and Services in Wireless Networks, 2008.

R. Bonica, D. Gan, D. Tappan, C. Pignataro, "Extended ICMP to Support Multi-Part Messages, IETF RFC 4884", 2007.

R. Housley, W. Polk, W. Ford, D. Solo, IETF RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002.

R. Pereira, R. Adams, "The ESP CBC-Mode Cipher Algorithms" IETF RFC 2451, November, 1998.

R. Rivest, IETF RFC 1321, "MD5: Message Digest Algorithm", April 1992.

R. Sparks, "The Session Initiation Protocol (SIP) Referred-By Mechanism", IETF RFC 3892, September 2004.

Radu State, "New Frontier in VoIP Security" and "Building Management and Security Solutions of Tomorrow's Internet" Madynes Research Project, INRIA Nancy Universités Centre de Recherché Grand Est., France, 2007.

Rahnnan, M., Bin Hu, Buford, J., Kaplan, A, "Mobile multimedia instant messaging and presence services: the architecture and protocols", IEEE International Symposium on Consumer Electronics, 2004.

Ravi Jain, John-Luc Bakker, Farooq Anjum, "Programming Converged Networks – Call Control in Java, XML, and Parlay/OSA", ISBN 0-471-26801-1, John Wiley & Sons, Inc. 111 River Street, Hoboken, NJ 07030, USA, 2005.

Rebahi, Y., Sher, M., Magedanz, T., "Detecting flooding attacks against IP Multimedia Subsystem (IMS) networks", IEEE/ACS International Conference on Computer Systems and Applications, 2008.

Rishi, L. Kumar, S, "Presence and its effect on network", IEEE International Conference on Personal Wireless Communications, 2005.

Roach, A., "SIP-Specific Event Notification", RFC 3265, June 2002.

Robert Dinoff, Richard Hull, Bharat Kumar, Daniel Lieuwen, and Paulo Santos, "Learning and Managing User Context in Personalized Communications Services", Proceedings of AVI '06, Venice, Italy, May 23, 2006.

Roman Levenshteyn, Ioannis Fikouras, Salvatore Loreto, Gonzalo Camarillo, Gonzalo Camarillo, "Addressing & Invocation of IMS-attached Services", Proceedings of IPTCOMM '07, New York USA, 2007.

Roman, Ioannis Fikouras, Salvatore Loreto, Gonzalo Camarillo, "Addressing & Invocation of IMS-attached Services ", ACM IPTCOMM '07, 2007.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

Rudolf Pailer, Johannes Stadler and Igor Miladinovic, "Using PARLAY APIs Over a SIP System in a Distributed Service Platform for Carrier Grade Multimedia Services" Wireless Networks 9, 353–363, 2003.

Rudolf Pailer, Florian Wegscheider, Sandford Bessler, "A Terminal-Based Location Service Enabler for the IP Multimedia Subsystem", proceedings of WCNC 2006.

Rui Santos Cruz, Mário Serafim Nunes, Guido Varatojo, Luís Reis, "Push-to-Talk in IMS Mobile Environment", Proceedings of the 2009 Fifth International Conference on Networking and Services, 2009.

S. Bellovin, J. Ioannidis, A. Keromytis, R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPSec", IETF, RFC 3554, July 2003.

S. Frankel, R. Glenn, S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPSec" IETF RFC 3602, September, 2003.

S. Kent, "IP Encapsulating Security Payload (ESP)", IETF RFC 4303, December 2005.

S. Kent, K. Seo, "Security Architecture for the Internet Protocol", IETF RFC 4301, December 2005.

S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, 1998.

S. Kiran, P. Lareau, S. Lloyad, "PKI Basics – A Technical Perspective", November 2002.

S. Santesson, R. Housley, IETF RFC 4325, "Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension" 2005.

Salekul Islam and Jean-Charles Grégoire, "User-Centric Service Provisioning for IMS", Proceedings of Mobility, France, sep 2-4, 2009.

Scott Bradner, "NGN Replacement or Evolution?" Harvard University 12 September 2005.

Sher, M.; Magedanz, T.; Penzhorn, W.T., "Inter-domains security management (IDSM) model for IP multimedia subsystem (IMS)", The First International Conference on Availability, Reliability and Security, 2006.

Sipera Technical Security Report, "Protecting IMS Netwroks from Attacks: Operators Need More than Encryption and Authentication" 2007.

SIPSEE (SIP Servlet Execution Environment) is the FOKUS development of a SIP Application Server (SIP AS) based on SIP Servlet Technology, 2006.

Skĕnder Rugova, Arianit Maraj, "Analysis of call scenario in NGN network",Proceedings of the 8th WSEAS international conference on Electronics, hardware, wireless and optical communication, 2009.

Stefan Wahl, Konrad Rieck, Pavel Laskov, Peter Domschitz, Klaus-Robert Müller, " Securing IMS against novel threats", Bell Labs Technical Journal, Volume 14 , Issue 1, May 2009.

Stefanie Richter, Andreas Bohm, "A location and privacy service enabler for context-aware and location-based services in NGN", 12th International Telecommunications

Network Strategy and Planning Symposium, 2006.

Subharthi Paul, Jianli Pan, Raj Jain, "Architectures for the future networks and the next generation Internet: A survey", Computer Communications, Volume 34 Issue 1, January, 2011.

Sumit Mittal, Dipanjan Chakraborty, Sunil Goyal, and Sougata Mukherjea, "SewNet - A Framework for Creating Services Utilizing Telecom Functionality", WWW 2008, Beijing, China, April 21–25, 2008.

Sun Ok Park, I Jin Lee, Jae Cheon Han, Mi-Young Huh, Shin Gak Kang, "A study on XCAP client system for SIP-based IMPP services", The 7th International Conference on Advanced Communication Technology, 2005.

Sung Bo Yang, Sung Gon Choi, Se Yun Ban, Yoo-Jung Kim, Jun Kyun Choi, "Presence service middleware architecture for NGN", The 8th International Conference on Advanced Communication Technology, 2006.

Sven Ehlert, Yacine Rebahi, Thomas Magedanz, " Intrusion Detection System for Denial-of-Service flooding attacks in SIP communication networks",International Journal of Security and Networks Volume 4 , Issue 3 Pages: 189-200, 2009.

Swapnil Kumar Raktale, "3Poc : An Architecture for Enabling Push To Talk Services in 3GPP Networks", IEEE International Conference on Personal Wireless Communications, 2005.

Syed A. Ahson, Mohammad Ilyas, "Location-Based Services Handbook: Applications, Technologies, and Security", 1st CRC Press, Inc. Boca Raton, FL, USA ©2010.

T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax, IETF RFC 3986" January 2005.

T. Magedanz, D. Witaszek, K. Knuettel, "The IMS Playground @ FOKUS – An Open Testbed for Next Generation Network Multimedia Services", Proceedings of the First International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities (TRIDENTCOM'05), 2005.

T. Magedanz, K. Knüttel, D. Witszek: "The IMS Playground @ Fokus – an Open Testbed for Next Generation Network Multimedia Services", 1st Int. IFIP Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (Tridentcom), Trento, Italian, February 23 - 25, Proceedings pp. 2– 11, IBSN 0-7695-2219-x, IEEE Computer Society Press, Los Alamitos, California, 2005.

T. Magedanz, M. Sher, "IT-based Open Service Delivery Platforms for Mobile Networks -From CAMEL to the IP Multimedia System", chapter of "Mobile Middleware" book, ISBN: 0849338336, edited by P. Bellavista and A. Corradi published by Chapman & Hall/CRC Press, 2006.

Teck Yoong Chai, Teck Kiong Lee, "An IMS-Based Testbed for Service Innovations", Proceedings of the 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies, 2009.

The Georgia Technology Information Security Center (GTISC), "Emerging Cyber Threats Report for 2008" USA, October 2007.

The University of Southern California and VeriSign "Building a Security Framework for Delivery of Next Generation Network Services" 2005.

Thierry Bessis, Vijay K. Gurbani, Ashwin Rana, "Session Initiation Protocol firewall for the IP Multimedia Subsystem core", Bell Labs Technical Journal Volume 15 Issue 4, March 2011, John Wiley & Sons, Inc. New York, NY, USA.

Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3GPP, TS 33.210, Network Domain Security (NDS); IP Network Layer Security V6.5.0, 2004.

Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3G Security; "Access Security for IP-based services (Release 6)", 3GPP, TS 33.203 V6.4.0, 2004.

Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3GPP, TS 33.210, Network Domain Security (NDS); IP Network Layer Security V6.5.0, 2004.

Third Generation Partnership Project Technical Specification, "Generic Authentication Architecture (GAA); Early Implementation of HTTPS Connection between a Universal Integrated Circuit Card (UICC) and Network Application Function (NAF) (Release 7)", 3GPP TR 33.918 V7, 2005.

Third Generation Partnership Project Technical Specification, "Network Domain Security (NDS); Authentication Framework (AF) Release 7" TS 33.310 V7.1.0, 2006.

Third Generation Partnership Project Technical Specification, "Sh Interface based on the Diameter Protocol (Release 7)", 3GPP TS 29.329 V 7.3.0. 2006.

Third Generation Partnership Project Technical Specification, "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 7)", 3GPP TS 31.111 V7, 2005.

Third Generation Partnership Project, "Presence Service, Architecture and Functional Description (Release 6)", 3GPP TR 23.841, V6.0.0. 2002.

Third Generation Partnership Project, Technical Specification, "3GPP, TS 29.208, Endto- end Quality of Service (QoS) Signalling Flows", March 2006.

Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6); 3GPP, TS 33.102 V6, 2004.

Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 7), 3GPP TS 33.220 V7, 2005.

Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 7), 3GPP TS 33.222 V7, 2005.

Third Generation Partnership Project; Technical Specification, "3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the

3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification", 3GPP TS 35.206 V 6.0.0, 2004.

Thomas Magedanz, "Tutorial IEEE ISCC", IEEE Symposium on Computer and Communications", Spain, 27 June 2005.

Timo Ali-Vehmas, Sakari Luukkainen, "Service adoption strategies of push over cellular", Personal and Ubiquitous Computing, Volume 12, Number 1 / January, 2008.

Timo Ali-Vehmas, Sakari Luukkainen, "Service Diffusion Strategies for Push to Talk Over Cellular", Proceedings of the International Conference on Mobile Business (ICMB'05), 2005.

Tomonori Aoyama, "A New Generation Network – Beyond NGN –", First ITU-T Kaleidoscope Academic Conference, 2008.

Tran Tuan Anh, Tapio Erke, Kalevi Kilkki, " Push to talk over cellular traffic modeling", 14th IEEE International Conference on Networks, 2006.

Transition to NGN Networks, White Paper, Telrad Networks Ltd. 2006.

Urban Sedlar, Darko Bodnaruk, Luka Zebec and Andrej Kos, "Using aggregated presence information in an enterprise environment", https://www.icin.biz/files/programmes/Poster-7.pdf

V. Gurbani, A. Jeffrey, draft-gurbani-sip-tls-use-00: The Use of Transport Layer Security (TLS) in the Session Initiation Protocol (SIP), February 2006.

V. Niemi, K. Nyberg, "UMTS Security" ISBN 0-470-85314-X, John Willey & Sons Ltd. West Sussex, England, 2003.

Verizon and Cisco, "Advances to IP Multimedia Subsystem (A-IMS) Architecture, White Paper", June 2006.

Victor C.M. Leung, Terrence Wong, Peyman TalebiFard, "Breaking the Silos – Access and Service Convergence over the Mobile Internet", Proceedings of MSWiM'08, Canada, October 27 - 31, 2008.

Victoria Beltran, Josep Paradells, "Middleware-Based Solution to Offer Mobile Presence Services", Mobilware'08, 2008.

Vignal Giovanni et al, A Stateful Intrusion Detection System for World-Wide WebServers (WEBSTAT), 2003.

Vishal K. Singh and Henning Schulzrinne, "A Survey of Security Issues and Solutions in Presence", www1.cs.columbia.edu/~vs2140/presence/presencesecurity.pdf

Wegscheider, F., "Minimizing unnecessary notification traffic in the IMS presence system", 1st International Symposium on Wireless Pervasive Computing, 2006.

Wei Zheng, Chunhong Zhang, Cuibo Yu, Peng Yang, Yuqi Mu, Xiaohua Zhang, "Design of Presence Based Dynamic Group IM in IMS", Proceedings of the 2009 Fifth International Joint Conference on INC, IMS and IDC, 2009.

Whai-En Chen, Yi-Bing Lin, Ren-Huang Liou, "A weakly consistent scheme for IMS presence service", IEEE Transactions on Wireless Communications, volume 8, issue 7, 2009.

William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta "Exploiting Open Functionality in SMS Capable Cellular Networks", ACM, CCS 05, Nov 7-11, 2005, Alexandria, Virginia, USA 2005.

William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta "Mitigating attack on Open Functionality in SMS Capable Cellular Networks", ACM, MobiCom'06, Sep. 23-26, Los Angeles, California, USA, 2006.

William Stallings, "Cryptography and Network Security", 4th Edition, ISBN 0131873164, Prentice Hall, 2005.

Writing Detection Signatures – Christopher Jordan www.usenix.org/publications/login/2005-12/pdfs/jordan.pdf.

Yong Zheng (Vincent), "The Next Generation Network: Issues and Trends", School of Computing and Mathematical Sciences, November 2008.

Yongmei Luo, Zhigang Jin, Ximan Zhao, "Implement push to talk function in WinCE based terminals", Proceedings of the 5th International Conference on Wireless communications, networking and mobile computing, 2009.

Yufei Cao, Jianxin Liao, Qi Qi Xiaomin Zhu, "A Cache Based Session Setup Mechanism for IMS", IEEE International Conference on Communications Workshops, 2008.

Yu-mei WANG, Jian QIN, Jia-Jia WEN, Yu Liu, "Managing Feature Interaction based on Service Broker in IP Multimedia Subsystem", Conference on Mobile Technology, Applications & Systems 2008 (Mobility Conference), Taiwan, 10-12 September, 2008.

Yu-mei Wang, Kai Yang, Lina Ren, Ke Yu, "An Improved SCIM-based Service Invocation Mechanism for Integrated Services in IMS", Conference on Mobile Technology, Applications & Systems 2008 (Mobility Conference), Taiwan, 10-12 September, 2008.

Yu-Sung Wu, Saurabh Bagchi, Schin Garg, Navjot Singh, Tim Tsai, SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments, 2004.

Yu-Sung Wu, Saurabh Bagchi, Schin Garg, Navjot Singh, Tim Tsai, SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments, 2004.

Zhigang Jin, Hui Jin, Lu Han, "Instant messaging and presence services using simple", ieeexplore.ieee.org/iel5/9709/30648/01414731.pdf?arnumber=1414731

Zhongwen Zhu, "An IMS Based Inter-working Solution for Multimedia Service in a Converged Network", International Conference on Multimedia and Ubiquitous Engineering, 2008.

Zhongwen Zhu, Fatna Belqasmi, Chunyan Fu, Roch Glitho, "A novel lookup service enabler for presence-based applications and its architecture in the 3GPP IP multimedia subsystem", Proceedings of the 3rd international conference on New technologies, mobility and security, 2009.

Zhou Xing, Lu Meilian, "Performance evaluation of IMS-based push-to-talk service over multiple wireless access networks", Proceedings of the 5th International Conference on Wireless communications, networking and mobile computing, 2009.

Web-Links

www.3gpp.org/specs/releases-contents.htm

http://www.dslforum.org/

http://portal.etsi.org/tispan/

http://www.thefmca.com/

http://cve.mitre.org/

http://en.wikipedia.org/wiki/Intrusion-detection_system

http://iptcomm.org/

http://nvd.nist.gov/

http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_27_Sophia_Antipolis/Docs/PD

http://www.acmepacket.com/html/page.asp?PageID=%7B51CB22C4-7243-43D1-

http://www.fokus.fraunhofer.de/bereichsseiten/testbeds/ims_playground/components/si

http://www.fokus.fraunhofer.de/bereichsseiten/testbeds/national_host/testbed/testbed.p

http://www.fokus.fraunhofer.de/home/index.php?lang=en

http://www.fokus.fraunhofer.de/ims/index.php?lang=en

http://www.fokus.fraunhofer.de/ngni/topics/ims_core.php

http://www.gtisc.gatech.edu/pdf/GTISC%20Cyber%20Threats%20Report.pdf

http://www.juniper.net/solutions/literature/solutionbriefs/351218.pdf

http://www.netfilter.org/

http://www.oasis-pki.org/pdfs/PKI_Basics-A_technical_perspective.pdf.

http://www.sans.org/reading_room/whitepapers/detection/

http://www.sans.org/reading_room/whitepapers/intrusion/

http://www.sipfoundry.org/sip-forum-test-framework/sip-forum-test-frameworksftf.

http://www.verisign.com/static/035478.pdf

http://jetty.mortbay.org/jetty/index.html.

http://www.linuxjournal.com/

http://www.openmobilealliance.org/

http://sipp.sourceforge.net/

http://www.parlay.org/en/index.asp.

www.nessus.org

www.securityfocus.com

www.snort.org

www.snort.org/

http://www.openimscore.org

http://www.iptel.org/ser/

http://www.umts-forum.org/

Research Publications: Zeeshan Shafi Khan

Journal Publications

Publications From Thesis

1. **Zeeshan Shafi Khan**, Nazish Munawar, Muhammad Sher, Khalid Rashid, Aneel Rahim, "An Extended Push to Multimedia Service for IP Multimedia Subsystem" International Journal of Innovative Computing, Information and Control, vol 7, issue 10, October 2011 *(Impact Factor 1.67)*

2. **Zeeshan Shafi Khan**, Khalid Rashid, Fahad Bin Muhaya, Qutbuddin, Aneel Rahim, "Realization of Call-Back Authentication (CBA) for secure web to cellular phone SMS communication", Computers and Mathematics with Applications 60 (2010) pp. 198_208 *(Impact Factor 1.19)*

3. **Zeeshan Shafi Khan**, Muhammad Sher, Khalid Rashid, Aneel Rahim, "Presence Based Conditional Call Setup for IP Multimedia Subsystem", International Journal of Physical Sciences Vol. 5(8), pp. 1248-1255, 4 August 2010 *(Impact Factor 0.55)*

4. **Zeeshan Shafi Khan**, Khalid Rashid, Muhammad Khurram Khan, Muhammad Sher, "An Extended Intrusion Detection and Prevention System for IP Multimedia Subsystem" Information, Volume 14, Issue 1, 2011 *(Impact Factor 0.09)*

5. **Zeeshan Shafi Khan,** Muhammad Sher, Khalid Rashid "Extended Role of Presence in IMS Call Setup" Information Journal (Accepted) *(Impact Factor 0.06)*

6. **Zeeshan Shafi Khan**, Muhammad Sher, Khalid Rashid, Aneel Rahim, "A Three Layer Secure Architecture for IP Multimedia Subsystem Based Instant Messaging", Information Security Journal: A Global Perspective, ISSN: 1939-3547, Volume 18, Issue 3 2009 , pages 139 – 148

Other Publications

7. Aneel Rahim, **Zeeshan Shafi Khan**, Fahd Bin Muhaya, Muhammad Sher, " Sensor based Framework for Secure Multimedia Communication in VANETs" Sensors 2010, 10(11), 10146-10154; doi:10.3390/s101110146 *(Impact Factor 1.81)*

8. Farzana Azam, **Zeeshan Shafi Khan**, Muhammad Sher, Khaled Alghtaber, Muhammad Khurram Khan "Attack Containment in Mobile Ad-hoc Network through Fair Distribution of Processing Resources" Telecommunication Systems Journal (Accepted) *(Impact Factor 0.67)*

9. Aneel Rahim, **Zeeshan Shafi Khan**, Fahad Bin Muhaya, Muhammad Sher, Muhammad Khurram," Information Sharing in VANETs", International Journal of Computers, Communications & Control (IJCCC), Vol. V (2010), No. 5, pp. 884-891, 2010 *(Impact Factor 0.37)*

10. Aneel Rahim, Muhammad Sher, **Zeeshan Shafi Khan** "Performance evaluation of Broadcast Approaches in VANETS" , Indian Journal of Science and Technology ISSN: 0974- 6846, Vol.2 No. 10, Oct 2009

11. **Zeeshan Shafi Khan**, Saira Shokat, Aneel Rahim, Muhammad Sher, Khalid Rashid "Ordering and Organization of SIP Requests within IMS Core by Using Load Awareness and Priority" International Journal of Recent Trends in Engineering, ISSN: 1797-9617, Vol 2, Issue 3 pp: 24-26

12. Aneel Rahim, Imran Ahmad, **Zeeshan Shafi Khan**, Muhammad Sher, "A Comparative Study Of Mobile And vehicular Adhoc Networks" I International Journal of Recent Trends in Engineering, ISSN: 1797-9617, Vol 2, Issue 3 pp: 125-127.

13. Aneel Rahim, **Zeeshan Shafi Khan**, M.A. Ansari, Muhammad Sher, "Enhance Relevance based approach for Network Control Relevance", Infomatica Journal ISSN: 0350-5596 (Accepted)

Conference Proceedings

Publications from Thesis

14. **Zeeshan Shafi Khan**, Muhammad Sher, Khalid Rashid "Presence Based Secure Instant Messaging Mechanism for IP Multimedia Subsystem", The 11th International Conference on Computational Science and Its Applications (ICCSA 2011), 2011, Spain (Accepted)

15. M. Zubair Rafique, **Zeeshan Shafi Khan**, Muhammad Khurram Khan, Khaled Alghtbar "Securing IP-Multimedia Subsystem (IMS) Against Anomalous Message Exploits by using Machine Learning Algorithms" 8th International Conference on Information Technology: New Generations, April 11-13, 2011 Las Vegas, USA

16. **Zeeshan Shafi Khan**, Nabila Akram, Khaled Alghtbar, Muhammad Sher, Rashid Mehmood "Secure Single Packet IP Traceback Mechanism to Identify the Source of Spoofed IP Users", The 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010), November 8-11, 2010, London, UK

17. **Zeeshan Shafi Khan**, Khaled Alghtbar, Muhammad Sher, Khalid Rashid, "Issues of Security and Network Load Balancing in Presence – A Survey", International Conference on Security Technology, 2010, Jeju, South Korea

18. **Zeeshan Shafi Khan**, Aneel Rahim, Fahad Bin Muhaya, "A Mechanism of Handling Internal Threats of IMS Based Push to Talk and Push to Multimedia Services", IEEE International Workshop on Advances in Multimedia Security (AIMS 2010), 2010, South Korea

19. **Zeeshan Shafi Khan**, Muhammad Sher, Khalid Rashid, Imran Razzak, "Towards Security and Enrichment of the IP Multimedia Subsystem Based Multiparty Conference" International Conference on Communication Systems and Applications, 18-20 March, 2009, Hong Kong

Other Publications

20. Muhammad Waqar, **Zeeshan Shafi Khan**, "Web 2.0 content extraction", The 5th International Conference for Internet Technology and Secured Transactions (ICITST-2010), November 8-11, 2010, London, UK

21. Aneel Rahim, **Zeeshan Shafi Khan**, Fahad bin Muhaya, "Performance evaluation of video streaming in Vehicular adhoc network" International Workshop of Wireless and Network Security WNS, 2010, Japan

22. Sharjeel Gilani, **Zeeshan Shafi Khan**, Muhammad Zubair, "Receiver Based Traffic Control Mechanism To Protect Low Capacity Network In Infrastructure Based Wireless Mesh Network" First International Workshop on Wireless and Network Security (WNS 2010), 2010, Japan

23. Waheed Khan, Muhammad Sher, **Zeeshan Shafi Khan**, "Integration of Location Update mechanism in IP multimedia subsystem" 2010 International Conference on Networking and Information Technology (ICNIT 2010), 2010, Manila Philippines

24. Bashir Ahmed, **Zeeshan Shafi Khan,** Adeel Akhtar, "An Efficient Modified Hybrid Adaptive Intra Cluster Routing Mechanism for Wireless Sensor Networks", IEEE 2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC), 2010, Tamil Nadu, India

25. Zulfiqar Hussain, **Zeeshan Shafi Khan**, Rashid Mehmood, "Best Suitable Transport Protocols under various scenarios of Multi-Protocol Label Switching" IEEE 2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC), 2010, Tamil Nadu, India

26. Imran Razzak, **Zeeshan Shafi Khan**, Muhammad Sher, Syed Afaq Hussain "Combining Offline and Online Urdu Character Recognition", International Conference on Imaging Engineering, , 2009, Hong Kong

27. **Zeeshan Shafi Khan**, Farzana Azam, Muhammad Sher, Khalid Rashid "Securing the future of communication-Enhanced and Secure registration Procedure for IP Multimedia Subsystem", 6th IEEE International Bhurban Conference on Applied Sciences & Technology", January 2009, Islamabad, Pakistan

28. Aneel Rahim, Muhammad Sher, Muhammad Shoaib, **Zeeshan Shafi Khan**, "PBBS: Priority Based Broadcast Scheme for VANETs ", 6th IEEE International Bhurban Conference On Applied Sciences & Technology IBCAST, 2009, Islamabad, Pakistan

29. Aneel Rahim, Imran Ahmad, Muhammad Sher, **Zeeshan Shafi Khan**, "Relevance Based Approach with Virtual Queue Using 802.11e protocol for Vehicular Adhoc Networks", The 2nd IEEE International Conference On Computer, Control, PNEC, 14 Feb 2009, Karachi, Pakistan

30. Aneel Rahim, **Zeeshan Shafi Khan**, Muhammad Sher, "A Need of Secure Data Dissemination Scheme for VANETS ",Doctoral Symposium on Research in Computer Science", IEEE, 9-10 Aug 2008, Lahore, Pakistan

31. Aneel Rahim, Imran Ahmad, Adeel Javed, **Zeeshan Shafi Khan**, Muhammad Sher, "A Survey On Broadcast Approaches In VANETS", Mosharaka International Conference on Communications, Networking and Information Technolog, 2008, Jordan.