Attacks Analysis & Bio-Inspired Security Framework for IP Multimedia Subsystem (IMS)

MS Thesis By:

Aliya Awais

Submitted to the Department of Computer Engineering in partial fulfillment of the requirement for the degree of

Master of Science

In

Computer Software Engineering

Thesis Supervisor:

Dr. Muddassar Farooq

College of Electrical & Mechanical Engineering

National University of Sciences & Technology

Rawalpindi, Pakistan

2007

Dedicated to My Grandfather and to My Parents

Air Commodore (R) Sultan Ahmed (late),

Major (R) Ahmed Owais,

&

Mrs. Ismat Owais

Abstract

The aim of this thesis is to analyze the security vulnerabilities and requirement of IP Multimedia Subsystem (IMS), particularly the impact of Denial of service (DoS) and Distributed (DoS) attacks on IMS network. Finally, develop an intelligent Bio-inspired self-defending / self-healing security frame work for IMS and Next Generation All-IP Networks, which will complement existing authentication and encryption mechanisms to protect infrastructure nodes and subscribers against the attacks launched by malicious nodes in the network. The unique and real-time vulnerabilities which need to be addressed in the IMS include: IMS framework-related vulnerabilities, session initiation protocol (SIP) vulnerabilities, media plane related vulnerabilities, authentication and encryption protocol vulnerabilities, Voice-over-IP (VoIP)/video/messaging/Push-to-talk-over-Cellular (PoC) spam and service abuse of IMS applications like VoIP, video, PoC, messaging, presence and conferencing. This framework is expected to become a cardinal component that will protect against the misuse of the network resources of an operator.

This framework will be integrated into any IMS converged network infrastructure to provide defense against wide varieties of attacks particularly Denial of Service (DoS) attacks. The goal is that our system will ultimately become an integral part of security framework for IMS and Next Generation All-IP networks.

Acknowledgements

First of all, I praise to Allah Almighty the merciful, beneficent, the source of all knowledge, who granted me the courage and knowledge to complete this research successfully.

I am grateful to my supervisor Dr. Muddassar Farooq, for his guidance and professional acumen, throughout my research thesis. He has been available for helping me with research and provided valuable inputs for completion of thesis and providing friendly and supportive environment.

I am grateful to Brig. Dr. Muhmmad Younus Javed, Head of Department of Computer Engineering, for his guidance and benign support during my MS and thesis. I am also grateful to Ms. Assia Khanum and Dr. Shaleeza Sohail for guiding and encouraging me complete this thesis. I would also, to like to thank all the faculty members for teaching us in a very professional way, without whose help we would not have been where we are.

I would also like to thank Dr. Muhammad Sher who was my teacher and supervisor. He guided me to this project and provided valuable inputs for completing my thesis.

Above all I owe every thing to my beloved parents and unable to find words to express my gratitude for them, Major (R) Ahmad Awais, Mrs. Ismat Awais, my sister Saima Awais and my husband Zia Farani, for their love, guidance, moral support, and encouragement. Last but not the least my grandfather Air Commodore (R) Sultan Ahmed, he is no more with us but his prayers are always with me.

I would also like to thank all my colleagues and seniors who were there to support and motivate me, during my MS.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AS	Application Server
IMS	IP Multimedia Subsystem
NGN	Next Generation Networks
SDP	Service Delivery Platform
OMA	Open Mobile Alliance
3GPP	3rd Generation Partnership Project.
ETSI	European Telecommunications Standards Institute
3GPP2	Third Generation Partnership Project 2
SIP	Session Initiation Protocol
AIS	Artificial Immune System
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
CSCF	Call Session Control Functions
P-CSCF	Proxy Call Session Control Function
I-CSCF	Interrogating Call Session Control Function
S-CSCF	Serving Call Session Control Function
MGCF	Media Gateway Controlling Function
MRCF	Media Resource Control Function
AV	Authentication Vector
BGCF	Breakout Gateway Control Function
CDF	Charging Data Function
MGW	Media Gateway
HSS	Home Subscriber Service
DTMF	Dual-Tone Multi Frequency
AS	Application Server
IMS	IP Multimedia Subsystem
NGN	Next Generation Networks
PSTN	Public Switched Telephone Network
LB-IM	Location Based Instant Messaging
MSC	Mobile Switching Centre
PLMN	Public Land Mobile Network
CS	Circuit Switch
PS	Packet Switch
CBS	Client Billing Service
CFS	Call Forwarding Service

Chapter 1

Introduction

The objective of this research is to study existing security framework, investigate the use and feasibility of incorporating Artificial Immune System (AIS) for provision of security to IMS and Next Generation "all-IP" Networks, and prove the concept model by comparing AIS based security framework with an existing security framework. The Biological Immune System (BIS) is a robust, complex, adaptive system that defends the body from foreign pathogens. It is able to categorize all cells (or molecules) within the body as self-cells or non-self cells. It does this with the help of a distributed task force that has the intelligence to take action from a local and also a global perspective using its network of chemical messengers for communication. This remarkable information processing biological system has caught the attention of computer science in recent years. A novel computational intelligence technique, inspired by immunology, has emerged, known as Artificial Immune Systems. Goal is to be able to build a Biological Immune System (BIS) that learns the agent behavior and than detects misbehavior. This however has less processing and communication cost as compared to signature based Intrusion Detection Systems (IDS). Artificial Immune System (AIS) is an anomaly based system and can be viewed as a general pattern learning system and is distributive and scalable. The features of AIS that are particularly important are its self-identity which enables AIS to understand normal behavior of the agents or user and generate corresponding self-antigens. The AIS then generates a repository of anti bodies which can detect an anomalous behavior.

1.1 Problem Statement

In this research project we will develop an intelligent Bio-inspired self-defending/ self-healing security framework for IP Multimedia System (IMS) and Next Generation All-IP Networks, which will complement existing authentication and encryption mechanisms to protect infrastructure nodes and subscribers against the attacks launched by malicious nodes in the network. We will tackle all network level vulnerabilities above the physical layer: MAC, network and application related vulnerabilities (see Tables 3.1, 3.2 and 3.4 in Chapter 3 Section 3.1). This framework is expected to become a cardinal component of IMS core that will protect not only

against these vulnerabilities but also against the misuse of the network resources of an operator. In order to address the unique requirements stemming from the different and novel direction of our research project, we will follow a hybrid system engineering model for our research project which will foster creativity and novelty in our proposed framework on the one hand and a systematic monitoring on the basis of quantifiable deliverables on the other hand. We have to devise an efficient research methodology to incorporate the results of the research in the final solution in a timely fashion. Our proposed research methodology consists of following important work projects:

a. Analyzing the IMS core for vulnerabilities (see Chapter 3 Section 3.1)
b. Reviewing a list of possible attacks that a malicious node can launch (see Chapter 3 Section 3.1)
c. Analyzing security shortcomings in the architecture of IMS framework (see Chapter 6)
d. Mapping the list of attacks to IMS domains/layers (see Chapter 6)
e. Proposing a Bio-inspired lightweight solution for IMS core (Chapter 6)
f. Evaluating and validating the proposed solution (Chapter 7 ,Chapter 8)

1.2 Introduction to Thesis

Chapter 2 explains the Principles, Architecture and Applications of IP Multimedia Subsystem.

Chapter 3 in this chapter IMS security requirements and threats are discussed and define unique attack taxonomy for IMS networks and also discussed security weaknesses in 2G and 3G access and core networks.

Chapter 4 explains existing security frameworks for IMS and methodologies for Introduction detection and prevention systems.

Chapter 5 explains bio-inspired security and introduces the mechanisms present in the biological IS from which the field of AIS draws its inspiration.

Chapter 6 describes and explains the proposed bio-inspired AIS based self-healing self-defending security framework, AIS-IDP for IMS.

Chapter 7 explains the impact of DoS and DDoS attacks like, TCP SYN, UDP flood, ICMP, SIP flood and spoofing on IMS, describes the model for proposed AIS based framework AIS-IDP and explains the model of signature based IDS technique.

Chapter 8 this chapter validation the performance of our proposed model with classical cryptology based technique using different performance metrics and explains the simulation testbed.

Chapter 9 this chapter concludes the thesis plus recommends the enhancements and future work in this area

CHAPTER 2

Introduction to IP Multimedia Subsystem

2.1 Introduction

IP Multimedia System is an overlay architecture for the provision of Multimedia services, such as VoIP and video conferencing on top of globally emerging 3G broadband packet networks. A recent survey concludes that the volume of data exchange is statistically greater than the volume of voice exchange both in fixed and mobile networks. The maintenance of a data network is much cheaper than a voice network due to the fact that IP technology is much cheaper in deployment and operations. It is logical to think about relaying all communications on the data networks rather than maintaining two networks separately. On the other hand there is an increasing demand of novel multimedia applications that demand integration of the Internet with the classical telecommunication networks. As a result, the mobile communications community has defined within evolution of cellular system an all-IP network vision which integrates cellular networks and the Internet.

The IP Multimedia Systems (IMS) is a standard Next Generation Networking (NGN) architecture for media-services capable Internet, defined by the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP) [2] and 3GPP2 [3]. NGN is a broad term to describe some key architectural evolutions in telecommunication core and access networks. The general idea behind NGN is that one network transports all information and services (voice, data, and all sorts of media such as video) by encapsulating these into packets, like it is on the Internet. NGN are commonly built around the Internet Protocol, therefore, the term "all-IP" is also sometimes used to describe the transformation towards NGN.
IMS can be defined as a global, access independent, standards-based IP connectivity and service control architecture that enables various types of multimedia services to end-users, using common internet-based protocols.

IMS architecture makes it possible to establish peer-to-peer IP communications with all types of clients with the requisite quality of service. In addition to session management, IMS architecture also addresses functionalities that are necessary for

complete service delivery e.g. registration, security, billing, media control, roaming etc [33].

2.2. What problem does the IMS solve?

Figure 2.1 illustrates how different devices connect to their unique network through their access technology specific "cloud." Each of these clouds contains separate subscriber and service information for each device. There is no common repository to manage this information across all of these networks. Therefore these networks are largely independent of each other in many aspects.

Gateway interfaces enable communications between these networks by providing signaling (Control Plane) and data (Media Plane) inter-working.

Wired and wireless IP based devices obtain functionality by:

- Acting as an intelligent endpoint, effectively providing all required functionality with external servers.
- Acting as a simple endpoint – each application client requires support from specialized servers in the network.

Cell telephones and POTS landlines invariably depend heavily on the PLMN and PSTN infrastructure for their functionality. This creates a problem for the consumer who owns many different kinds of devices:

- Intelligent endpoints must be configured locally with the user's desired features and information.
- Simple endpoints use specialized servers – i.e. VoIP, Video, or messaging servers – each of which has their own unique features that are managed separately.

How do we integrate these different devices and access technologies into a converged solution? The IMS is an important step to answer this question. The IMS solution currently focuses on PLMN <-> IP network device and application convergence. However, many of the principles of the proposed IMS solution pave the way for a fully converged future across many other device and access technologies.

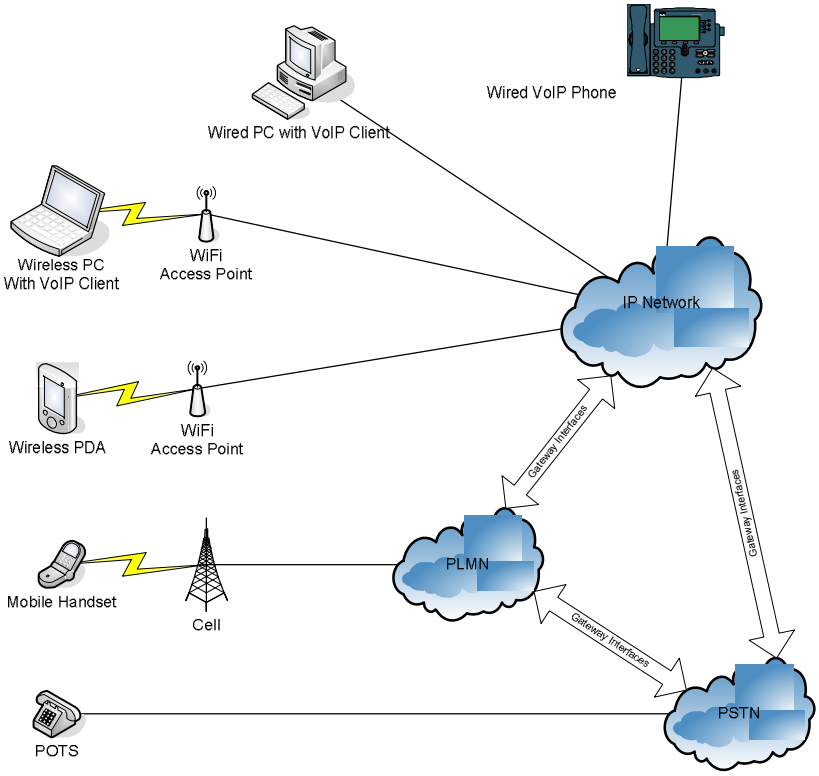

Figure 2.1: Separate IP, PLMN, and PSTN Networks (ref [34])

2.3. How can the IMS solve the convergence problem

The solution to the convergence problem is to have a centralized entity that can manage features and services across all device and access technologies. The first releases of the IMS define an architecture that does just that for the IP Network and the PLMN. The IMS defines a core network which provides service mediation and subscriber profile management across multiple devices. This IP based IMS core provides a unified application experience across all IP enabled devices.

With the appropriate 3G application support, this means that the users can see the same personal phone book information on their PDA, WiFi laptop, and PC based VoIP phone. When the users set their personal presence status it can be applied to all of their devices with a single action. All incoming calls can be routed to all devices or to specific devices in an order specified by the user. All of these devices and applications are part of a truly converged solution.

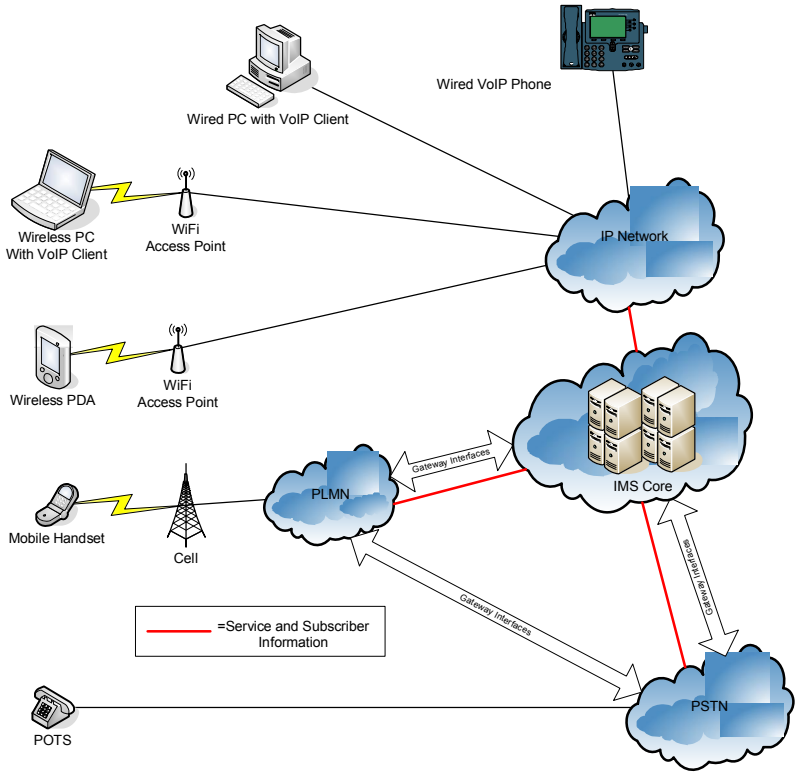

Figure 2.2: The IMS Core provides common application management across multiple networks (ref [34])

2.4 Standardization and Protocols

The main objective of the IP Multimedia subsystem is to provide value added services using existing cellular technologies such as GPRS, EDGE and UMTS. In the world of Internet, a number of protocols already defined have been used by IMS and but still there is a need for the creation of a number of new protocols. To further investigate into the protocols that are used in the IMS it is very important to have a look on different standardization bodies that are responsible for the development of the IMS as an entity and the collaboration between them.

2.4.1 Standardization bodies

2.4.1.1 Third Generation Partnership Project (3GPP)

The Global System for Mobile Communication (GSM) during the early 1990s was created by the European Telecommunications Standards Institute (ETSI). The

same body was also responsible for the standardization of the General Packet Radio Service (GPRS) known as the first step in the evolution of the GSM network towards a true third generation system. The purpose of 3GPP creation was to develop a third generation telecommunication system based on the GSM specifications. The 3GPP is organized into a number of working groups, known as Technical Specifications Groups (TSG) whose work is overseen by the Project Coordination Group (PCG). Hence the output takes the form of Technical specifications (TS) and Technical Reports (TR). Further the task of TSG is to approve these reports so that it can be used in a particular region of the world. All specifications are grouped by the 3GPP in the form of Releases.

The IMS was first introduced in 3GPP Release 5. All technical reports and specifications are available to the public through the 3GPP website at:
http://www.3gpp.org/specs/specs.htm

2.4.1.2 Third Generation Partnership Project 2 (3GPP2)

The 3GPP planned the evolution of the cellular networks based on the GSM (European) specifications into a third generation system. After the successful approach, a similar need was felt to create an organization which would do the same for the North American and Asian cellular networks based on ANSI standards and this led to the creation of 3GPP2. The organization structure of 3GPP2 closely resembles with 3GPP and the technical work being done by Technical Specifications groups whose work is overseen by the Steering Committee (SC). 3GPP2 suggests that the IMS was first introduced in Release A of the specifications.

The Technical Reports and specifications are available to the public through the 3GPP2 web site http://www.3gpp2.org/Public_html/specs. It is however important to note that both the 3GPP and the 3GPP2 have standardized different versions of the IMS. Although both versions, of the IMS quite similar, but still they do significantly differ in many aspects.

2.4.1.3 Internet Engineering Task Force (IETF)

The IETF is known as an organization of operators, vendors, network designers and researchers. Their common goal is to work towards the evolution of the Internet architecture and protocols. The IETF is open to any interested individual without any

membership. Most of the protocols used today in the Internet were standardized by the IETF. The IETF is grouped into areas, and managed by Area Directors or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Internet Architecture Board (IAB) provides the architectural oversight. The technical work within the IETF is done by working groups. A particular task is assigned to each working group such as creating a new protocol. The documents created by the working groups are called Request for Comments (RFC). Individuals who are not part of any working groups can also formulate these RFCs.

2.4.1.4 Open Mobile Alliance (OMA)

OMA (http://www.openmobilealliance.org) was formed in 2002 by the mobile industry. The purpose was to specify mobile service enablers (e.g. digital rights management, and push to talk over cellular – PoC) to ensure service interoperability across different platforms, operators, and networks. OMA recognized that in order to operate efficiently for service enablers, a common set of basic service capabilities such as security, quality of service, charging and session management need to be used. Since IMS has the ability to provide the interface to these basic capabilities, using IMS will make service architecture modular and easier to specify and develop [2]. OMA as a body specifying applications and services (application layer) does not explicitly require the use of IMS (session layer).

2.4.2 Collaboration between Standardization Bodies

To have collaboration between standardized bodies, it affirms that when the IMS standardization body needs a particular protocol to perform a specific task, it uses the Internet protocol for that particular task and makes it the protocol of choice for the IMS. There are cases where the existing protocols do not fulfill the requirements of the IMS, so an extension to the protocol is drafted or a totally new protocol is created by the IETF. Already several protocol specifications and protocol extensions have been written by the IETF in the form of RFCs or Internet Drafts. The collaboration between the 3GPP and the IETF is explained in RFC 3113[6]. At the moment, there is no formal co-operation between OMA and 3GPP, however, due to the benefits of using standards based service interfaces to the network infrastructure

(i.e. the interfaces provided by IMS), the co-operation between OMA and 3GPP is likely to increase.

2.5 Protocols

The protocols that have been defined in the architecture of the IMS can be classified in three broad categories:

a) Protocols used in the signaling or session control plane.

b) Protocols used in the media plane.

c) Authentication and security protocols.

2.5.1 Session Control Protocol

Session Initiation Protocol (SIP) is used widely in the Internet for existing IP based telephony, conferencing, and multimedia applications. SIP is an "application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences." Core SIP functionality is defined by the Internet Engineering Task Force (IETF) in RFC 3261. Many of the most popular consumer VoIP applications extensively use SIP in their implementations.

The 3GPP and 3GPP2 chose SIP as the protocol to handle user registrations and session management in the IMS. The IMS has identified a number of specialized functions for SIP, so the IETF has published a number of IMS unique extensions to the SIP standard.

2.5.2 SIP Call Model

Before we examine the IMS infrastructure, let's take a look at some key characteristics of a SIP based call model. In the example below, both endpoints are IP enabled SIP messages contain the information needed to establish a session between the calling and called party. The calling party is configured to send requests to open a new session (a SIP "INVITE") to a SIP server (or "Proxy") that is responsible for forwarding all SIP messages and responses between the two endpoints. The proxy is aware of any specialized services or handling that an endpoint requires – such as forwarding a call to voicemail or sending a busy if the called party has set "Do Not

Disturb" on their number. The exchange of SIP messages between endpoints, proxies, and other application servers occurs in the "Control Plane". These messages are used to request, establish, and modify sessions with other network entities.

The exchange of media (including audio, video, or data) between the endpoints during the communications session occurs in the "Media Plane". In some sessions, other network entities (such as Gateways, media servers, and voice mail servers) are included in the Media Plane. The concept of the Control Plane and the Media Plane is central to the IMS architecture.

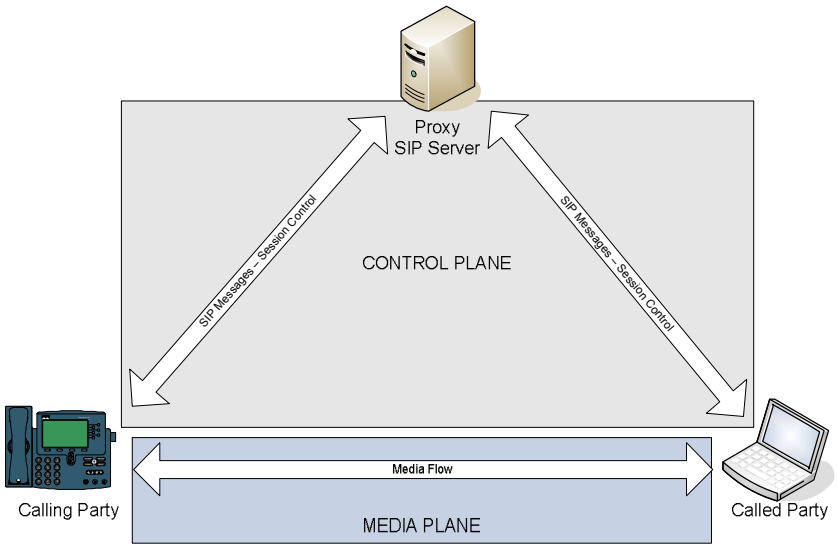

Figure 2.3: Simplified SIP Call model (ref [34])

2.5.3 Media Plane Protocols

The IMS uses the Real Time Protocol (RTP) and the Real Time Control Protocol (RTCP) for media delivery. RTP defined in RFC 3550 transports real time media such as audio and video using UDP as the transport protocol. RTP is always used in combination with RTCP, which provides statistics and information about the media stream. Since the media packets are delivered over an IP network, there may be cases in which packets are delayed in their arrival at the receiver. If two IP packets are sent out consecutively, it may happen that the second IP packet may be received earlier than the first one due to delays and jitter in the IP network. To enable the receiver to play media at the desired pace, RTP timestamps are used in media packets. The receiver puts the media packets in a buffer in order of their RTP timestamps and

then starts playing the media. RTP packets also have sequence numbers associated with them. These sequence numbers are used to determine the packet loss in the network. If the network congestion results in more packets being lost, the sender and the receiver can switch to a different codec that can provide better quality of service.

RTCP is always used in conjunction with RTP. It is used to provide quality of service statistics and information to perform inter-media synchronization. The QoS statistics are generated by using RTCP to report the number of RTP packets that have been sent and received by peer entities. Thus, packet loss can be calculated. Perhaps the most important use of RTCP is to perform the mapping between the RTP timestamps and a reference clock. Using this reference clock enables the receivers to perform media synchronization such as co-relating audio and video packets so that both are played back at the same instance. This is important in video conferencing applications.

2.5.4 Security and Authentication Protocols

Three interfaces, Cx, Dx and Sh, in the IMS architecture provide authentication functions. In all these interfaces the authentication protocol used is DIAMETER. DIAMETER is an improved version of an earlier authentication protocol called RADIUS [10]. DIAMETER is specified as consisting of a base protocol and other Diameter applications that use this base protocol. A Diameter application is one in which the basic functionality is customized to suit a particular functionality. Diameter is run over reliable transport protocols like TCP and SCTP.

2.6 How the IMS works?

Figure 2.4 shows a simplified view of the key components in an IMS Network. Assume that you own multiple IP enabled devices that provide you with voice, multimedia, messaging, and presence enabled services. In the pre-IMS world, these devices were largely independent of each other. However, using the IMS infrastructure, these devices and their features can now be centrally managed.

2.6.1 HSS

A key component of the converged IMS solution is the concept of the HSS or Home Subscriber Service. The Home Subscriber Server is the central repository for

user related information. The HSS stores IMS user profiles including location information, security information, individual filtering information (a set of triggers that cause a SIP message to be routed to application servers), user status information and application server profiles. It is a centralized control and management point that controls a subscriber's devices, preferences, and features. The HSS knows what devices a subscriber has, which ones are registered on the network, and how to contact each of them. This information can be very powerful when combined with an effective presence application. For example, you may specify that between the hours of 8 and 5 PM all calls must be routed to your VoIP terminal at office. Evening calls must be routed to your home phone. When you are in transit, calls are routed to your cell phone. If you are in an important meeting, you want to send all calls to voice mail right away. The HSS ties all of your devices together; telephony and presence applications can therefore be consistently applied across multiple devices.

2.6.2 P-CSCF, S-CSCF, I-CSCF

IP enabled devices become active in the IMS network by registering with a SIP proxy that knows each device is valid and to which subscriber it belongs to. In IMS, the call control SIP proxies are called Call Session Control Functions (CSCFs). Each IP based device must register in the IMS network and these registrations as well as all subsequent requests to initiate or modify communications sessions must traverse the CSCFs. All communications between the subscriber devices and the CSCFs occur in the MEDIA PLANE. The IMS model defines three different types of CSCF

- P-CSCF: Proxy CSCF. This is the CSCF that each device sends all IMS control plane traffic to. Which P-CSCF you are connected to depend on what physical IP network your device is connected.
- S-CSCF: Serving CSCF. The Serving Call State Control Function is the central node in the signaling path. This is the CSCF that is providing the call control and applications support to the User. It maintains the session state as needed by the network operator for support of the services. When a device registers, the P-CSCF sends the registration request to the owning S-CSCF. The S-CSCF uses information stored in the HSS to authenticate the device, as well as determine what services and preferences exist for that device. The S-CSCF can include specialized application servers (presence, telephony,

messaging, etc) in session control traffic as appropriate. Within an operator's network, different S-CSCFs may have different functionalities.

- I-CSCF: Interrogating CSCF. This is needed when a device first tries to register with a P-CSCF, when the P-CSCF does not know which owning S-CSCF to send control messages to. The IMS has defined procedures for a P-CSCF to query an I-CSCF to determine the correct S-CSCF for a given device/subscriber. Performing SIP registration, charging and resource utilization generation of Charging Data Records (CDRs), acting as a Topology Hiding Inter-working Gateway (THIG).

Once a device has been registered with the IMS S-CSCF, all subsequent transactions will go from the device through the P-CSCF to the S-CSCF. The S-CSCF will forward messages to application servers when specific service triggers are invoked, or may simply forward the transactions to the called party or another CSCF. The S-CSCF caches HSS information for the subscribers and may read more information later in support of specific session requests.

For simple IMS to IMS calls, the CONTROL PLANE may reside in a single S-CSCF. The Media Plane for a simple VoIP IMS call (ex: the IP enabled handset in the diagram calls the wired laptop) may be direct from the calling device to the called device. The use of firewalls and Session Border Controllers increase the complexity of the Control and Media Planes.

2.6.3 BGCF, MGCF, MGW

For IMS sessions that leave the IMS domain, such as PLMN and PSTN calls, there is a need for both control and signaling gateway functions between the networks. The IMS components of this gateway functionality are:

- BGCF: Breakout Control Gateway Function. The S-CSCF communicates with the BGCF using SIP. The BGCF identifies the appropriate MGCF and MGW that will be used to support a specific call instance. This is required when a session passes outside (Breaks Out) of the IMS domain. The routing for the BGCF is based on telephone numbers.

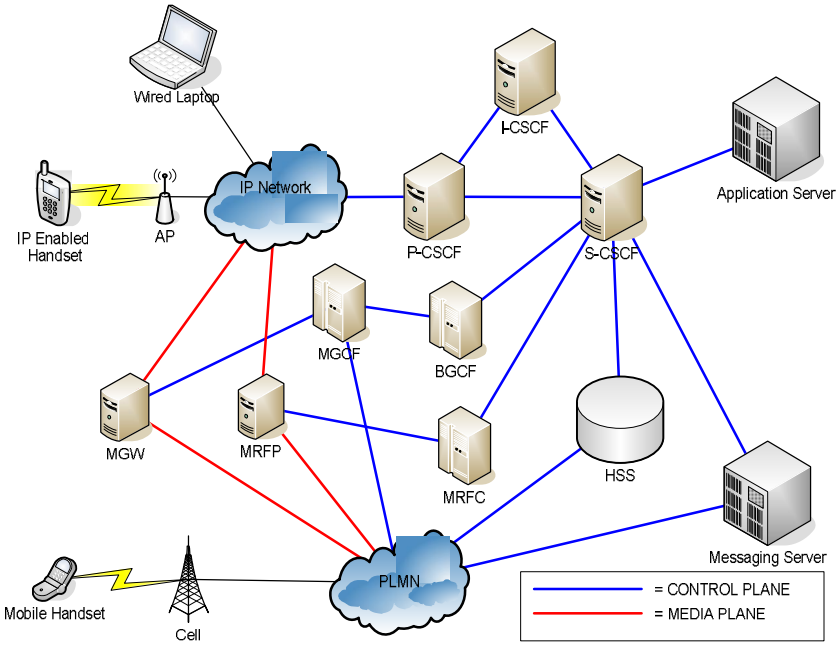

Figure 2.4: Simplified IMS Network (ref [34])

- MGCF: Media Gateway Controlling Function. The MGCF converts the Control Plane information on the IMS side to the specialized signaling used in the PLMN/PSTN network and vice versa. This allows the information needed to initiate, modify, or terminate a session to be passed between networks that use different signaling systems. The MGCF is the Control Plane Gateway.
- MGW: Media Gateway. The MGW acts as the interface between the IMS device Media stream and the PLMN / PSTN device media stream. The MGW is the Media Plane Gateway.

Using the S-CSCF, BGCF, MGCF, and MGW, sessions can be requested (Control Plane) and established (Media Plane) between the IMS and other networks.

2.6.4 MRFC, MRFP

Another important function in the network requires the use of Media Resource Servers. These media functions are needed for:

- Collection of DTMF digits contained in the audio path.
- Playing of announcements (audio/video)
- Multimedia conferencing (e.g. mixing of audio streams)

- Text-to-speech conversion (TTS) and speech recognition.

In the IMS network, these Media Resource Functions are provided by the:

- MRFC: Media Resource Control Function. The MRFC is a SIP proxy that controls the MRFP. The MRFC is in the Control Plane.
- MRFP: Media Resource Control Processor. The MRFP performs the required media functions by sending or receiving media. The MRFP is in the Media Plane.

In the converged 3G environment, the IMS, PLMN, and PSTN should use Media Resource Servers that are capable of supporting all three networks (ref [34]).

2.7 IMS Reference points: (ref [33])

Unlike an interface where any device can communicate to a particular element, a reference point is a well-defined set of rules that associate two functions of the communicating elements. Reference points provide a controlled and restrictive set of specifications that describe all communications between two functional elements, including protocols for various types of signaling and bearer traffic. Reference points specify how IMS entities interact with their peers and also dictate which entities are allowed to utilize a particular function. Regardless of the reference point types, all IMS signaling and communications are based on IP protocol.

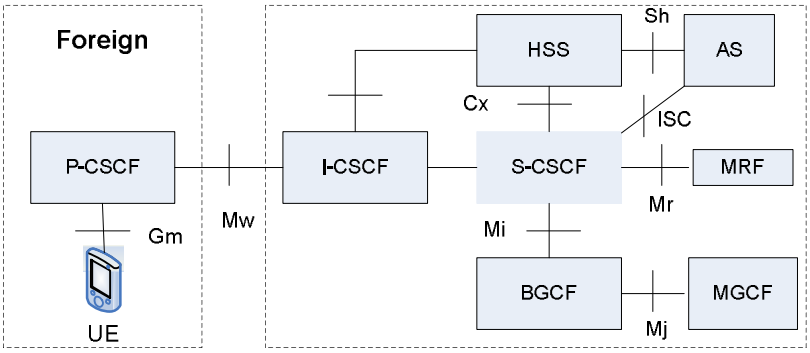

Figure 2.5: Simplified IMS Network Showing Different Point Of Interfaces (ref [6])

Table 2.1: Interface points

Name of reference point	Involved entities	Purpose	Protocol
Gm	UE, P-CSCF	This reference point is used to exchange messages between UE and CSCFs.	SIP
Mw	P-CSCF,S-CSCF, I-CSCF	This reference point is used to exchange messages between CSCFs.	SIP
ISC	S-CSCF, I-CSCF, AS	This reference point is used to exchange messages between CSCF and AS.	SIP
Cx	I-CSCF, S-CSCF, HSS	This reference point is used to communicate between I-CSCF/ S-CSCF and HSS.	Diameter
Dx	I-CSCF, S-CSCF, SLF	This reference point is used by I-CSCF/S-CSCF to find a correct HSS in a multi-HSS environment.	Diameter
Sh	SIP AS, OSA SCS, HSS	This reference point is used to exchange information between SIP AS/OSA SCS and HSS.	Diameter
Si	IM-SSF,HSS	This reference point is used to exchange information between IM-SSF and HSS.	MAP
Dh	SIP AS, OSA, SCF, IM-SSF,HSS	This reference point is used by AS to find a correct HSS in a HSS multi-HSS environment.	Diameter
Mm	S-CSCF, I-CSCF, external IP network	This reference point will be used for exchanging messages Not specified network between IMS and external IP networks.	Not specified
Mg	MGCF =>I-CSCF	MGCF converts ISUP signaling to SIP signaling and forwards SIP signaling to I-CSCF.	SIP
Mi	S-CSCF=>BGCF	This reference point is used to exchange messages between S-CSCF and BGCF.	SIP
Mj	BGCF=>MGCF	This reference point is used to exchange messages between BGCF and MGCF in the same IMS network.	SIP
Mk	BGCF=>BGCF	This reference point is used to exchange messages between BGCFs in different IMS networks.	SIP
Mr	S-CSCF,MRFC	This reference point is used to exchange messages between S-CSCF and MRFC.	SIP

Mp	MRFC,MRFP	This reference point is used to exchange messages between H.248MRFC and MRFP.	H.248
Mn	MGCF,IMS-MGW	This reference point allows control of user-plane resources.	H.248
Ut	UE,AS(SIPAS,OSA SCS, IM – SSF)	This reference point enables UE to manage information related to his services	HTTP
Go	PDF,GGSN	This reference point allows operators to control QoS in a user plane and exchange charging correlation information between IMS and GPRS network.	COPS
Gq	P-CSCF,PDF	This reference point is used to exchange policy decisions-related information between P-CSCF and PDF.	Diameter
Ro	AS,MRCF,S-CSCF,OCS	This reference point is used by AS/MRFC/S-CSCF for online charging towards OCS. Note: there might exist an interworking function between the S-CSCF and OCS.	Diameter
Rf	P-CSCF,S-CSCF, I-CSCF ,BGCF,MGCF,AS,MRFC,CDF	This reference point is used by IMS entities for offline charging BGCF, MGCF, AS, MRFC, towards CDF.	Diameter
Rx	P-CSCF,AS, Charging Rule Function	This reference point allows dynamic charging-related service Function information to be exchanged between Charging Rules Function (CRF) and IMS entities. This information is used by the CRF for the selection and completion of charging rules.	Diameter

Chapter 3

IMS Security Threats

One of the main identified weaknesses of 2G systems is the lack of standardized security solutions for core networks. Even though radio access from the mobile terminal to the base station is usually protected by encryption, nodes in the rest of the system pass traffic in a plain fashion. Sometimes these links even run over unprotected radio hops, so an attacker that has access to this medium can easily eavesdrop on communications.

Having learned from these shortcomings in 2G, 3G systems have set out to protect all IP traffic in the core network. Network Domain Security NDS accomplishes this by providing confidentiality, data integrity, authentication and anti-replay protection for the traffic. To achieve this objective a combination of cryptographic security mechanisms and protocol security mechanisms is embedded in the IP security (IPsec). In the IMS, the NDS only protects traffic between network elements in the IP layer, therefore, further security measures are required.

For IMS most of the security work like authentication, encryption, confidentiality and reliability are standardized by 3GPP release 5 and onwards that provide security at the first level. However, intruders can penetrate into the network through security trap doors by breaking the first level security or misuse of network resources and services. This is harmful as they not only steal the user's confidential information, but it is also dangerous for the network operators because it can damage the network operator's resources and assets. There should be an inbuilt security monitor that can detect and stop the activities of these hackers and intruders. IMS and Next Generation Mobile Networks are designed and implemented on top of IP protocols and by using wireless links. So it is very important to protect network resources, operator's assets and provide security to the users from clever hackers and criminals. Today the network operators and telecommunication community are facing the challenges of three serious types of security threats and attacks in the network:

- Known Attacks & Threats
- Unknown Attacks & Threats
- Denial-of-Service (DoS) / Distributed DoS Threats

IMS is still being defined and there are still many open issues within the IMS architecture. The 3GPP IMS standardization is ongoing, and there is not yet any commercial deployment of IMS within operator's networks.

3.1 Attack Taxonomy

In the following subsections we present a formal taxonomy of attacks on 3G Networks and IMS. The taxonomy is the result of our extensive literature review of IMS security and we believe that this survey is of significant value for our proposal as it lays the foundation for our security system.

3.1.1 Taxonomy of Attacks on 3G Networks and IMS

In order to devise taxonomy of attacks on the 3G Network, we consider the attacker's physical access to the network, the type of attack categories and the means used to launch the attack. Attacks are classified into three dimensions:

Dimension I: Physical Access to the Network,

Dimension II: Attack Categories and

Dimension III: Attack Means.

Dimension I: Physical Access to the Network

In this dimension, attacks are classified based on the level of physical access the attacker has to the 3G wireless telecommunication network. Dimension I may be further classified as

Single Infrastructure Attack (Level I-III) and

Cross Infrastructure Cyber Attack (Level IV-V):

Level I: Access to air interface with physical device: The attacker has access to standard inexpensive "off-the-shelf" equipment that could be used to impersonate parts of the network. The attacker may put up a false base station. Victims camping on the false base station are subject to false base station attacks. Attackers may also use modified mobile stations to broadcast at a high frequency, eavesdrop and as a result launch the man in the middle attack.

Level II: Access to Cables connecting Central Offices (3G core network entities): The central offices house the 3G core network entities. Typically authorized personnel only may access these central offices. If the attacker has access to cables connecting

these central offices then he may cause the damage by disrupting normal transmission of signaling messages.

Level III: Access to 3G core network entities in the Central Office: In this case the attacker may be a disgruntled employee or a terrorist who has managed to gain access into the central office. Here the attacker can cause damage by editing the service logic or modifying subscriber data (profile, security and services) stored in the network entity.

Level IV: Access to Links connecting the Internet and the 3G core network: This is a Cross Infrastructure Cyber Attack. The attacker has access to links connecting the 3G-core network and the Internet based Cross Network Services. In this case the attacker can cause damage by disrupting normal transmission of signaling messages traversing the link and inserting signaling messages into the link between the two networks. Level IV may be sub divided based on the interworking approaches used to connect the 3G core network and the Internet.

Level V: Access to Internet Servers or Cross Network Servers (provides multimedia or other services to mobile subscribers) connected to the 3G networks: This is a Cross Infrastructure Cyber Attack. In this case the attacker can cause damage by editing the service logic, modifying subscriber data (profile, security and services) stored in the Cross Network Servers. This level of attack is easier to achieve than Level II and Level III.

Dimension II: Attack Categories

In this dimension, attacks are classified based on the type of attack. The attack categories are reported in [30].

Interception: The attacker intercepts information e.g., reads signaling messages on a cable (Level II), but does not modify or delete them. This is a passive attack. This affects the privacy of the subscriber and the network operator. The attacker may use the data obtained from interception to analyze traffic and eliminate the competition provided by the network operator.

Fabrication/Replay: In this case the attacker may insert spurious objects into the system. These objects depend on the level of the attacker's physical access to the system e.g. In a Level II, the attacker may insert fake signaling messages, in a Level III, the attacker may insert fake service logic or fake subscriber data into this system. The effects could result in the attacker masquerading as a legitimate authority.

Modification of Resources: The attacker causes damage by modifying system resources e.g. In a Level II, the attacker may modify signaling messages in and out of the cable. In a Level III, the attacker may modify service logic or modify subscriber data in the entity.

Denial of Service: The attacker causes an overload or a disruption in the system such that network functions in an abnormal manner. The abnormal behavior could result into denial of service to the legitimate subscribers, or illegitimate subscribers receiving the service or the entire network may be disabled as a result of the attack.

Interruption: The attacker caused an Interruption by destroying resources e.g. In a Level II, the attacker may delete signaling messages in and out of the cable. In a Level III, the attacker may delete a subscriber data in the entity such as an HLR and the attacker may not receive service.

Dimension III: Attack Means

In this dimension, attacks are classified based on what means are used to launch an attack. The attack means are as follows:

Data: The attacker attacks the data stored in the system. Damage is inflicted by modifying, inserting and deleting the data stored in the system.

Messages: The attacker attacks the system through the signaling messages. The attacker may insert, modify, delete and replay signaling messages going in and out of the network.

Service Logic: The attacker inflicts damage by attacking the service logic running in the various 3G core network entities e.g. Interruption attack on service logic would be to completely delete the logic running on an entity such as the MSC.

3.1.2 Attacks on IMS Domain

In this section we will use classification detailed in above section to tabulate a list of possible attacks on the IMS Domain. The attacks are tabulated as

Case 1: Dimension I-Physical Access Vs Dimension II-Attack Categories and

Case 2: Dimension II-Attack Categories Vs Dimension III-Attack Means.

Table 3.1 shows the Case 1 tabulation of possible Single Infrastructure attacks on IMS Domain. Table 3.2 tabulates possible Cross Infrastructure cyber attacks and Table 3.3 tabulates attacks classified by Case 2.

Table 3.1: Single Infrastructure attacks on the IMS Domain Classified by Case 1 (ref [35])

Physical Access	Interception	Fabrication/ Insertion	Modification of Resources	Denial Of Service	Interruption
Level I	-Observe time, rate, length, source and destination of victim's locations. -With modified MS, eavesdrop on victim.	- When target camps at false base station, calls made by the victim may be hijacked and used to make fraud calls, while the victim is charged.	- With modified base station and modified mobile station, the intruder can come between the target and the network	- When victims camp at false base stations, then victims are out of reach of signals from the serving network and can no longer receive calls and other network related services.	-Jam victims traffic channels so the victim cannot access the channel. -Broadcast at a higher intensity than allowed hogging bandwidth
Level II Links Connecting IMS Entities	-Analyze traffic patterns, gather subscriber/company data. -Eavesdrop on calls and voice messages -Capture AV's sent from Authenticator Agent (HSS) to S-CSCF (Serving Authenticator Agent) and use in replay attacks.	- Send repeated INVITE messages to S-CSCF (Session Control Agent): overload Home Network, this way it cannot service valid incoming requests and generate outgoing requests. - Send Registration/ Location Update messaged to Subscriber Registration Agent (HSS): cause incorrect call routing, shutting	-Change the SIP:URI [Uniform resource identifier] (IMS User Address) in Registration signaling message so that the subscriber cannot be registered. -Change the other party's SIP: URI address in outgoing INVITE service request signaling messages and the request is sent to incorrect party. -Change the SIP:URI	- Send repeated INVITE messages to SCSCF (Session Control Agent): overload Home Network. - Large number of auth request to Authenticator Agent (HSS) slow down Authenticator Agent and surrounding links. - Send repeated Registration / Location Update messaged to Subscriber Registration Agent (HSS):	-Delete Registration / Location Update messaged to Subscriber Registration Agent (HSS): incorrect call routing - Delete Call Invite Requests - Delete AV's sent from Authenticator Agent (HSS) to SCSCF (Serving Authenticator Agent) Send authentication -Delete Ringing Messages.

		down MN - Send profile change messages to HSS (Session Control Agent Data Manager) - Request AV's from Authenticator Agent (HSS).	addresses in the Incoming Session Invite Messages; message does not reach the subscriber -Change the AV's sent to authenticate the User Agent, so that the User Agent is never authenticated.	cause incorrect call routing, shutting down MN - Send profile change messages to HSS (Session Control Agent Data Manager).	
Level III a Remote Connection To IMS Entities	-Analyze traffic patterns, gather subscriber/ company data arriving at the compromising entity.	- Insert new service logic to the compromised entity so that it directs all traffic to the Intruders service location.	- Buffer overflow attacks cause execution of malicious code and hence modification of Service Logic.	-Buffer overflow could also cause a denial of Service at the IMS Entity.	-Delete data sources in the entities.
Level III b Direct Connection To IMS Entities	-Gather data stored in entity and sell it to competition -Track a particular Subscribers activities at the Session Control Agent and Data sources in the HSS	- Insert new service logic to the compromised entity so that it is disabled at a particular time. -Access to HSS : Add new subscribers to the Profile Setting, Subscribed Data stores and not the billing data store, this way the fraud subscribers can access the services without paying.	-Modify destination of Session Invite Messages. -Modify Session Descriptors -Change Subscriber Profile, AV, location mapping at SCSCF & HSS data sources - Modify the session handling capabilities at the Session Control Agent and Proxy Session Control Agent.	-Modify a parameter in the Authentication Vector calculating algorithm so that none of the MS's may be authenticated and hence do not get service.	- Delete subscriber preferences - At Authenticator Agent (HSS), delete Ciphering algorithm and replace with another one, fail to authenticate all MN. - Delete subscriber Preferences.

			-Modify Service Logic in Subscriber Home Domain Manager so that User Session Control Agent mapping is corrupted and the user's requests may not be serviced.		

Table 3.2: Cross Infrastructure Cyber attacks on the IMS Domain Classified by Case 1 (ref [35])

	Interception	Fabrication/ Insertion	Modification Of Resources	Denial Of Service	Interruption
Level IV	-Analyze traffic patterns, gather subscriber/company data - View details of messages between the Cross Network Servers and 3G, IMS core network entity.	- Send profile change messages to Cross Network Servers: Subscriber Profile Manager Agent - Send a large number of authentication requests to the Cross Network Servers. -Bombard the Cross Network Servers with requests.	-Modify messages passing on the link : Change the challenge response to incorrect value: device is never authenticated. : Change replies to queries to incorrect values. : Modify parameters in the signaling messages.	- Send the MSC, S-CSCF: Session Control Agent/ Subscribed Services Support Agent a large number of replies for a particular query or spoof it to be queries for different subscribers. - Send the Cross Network Servers large number of Authentication Requests and slow them down.	- Delete all messages arriving and leaving the Cross Network Servers.
Level V	-Analyze traffic patterns, gather subscriber/ company data - Steal personal information of subscribers registered. Service Logic at the Cross Network Servers.	- Insert subscribers not subscribed for service into the Cross Network Servers, they receive service but are not charged. - Insert fake data into the data stores of the Cross Network Servers.	-Modify Service Logic and data sources in the Cross Network Servers.	- Caused by editing the data sources.	- Delete data sources and service logic in the Cross Network servers.

Table 3.3: Attacks Classified by Case 2 on IMS Domain. (ref [35])

Attack Categories	Data	Messages	Service Logic
Interception	- Gather customer information by reading data stored in database. At the Cross Network Servers invoke Subscriber Parameter manager Agent.	-Analyze traffic patterns, gather subscriber/company data.	- Gather system information by observing/reading operations in the system -At the Cross Network Servers invoke read the service logic.
Insertion/ Fabrication	-Add users to the database that are not subscribed/ paying for the service. -At the Cross Network Servers invoke Subscriber Parameter manager Agent to insert into the Subscriber Parameter Data Store.	- Send a large number of routing requests to the Routing Agent (MSC): exhaust RN's, so the MSC cannot support more call requests. - Send Registration / Location Update messages to Registration Agent (HSS) to cause incorrect call routing, shutting down of the mobile station's - Send profile change messages to Subscriber Profile Manager at HLR - Request AV's from Authenticator Agent at HSS.	-Insert new service logic to the compromised entity so that it is disabled at a particular time.
Modification of Resources	- Modify Subscriber profile Information so that the subscriber receives services he is not paying for. (E.g.: Receive National wide service when subscribed for local service.) -Remove subscribers name from database. (E.g.: Deny Service for those already registered)	-Modify messages passing on the link : Change the challenge response to incorrect value: device is never authenticated. : Change replies to queries to incorrect values.	-Modify Service Logic : Fwd Calls to wrong Location : Change Call Forwarding Logic : Show Wrong Buddies subscriber Location Information : Service Logic in request IM : Change E-mail Time Stamps : Service Logic Mail Server : Client Phone Book : Client Checker Agent.

Denial of Services	-Deny Service for those already registered by removing subscribers name from database: Invoke the Registration Agent	- Send Multiple Challenges to Authenticator Agent at HSS &HLR requesting authentication for multiple users. This could clog the HLR &HSS. -Send the MSC, CSCF : Session Control Agent a large number of replies for a particular query or spoof it to be queries for different subscribers	- Modify Service Logic : Fwd Calls to wrong Location : Change Call Forwarding Logic.
Deletion / Interruption	- Delete subscriber data / Subscriber preferences stored in the Cross Network Server : Mail Data : Phone Book Data : CF Data : Buddy List	- Delete all messages arriving at the Cross Network Server : CF messages -Delete all messages leaving the Cross Network : Challenges to HSS & HLR : Response to queries (MSC) ,(CSCF'S)	- Delete service logic Cross Network Server : CF rules set by the subscriber : CFS Subscriber Parameter Manager agent. : CBS service logic : Permissions and Buddy list LB-IM Subscriber Parameter Manager agent

In this analysis we have defined unique attack taxonomy for IMS networks on the basis of our abstract case-based model. The abstract model will play a critical role in the evolution of the IMS attack taxonomy, which emphasizes the *Cross Infrastructure Cyber attacks* in IMS infrastructure. In future, once more vulnerabilities will be discovered, and then we simply expand the taxonomy. We have demonstrated that with the help of the abstract model, it is straightforward to pinpoint security threats, vulnerabilities and attacks at specific points in the IMS the infrastructure.

3.2 IMS Vulnerabilities

As mentioned at the outset, IMS and SIP enable a rich set of converged services, but, at the same time, open up networks to a host of known IP-based vulnerabilities.

Looking in more detail at the potential attacks that may exist in IMS networks, the more prevalent and potentially damaging application level threats that can be used to attack the core infrastructure and take down the service or used to attack the end-users are:

- Flood DoS and Distributed Floods
- Protocol Fuzzing
- Stealth Floods
- VoIP Spam
- Fraud
- Rogue Devices

3.2.1 Flood DoS and Distributed Floods: Flood DoS and DDoS attacks are those attacks whereby a malicious user deliberately sends a tremendously large amount of random messages to one or more core network elements from either a single location (DoS) or from multiple locations (DDoS). Typically, the flood of incoming messages is well beyond the processing capacity of the target system, quickly exhausting its resources and denying services to its legitimate users.

3.2.2 Protocol Fuzzing: Malicious users will send messages whose content, in most cases, is, on the surface, good enough that the target will assume it's valid. In reality,

the message is “broken” or “fuzzed” enough that when the target system attempts to parse or process it, various failures result. These can include application delays, information leaks, and even catastrophic system crashes. Fuzzed messages can easily be transmitted using encrypted and authenticated traffic, all the way to the IMS core. Existing security devices do not generally have the ability to decrypt the traffic at wire speeds, and look at all the details of the protocol (header, body, content, etc.) to make sure there is no malicious intent, and therefore cannot protect against some of the most damaging attacks towards the infrastructure.

3.2.3 Stealth Floods: Stealth attacks are those in which one or more specific end-points are deliberately attacked from one (DoS) or more (DDoS) sources, although at a much lower call volume than is characteristic of flood type attacks. Detection of stealth attacks is vital for VoIP systems, as they have the potential to be far more annoying than what we are familiar with in the data world. IMS security solutions must be more sophisticated and use different techniques to protect against stealth and VoIP spam.

3.2.4 VoIP Spam: VoIP spam or Spam-over-Internet Telephony (SPIT) is unsolicited and unwanted bulk messages broadcast over the IMS network. In addition to being annoying and having the potential to significantly impinge upon the availability and productivity of the end-point resource, high-volume bulk calls routed over IP are often times very difficult to trace, and have the inherent capacity for fraud, unauthorized resource use and privacy violations. VoIP spam attacks can be launched like stealth attacks cited above, and target subscribers of IMS services.

3.2.5 Fraud: once hackers gain access to an IMS network and servers, they can commence toll fraud by acting as a gateway between the local PSTN and the IMS network, similar to last year’s publicized, million dollar toll fraud exacted on several VoIP networks.

In addition, a fraudulent user can access an entire IMS network and servers by hacking routers, firewalls and operating systems, which can expose sensitive details of subscriber call records. In order to protect against fraud, the behavior of all subscribers must be monitored in real time, with misbehaving subscribers blocked.

Rogue devices. Smart device proliferation and new access capabilities including USB, Bluetooth and downloadable software, devices themselves can inadvertently pose a great risk to IMS networks. These devices can be recruited by hackers as bots on the Internet, to proliferate attacks deep into IMS networks and applications.

Building an Attack Tool is Easy Compounding the issue of threats is the fact that building an attack vector takes very little investment in terms of time or money. The required components are available free of charge, as open-source software and all the required specifications are publicly available at the 3GPP website. Hackers, in a few days, can easily write scripts required to read U/I-SIM cards, which are easily acquired and can be used to launch various attacks.

Chapter 4

Existing Security Frameworks for IDS

4.1 Methodologies for IDS

Researchers have applied the following methodologies to control plane to successfully counter the attacks launched by malicious nodes. (See Figure 4.1)

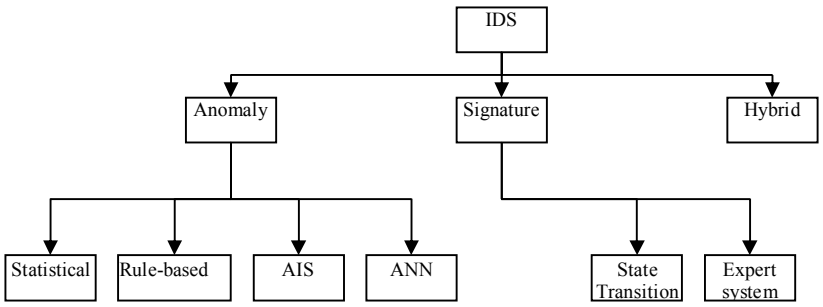

Figure 4.1 Taxonomy of Intrusion Detection Systems (ref [40], [41])

4.1.1 Statistical Based Algorithm Technique:

Statistical based intrusion detection (SBID) techniques determine the normal behavior of a system by learning traffic pattern on a particular network. This process of traffic analysis continues as long as statistical based intrusion detection system is active. All traffic which does not match with the normal learned behavior is considered as anomalous. The longer SBID learns the traffic behavior of the network, more stable and accurate it becomes. SBID looks for anomalies in normal network traffic patterns by analyzing traffic and other related information using relatively complex statistical algorithms. In SBID system each packet is given an anomaly score which indicates the irregularity of the specific event and if this score is higher than a specific threshold level, then IDS will generate an alarm. The key to SBID system is to learn the normal traffic behavior and distinguish normal from anomalous traffic patterns.

Through the application of statistical methods, novelty can be quantified as a deviation from a probability distribution p(x) which is generated from normal data. The quantity can be expressed by a threshold, where (unseen) data samples for which

p(x) falls below this threshold are considered as abnormal samples. By applying such a threshold, all new data samples can be classified into two classes C_0 or C_1, where the training data is assumed to be drawn entirely from C_0. To minimize the probability of misclassification, a new data sample **x** is assigned to the class with the larger posterior probability. This classification decision is based on the Bayes theorem and can be written as:

Decide C_0 *if* $p(\mathbf{x}|C0) > p(\mathbf{x}|C_1)\mathrm{p}(C_1)/P(C_0)$; otherwise *decide* C_1

Where $P(C_k)$ is the *prior* probability of a sample belonging to each of the classes C_k and $\mathrm{P}(\mathbf{x}|C_k)$ is the class-conditional density. The class-conditional density $\mathrm{P}(\mathbf{x}|C_1)$ of the novel data represents the threshold and is unknown *a-priori*. Therefore, it can be modeled as a uniformly distributed density (see Fig 4.2), which is constant over some large region of the input space.

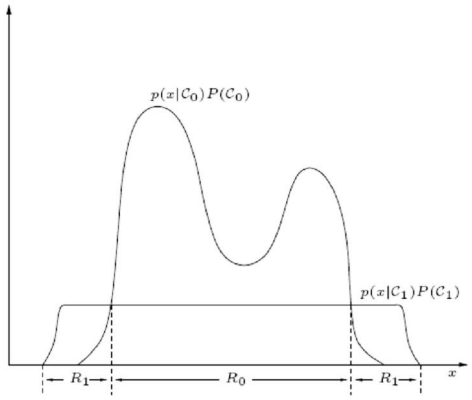

Figure 4.2: Bayesian decision for determining whether an input sample belongs to class C_0 (falling in region R_0) or C_1 (falling in region R_1) modeled with class-conditional density functions [36]

The points of intersections divide the input space into two *decision regions* R_0 and R_1. An input sample falling in region R_0 is assigned to class C_0, otherwise it falls in region R_1 and is assigned to class C_1 [36].

A Survey of Statistical based Anomaly Detection System

i) NIDES (Next-Generation Intrusion Detection Expert System)

The NIDES is a comprehensive intrusion-detection system that performs real-time monitoring of user activity on multiple target systems connected via Ethernet. NIDES

run on its own workstation (the NIDES host) and analyze audit data collected from various interconnected systems, searching for activity that may indicate unusual and/or malicious user behavior. Analysis is performed using two complimentary detection units: a rule-based signature analysis subsystem and a statistical profile-based anomaly-detection subsystem. The NIDES rule-base employs expert rules to characterize known intrusive activity represented in activity logs, and raises alarms as matches are identified between the observed activity logs and the rule encodings. The statistical subsystem maintains historical profiles of usage per user and raises an alarm when observed activity departs from the established patterns of usage for an individual. The alarms generated by the two analysis units are screened by a resolver component, which filters and displays warnings as necessary through the NIDES host X-window interface [37].

ii) Snort is an open source network intrusion detection and prevention system capable of performing packet logging and real-time traffic analysis, on IP networks. Snort is capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, amongst other features. The system can also be used for intrusion prevention purposes, by dropping attacks as they are taking place. Snort can be combined with other software such as SnortSnarf, sguil, OSSIM, and the Basic Analysis and Security Engine (BASE) to provide a visual representation of intrusion data. Developers have patched the snort source code from Bleeding Edge Threats, for supporting packet stream antivirus scanning with ClamAV and network abnormality with SPADE, in the network layer 3 and 4 respectively, through utilizing the historical patterns [38, 39].

4.1.2 Rule Based Algorithms Technique

Intrusion detection system is based on assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified but we can not expect that assumption to be crisp. Rule based intrusion detection system detect intrusion by observing events in the system and apply set of rules that lead to the decision weather a given pattern of activity is or is not suspicious. RBID systems use an attack "signature" to identify a potential attack and subsequently alert on the suspect network traffic. Signatures can be made to look for anything from a port

number in the packet header to a specific byte sequence in the payload of a series of packets. Once a signature has been developed and implemented, it is usually quite effective at detecting the said network activity.

4.1.3 Machine Learning Based Algorithms Technique:

The Biological Immune System (BIS) is a robust and adaptive system that defends the body from foreign pathogens. It is able to categorize all cells (or molecules) within the body as self-cells or non-self cells. It does this with the help of a distributed task force that has the intelligence to take action from a local and also a global perspective using its network of chemical messengers for communication. This remarkable information processing biological system has caught the attention of computer scientists in recent years. A novel computational intelligence technique, inspired by immunology, has emerged, known as Artificial Immune Systems (AIS). Goal is to be able to build a Biological Immune System (BIS) that learns the agent behavior and than detects misbehavior. This however has less processing and communication cost as compared to signature based intrusion detection systems (IDS). Artificial Immune System (AIS) is an anomaly based system and can be viewed as a general pattern learning system and is distributive and scalable. The features of AIS that are particularly important are its self-identity which enables AIS to understand normal behavior of the agents or user and generate corresponding self-antigens. The AIS then generates a repository of anti bodies which can detect an anomalous behavior.

The self-identity enables AIS to understand normal behavior of the agents to generate corresponding self-antigens. The AIS then generates a repository of antibodies, which can detect an anomalous behavior due to malicious agents (non-self antigens). The antigens and antibodies must be in a shape space format to facilitate the definition of affinity between them, which is often a mathematical distance function. The negative selection algorithm randomly generates a number of antibodies and adds only those to the repository whose affinity with the self-antigens is not above a certain threshold value. This generation process for the antibodies is known as thymus model, which enables an AIS to do anomaly detection through self/non-self differentiation. The security framework based on AIS provides a number of benefits: small processing overhead due to a simple anomaly detection algorithm, no significant increase in control overhead because the agents need not carry any signatures, and finally the size

of the database required to store antibodies is reasonably small. These benefits of AIS make it perfectly suitable for securing agent-based adaptive routing protocols in an efficient manner in real time [21].

4.2 Related Research

IMS security has received little attention in the communication community and research groups from the most advanced countries have just started the work on it. However, we do want to cite some preliminary work that has been recently started in the domain.

4.2.2 IMS Security Literature Review

Research work is being carried out at Technical University Berlin and FOKUS Fraunhofer Germany to provide Security for IMS; they proposed a framework which is called Intrusion Detection and Prevention Supervisor for IMS and Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS).

4.2.2.1 IMS IDP-SAT Supervisor

The authors have proposed the design and architecture of Intrusion Detection and Prevention (IDP) Supervisor for IP Multimedia System (IMS) and Next Generation All IP Networks to monitor detect and prevent the security attacks and threats to provide secure and protected environment to IMS operators. The proposed IDP supervisor provides mechanisms for monitoring, detecting and preventing malicious activities.

This research work will be used to provide Secure Service Provisioning Framework (SSPF) [14] for IMS applications at IMS Playground [4] and 3Gb (Third Generation and beyond) Testbed [5] of FOKUS Fraunhofer in Germany. They use a modular approach for detection of Intrusion in IMS and Next generation All-IP network. It is a real time light weight protocol based attacks and threats monitoring system based on modular architecture approach. This framework is still in its implementation and testing phase.

Their solution consists of four core components (See Figure 4.3):

1-Security Attack & Threat (SAT) Monitor

2- Security Attack & Threat (SAT) Detector

3- Security Attack & Threat (SAT) Analyzer

4- Security Attack & Threat (SAT) Prevention Gateway

They have used different modules for different kind of attacks; SAT Monitor monitors the user and component behavior. SAT-Detector is used to detect anomaly. They proposed to use credit card fraud detection algorithms for misuse detection. SAT-Analyzer uses data from the monitoring module and performs both signature and statistical anomaly analyses. SAT-Prevention Gateway implements policy base security decisions.

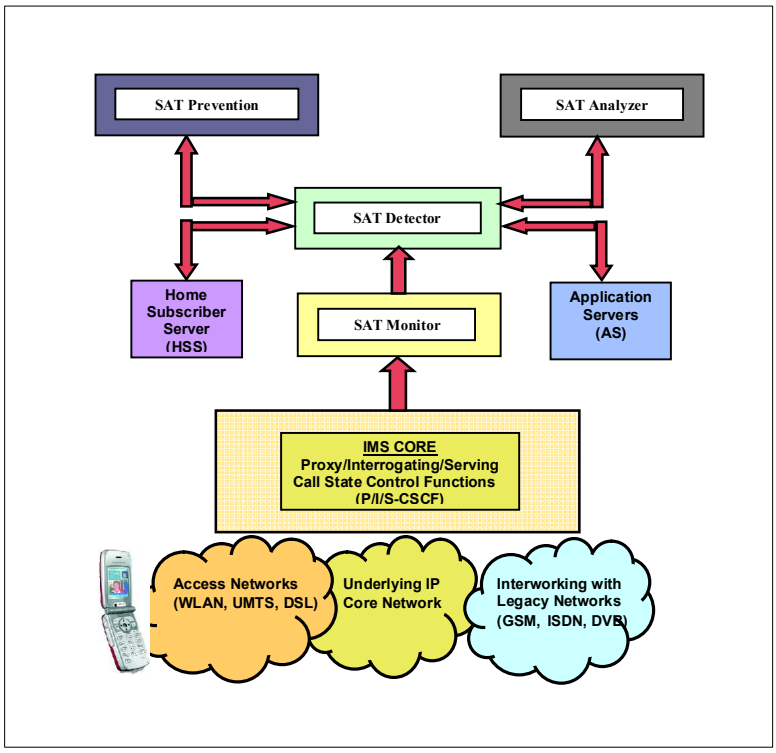

Figure 4.3: Components of IDP-SAT Supervisor (ref [14])

4.2.2.2 Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)

In [8], the authors have proposed architecture and design methodology for the Inter-Domains Security Management (IDSM) Model for the IP Multimedia System (IMS). The IDSM Model is based on Trust Domain Relationship between different network domain operators using policy based security associations and managements.

The design methodology introduces inter-domain security gateways for generating and managing keys and certificates based on Public Key Infrastructure (PKI) architecture. IPSec protocol is used for implementing Confidentiality and Integrity protection. This research work is part of Secure Service Provisioning (SSP) Framework [8] for the IMS Playground [4] and Third Generation Beyond (3Gb) Testbed [5] at the FOKUS Fraunhofer Institute.

4.2.2.3 Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)

In this paper authored have explore security threats and attacks possibility and security solution for Application Server of IP Multimedia Subsystem (IMS-AS). The SIP Application Server is an important entity of IP Multimedia Subsystem (IMS) because applications providing value added services are deployed on the Application Server. The SIP Application Server is triggered by Serving Call State Control Function (S-CSCF) which will redirect certain messages to IMS-AS based on internal filters and criteria or by requesting filter information from Home Subscriber Server (HSS). The critical security attacks on IMS-AS include flooding attacks, messages flows attacks etc. We will propose two tiers security mechanism based on Security Architecture for the TLS (Transport Layer Security) and Intrusion Detection System (IDS) against these attacks to secure IMS Application Server.

Chapter 5

Introduction to Bio-Inspired Security

This chapter introduces the mechanisms present in the biological IS from which the field of AIS draws its inspiration. It should be noted that the exploration of how the biological IS works is still the focus of much research. Hence there is a possibility that the information presented will be proven incorrect over the course of time.

5.1 IMMUNITY

In biology, immunity is the ability of an organism to resist attacks by invasive foreign substances. Such a foreign substance is called a pathogen and is recognized by the IS as an antigen (Ag). The Ag can be virtually any kind of large foreign molecule inside the body, including those contained in infective agents, snake and scorpion venom, food, and other cells and tissues from various species, including humans.

Two components of Immune System

There are two kind of immunity namely,

i) **Innate Immune System:** The system must be capable of detecting the presence of a high proportion of threats that are unknown to it particularly.

ii) **Adaptive Immune System:** The system must be capable of automatically deriving from a single sample a "prescription" for detecting. To cover the space of all possible non-self proteins the immune system uses detectors with low specificity.

To be able to resist attacks by Ags, the IS must be able to distinguish between the materials of the body and the materials of the foreign substance. As all living creatures are made up of basically similar building blocks, the ability of an organism to distinguish the molecules of which itself is composed-i.e., self-from practically all others-i.e., nonself-is remarkable. This ability is, to some degree, present in all living creatures, but among vertebrates it is especially a feature of the white blood cells called lymphocytes.

5.2 Lymphocytes and Antigens

Lymphocytes are the cells responsible for the body's ability to distinguish and react to an almost infinite number of different Ags. There are two main kinds of lymphocytes, i.e., B- and T-lymphocytes (also known as B- and T-cells). The stem cells for both B- and T-lymphocytes originate in the bone marrow. Recognition of foreign Ags in the 'IS' is carried out by receptors on the surface of both the B- and T-lymphocytes.

The part of an Ag that is recognized by a receptor, the antigenic determinant, is called an epitope (Roitt and Delves 2001). Hence, an epitope is a location on the surface of a pathogen or a protein fragment, which is called a peptide. Many Ags have a variety of epitopes on different areas of their surface. Thus, complex Ags may invoke responses from a variety of specific lymphocytes.

Lymphocytes are mainly a dormant population, awaiting the appropriate signals to be stirred into actions. They move only sluggishly on their own, but they can be transported around the body, carried along in the blood or the lymph. At any one time, an adult person possesses about 2×10^{12} Lymphocytes, about 1% of which are n the bloodstream.

5.3 Negative Selection

When T-lymphocyte precursors leave the bone marrow on their way to mature in the thymus, they are indifferent to stimulation by Ag as they do not yet express receptors. When they enter the thymus they are called immature lymphocytes and when, or if, they leave they are called mature lymphocytes. This maturation process is often called tolerization.

In the body, of the immature T-lymphocytes entering the thymus, only 2% complete the maturation process and become functioning T-lymphocytes (Forrest, Hofmeyr, and Somayaji 1997). This means that most of the T-lymphocytes entering the thymus also die there, during tolerization. This may seem very wasteful, but as the Ag receptors are randomly created, a lot of them will recognize self Ags. Self Ags are molecules present on the body's own constituents. If lymphocytes which are autoreactive .i.e., they react to self become mature they will attack the body's own tissues. Therefore most of them are deleted by apoptosis in the thymus. Apoptosis is a kind of programmed cell death. This mechanism for preventing the development of

autoimmune lymphocytes is called negative selection. Negative selection of developing B-lymphocytes is also thought to occur if they encounter high levels of self Ag in the bone marrow (Roitt and Delves 2001, p. 231).

5.4 Clonal Selection

The first encounter between a naïve lymphocyte and a given Ag is called a primary immune response. This response is relatively weak, compared to the secondary immune response, which is a qualitatively and quantitatively improved response that occurs upon the second encounter of primed lymphocytes with a given Ag (Roitt and Delves 2001, pp. 28.30). Part of this improved response is due to a process called clonal selection, which occurs after a lymphocyte has recognized a specific Ag. Lymphocyte selected for by a specific Ag undergoes many divisions during the clonal proliferation and the offspring mature to form an expanded population of Ab forming cells. A fraction of the offspring of the original Ag-reactive lymphocytes becomes non-dividing memory cells. See [32] for more details.

5.5 Somatic Hyper-mutation

Somatic hyper-mutation creates the essential differentiation among the replicated lymphocytes to increase their affinity against the matched antigen. After affinity maturation lymphocyte population is able to detect both specific non-self antigens and their variants. See [32] for more details.

5.6 Costimulation

Because some self peptides are never expressed in the thymus, mature lymphocytes that have been tolerized in the thymus may bind to these proteins and cause an autoimmune reaction (Hofmeyr and Forrest 2000, p. 450). In practice this does not happen because in addition to binding to an Ag, a T-lymphocyte needs to receive a costimulation signal in order to be activated. This signal is usually some kind of a chemical signal that is produced when the body is damaged in some way. See [32] for more details.

5.7 Artificial Immune System

Each antibody interacts with all those antigens, whose complement lies within a small surrounding region, characterized by a *cross reactivity threshold* [23]. In [23] the generalized shape of a molecule, in a 'shape-space', is represented by an attribute string of length *L*. Therefore, an attribute string of length *L* can be regarded as a point in *L*- dimensional shape-space, i.e. m ϵ U^L, where U represents the universal set of strings. A string may be represented by integers, binary numbers or even symbols. In most common shape-space models, peptide is modeled as a binary string (cardinality=2) of fixed length. Binary representation of peptide helps in preserving generality [42]. Therefore, Redefined? if U represents the universal set containing all the strings then the necessary condition that must hold for this definition is,

$$U = S \cup N, S \cap N = \varnothing \ ,$$

Where *S* represents self-set and *N* represents non-self set. Several matching techniques have been presented in [23] for matching a detector with the input string. Most relevant techniques are: Hamming distance matching, Manhattan distance matching, r-contiguous matching and Euclidean Distance matching. For a successful match, a pre-defined *threshold* needs to be reached. An *activation level* present in a detector should also increase by a given factor after every match. This level should reach a certain threshold in a fixed time interval to activate the detector. As proposed in [42], the activation level should be set to zero after the detector has been activated.

The errors produced by AIS can be characterized into two groups: false-positives and false-negatives. False-positive refers to a match made to a self cell and false-negative refers to a match not made to a non-self cell.

Table 5.1: Mapping between the network intrusion detection system and the immune System (ref [32])

Immune System	Network Environment
Thymus	Primary IDS that generates the detectors
Secondary Lymph Nodes	Local Hosts
Antibodies	Detectors
Antigens	Network Intrusions
Self	Normal Activities
Non-self	Abnormal Activities

Chapter 6

Proposed Bio-Inspired security Framework for IMS

The probability of malicious attacks and service abuse of VoIP and other real-time, IP communications applications continued to increase, together with the increase in attack sophistication or complexity (See Chapter 3 Section 3.1 and Section 3.2). All of these developments are creating a new level of security requirements for the operator that go beyond anything that has been traditionally deployed. The existing IDS products available in the market and related research work done are mostly suitable for specific network, application or environment e.g. Ethernet, Wireless Network or ad hoc network and are facing many challenges [14]

- Low scalability
- Low computation Rate
- Low Performance
- No Multiple policy Enforcement

In view of the above limitations and problems, there is need to have an intelligent, accurate, efficient, real time and lightweight protocols based attacks and threats monitoring system. The only way to provide the required level of protection is to adopt an IMS application-level approach that utilizes the best, existing security techniques but also incorporates a variety of sophisticated VoIP-specific security methodologies that include behavior learning, traffic filtering anomaly detection and verification. Together, these practices proactively protect the IMS network from attacks, misuse and service abuse which networks and end-users face today and in the future.

This chapter will describes the proposed architecture for intelligent Bio-inspired self-defending/ self-healing security framework for IP Multimedia System (IMS) and Next Generation All-IP Networks, which will complement existing authentication and encryption mechanisms to protect infrastructure nodes and subscribers against the attacks launched by malicious nodes in the network. We will tackle all network level vulnerabilities above the physical layer: MAC, network and application related vulnerabilities (see Tables 3.1, 3.2 and 3.4 in Chapter 3 Section 3.1 and Section 3.2).

6.1 Layered Architecture of IMS Framework

We have already mentioned in Chapter 2 that IMS is a key enabler for convergence of fixed-and mobile networks. Moreover, it also provides a service delivery platform for new multimedia applications i.e. Voice over IP (VoIP), Instant Messaging and Interactive Push to talk etc. independent of the access type, which can be either cellular or broadband. Its layered architecture allows services and common functions to be reused for multiple applications and access types. IMS also specifies interoperability and roaming that is well integrated within existing voice and data networks, while adopting the benefits of the IT domain.

In order to better analyze security shortcomings in the architecture of IMS framework we have to look at the IMS core with a different angle that emphasizes a layered based logical view of the IMS core. This layered based logical view will significantly help in localizing the causes of vulnerabilities to a handful of modules/components and hence will simplify the task of adapting the architecture to counter the vulnerabilities in a robust and reliable manner. IMS framework can alternatively be viewed as a stack that consists of three layers that nicely separate application, control and transport functions, allowing for an open communications platform rather than having a monolithic and closed architecture. In essence, the IMS layered architecture decouples the service delivery components from the physical network making it possible for services to be independent of the network over which they are delivered. Figure 6.1 illustrates the 3 layered IMS architecture and important functional elements at different layers in it.

The **application plane** contains applications and multimedia content servers and provides services of that particular application along with its control logic to the end users. The Application Server (AS) is responsible for execution of service specific logic and delivering value added services. The application plane also contains HSS and Authentication Authorization Accounting Server (AAA) servers. HSS hosts the main data storage for all subscribers and service related data, and (AAA) controls the database about the authorized users who are allowed to access the network and also tracks the billing data for each user.

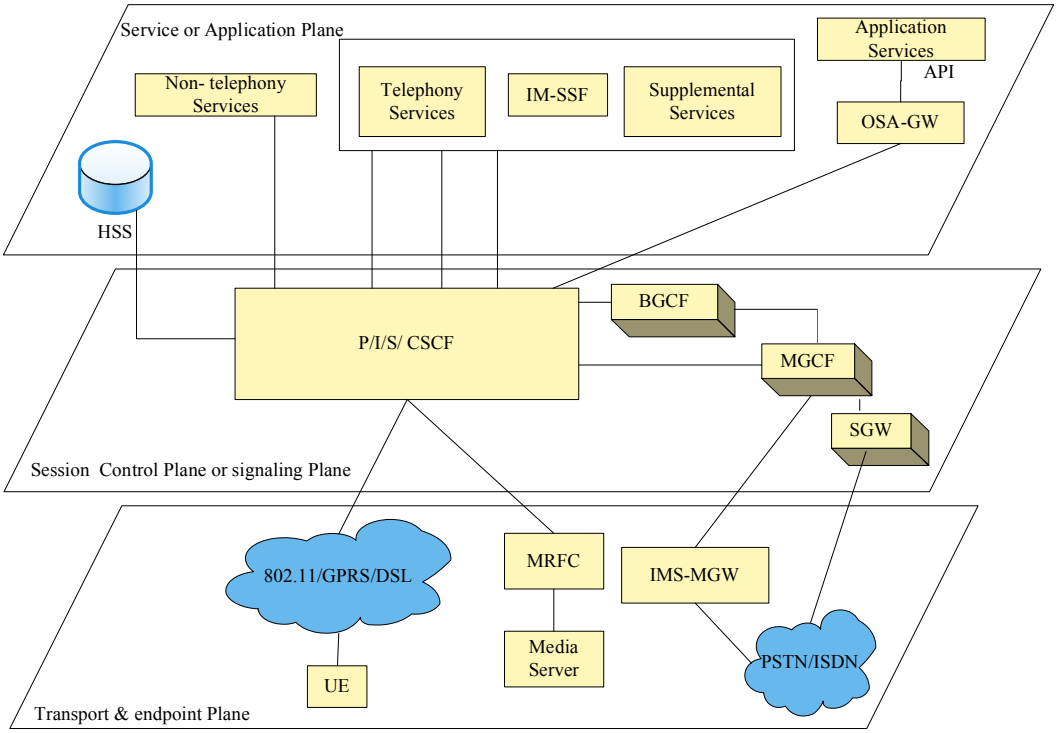

Figure 6.1: Three layer IMS framework: network components and Functions per layer (inspired from ref [33])

The **control plane** comprises of servers that are required for doing critical functions, which include but are not limited to call setup, modification, release and session control functions (CSCF). Several SIP servers are used to process SIP signaling packets in the IMS core. Control plane consists of Media Gateway Controller Function (MGCF), Signaling Gateway (SGW), and Media Gateway (MGW).

The **transport plane** consists of routers and switches both at the edge access networks and at backbone networks. IMS based services can be delivered to the users across different access technologies such as WCDMA, GSM, GPRS, WLAN, DSL.

IMS functional elements communicate via standard ***reference points*** instead of the classical way of via *interfaces*. Unlike an interface where any device can communicate to a particular element, a reference point is a well-defined set of rules that associate two functions of the communicating elements. Reference points provide a controlled and restrictive set of specifications that describe all communications

between two functional elements, including protocols for various types of signaling and bearer traffic. Reference points specify how IMS entities interact with their peers and also dictate which entities are allowed to utilize a particular function. Regardless of the reference point types, all IMS signaling and communications are based on IP protocol. Table 2.1 (Chapter 2) shows reference points between key 3GPP defined IMS functional elements. Likewise, IMS information streams can be divided into three types: control stream, media or user stream and management stream. A malicious node/user can modify one of these streams to launch a number of effective attacks that can play havoc with the normal operations of the IMS network (see Chapter 3 Section 3.1). Therefore, it is important to understand that these streams pass through which reference points of which functional elements and in which layers. This will help us in proposing our security adaptations to the IMS architecture.

6.2 IMS Security Requirement

Functional entities separated by IP reference points provide a number of benefits in terms of application flexibility, reuse of common components and interoperability between equipment of different vendors. But this architecture also has its own set of drawbacks. Distribution of IMS core network functions to different entities in an IP network provides even greater number of opportunities for a hacker to break the IMS architecture from a security perspective. Therefore, IMS network is not only open for known IP-based vulnerabilities but also to a completely new set of IMS applications based vulnerabilities. These unique and real time vulnerabilities which need to be addressed in the IMS network include but are not limited to: IMS framework-related vulnerabilities, SIP protocol vulnerabilities, VoIP/ video/ PoC/ Messaging/ Presence/ Conferencing application vulnerabilities, voice spam, and media plane related vulnerabilities. As a result, our IMS security framework must provide security in eight different aspects: access control, authentication, non-repudiation, data confidentiality, communication security, data completeness, availability, and privacy. As mentioned earlier these all aspects can be achieved if we secure the above-mentioned three types of information streams (media/user, control and management), which are transmitted over the IMS network. In conclusion, our framework will provide protection against Case 1 and Case 2 attacks (See Tables 3.1, Table 3.2 and 3.3 in Chapter 3 Section 3.1). In Table 6.1, we have mapped different

types of attacks that can be launched in the IMS network to different IMS components and streams. Please note that the table only shows the most important types of attacks that are representative of a broader class of attacks for the sake of the brevity.

6.2.1 QoS constraints of an IMS

AIS is a classification system and it will have true positives, false positives, true negatives and false negatives. As an engineer one has to strike for a compromise between true positives and false positives because if we enhance true positives then false positives also increase and vice versa. Now the dilemma is that *"how to maximize the detection accuracy while keeping false positives near to zero"*. If we want to reduce false positives then as a consequence of that true positives will also decrease. It means then malicious packets get a better chance to reach the destination and disrupt the service. We believe that here have to do a challenging job: a comprehensive analysis needs to be carried out to study the impact of true positives and false positives on QoS of the multimedia application. This puts a challenging requirement on our system: to keep false positives low while maintaining high detection accuracy. Moreover one has to relate it with the fact that few packet drops are not that much catastrophic for the multimedia application running on an IMS system. Even if it does result into a problem then we can incorporate intelligent video processing algorithms which are designed for unreliable wireless channels where a similar problem exists.

6.2.2 Security Issues of IPSec and DIAMETER

Because IMS specifies IPSec as the preferred form of core-level network-layer security protocol, therefore, once tunnels are established with the packet data gateway(P-CSCF), the clever hacker can readily launch huge floods of traffic-up to 10,000 messages per second, which is equivalent to the traffic from 10 million subscribers, bringing down multiple nodes in the network, including the PDG itself.

DoS attacks basically flood the IMS network with a significantly large number of random messages. Whether sent from a single location or from multiple locations (DDoS), the flood of messages is well beyond the processing capacity of the target system, thereby quickly exhausting its resources and denying services to its legitimate users.

Table 6.1: Mapping of Attacks to IMS domains and streams

Attack name	IMS Layer	IMS Component affected	Information Stream	Attack type OSI layer Mapping	Protocol	Traffic features
Media flood	Transport	MGW	Media	Application Layer, CASE 1	RTP, RTCP	<session id, src address, Dest address, port, transport protocol, service, timestamp(msec)>
Talk Burst Request Flood	Transport	MGW	Media	Application Layer, CASE 1	RTP, RTCP	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Presence Update Fuzzing	Session	P-CSCF, I/S-CSCF	Control, Management	Application Layer, CASE 1	SIP	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Stealth Call Origination Attack	Transport	Mobile	Media, Control, Management	Application Layer, CASE 1		<user activity profile, user mobility profile>
Register Request Fuzzing	Application, Session	I/S-CSCF,HSS	Control, Management	Application Layer, CASE 1	SIP	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Presence Update Flood	Application, Session	P-CSCF,I/S-CSCF,AS	Media, Control, Management	Application Layer, CASE 1	SIP	<session id, src address, dest address, port, transport protocol, service, timestamp (msec)>
IMS Register Request Flood	Application, Session	I/S-CSCF,HSS	Media, Control, Management	Application Layer, CASE 1	SIP	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Security Authentication	Application, Session	P-CSCF, HSS	Media, Control, Management	Application Layer, CASE 1	Diameter	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Security init Flood	Session	P-CSCF	Media, Control, Management	Application Layer, CASE 1	Diameter	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Security init Fuzzing	Session	P-CSCF	Media, Control, Management	Application Layer, CASE 1	Diameter	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
ICMP Flood	Session	P-CSCF, I/S-CSCF	Media, Control, Management	Network Layer 3, CASE 1	ICMP	<src address, dest address, port, service,

						timestamp(msec)>
UDP Flood	Session	P-CSCF, I/S-CSCF	Media, Control, Management	Transport Layer, CASE 1	UDP	<src address, dest address, port, service, timestamp(msec)>
TCP SYN flood based DDoS attacks	Session	P-CSCF, I/S-CSCF	Media, Control, Management	Transport Layer, CASE 1	TCP	<src address, dest address, port, service, timestamp(msec)>
MAC Flood attacks	Transport	Mobile, 802.11 networks	Media	MAC Layer, CASE 1	ARP	<MAC address, src address, dest address, timestamp(msec)>
Clog the HSS by sending authentication for Multiple users.	Session	HSS	Control, Management	Application Layer, CASE 2	Diameter	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Deny Service for those already register by removing subscribers name from database.	Session	HSS	Control, Management	Application Layer, CASE 2	SIP, Diameter	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>
Analyze traffic patterns; gather subscriber/company data, customer info, and system info.	Session, Service, Transport	P-CSCF, I/S-CSCF,HSS, UE	Media, Control, Management	Network Layer 3, CASE 2		<session id, src address, dest address, port, transport protocol, service, timestamp(msec)> User call profile , user mobility profile.
SIP DoS attacks	Service	I/S-CSCF	Control, Management	Application Layer, CASE 1	SIP	<session id, src address, dest address, port, transport protocol, service, timestamp(msec)>

The nature of these flood attacks is very similar to what can be launched in other classical networks, but the impact could be much more devastating. Floods that are extremely damaging to IMS networks include those based on the Internet Key Exchange (IKE), such as IKE_SA_INIT floods and IKE_SA_AUTH floods, both of which are possible even before setting up the IPSec tunnel. Application specific floods such as Register Request Floods and Presence Update Floods are also possible. These attacks can be easily launched using publicly available tools.

6.3 Proposed Architecture for Bio-inspired security frame work

Now we propose our Bio-inspired AIS based self-healing self-defending framework, AIS-IDP, (see Figure 6.2), for IMS and Next Generation All IP networks. The main objective that we want to achieve is to design a generic security solution which would be based on the principles of AIS. This framework must be able to integrate into any component of the IMS core. This security framework will not only detect all types of known attacks and threats but would also protect a user and the operator assets, and the network resources from misuse and other vulnerabilities resulting from the zero day attacks. The reason for utilizing AIS paradigm is that our group is working with it for the last 2-3 years now and an important outcome of our learning by doing philosophy is: AIS provides an ideal paradigm for designing, developing, implementing and realizing lightweight security framework which demands no additional resources: fast processors, larger memories or faster network cards. Moreover, AIS is a passive learning classifier that puts no additional signature bytes in the packet's header or in its payload. IMS network consists of a number of handheld embedded devices like cell phones, PDAs etc and hence this light weight Intrusion Detection Prevention (IDP) would be an ideal solution which can be hosted on them. The lightweight IDP would be placed at the Home Subscriber Server (HSS), IMS Core (Proxy/Interrogating/Serving -Call State Control Functions (P/I/S-CSCF)), and applications and media servers to monitor the network traffic in real time that is passing through them (see Figure 6.2). The traffic monitoring is a key activity on the basis of which IDP would learn the normal traffic patterns passing though a particular node during the learning phase. Once the learning phase is finished then the system has learnt the "self" and now it would create the detectors database that would match "non self" (which results due to malicious traffic) with the detector database in the

protection phase. Any intrusion would result into a traffic pattern which is not part of "self" learnt during the learning phase.

As mentioned before, the philosophy of AIS based solution is opposite to the one being followed by current systems. If we model the universe (universal set, U) as combination of normal (self set, S) and malicious (non-self set, N) such that S U N = U and S ∩ N = Φ, then most of state-of-the-art intrusion detection systems use some priori information about N (malicious) to detect it. For example, current intrusion detection systems use the signatures extracted by security experts to detect intrusion. The biggest drawback of this approach is that it detects only those intrusions which have known signatures (see Figure 6.3). Signatures set must also be kept up to date. Even if all the intrusion detection systems are able to keep their signatures updated, an intruder can easily change signatures and devise new methods of attacks or can enter into the system as a legitimate user or misuse network recourses.

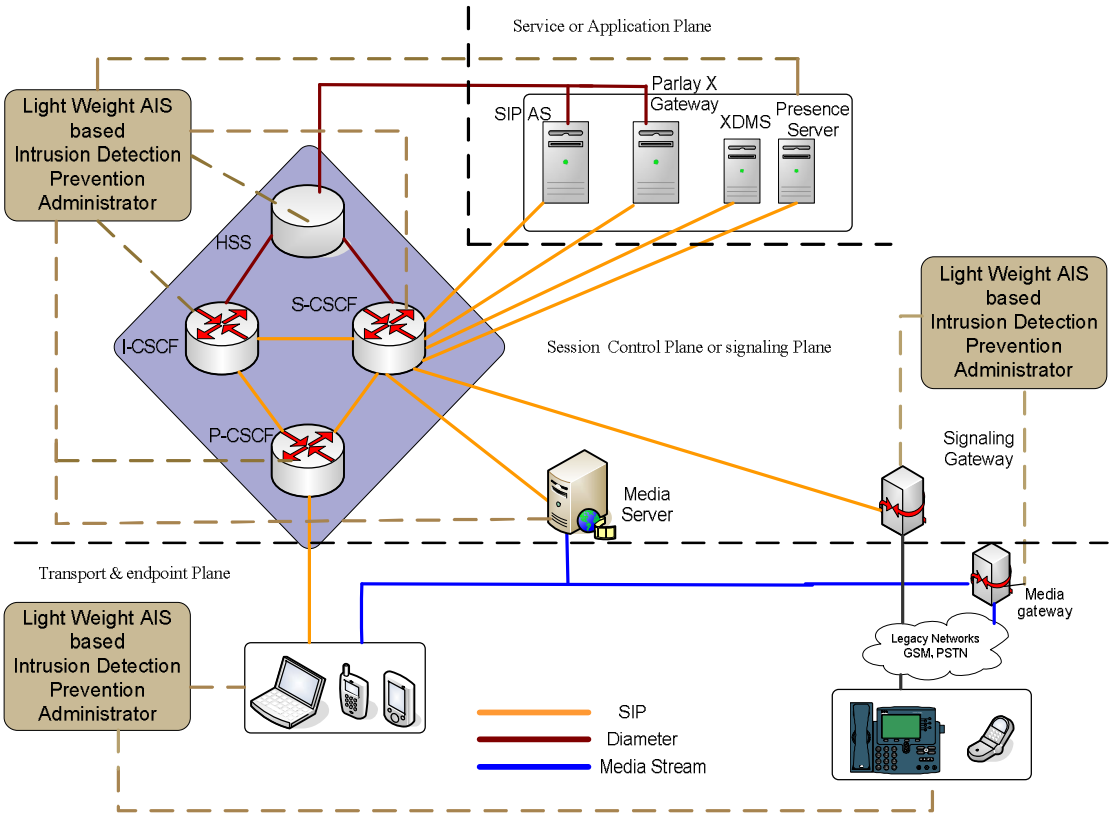

Figure 6.2: Conceptual Model of AIS-IDP

A new class of intrusions— polymorphic intrusions, try to hide themselves between malicious code such that it is very difficult to identify a signature for them. Even the best of experts have been known to select poor signatures that often result in misclassification.

The IMS security has put a significant demand on the classical security paradigm because IMS and NGN, as mentioned before, suffer from a unique set of vulnerabilities (see Tables 3.1, 3.2 and 3.3) previously unknown in the data communications community. A unique class of attack protocols namely Fuzzing is a legitimate method of testing software systems for bugs. In this approach the objective is accomplished essentially by providing an application with a semi valid input to see its output and if it deviates too much from the desired behavior then relevant fixes can be incorporated in the software system. Malicious users, however, employ this same methodology to exploit vulnerabilities in a target system. They do this by sending messages whose content, in most cases, is good enough that the target will assume that it is valid. In reality, the message is 'broken' or 'fuzzed', and as a result, the target system attempts to parse or process it which results in failures. The examples of important failures include application delays, information leaks, or even catastrophic system crashes. Our approach follows the opposite philosophy, a.k.a., anomaly detection. In anomaly detection systems, information collected about S (normal) is used to differentiate anomalous activities from normal ones. Anomaly detection systems model normal trend/behavior of a system. Any deviation of the system from this behavior is an indication of an attack (see Figure 6.4). This is why such schemes are able to detect unknown attacks because an attack is part of "non-self" space. Special tools can be built to learn such trends/behaviors in real time. AIS provide an ideal framework to design and develop such adaptive real time learning classification systems for anomaly detection. We believe that AIS paradigm will give us the flexibility to provide a more generic intrusion detection system for IMS, and as a result, it will be able to detect new attacks, formulate a response to counter them and then adapt its behavior through it online learning classification system. We believe that such an evolving system is the key to IMS and NGH networks.

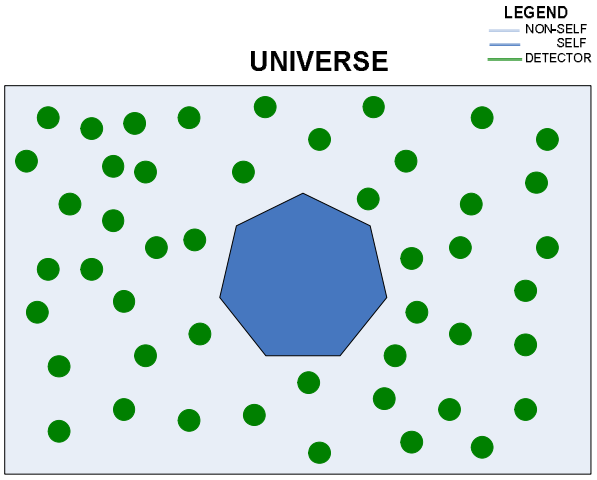

Figure 6.3: Detectors covering non-self space. This approach is used by the state-of-the-art Security systems. Priori information about malicious (non-self) behavior is used to detect malicious activities.

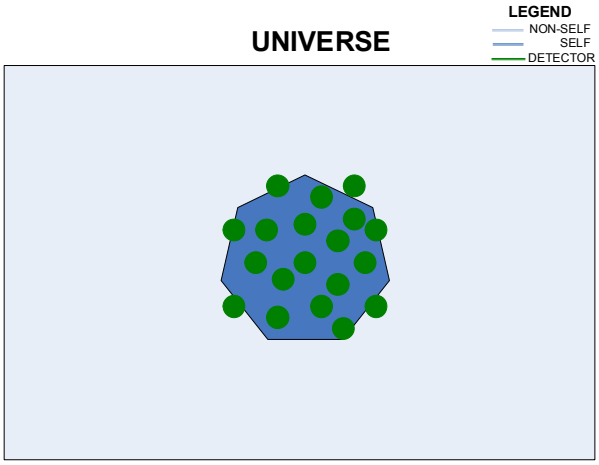

Figure 6.4: Detectors covering self space. In anomaly based systems, priori information is established about normal (self) behavior. This is used to discriminate malicious behavior from normal behavior.

6.4 Components of AIS-IDP

An intelligently envisaged IMS network must be able to counter malicious attacks originating by the nodes within the network or being launched by external network entities. The required security solution must be able to analyze both packet's header and payload in real time, must be able to maintain service transparency and at the same time must not degrade the performance of the IMS network. The key objective of course is to control/secure access to the IMS network and to protect its core and the underlying infrastructure. The secure access within the IMS framework is envisioned to allow only authenticated traffic to pass through different entities of the IMS core. Every user must be authenticated and a secure connection must be established between him and the IMS network. However, protecting the rest of the IMS infrastructure demands protecting the network peering borders, IMS elements and protocols from intrusion and attacks. Light weight AIS-IDP will provide an integrated solution against all types of attacks on IMS infrastructure. We now briefly provide an overview of our proposed AIS-IDP and discuss its six distinct components (see Figures 6.5, 6.6 and 6.7):

6.4.1 Detector database

We have already mentioned that AIS based solution needs to learn the normal behavior of a network system by analyzing the network traffic passing through the node on which it is housed. During this learning phase we try to collect "self antigens", which form the "self" of the system (see Figure 6.5). Once the learning phase is finished then we create detectors' database which is then used to match the "non-self" antigens, which result due to the malicious traffic in the protection phase (see Figure 6.6). It is necessary requirement that the size of this database must be significantly small in order to house it on a memory constrained mobile device. Moreover this would also reduce the search time during the protection phase because we need to match the network traffic with the detectors' database during the protection phase. Our experience with our previous research projects is that the size of the database is of the order of few kilobytes only (typically 8 to 16 Kbytes) which is reasonably small.

6.4.2 MAC Layer learning/detection module

This module will counter different types of MAC layer vulnerabilities with the help of anomaly detector at MAC layer for wireless networks. These vulnerabilities include but are not limited to De-authentication, Disassociation attacks etc. The detector module will detect these vulnerabilities by matching them with the detector's database. The detectors are created during the learning phase by the learning module that leans the normal behavior of MAC layer. If no anomaly is found at this layer then packet will be handed over to upper layer (Network layer 3) for further processing (see Figure 6.7).

6.4.3 Network Layer 3 learning/detection module

The IMS network must be able to thwart flood, sweep, scan, malformed packets, spoofing and fragmentation attacks against IP, ICMP, IGMP protocols at the network layer of OSI reference model. If no anomaly is detected at this layer then the packet will be handed over to the upper layer (i.e. Transport layer 4) for further processing (see Figure 6.7).

6.4.4 Transport Layer 4 learning/detection module

The IMS network must be able to prevent flood, sweep, scan, malformed packets, spoofing and fragmentation attacks against UDP, TCP protocols. TCP SYN flood based DDoS attacks are launched in the session plane of the IMS layered architecture and are mapped to the transport layer of OSI reference model (see Table 6.1). The Transport layer AIS-IDP detector module will then detect these different types of attacks at the transport layer of OSI reference model and accordingly secure different components of the IMS network at different planes of the IMS layered architecture. If the packet is not detected as an anomalous one at this layer, then the packet will be handed over to the application layer for further processing (see Figure 6.7).

6.4.5 Application Layer learning/detection module

It is the also an important responsibility of our AIS-IDP that it enables the IMS network to have flow isolation to ensure that proper bandwidth and priority is given to a particular application flow. As a result, it can protect against theft of service within the application flows (i.e., user cannot receive streaming video

bandwidth while only paying for streaming audio). This module will detect all such types of known and unknown attacks i.e. anomaly, misuse, signature based , DoS/DDoS, sweep, scan, malformed packets, spoofing, and fragmentation attacks against SIP, RTP, RTSP and IKE protocols by matching it with the detectors' database. This detector must be able to detect application (Case 1 and CASE 2 attacks as mentioned in Chapter 3 Section 3.1 and Tables 3.1, 3.2, 3.3). However, it is possible that due to the detection error (a characteristic of any intrusion detection system) that a number of anomalies would go undetected. We want to make sure that in those anomalies we do not have voice, mail and SMS spams. Therefore, we apply additional rigorous filters (User finger printing and behavior Learning/Detection Module) to ensure that spam anomaly is verified and hence filtered as per user choices. But if this filter also does not detect any anomaly then we allow the traffic to propagate further into the IMS network. If no anomalous packet is found by the detector then it is given to the User Fingerprint & behavior learning module to ensure that voice, mail and SMS spams are rigorously detected with more accuracy (see Figure 6.7).

6.4.6 User Fingerprint & behavior learning/detection Module:

This module will learn in real time the call patterns, end-point figure prints, user and device behavior. Call and session can be classified as normal or anomalous type depending whether there is a successful match with the detectors in the database or not. If the level of threat is above a certain threshold value then the alarm is generated. Such behavior learning and verification capabilities are of paramount importance to block the malicious end-points. This module would also analyze the impact of a subscriber behavior on various entities of IMS. Of course the module is responsible for creating detectors in the detectors' database for the vulnerabilities relevant to this module (see Figure 6.7).

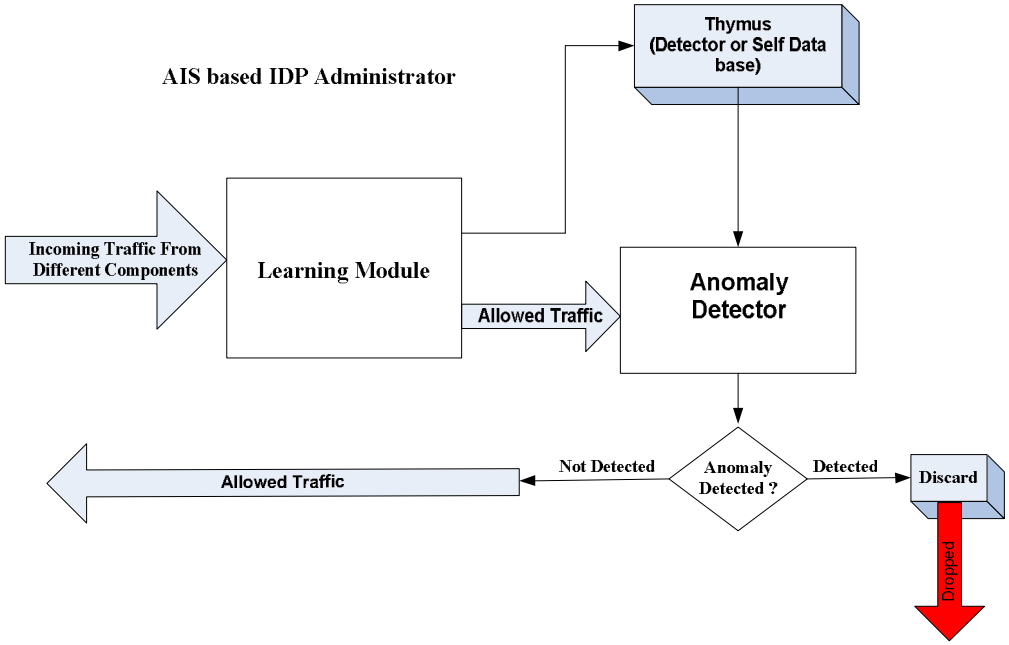

Figure 6.5: Components of AIS-IDP

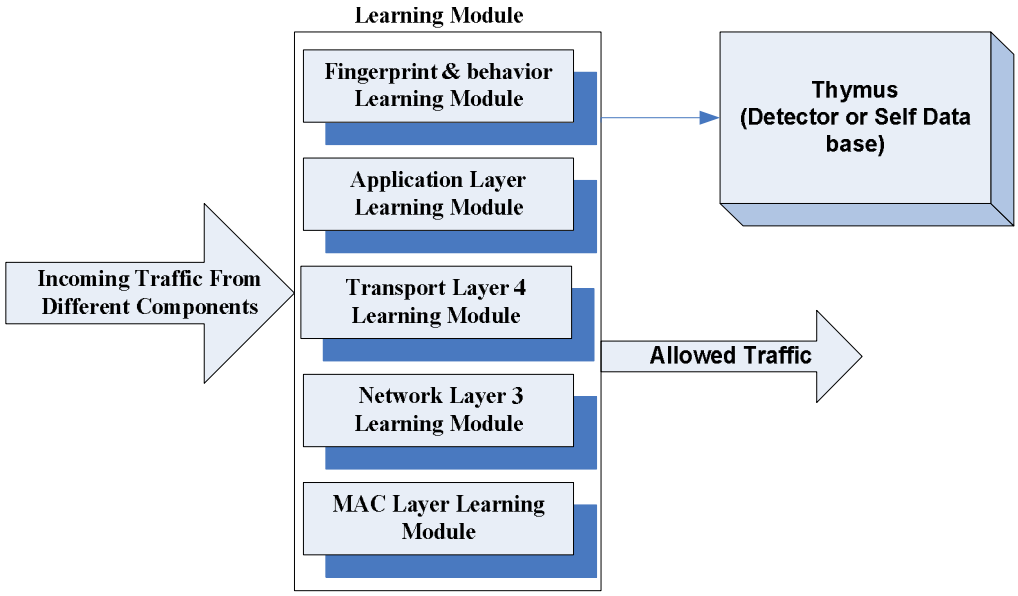

Figure 6.6: Packet processing in the learning phase of AIS-IDP

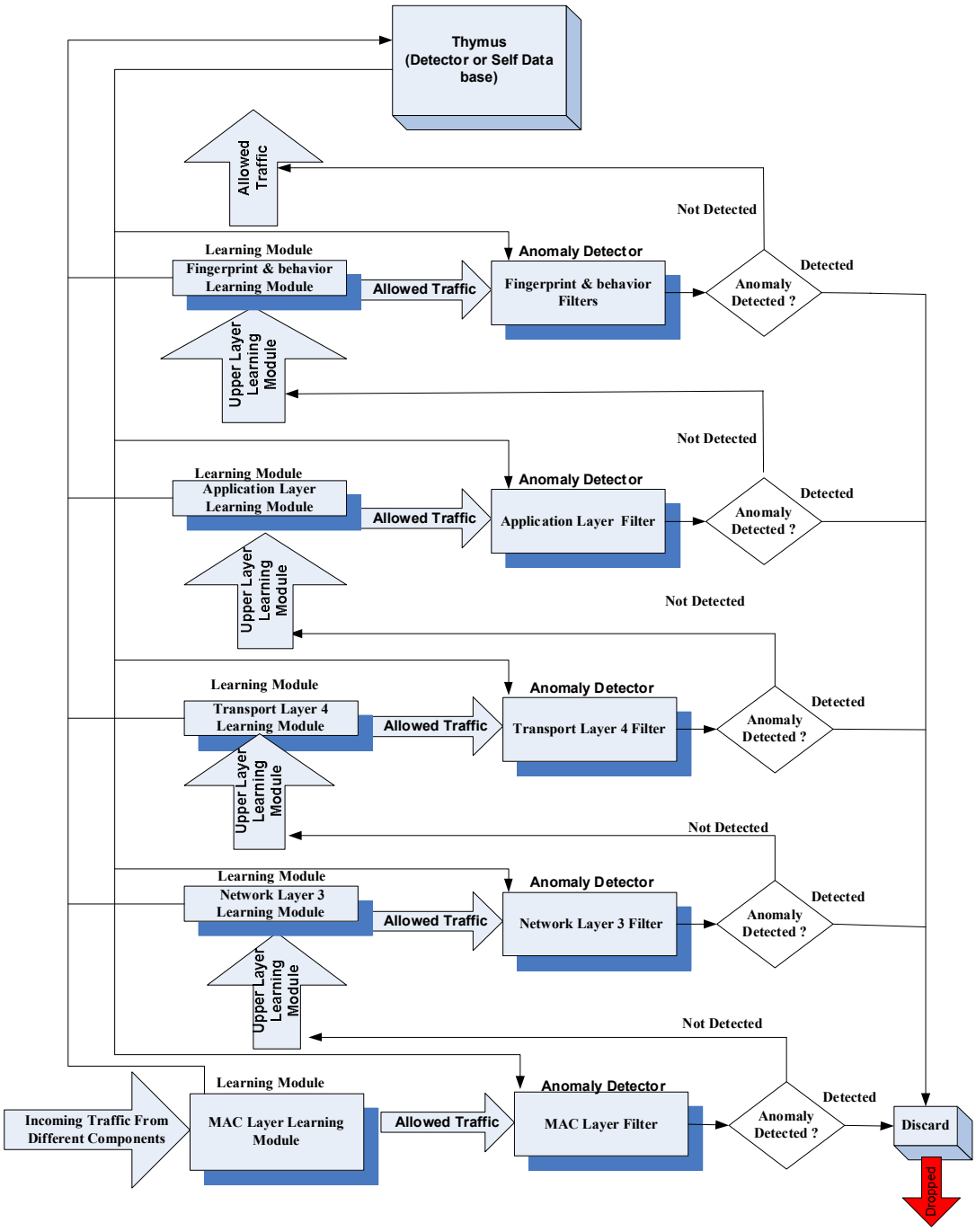

Figure 6.7: Packet processing in the protection phase of AIS-IDP

Chapter 7

Implementation of AIS-IDP

7.1 DoS and DDoS Attacks

A **denial-of-service attack** (**DoS attack**) or **distributed denial of service (DDoS attack)** is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for and targets of a DoS attack may vary, it generally comprises the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

In DDoS attacks, a large number of control packets are simultaneously sent from multiple malicious nodes to a victim router/node so that the victim node and legitimate nodes can no longer communicate properly. Generally, malicious nodes in DDos attacks exploit shortcomings in networking protocols like Internet Control Message Protocol (ICMP). Relevant examples are SMURF attacks, Ping of Death attacks, TCP-SYN floods, UDP floods and attacks on application protocols like different types of SIP flood attacks on VoIP and SIP signaling related flood attacks on IMS infrastructure.

7.1.1 ICMP Flood Attack

In SMURF attack (Figure 7.1), ICMP echoes a request to the broadcast address with the victim's address as source. In Ping of Death attacks, ICMP packets with a payload of more than 64K are launched towards a victim node which can crash the victim node running on Windows 98 or its earlier version.

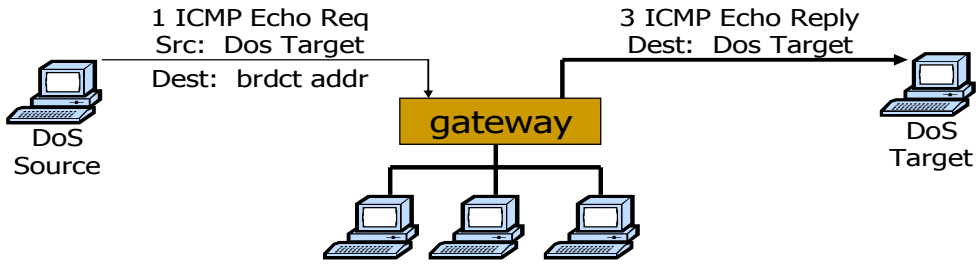

Figure 7.1: Smurf DoS Attack

7.1.2 UDP Flood Attack

In DoS attack, a malicious node can send additional control packets by spoofing the IP address of another node. As a result, this malicious traffic consumes the limited resources of a victim router/node so that it can no longer provide services to legitimate nodes in the network. In UDP floods, bandwidth is exhausted by sending large number of bogus UDP packets. Figure 7.2, 7.3, 7.4 shows the affect of spoofed UDP flood attack on different components of IMS framework. It has drastic effect on S-CSCF as it maintains the signaling path and provides applications support to the User. Any attack on this component will affect the availability of services to user for which he/she has subscribed for. As we already know that I-CSCF is needed when a device first tries to register with a P-CSCF, when the P-CSCF does not know which owning S-CSCF to send control messages to, performs SIP registration, charging and resource utilization generation of Charging Data Records (CDRs), and act as a Topology Hiding Inter-working Gateway (THIG). Any DoS attack on I-CSCF will not only affect user registration but also damaging for operators resources and assets, as it affects user charging who are already register to the operators network for converged services.

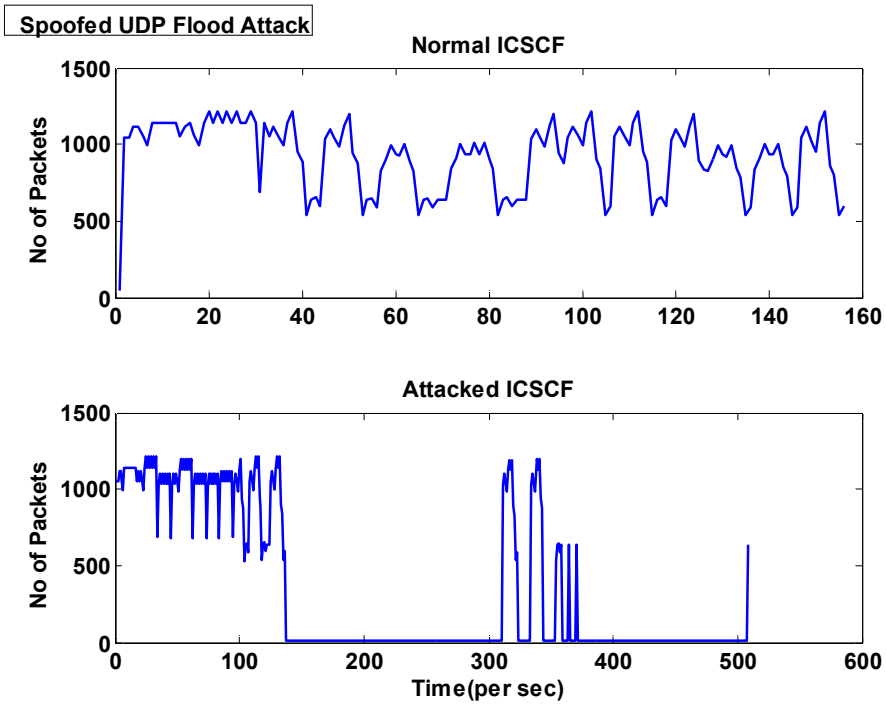

Figure 7.2: Spoofed UDP Flood attack on ICSCF

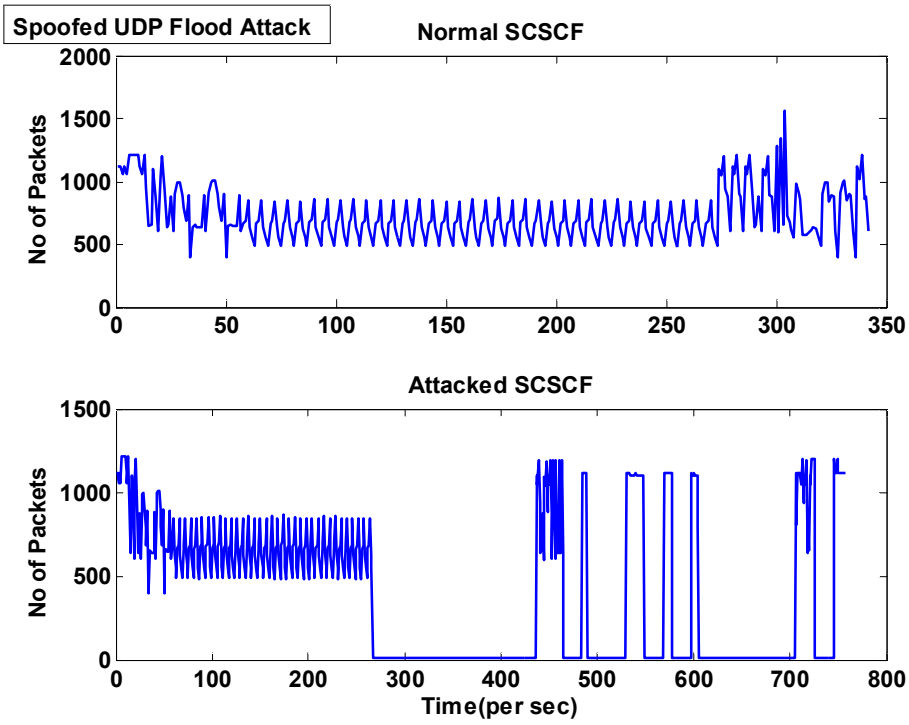

Figure 7.3: Spoofed UDP Flood attack on SCSCF

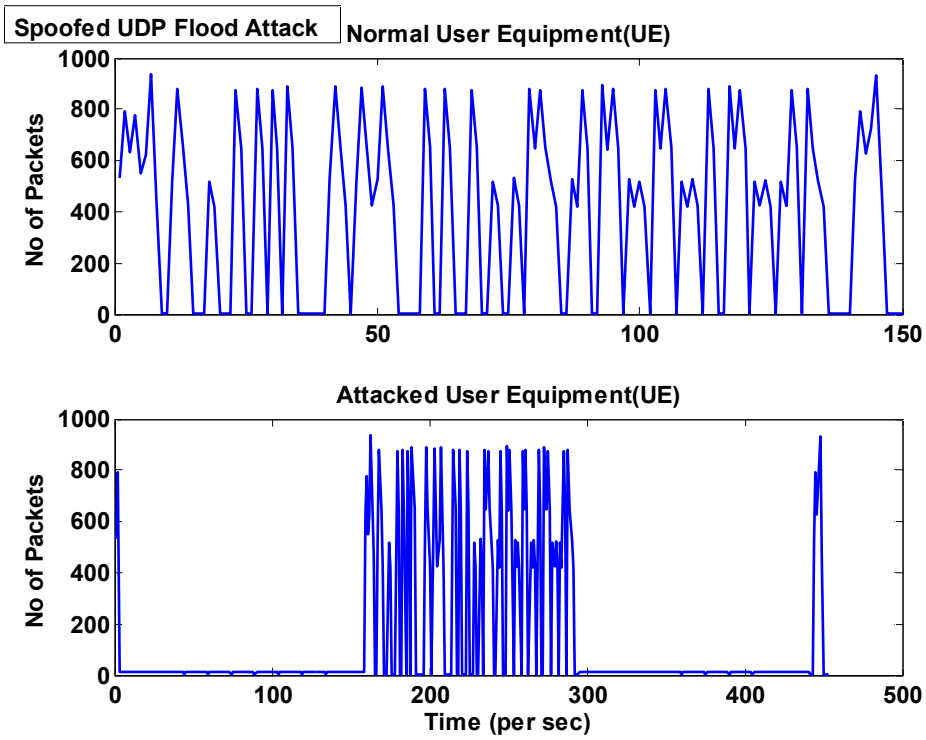

Figure 7.4: Spoofed UDP Flood attack on User Equipment

7.1.3 TCP Flood Attack

In TCP- SYN floods, fake TCP connections are requested by malicious nodes by spoofing IP addresses of other nodes in the network. The most common form of DDoS attacks is TCP-SYN attacks. In these attacks, a malicious node floods the victim node, running a TCP server, by sending TCP-SYN packets with forged source addresses (a.k.a. *IP Spoofing*). Consequently, the server allocates resources for the request. The connection state is maintained till timeout. The server then sends back SYN_s+ACK_{c+1} (see figure 7.5) packets while waiting for ACK_{s+1} packet, which never comes (see figure 7.6). In DDoS version, the victim node running TCP server is flooded with SYN packets from various malicious nodes with spoofed IPs that have no common pattern. As a result, the resources of the victim node are exhausted resulting in denial of service to legitimate nodes running TCP clients.

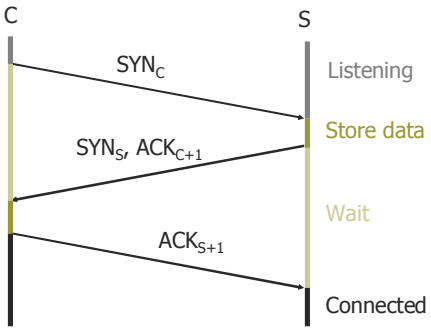

Figure 7.5: 3 Way TCP Connection Handshake

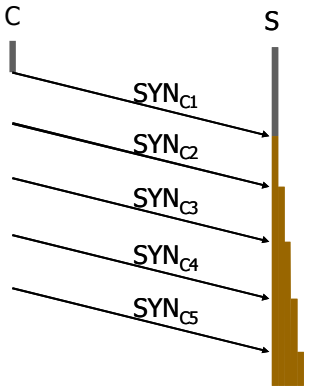

Figure 7.6: TCP: SYN Floods

7.1.4 SIP Flood Attack

DoS against a SIP system can occur through registration hijacking, proxy impersonation, message tampering, and session tear down and through additional DoS-specific attacks. Because strong authentication is rarely used, SIP processing components must trust and process SIP messages from possible attackers. DoS can take the form of malformed packets, manipulating SIP states, and simple flooding, such as a "REGISTER" or "INVITE" storm (a flood of packets). Research has shown that many SIP implementations are highly vulnerable to these types of attacks.

DoS can be especially damaging if your key voice resources are targeted (e.g., media gateways, AAA, IVR, VM, and other systems). DoS can also be used to generate large numbers of toll, information (411), or emergency calls (911). Your network can also be used as a DoS launching point, from which the generated calls are directed at another enterprise.

DoS can also be directed at a firewall. SIP requires management of UDP ports for media. A DoS attack that floods the firewall with calls can prevent it from properly managing ports for legitimate calls.

Defense schemes against such attacks include Packet Authentication, Source Identification and Traffic Filtering. Packet authentication is not suitable for IP networks because it employs cryptographic signature based schemes that have significant amount of processing and bandwidth overheads. Source identification uses link testing, packet logging or IP trace back schemes which require modification of existing routing infrastructure. In comparison, traffic filtering does not suffer from the above-mentioned shortcomings of the other two techniques because it usually employs victim-end packet filtering. This scheme is more preferable over other schemes in case of Distributed Denial of Services (DDoS) attacks.

In [55], Hofmeyr and Forrest proposed an architecture to cater for TCP-SYN flood based attacks. Their proposed architecture (implemented as LISYS) derived inspiration from ARTIS [55]. In the next section, we briefly review their architecture and also present the improvements (such as somatic hypermutation) proposed and implemented in [44]. It is to be noted that the notion of thymus was not implemented in LISYS. Its implementation was first presented in [44].

7.2 Implementation of Immune Algorithm

7.2.1 Detector

A detector plays the combined role of both a lymphocyte and an antibody in AIS (see figure 7.7). It detects non-self antigens and acts against them. A population of various types of detectors, based on *least activation rule* [44], is stored in the memory.

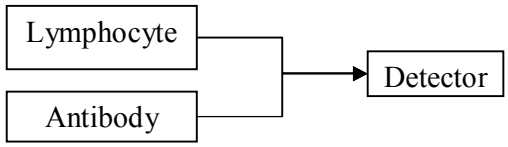

Figure 7.7: Lymphocyte and Antibody merged as Detector

The detector fields consist of its state, peptide, age and activation level as shown in table 7.1.

Table 7.1: Representations for Detector fields

Fields	**Representations**
State	Immature, Mature, Activated, Memory, Dead
Peptide	L bits
Age	$0\text{-}T_{death}$
Activation Level	A

Each of the implemented detectors has a small set of attributes, as shown in Table 7.1 on the preceding page. The state of a detector may be either immature, mature, memory or dead and any of these may be combined with the state active. The peptide of a detector is the abstraction of the receptors on the surface of a lymphocyte. It is represented as a bit string of length 57. Figure 7.8 on the next page shows the life-cycle of a detector. First, a detector *d* is created with a randomly generated bit string. The state of *d* is then set to immature. It has now begun its tolerization period. If *d* matches anything, even just once, during this period, its state is changed to dead, just

like programmed cell death (or apoptosis) in the biological immune system. This is the implementation of negative selection in the AIS.

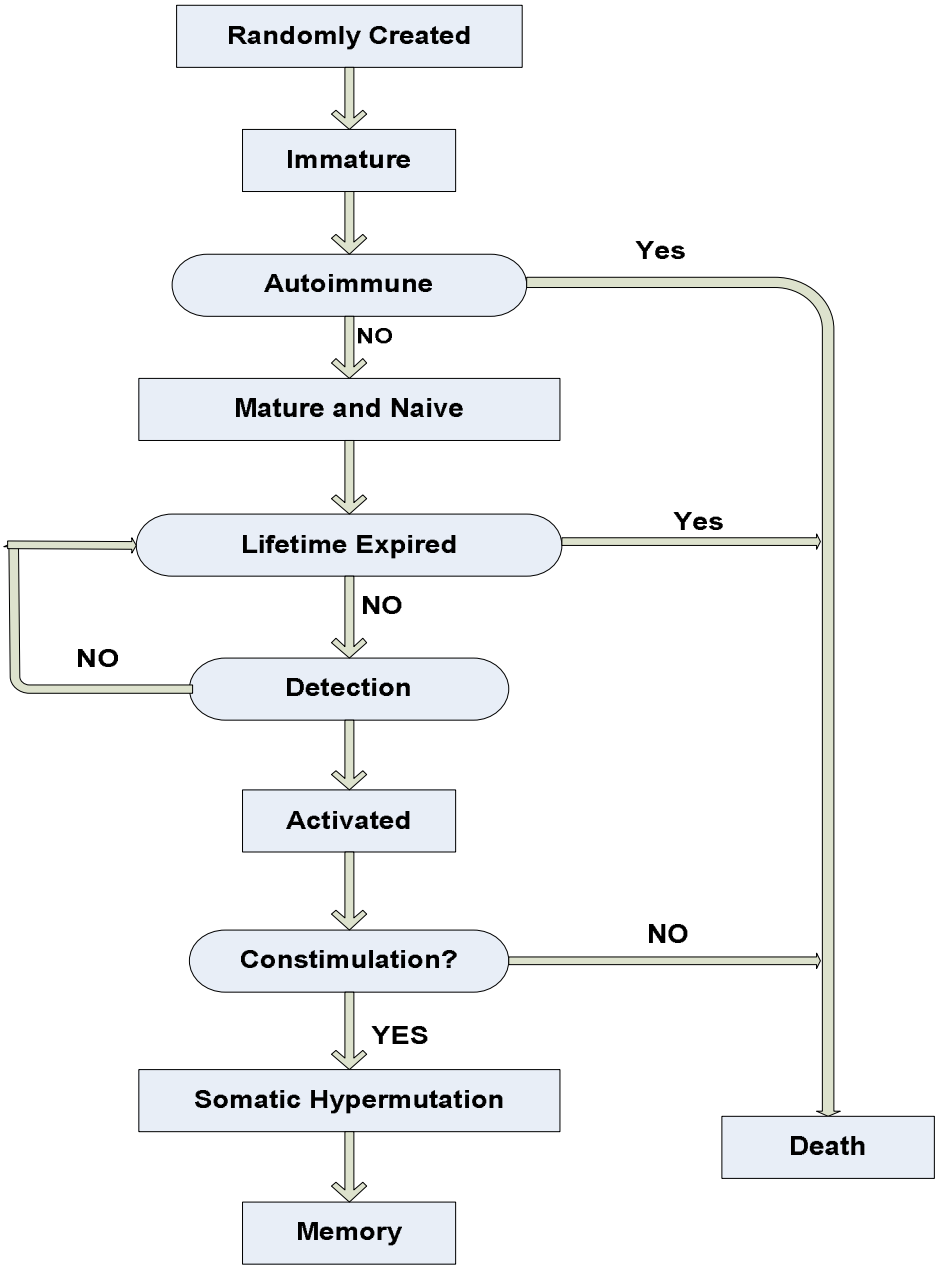

Figure 7.8: Life cycle of Detector

When a detector has reached the mature state, it is capable of detecting nonself. If the detector matches nonself frequently enough, its state is set to active.

7.2.2 Antigen Representation

Peptide representation consists of following important parameters:

- String Length (L)
- Cardinality (m)
- Fields

The selection of string length and fields depends on the type of information to be stored in an antigen. Cardinality is chosen to be *two* (m=2) because binary representation of IP addresses are used. DDoS prevention requires encoding of TCP-SYN packets, UDP, ICMP and SIP packets. The proposed bit format is 57-bit string for TCP-SYN, UDP, ICMP and SIP register request packets, which contain the following fields. This scheme has shown remarkably better results as compared to other schemes [44].

Table 7.2: Antigen Representations

Bits	Bit-Length	Field Description
0-7	*8*	*LSB of Server's IP*
8-39	*32*	*Client's IP*
40	*1*	*Flags*
41-56	*16*	*Port Number*

7.2.3 Algorithm

Light weight intrusion detection and prevention framework works in three phases: (i) Initialization Phase in which AIS randomly initializes the population of detectors; (ii) learning phase (which lasted approximately for 30 sec to 1 minute) in which AIS-IDP tunes/tolerizes the detector to the normal behavior of network traffic obtained from benign traffic profile; (iii) detection phase in which the AIS classifies the run-time traffic as normal or malicious. Different immune algorithms are utilized in these phases. Immature detectors mature by undergoing negative selection to develop tolerization to the self antigens. A detector undergoes clonal proliferation (replication) and somatic hypermutation (differentiation) after the match with a non-

self antigen. This helps to improve the secondary response of AIS. Algorithm highlighting the phases for AIS-IDP is given below

Algorithm 1: Learning Phase

```
While (received packets at each component of IMS core and all layers)
    if(Learning Phase AND Network Layer OR Transport Layer OR Application Layer)
        get header fields (Client-ID , Server-ID, Flag, Port-Number)
        form layer Self-Antigen bit-string
        determine Hamming Distance of Network Layer Self-Antigen
        if ( Self-Antigen matches previous collected Self-Antigens ) then
           drop layer Self-Antigen
        else
        Store network layer Self Antigen in network layer Self Antigen List for this node
        end if
    end if
end while
```

Algorithm 2: Detector Generation

```
if ( current time == end of Learning Phase ) then
   while ( Detectors < Num-detectors ) do
      randomly generate all four Gene values
      form an Immature Detector
      retrieve Self-Antigen List for this node
      if ( Detector matches a Self Antigen ) then
         discard Immature Detector
      else
          store Detector in  Detector List for node
      end if
   end while
end if
```

Algorithm 3: Protection & Detection Phase

```
while ( received  packets  at each component of core ) do
  if ( Protection Phase ) then
     get layer header fields (client-ip, server-ip, client-port, server-port ,protocol)
     form a layer Self Antigen bit-string
     determine Hamming Distance of  layer Self Antigen
     retrieve layer Detector List for this node
     if (Self Antigen matches any  Detector  )
     then
          if(match> Costimulation)
          drop network layer packet
          Selection (Proportionate to Affinity)
          Reproduce (Clonal Selection/Expansion)
          Mutation (Somatic Hypermutation)
          Update detector database
          end if
     else
     move to upper layer
     end if
  end if
end while
```

7.2.4 Matching Methods

The system was tested using a non-self traffic. Hamming and r-contiguous distances are compared with a reactivity threshold $r_{(0 \le r \le l)}$. The Hamming distance (D) is defined as:

$$D = \sum_{i=1}^{L} \delta \qquad \text{Where } \delta = \begin{cases} 1 & Ab_i \neq Ag_i \\ 0 & otherwise \end{cases}$$

r-contiguous distance is the same as hamming distance except that it looks for *contiguous* bit positions. A simple algorithm for L-bit contiguous matching is given in Algorithm 1.

Algorithm 1: Contiguous Distance Matching

```
Distance_max=0
Distance=0
for (First to Last Bit)
    if (δ==1) then
       Distance++
    else
        if (Distance_max < Distance)
            Distance_max = Distance
        end if
        Distance=0
    end else
end for
return Distance_max
```

7.2.5 Costimulation

Costimulation is provided by the AIS when the number of *different* matches increases above a threshold. As a result, the response time of AIS to detect attacks and accordingly discard malicious packets is increased. This slow startup significantly helps in reducing *false-positives*. Figure 7.9 depict the effect of changing costimulation threshold on the percentage of non-self detection for hamming and r-contiguous matching techniques.

7.2.6 Tolerization (Extended Thymus Action)

In chapter 5 we highlighted the role of thymus in developing self-tolerization i.e., lymphocytes may not detect self-antigens. The summary of mapping between NID systems and Immune System are presented in table 5.1. The system is tuned for

tolerization to self-data using *thymus action*. The growth algorithm for generating detector set is shown below *(*See Figure 7.10).

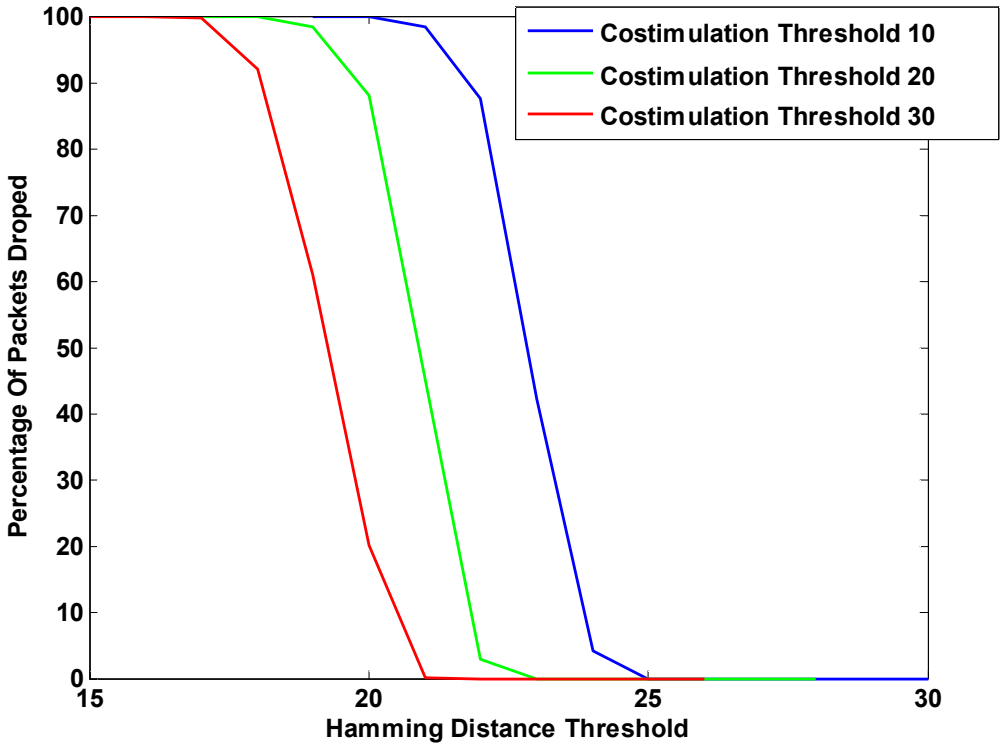

Figure 7.9: Effect of changing costimulation threshold on percentage of non-self match (Hamming matching)

A randomly generated set of detectors is evolved for multiple generations in thymus. Negative selection principle is used to tolerize detectors to *self* .If stop criterion i.e. '*Generations* = 0', and detector still has not developed tolerization for self-data, then the detector undergoes programmed cell death, also known as apoptosis. Otherwise detector fields are varied randomly using mutation and are checked for self-match till '*Generations* = 0' or self-match does not occur. The number of self-matches converge to zero for 'Generations>>1'. Figure 7.11 shows the convergence of detectors for different hamming thresholds.

Growth Algorithm

- Step 1. Generating self set *S* with its number *Ns*.
- Step 2. Generating one detector generating seed which is randomly selected from the whole shape space.

- Step 3. Matching the new detector candidate with *S*.
- Step 4. Experiencing a negative selection process. If the candidate is not matched with *S*, then a new one is generated and added into *R*.
- Step 5. If the stop criterion is met, then exit.
- Step 6. Mutating the candidate and going to step 3.

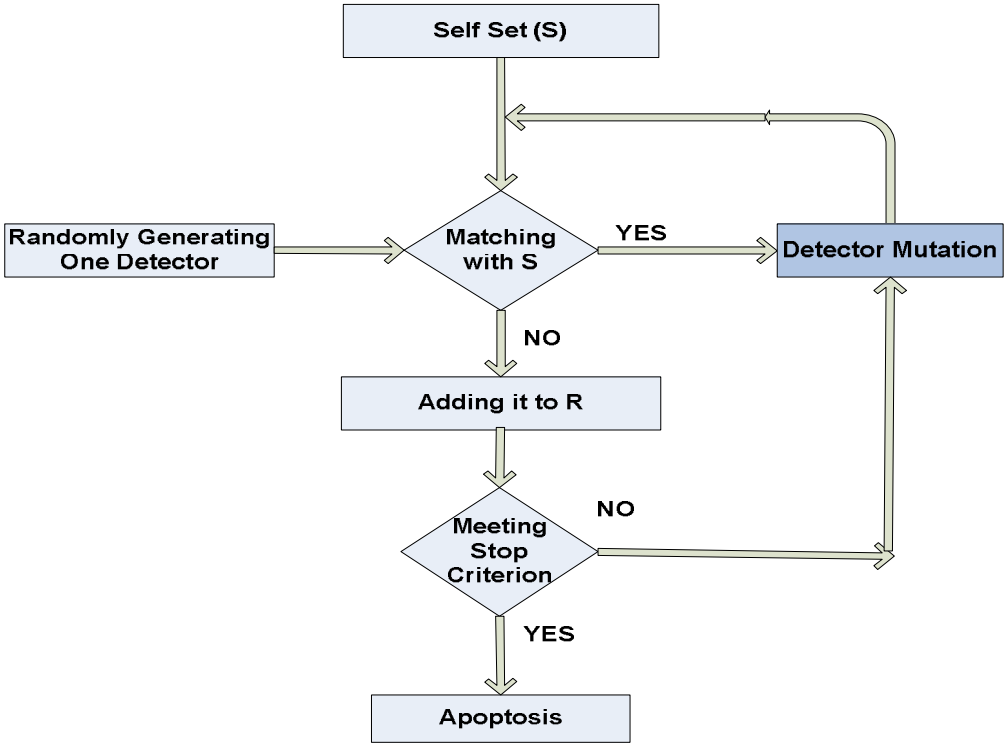

Figure 7.10: Flow chart of detector generation growth algorithm

7.2.7 Affinity Maturation

Once a detector detects a non-self antigen (malicious TCP- SYN, UDP, ICMP, SIP packets), it reports this to a Central Alarm System (CAS). The detected packet is dropped only if CAS provides *secondary costimulation*. The original detector undergoes affinity maturation. Affinity maturation is an important part of AIS for improving immune response (*acquired immunity*). Affinity maturation consists of the following two processes.

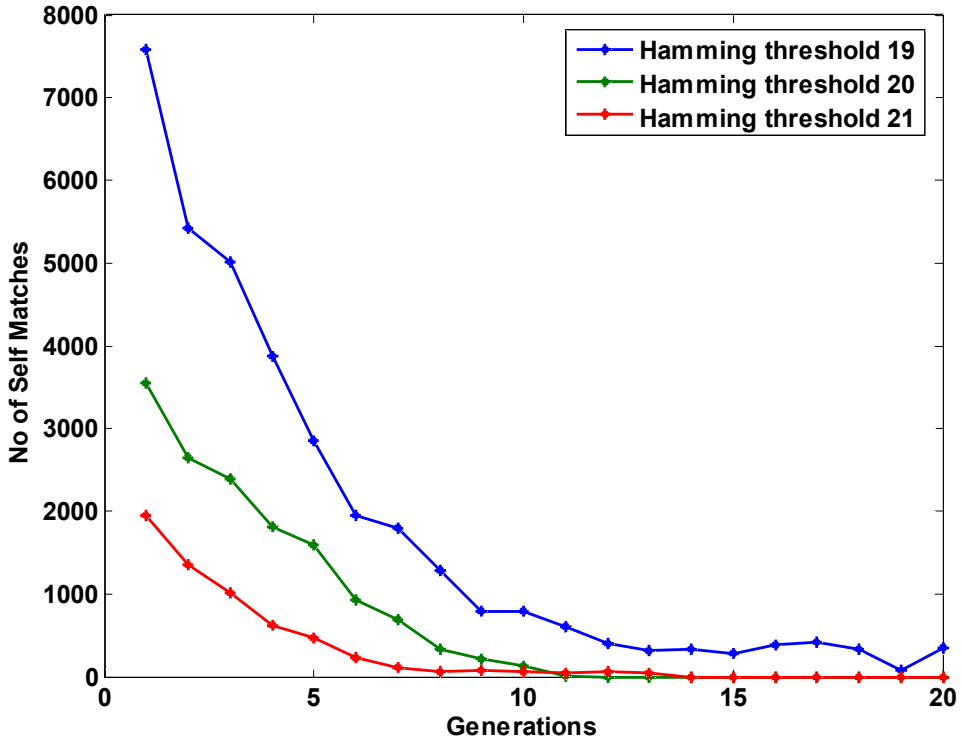

Figure 7.11: Increased tolerization to self for multiple generations

7.2.7.1 Clonal Proliferation.

Detector undergoes multiple replications during clonal proliferation which results in the formation of large population of the original detectors.

7.2.7.2 Somatic Hypermutation.

Detectors undergo random mutation so as to differentiate themselves from multiple clones. This is to increase their diversity against a particular attack. Only those detectors are left to mature whose affinity with the detected packet is greater than or equal to earlier affinity. This helps to improve the secondary response of AIS against malicious traffic.

7.3 Signature based Algorithm

Digital signature algorithm, is used for creating signature using a private key, the user can compute a signature for an arbitrary piece of data. Anyone possessing the public key that corresponds to the private key used to compute a signature can

then verify that signature. The algorithm works in conjunction with the Secure Hash Algorithm (SHA).

Essentially, the hash of the data to be signed is computed, and the hash is actually signed, rather than the data itself. The public key that corresponds to the private key used to compute a digital signature can then be used to obtain the hash of the data from the signature. This hash is compared with the hash computed by the party verifying the signature. If they match, the data is considered authentic. If they don't match, the data is not identical to the data that was originally signed.

A digital signature is useful for verifying the integrity of data, ensuring that it has not been corrupted or tampered with. It also provides non-repudiation since only one person should have access to the private key used to compute a signature. The utility of a digital signature when combined with a key exchange algorithm such as Diffie-Hellman is easy to see. If the two parties performing a key exchange trust that the public key actually belongs to the party with which they're communicating, a digital signature can be used to prevent a man-in-the-middle attack.

Signature-based ID systems detect intrusions by observing events and identifying patterns which match the signatures of known attacks which are store in signature database. IDS attempts to flag behavior that is close to some previously defined pattern signature of a known intrusion. An attack signature defines the essential events required to perform the attack, and the order in which they must be performed. Signatures are set of rules pertaining to a typical intrusion activity e.g. simple example rule nay ICMP packet>10,000 bytes or several thousand SYN packets to different ports on same host under a second.

7.3.1 Algorithm for signature based technique

We compared our proposed AIS-IDP system with a signature based security framework. The signature based security framework uses Secure Hash Algorithm (SHA1) for hashing and Digital Signature Algorithm (DSA) for digital signatures.

To implement these security algorithms, we included a crypto-library, OpenSSl [15] into our C++ environment.

In this algorithm sending node computes digital signatures on the header fields such as *source address, packet ID, destination address, source port, destination port*, using its private key. The receiving node can then use the public key of the sending node to verify that the message did originate from the sender and that the message

contents have not been tampered or forged by the nodes it visited this will counter fabrication, tempering and spoofing attack

We selected a key length of 1024 bits. The hash function produced a 20 byte value while the size of digital signature varied between 40 to 45 bytes. A packet can be authenticated with the keys of a node using digital signatures stored in the packet header. All keys were pre-distributed for our experimental simulations. We used client-puzzle algorithm to provide defense against connection depletion attacks [56].

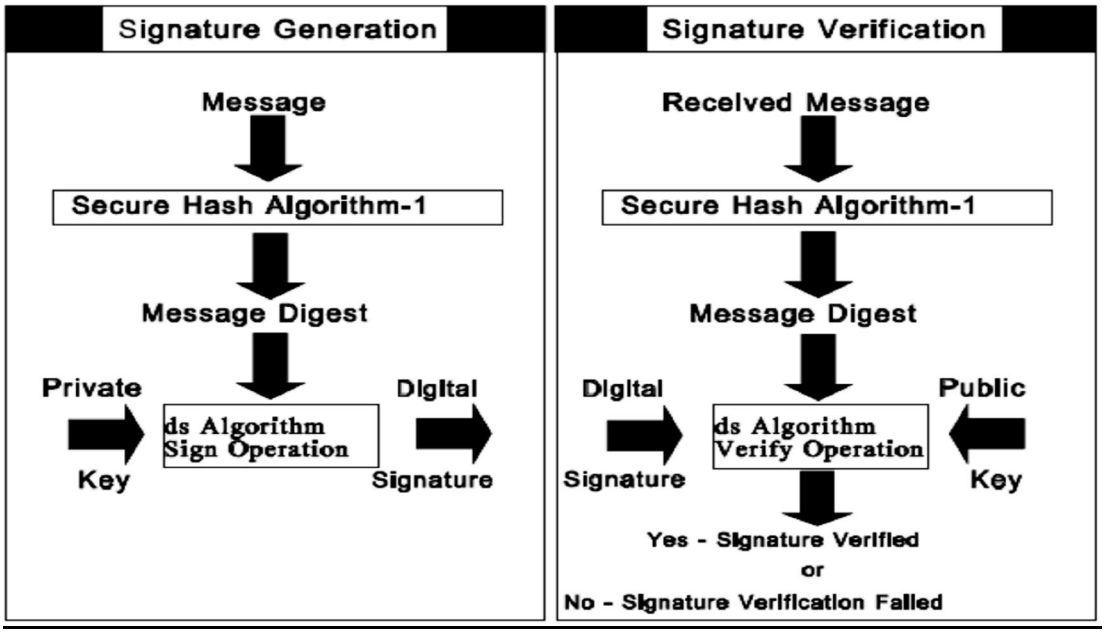

Figure 7.12: Signature Generation and Verification (ref [57])

7.3.2 Limitations to signature detection

The limitations of signature based system are that it requires previous knowledge of attack to generate accurate signature. Signature based IDS is not adequate solution for blind to unknown attacks. It can trigger alarm if traffic is benign. The packet over head of signature base IDS are much more than other packet filtering Intrusion detection techniques.

Chapter 8

Experimental Validation

This section describes the experiments performed in order to investigate the performance of AIS-IDP.

8.1 ROC Analysis

ROC (Received Operating Characteristic) analysis is introduced in signal detection theory to describe how well a receiver can distinguish a signal from noise or more generally, depict a tradeoff between hit rates and false alarm rates of classifiers. To motivate the ROC analysis, we give a simple example of a binary classifier and the resulting evaluation problems.

8.2 Performance Metrics

AIS-IDP presented in this paper is an anomaly detection framework which classifies network traffic in a time window as either benign or malicious. Therefore, the classification problem of AIS-IDP is a binary classification problem. We carry out the standard ROC (Receiver Operating Characteristics) analysis of AIS-IDP. There can be four possible outcomes of a binary classifier:

1. TP (True Positive),
2. FP (False Positive),
3. TN (True Negative) and
4. FN (False Negative).

If we define P = TP +FN and N = FP +TN then we may define the performance metrics for our classification framework as follows:

TP-Rate = TP/P and

FP-Rate = FP/N.

The results of AIS-IDP presented in this section were optimized for accuracy which is defined as: Accuracy= (TP+TN)/(P+N). A suitable value of distance matching

threshold was set for every end-point for optimized accuracy. Figure 8.4 and 8.5 shows the TP-Rate and the FP-Rate plots of AIS-IDP.

8.3 Simulation Testbed

Simulations experiments were performed on Open IMS Core. The Open IMS Core is an implementation of IMS Call Session Control Functions (CSCFs) and a lightweight Home Subscriber Server (HSS), which together form the core elements of all IMS/NGN architectures (See Figure 8.1) as specified today within 3GPP, 3GPP2, ETSI TISPAN and the Packet Cable initiative. The four components are all based upon Open Source software (e.g. the SIP Express Router (SER) or MySQL) and available as an open source on there project home page. For almost three years the Open IMS Core has formed the heart of the Open IMS Playground @ FOKUS.

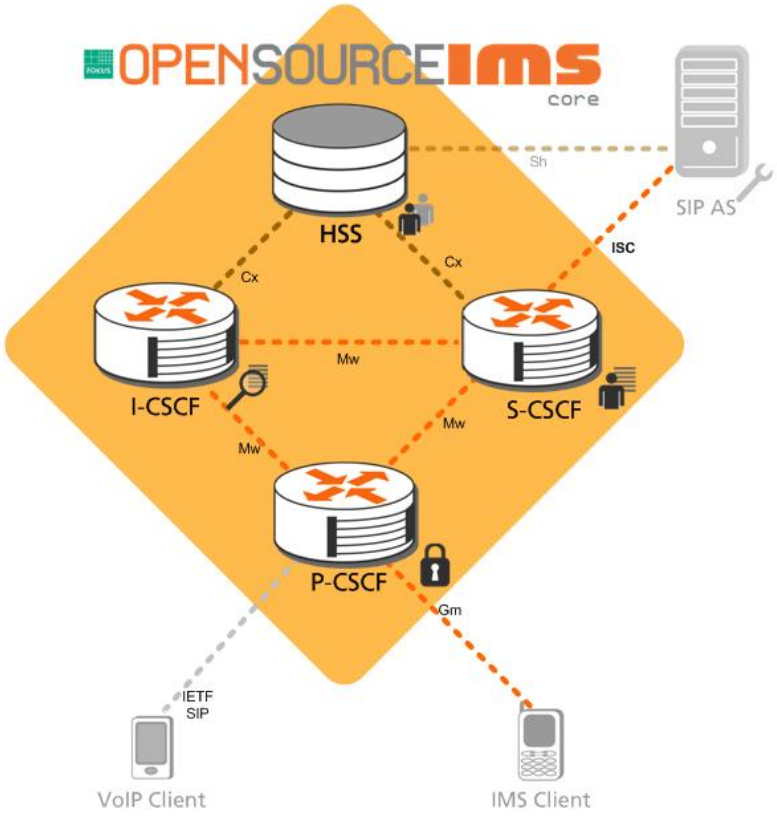

Figure 8.1: Open IMS Core (ref [5])

Figure 8.1 shows the components and the reference points for each component (for details see chapter 2- section 2.7 -Table 2.1). Table 8.1 shows the port numbers on which each component listens for control plane signaling.

Table 8.1: Component and ports

Components	Ports in OpenIMSCore
PCSCF	4060
ICSCF	5060
SCSCF	6060
HSS	3868, 3869, 3870
UE	Any

Traffic set for experimentation and validation were collected through network protocol analyzer Ethereal (Wireshark) and through packet sniffer tcpdump. Since the data monitored by AIS-IDP consists of SYN packets, UDP packets, ICMP and SIP packets TCPdump is used to obtain it. The TCPdump program outputs the headers of packets on a network interface. The general format of the TCP headers output byTCPdump is shown in Figure 8.2. The fields src and dst are the source and destination IP addresses and ports. The flags field may be a combination of S (SYN), F (FIN), P (PUSH), R (RST) or a single '.' (No flags). Figure 8.3 shows traffic capture of SIP packets for S-CSCF component.

src > dst: flags data-seqno ack window urgent options

Figure 8.2: General format of a TCP line

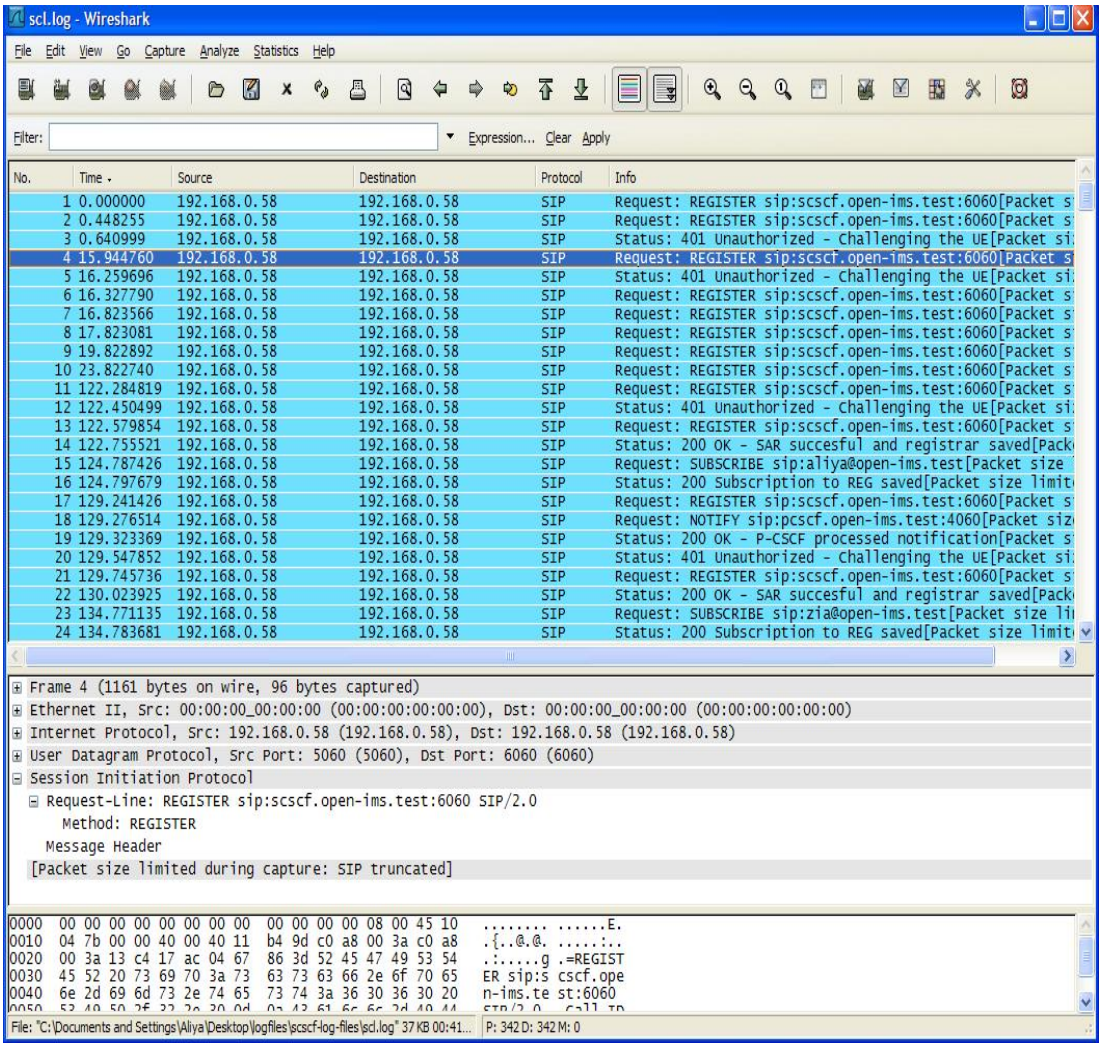

Figure 8.3: Traffic Capture of SIP for S-CSCF

8.4 Discussion on Results

AIS-IDP has an average fp-rate of 4.9% (peaking at 7.8% for UE2) and an average tp-rate of 95.15% (peaking at 98.3% for component S-CSCF). See Table 8.2 for results. The reason for high True positive rate for component S-CSCF and I-CSCF is that traffic pattern is very deterministic as compare to traffic pattern of UE's and P-CSCF which is random.

Table 8.2: False Positive Rate and Accuracy for 100% True Positive Rate

Component ID	Component Name	*fp* Rate (%)	*tp* Rate(%)	Accuracy (%)
1	S-CSCF	1.7	98.3	98.3
2	I-CSCF	2.8	97.2	97.2
3	P-CSCF	6.1	93.9	93.9
4	HSS	3.3	96.7	96.7
5	UE1	7.7	92.3	92.3
6	UE2	7.8	92.2	92.2

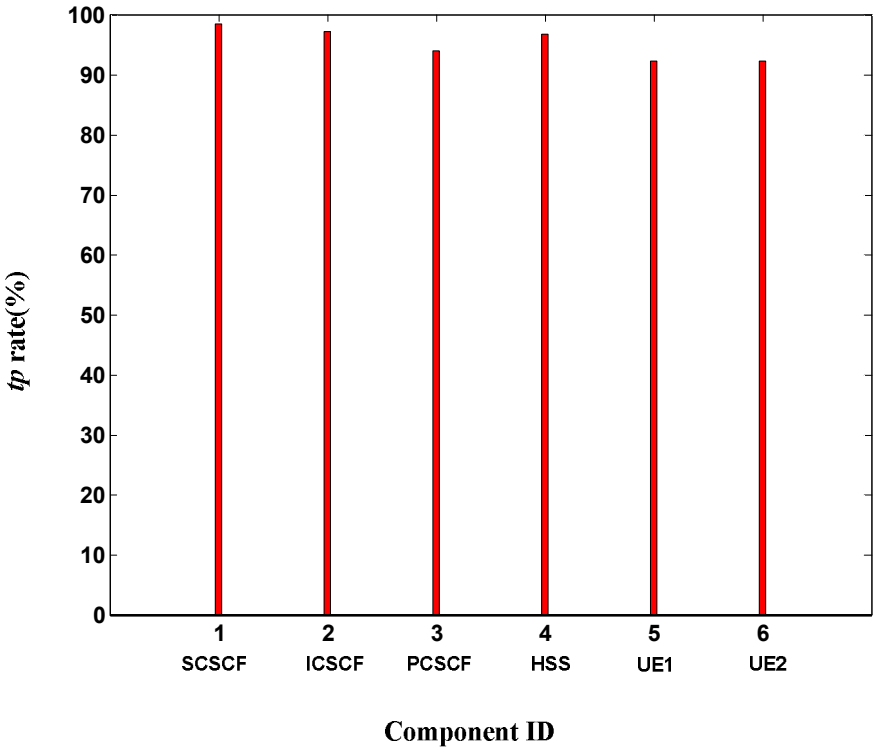

Figure 8.4: True positive rates of AIS-IDP

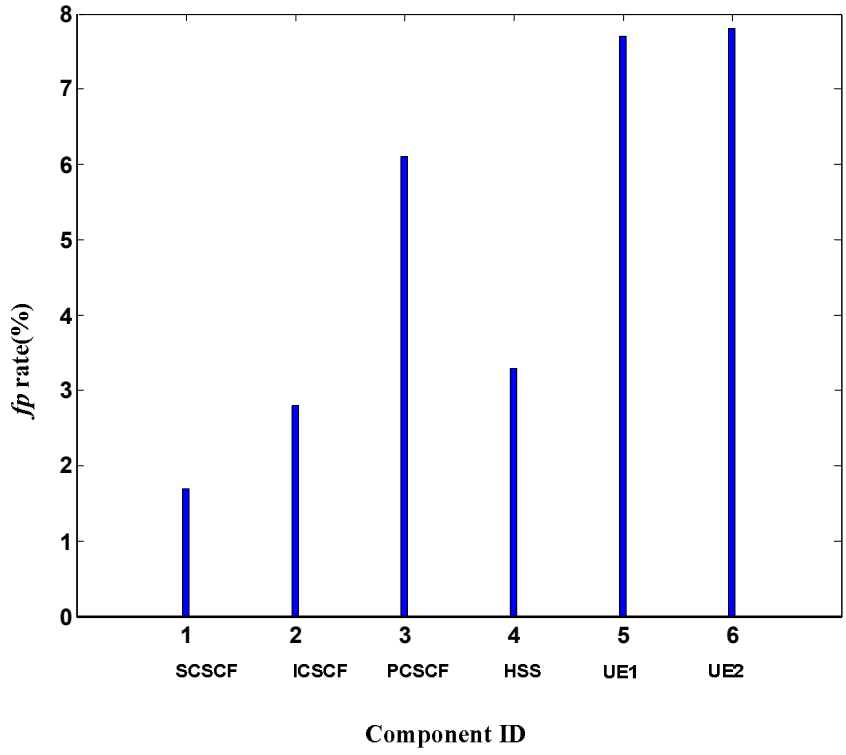

Figure 8.5: False positive rates of AIS-IDP

8.5 Comparison of AIS-IDP with Signature based IDP

The over head of signature based techniques is much more than packet filtering technique for simple DSA with 1024 key length creates 320 bits of signature which is equivalent to 40 bytes that mean 40 additional bytes travel with each packet. The other main bottleneck with crypto based IDS are that signature creation using DSA, takes about **0.687000 second of CPU cycles** to run on a Pentium IV 1.83 GHz with core2 duo processor machine. Table 8.3 shows the control over head of AIS and signature based algorithm. The time require to create and verify 342 traffic signatures is 326.279000 seconds CPU cycles as compare to AIS-IDP which is 0.859000 seconds of CPU cycles.

Table 8.3: Overhead Comparison of AIS-IDP and Signature based Algorithm

Component Name	**Normal Traffic** AIS based Algorithm	**Attacked Traffic** AIS based Algorithm	**Normal Traffic** Signature based Algorithm DSA	**Attacked Traffic** Signature based Algorithm DSA
SCSCF	144226 (342 sessions)	171543 (757 sessions)	157906 (342 sessions)	207879 (757 sessions)
ICSCF	248138 (156 sessions)	295297 (508)	255625 (156 sessions)	319681 (508 sessions)
UE	60704 (150 sessions)	64836 (453 sessions)	67904 (150 sessions)	86580 (453 sessions)

8.6 Performance Evolution of AIS-IDP

The important consideration of AIS-IDP is that it must not cause much delay during online and real time processing to avoid message retransmission. In practical environment IMS core, especially P-CSCF process lot of registration and authentication messages. Therefore performance is very critical when IDP is deployed in real world senior. The performance metric is the average delay per message in millisecond which we measure in normal and heavy load seniors. Our AIS based solution is light weight with much less processing cost as compare to classical cryptology based solutions.

Chapter 9

Conclusion & Future Recommendations

In the previous sections, securitoky frame work has been proposed for IMS and NGN All-IP network and the architecture of AIS has been reviewed for DoS and DDoS attacks on IP Multimedia Systems (IMS).

AIS-IDP can scale its complexity, accuracy, and underlying traffic features in accordance with the point-of-deployment and security requirements.

In this thesis, the negative selection has been investigated, as an immune inspired paradigm when applied for anomaly detection and (network) intrusion detection problems. In following works, different algorithms for generating detectors were proposed [47, 48, 17] and the scope of the negative selection was extended to general anomaly detection [50, 51, 52, 53] and (network) intrusion detection problems [54, 55]. However, in several works [28, 49] different problems in negative selection were mentioned, but not closer investigated from the perspective of a pattern classification problem. This investigation was done in [46].

In this thesis an immunological principle of negative selection has been described. Furthermore, it is described how the immune system is able to recognize a nearly unlimited number of antigens with a limited number of antibodies. For developing immune-inspired algorithms, a proper representation of the immune elements and an abstraction of the immune principles must be formulated. Work in theoretical immunology has proposed different immune elements representations and affinity metrics and provided much of the foundations for the development of artificial immune systems. In artificial immune systems, a framework is commonly used, as it guides in 3-step formalization to a solution for a given problem.

Growth Algorithm for thymus action in AIS is also presented. We further gave a more in-depth analysis of its response to deceptive traffic sets of TCP-SYN, UDP, ICMP, SIP floods. Response of AIS to *deceptive traffic* is an area that is yet to be explored completely. This is also important as more sophisticated SYN-flood and SIP based attacks appear similar to legitimate traffic. So, it becomes difficult for a victim-end filter to distinguish self traffic from attack traffic. The performance of enhanced thymus action model is much better than simple thymus action model, as it clearly

shows significant reduction in number of false positives without affecting other performance parameters.

The immune system is a complex system which protects the body against intruders like viruses, fungi, parasites and bacteria. By reading this sentence is seems to be obvious to develop an intrusion detection system which is inspired by the outstanding adaptive detection principles of an immune system.

However, as mentioned by Vapnik [45], this is not necessarily the best way for creating an artificial learning machine (or in our context an intrusion detection system).

9.1 Future Work

In this thesis, we proposed a security framework for IMS. We presented the architecture of AIS for DoS and DDoS attacks on various layers of IMS. Our results show that the AIS provide very good detection accuracy with relatively lesser memory and computational overheads as compared to the signature based scheme. This makes AIS-IDP an ideal candidate to be integrated into the IMS framework.

The proposed model was tested for r-contiguous and hamming distance matching techniques. It would be interesting to investigate the performance of other matching techniques such as r-chunk matching and variations of hamming distance matching (e.g. Rogers and Tanimoto, R&T matching) against deceptive traffic sets.

Our future work focuses on a comprehensive security solution for IMS and NGN all-IP networks to give protection at all layers. We want to extend this work to include different intelligent traffic features that would improve the performance of AIS in terms of detection accuracy.

In the field of artificial immune systems exists a lot of immune inspired algorithms and techniques which have a great potential in their application areas. Artificial immune systems are a young and exciting research field and we are convinced that immune-inspired algorithms and techniques will become well established problem solving methods in the near future, as for instance genetic algorithms and genetic programming approaches.

We also want to extend this work and compare the results of negative selection based AIS with other Bio-inspired techniques such as danger theory based AIS and machine learning schemes such as one-class Support Vector Machines (SVM).

References

IETF RFC Selection

- RFC 3261-SIP Session Initiation Protocol.
- RFC 3310-Hypertext Transfer Protocol (HTTP) Digest Authentication using Authentication and Key Agreement (AKA).
- RFC 3455-SIP Private Header Extension.
- RFC 3588-Diameter Based Protocol.
- RFC 3680-SIP Event Package for Registration.

3GPP IMS Release 6 Specifications Selection

- TS 23.228-IMS Stage 2
- TS 24.299-IP Multimedia Call Control Protocol (SIP) and Session Description Protocol (SDP); Stage 3
- TS 29.288- Cx and Dx Interfaces; Signaling flows and message contents
- TS 33.102- Sh Interfaces; Signaling flows and message contents
- TS 33.102- 3G Security; Security Architecture
- TS 33.203- Access Security for IP-based Services
- TS 33.210- 3G security; Network Domain Security

IP Multimedia System

1. Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3GPP, TS 23.228 V6.7.0 (2004-09), "IP Multimedia Subsystems (IMS)", www.3gpp.org.
2. Third Generation Partnership Project (3GPP), www.3gpp.org.
3. Third Generation Partnership Project 2 (3GPP2), www.3gpp2.org.
4. IMS Playground: www.fokus.fraunhofer.de/ims.
5. 3Gb Testbed: www.fokus.fraunhofer.de/national_host. www.openimscore.org.
6. T. Magedanz, D. Witaszek, K. Knuettel: "The IMS Playground @ Fokus – An Open Testbed for NextGeneration Network Multimedia services." Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005. First International Conference on 23-25 Feb. 2005 Page(s):2 – 11,IEEE.
7. 3GPP Technical Specification of Security: http://www.3gpp.org/ftp/Specs/html-info

8. Grech M, Torabi M, Unmehopa, MR, “Service Control Architecture in the UMTS IP Multimedia Core Subsystem.” 3G Mobile Communications Technologies, IEEE conference Publication #489, May 2002.
9. Rashid O, Coulton P, Edwards R, “Implications of IMS and SIP on the Evolution of Mobile Applications.” IEEE Tenth International Symposium on Consumer Electronics, June 2006.
10. Marsic B, Borosa T, Pocuca S, "IMS to PSTN/CS interworking" Proceedings of the 7th International Conference on Telecommunications, Volume 2, June 2003
11. UMTS Overview, UMTS World, http://www.umtsworld.com/technology/overview.htm
12. GSM Association, What is GSM? http://www.gsm.org/technology/what.shtml
13. CDMA Development Group, http://www.cdg.org/

IP Multimedia System Security

14. M. Sher, T. Magedanz, “Secure Service Provisioning Framework (SSPF) for IP Multimedia System and Next Generation Mobile Networks” 3rd International Workshop in Wireless Security Technologies, London, U.K. (April 2005), IWWST’05 Proceeding (101-106), ISSN 1746-904X, *www.iwwst.org.uk.*
15. M. Sher, T. Magedanz,”Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)”, Proceedings of the First International Conference on Availability, Reliability and Security (ARES’06), In IEEE, 2006.

Artificial Immune System

16. M. Zubair Shafiq and Muddassar Farooq, Defence against 802.11 DoS attacks using Artificial Immune System, 6th International Conference on Artificial Immune Systems, In LNCS, Brazil, 2007. (In Press)
17. M. Zubair Shafiq, Mehrin Kiani, Bisma Hashmi and Muddassar Farooq, Extended Thymus Action for reducing False Positives in AIS based Network Intrusion Detection Systems, In Proc. of Genetic and Evolutionary Computation Conference (GECCO), UCL, London, 2007. (In Press)
18. M. Zubair Shafiq, Mehrin Kiani, Bisma Hashmi and Muddassar Farooq, Extended Thymus Action for Improving the reponse of AIS based NID against Malicioius Traffic, In Proc. of IEEE Congress of Evolutionary Computation (CEC), Singapore, 2007. (In Press)
19. Nauman and M. Farooq, Vulnerability Analysis and Security Framework (BeeSec) for Nature Inspired MANET Routing Protocols In Proc. of Genetic and Evolutionary Computation Conference (GECCO), UCL, London, 2007. (In Press)

20. Nauman and M. Farooq, BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc, 6th International Conference on Artificial Immune Systems, Brazil, 2007. (In Press)
21. H.F. Wedde, C. Timm, and M. Farooq. Beehiveais: A simple, efficient, scalable and secure routing framework inspired by artificial immune systems. In PPSN, pages 623–-632, 2006.
22. Muddassar Farooq, Intelligent Network Traffic Engineering through Bee inspired Natural Protocol Engineeirng, Natural Computing Seires, Springer Verlag, 2007. (In press).
23. Steven A. Hofmeyr and S. Forrest, Architecture for an Artificial Immune System, Evolutionary Computation Journal, pp. 443-473, 2000.
24. A. Soule, K. Salamatian, and N. Taft, Combining filtering and statistical methods for anomaly detection, ACM/Usenix IMC, October 2005.
25. Y. Gu, A. McCullum, and D. Towsley, Detecting anomalies in network traffic using maximum entropy estimation, ACM/Usenix IMC, October 2005.
26. S. Balachandran, D. Dasgupta and L. Wang. A Hybrid Approach for Misbehavior Detection in Wireless Ad-Hoc Networks. Published in Symposium on Information Assurance, New York, June 14-15, 2006.
27. S. Sarafijanovic and J.-Y. Le Boudec, An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors, 3rd International Conference on Artificial Immune Systems, pp. 342-356, 2004.
28. Kim J. & Bently P. J., Investigating the Roles of Negative Selection in an AIS for NID, IEEE Transactions of Evolutionary Computing, Special Issue on AIS, 2001.
29. Tao Peng, Defending against Distributed Denial of Services Attacks, Ph. D. dissertation, Department of Electrical and Electronics Engineering, University of Melbourne, April, 2004.
30. Stallings, “Cryptography and Network Security: Principles and Practice”, Second Edition, Copyright 2000.
31. Kruegel, Valeur, Vigna, “Intrusion Detection and Correlation Challenges and Solutions” 2005 Springer Science + Business Media, Inc.
32. Leandro N. de Castro and Jonathan Timmis, “Artificial Immune Systems: A New Computational Intelligence Approach,” Springer, 2002.

33. poikeselka, Mayer, Khartabil, Niemi, “The IMS IP Multimedia Concepts and Services”, Second Edition, 2006 Jhon Wiley & Sons,LTD.
34. Clinton M.Banner, ”The IP Multimedia Subsystem(IMS)- an Introduction”.
35. Kotapati,Liu,Sun, LaPorta, “Taxonomy of Cyber Attacks on 3G networks”, The Pennsylvania state University Park.
36. Stibor, Timmis, Eckert, “A Comparative Study of Real-Valued Negative Selection to Statistical Anomaly detection” Department of Computer science, Darmstadt University of Technology.
37. NIDES Project: http://www.sdl.sri.com/projects/nides
38. SNORT Project: http://www.snort.org/
39. http://en.wikipedia.org/wiki/Snort_(software)
40. S.E. Smaha, “Haystack: An intrusion detection system”, IEEE 4th Aerospace Computer Security Applications Conference, 1988, USA.
41. Debar H., Dacier M. and Wepsi A., “Towards a taxonomy of intrusion detection systems”, Computer Networks, pp. 361-378.
42. Steven A. Hofmeyr and S. Forrest, “Architecture for an Artificial Immune System”, Evolutionary Computation Journal, pp. 443-473, 2000.
43. Tao Peng, “Defending against Distributed Denial of Services Attacks”, Ph. D. dissertation, Department of Electrical and Electronics Engineering, University of Melbourne, April, 2004.
44. Martin Thorsen Ranang, “An Artificial Immune System Approach to Preserving Security in Computer Networks”, Master Thesis, Faculty of Information Technology, Mathematics and Electrical Engineering (IME) at the Norwegian University of Science and Technology (NTNU), June 2002.
45. Vladimir N. Vapnik. “The Nature of Statistical Learning Theory”. Springer-Verlag, second edition, 1999.
46. Stibor Thomas” On the Appropriateness of Negative Selection for Anomaly Detection and Network Intrusion Detection” PhD Dissertation 2006.
47. Modupe Ayara, Jonathan Timmis, Rogerio de Lemos, Leandro N. de Castro, and Ross Duncan. Negative selection: How to generate detectors. In Proceedings of the 1nd International Conference on Artificial Immune Systems (ICARIS), pages 89–98. University of Kent at Canterbury Printing Unit, 2002.

48. Patrick D'haeseleer, Stephanie Forrest, and Paul Helman. An immunological approach to change detection: algorithms, analysis, and implications. In Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy, pages 110–119. IEEE Computer Society, IEEE Computer Society Press, May 1996.
49. Alex Alves Freitas and Jonathan Timmis. Revisiting the foundations of artificial immune systems: A problem-oriented perspective. In Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS), volume 2787 of Lecture Notes in Computer Science, pages 229–241. Springer-Verlag, 2003.
50. Zhou Ji and Dipankar Dasgupta. Real-valued negative selection algorithm with variable-sized detectors. In Genetic and Evolutionary Computation – GECCO-2004, Part I, volume 3102 of Lecture Notes in Computer Science, pages 287–298, Seattle, WA, USA, 26-30 June 2004.Springer-Verlag.
51. Zhou Ji and Dipankar Dasgupta. Augmented negative selection algorithm with variable-coverage detectors. In Congress on Evolutionary Computation, pages 1081–1088. IEEE, 2004.
52. Fabio Gonz´alez, Dipankar Dasgupta, and Robert Kozma. Combining negative selection and classification techniques for anomaly detection. In Congress on Evolutionary Computation, pages 705–710. IEEE, May 2002.
53. Fabio Gonz´alez, Dipankar Dasgupta, and Luis Fernando Nio. A randomized real-valued negative selection algorithm. In Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS), volume 2787 of Lecture Notes in Computer Science, pages 261–272, Edinburgh,UK, 2003. Springer-Verlag.
54. Fabio Gonz´alez, Dipankar Dasgupta, and Robert Kozma. Combining negative selection and classification techniques for anomaly detection. In Congress on Evolutionary Computation, pages 705–710. IEEE, May 2002.
55. Steven Hofmeyr and Stephanie Forrest. Architecture for an artificial immune system. Evolutionary Computation, 8(4):443–473, 2000.
56. Juels and Brainard, "A Cryptographic Defense against Connection Depletion Attacks", RSA Laboratories.
57. William Mehuron "Specifications for the Digital Signature Standards (DSS)" Federal Information Processing Standards Publication 186-2, 2000 January 27.