Hybrid Intrusion Detection System using Fuzzy logic and Signature based approach for SIP Based DoS Attacks

MS Research Dissertation

By

Saadia Khan

(594-FBAS/MSCS/F09)

Supervised By

Prof. Dr Muhammad Sher

Department of Computer Science and Software Engineering

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

(2012)

A Dissertation Submitted to the

Department of Computer Science and Software Engineering

International Islamic University Islamabad

As a partial fulfillment of requirements for the award of the degree of

MS in Computer Science

2869

2346

International Islamic University, Islamabad

Dated: June 29, 2012

Final Approval

It is certified that we have examined the thesis titled "Hybrid Intrusion Detection System using Fuzzy logic and Signature based approach for SIP Based DoS Attacks" submitted by Saadia Khan, Registration Number 594-FBAS/MSCS/F09 and found as per standard. In our judgment, this research work is sufficient to warrant its acceptance by the International Islamic University, Islamabad for the award of MS Degree in Computer Science.

Committee

External Examiner

Dr. M. Hussain
Associate Professor,
Department of Computer Science,
SZABIST Islamabad

Internal Examiner

Dr. Ayyaz Hussain
Assistant Professor
Department of Computer Science& Software Engineering.
International Islamic University, Islamabad

Supervisor

Prof. Dr. Muhammad Sher
Chairman,
Department of Computer Science & Software Engineering.
International Islamic University, Islamabad

Declaration

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

Saadia Khan
(594-FBAS/MSCS/F09)

I dedicate this thesis to my
Parents for their immense love and support

Acknowledgment

First of all I am obliged to Allah Almighty the Merciful. the Beneficent and the source of all Knowledge, for granting me the courage and knowledge to complete this Project.

I am grateful to my advisor, Prof. Dr Muhammad Sher, for the outstanding motivation, guidance, support, and knowledge he has provided throughout the course of this work. He kindly took me into his group and provided me with a great amount of freedom to work on things that I liked.

Last, but not the least, I thank my parents and my siblings. It has been their lasting love and support that enabled me to reach this point

PROJECT IN BRIEF

Project Title:	**Hybrid Intrusion Detection using Fuzzy Logic and Signature based approach for SIP Based DoS Attacks**
Undertaken By	Saadia Khan
Supervised By	Prof. Dr Muhammad Sher
Start Date	January 2011
Completion Date	February 2012
Tools and Technologies	Matlab 7.4, Wireshark
Documentation Tools	MS Office
Operating System	Windows 7
System Used	intel core i3

LIST OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
API	Application Programing Interface
ARP	Address Resolution Protocol
BPF	Berkeley Packet Filter
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
HIDS	Host Intrusion Detection System
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
NIDS	Network Intrusion Detection System
OS	Operating System
PBX	Private Branch Exchange
POP	Post Office Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SAP	Session Announcement Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPIT	Spam over Internet Telephony
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server

UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VoIP	Voice over Internet Protocol
XML	Extensible Markup Language

Table of Contents

List of Figures

List of Tables

Abstract

Traditionally separate networks are used to carry out voice and data e.g. circuit switched networks have been employed for voice transmission whereas packet switched networks are used for data transmission. Network convergence has come up with a benefit that it has merged the data and voice network to single shared infrastructure. This network convergence helps us in terms of cost and efficiency.

Voice over internet protocol (VoIP) is a protocol which allows multimedia communication on packet switched infrastructure of internet protocol. Session initiation protocol (SIP) is the standard signaling protocol for real time communication on VoIP. SIP is application layer protocol. It is text based protocol like http and has request/response architecture. SIP protocol is vulnerable to many security threats like Denial-of-service (Dos), social threats etc.

A lot of work has been done for the intrusion detection of SIP-VoIP network. Most of the work done so far uses signature based intrusion detection or anomaly based intrusion detection strategy. In our work we are going to describe Hybrid intrusion detection system which makes use of two types of modules. These two modules are signature based IDS and fuzzy rule based IDS. The first module which is signature based IDS will perform intrusion detection on SIP traffic based on various predefined intrusion signatures , the SIP traffic which is declared non-intrusive from signature based IDS module is further analyzed by Fuzzy rule based module. Thus with the help of two phases of intrusion detection false alarm ratio is decreased considerably which is the main characteristic of any intrusion detection system.

Chapter 1

1. Introduction

This chapter can be divided into two major parts. The first part will provide an overview about intrusion detection system, its types and characteristics, importance of intrusion detection.

In the second part Voice over Internet Protocol is discussed in detail. As VoIP is the technology used for the transmission of voice and multimedia sessions over internet, it consists of set of protocols for session establishment, data transfer and support protocol. Our research thesis mainly focuses on session initiation protocol. SIP has been established as a de-facto standard for session establishment over internet. Some details regarding SIP, vulnerabilities associated with SIP and attack scenarios are discussed in this part of the chapter. Some brief descriptions about other protocols involved in VoIP network is also discussed briefly.

1.1 Intrusion detection

An intrusion is an action which aims to compromise the integrity, confidentiality, or availability of any network resource. An Intrusion Detection System (IDS) is a second line of defense behind protection systems like authentication, access control and cryptography [1]. Anderson [2] was the first who introduced the concept of intrusion detection, he define intrusion as the risk of illegal attempt to Access information, Manipulate information or Render a system unreliable. The goal of Intrusion detection system is to provide a mechanism for monitoring a host or whole computer network against these security threats or intrusions.

1.1.1 Types of Attacks

Attacks can be classified into two major groups based on the effect which they made on victim host or network; these are active attack and passive attack. Active attacks penetrate through system protection. They try to steal or modify information or data present on the network. Active attacks may result in the release of some important information. Some common example of active attack includes Denial of Service, masquerade attack etc.

While on the other hand passive attacks try to get information about system resources without making any effect on the system but these attacks affect confidentiality of the system. Once this attack is launched it gets information about system which attacker may use to launch some other attack. Example of passive attack includes eavesdropping attack.

1.2 Classification of intrusion detection system

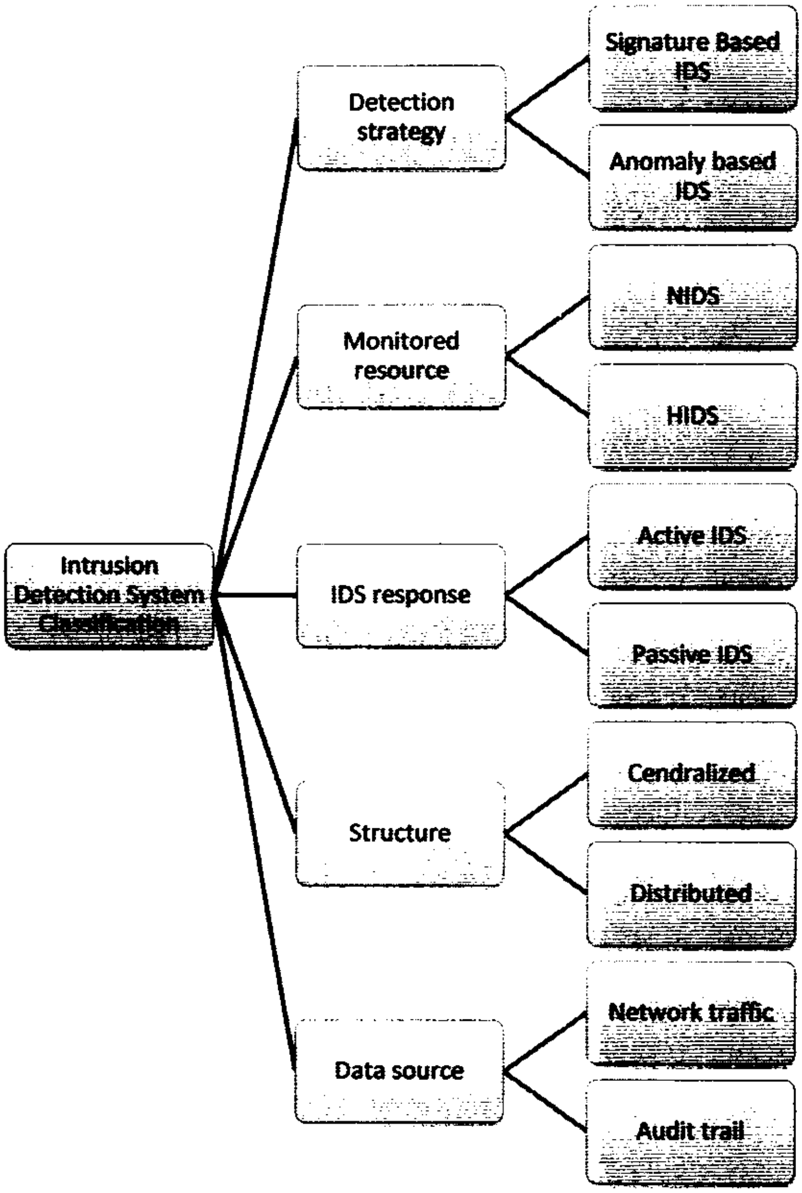


Figure 1-1 Intrusion detection classification

1.2.1 Intrusion detection methodology

On the basis of detection principle IDS can be classified into Signature based IDS and Anomaly based IDS.

Anomaly based intrusion detection

This method tries to find normal system behavior, the system usually identifies patterns of behavior that deviate from normal system behavior. Anomaly based IDS can detect new attacks but it produces a high number of false alarms. Accuracy of anomaly based approach depends on feature selection and threshold values upon which deviation from normal profile is measured [4].

Signature based intrusion detection

In signature-based detection various previously known intrusion patterns are stored in the signature database, if the network activity matches with the pattern or signature present in the database alarm is triggered [3]. Signature for intrusion detection models intrusive behavior of the network. Signature based IDS can detect only previously known attacks and couldn't detect new attacks, for new or unknown attacks it may trigger false alarms. Detection accuracy of signature depends greatly upon correct setting of threshold values. For example in port scan attack an attacker may try to send large number of TCP connection request to the target host machine, possible signature for this kind of attack is to count number of connection request to the host, alarm is triggered when number of connection request increases certain threshold.

1.2.2 Monitored resource of Intrusion detection system

Placement of intrusion detection system defends on the resource which it is going to monitor on the network. The two major categories include host based intrusion detection system (HIDS) and network based intrusion detection system (NIDS).

Host based Intrusion Detection (HIDS)

The host based IDS monitor's activities and access on an individual host machine of the network. HIDS is deployed on business critical hosts like proxy servers, web server, database server etc.it only protects the system where it is placed and has nothing to do with other network entities. Therefore it increases the load on the system where it is placed. HIDS utilizes operating system related information for intrusion detection.

Network based Intrusion Detection (NIDS)

NIDS monitors traffic from multiple hosts within a network. It utilizes network traffic to monitor any suspicious activity in the network. NIDS is placed at any strategic point in the network, where it monitors all the traffic coming inside or going outside from that point. NIDS doesn't create any overload on the network.

1.2.3 Characteristics of an Intrusion Detection System

The author in [4] has mentioned some of the characteristics of intrusion detection system

1. Coverage: Determines which types of attacks the IDS can detect under ideal conditions.
2. False alarm rate: Decides the rate of false alarms produced by IDS.
3. Hit rate: it determines attacks correctly detected in some particular time period.
4. High bandwidth traffic handling: Demonstrates how well IDS can perform under heavy traffic.
5. Novel attack detection: It shows the ability of system to detect new attacks [5].

1.3 VOIP

Voice over internet protocol also known as internet telephony or IP telephony is the technology used for transmitting voice or multimedia sessions over internet rather than public switched telephone network. After signaling and media channel establishment VoIP converts analog voice data into digital signals, which are further encoded and encapsulated into packets and send over packet-switched network. On reception, similar tasks are performed (in reverse order).

1.3.1 VoIP Advantages and Limitations

VoIP benefits in terms of cost. It provides features that are usually expansive in traditional PSTN like call forwarding, voicemail, CLI and three-way calling are some of the many services offered by Internet telephone with no additional charges .Through VoIP PC–to-PC calls are free, whereas PC-to-phone calls charge a little cost which is still cheaper than PSTN. Another advantage VoIP offers is portability; one can connect to the network anywhere through high broadband internet connection. This makes VoIP as simple as e-mail.

Despite the benefits which VoIP offers there are lots of vulnerabilities associated with this protocol which it inherits from IP and also have some of its own security concerns. Due to simplicity and openness of VoIP network it becomes easy target for attackers.

1.4 VoIP Protocols

VoIP utilizes various other protocols in order to perform multimedia transmission over IP. These protocols involve signaling protocol like SIP or H.323, Media transport protocol like RTP or RTCP and support protocol. These protocols are discussed later in this session.

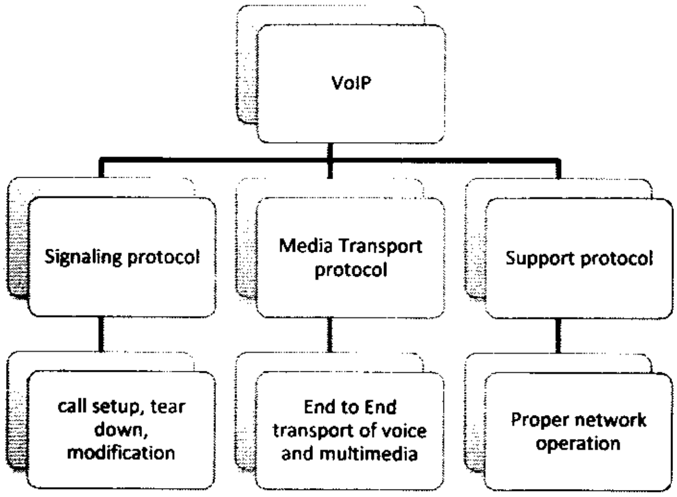


Figure 1-2 VoIP protocol types

1.4.1 SIP

Session Initiation Protocol SIP is developed be IETF. After 3GPP (The 3rd Generation Partnership Project) had selected SIP as the signaling protocol for IMS (IP Multimedia Core Network Subsystem), many other standards evolved to align with the 3GPP's IMS [8]. SIP is an application-layer control (signaling) protocol. It is used for creating, modifying, and terminating multimedia sessions over internet [6]. It can work independently of underlying transport protocols (Transport Layer protocol (TCP) or User Datagram Protocol (UDP)) and does not depend on the type of session that is being established.

1.4.1.1 SIP Network entities

A SIP session utilizes four major entities which are SIP User Agents, SIP Registrar Servers, SIP Proxy Servers and SIP Redirect Servers. Role of each entity is discussed below.

SIP User Agents

These are end user devices like PDAs, cell phones etc. There are basically two types of SIP User Agents namely SIP User Agent Client (UAC) and SIP User Agent Server (UAS). UAC has the ability to initiate call whereas UAS manages to receive calls.

SIP Registrar Servers

SIP register server contains databases in which information about the location of all user agents in a given domain is maintained. While establishing SIP session registrar servers provide participants' location information and other related information to the SIP Proxy Server [7].

SIP Proxy Servers

Routing of SIP messages is performed by proxy server. They accept session establishment requests made by a SIP UA and then it query to the SIP Registrar Server to get the recipient UA's location information. After getting location address it sends session establishment request to UA if it is located in the same domain otherwise request is forwarded to the Proxy Server of requested domain, if the UA lies in some other domain. There are two types of proxy server, namely stateless proxy server and state full proxy servers. Stateless proxy servers don't maintain any state for the transactions while on the other hand state full proxy server maintains call context or transaction state of all request/response made by user agents.

SIP Redirect Servers

SIP Redirect Server helps SIP Proxy Servers to redirect SIP messages to some external domains.

1.4.1.2 SIP Architecture

SIP is a request-response transaction-based protocol. In RFC3261 two categories of SIP messages are request and response are defined. There are six different types of request messages (according to RFC 3261), and six categories of responses are mentioned.

Table 1-1 SIP request methods defined in RFC3261 [6]

Request method	Description
REGISTER	Registering contact information
INVITE	Setting up session
ACK	Facilitates reliable message exchange for INVITEs
BYE	Terminates established session
OPTIONS	Querying server capabilities
CANCEL	Terminates pending request

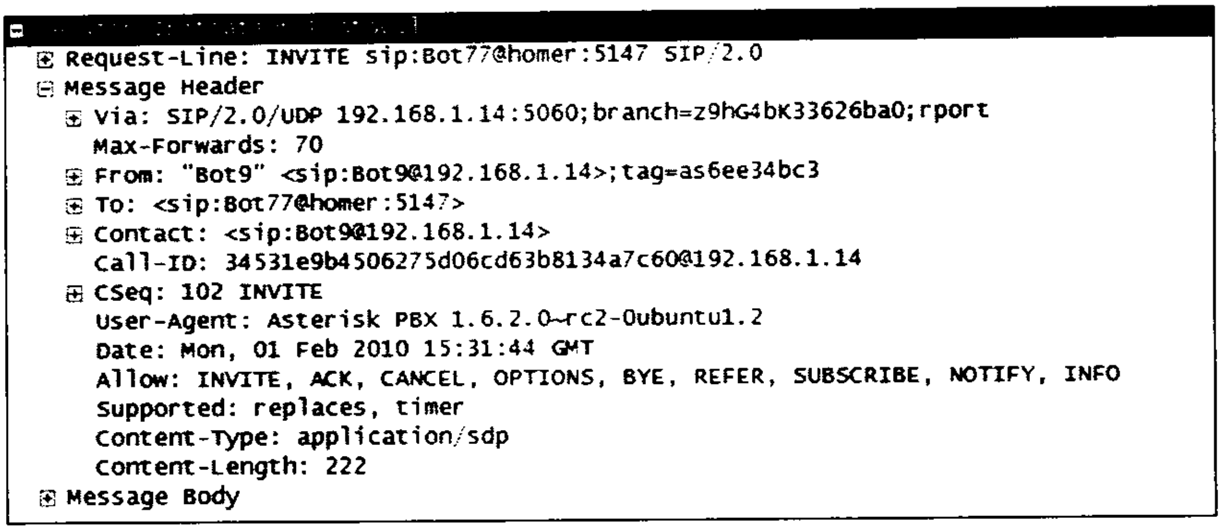
SIP response is a three digit status code. There are six categories of SIP responses 1xx Informational, 2xx successful, 3xx Redirection, 4xx request Failure, 5xx Server Failure and 6xx Global Failure.

SIP message consist of two parts message header and message body. The message header includes information like as URI (Uniform Resource Identifiers), method and Call-ID. A message body is described as SDP (Session Description Protocol) [9].

1.4.1.3 SIP Message

SIP message consists of message header and message body. Message header comprises of various fields, *Via* field indicates the transport used for the routing of SIP message and tells the location where the response is to be sent, *To* header field specifies address of record of recipient of the request, *From* header fields specifies the Address of Record of the sender of the request, *Call-id* header field is an exclusive identifier to gather a sequence of request and response send in a dialog, *CSeq* header field serves as a way to identify and order transactions, *Max-Forward* tells the maximum number of nodes a request can transfer on the way to its destination[6].

Simple example of INVITE message is shown below in this figure



```
⊞ Request-Line: INVITE sip:Bot77@homer:5147 SIP/2.0
⊟ Message Header
  ⊞ Via: SIP/2.0/UDP 192.168.1.14:5060;branch=z9hG4bK33626ba0;rport
    Max-Forwards: 70
  ⊞ From: "Bot9" <sip:Bot9@192.168.1.14>;tag=as6ee34bc3
  ⊞ To: <sip:Bot77@homer:5147>
  ⊞ Contact: <sip:Bot9@192.168.1.14>
    Call-ID: 34531e9b4506275d06cd63b8134a7c60@192.168.1.14
  ⊞ CSeq: 102 INVITE
    User-Agent: Asterisk PBX 1.6.2.0~rc2-0ubuntu1.2
    Date: Mon, 01 Feb 2010 15:31:44 GMT
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
    Supported: replaces, timer
    Content-Type: application/sdp
    Content-Length: 222
⊞ Message Body
```

Figure 1-3 SIP INVITE message

SIP message body is describes by Session description protocol, which is discussed later in this chapter.

1.4.1.4 SIP Registration example

Register server requires Address of record of user agents so that it can send request to it. UA registers themselves with the register server of their VoIP domain. This is a process which binds SIP URI with contact URIs [10]. For example Bob needs register himself with VoIP register server; he will first send REGISTER message to the Register server of his VoIP domain. In REGISTER request *To* header field will contain Address of Record (AoR), IP address of Bob can be found in *Contact* header field. Register server accepts these REGISTER request and places the information which it receives from these requests into the location service for the domain it handles.

In most cases register server use some authentication scheme in order to verify user authentication. In RFC3261, authentication was introduced originally through using HTTP digest mechanism, transport layer mechanism or Secure Multipart Internet Mail Extensions (S/MIME).

In figure 1-4 User agent sends REGISTER request to the Register server, Register server replies with "401 unauthorized". For the user agent point of view it means that REGISTER request has to be send once more. In the "401 Unauthorized" response, the important header is *WWW-Authenticate:* this header instructs the user agent to authenticate using the digest authentication. This header contains challenge of a shared secret. UAC will combine the challenge string with the user's password and compute the MD5 hash value. Register server will also compute its MD5 hash value using the same procedure and then compare this value with the one received from the UAC.

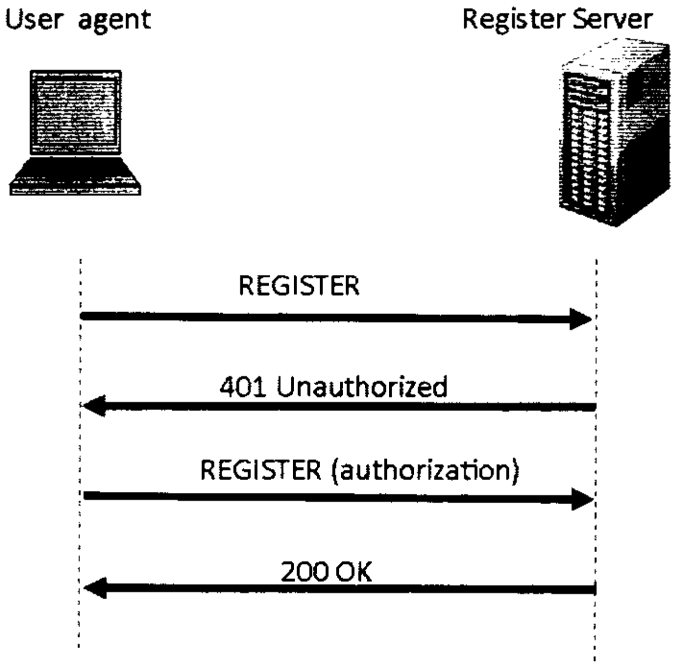


Figure 1-4 SIP registration example

1.4.1.5 SIP Call example

Figure 1-5 shows an example of SIP Call setup and teardown. In order to establish a call session, UAC sends an INVITE request to UAS. Proxy server sends 100 Trying responses to UAC after forwarding INVITE request to the requested UAS. UAS responds with 180

Ringing and 200 OK responses subsequently. Lastly the UAC receives OK response, sends ACK request and the connection is established [9].

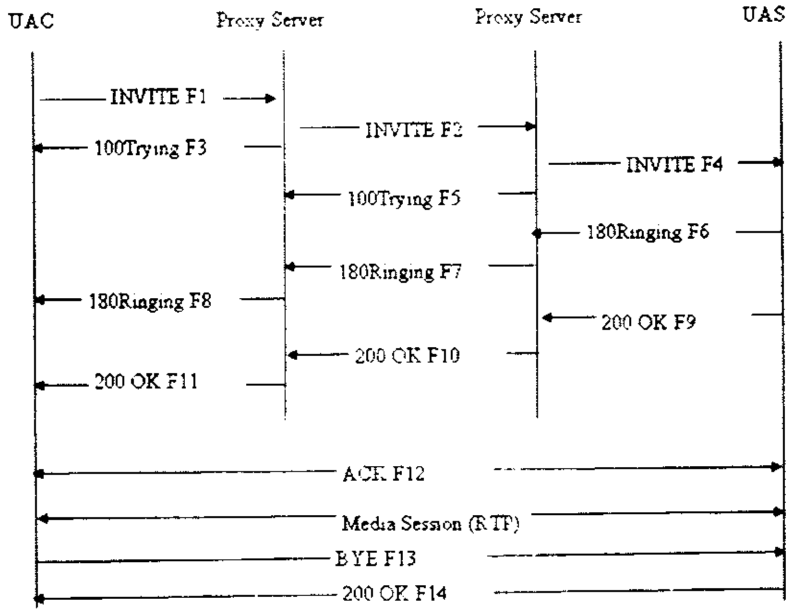
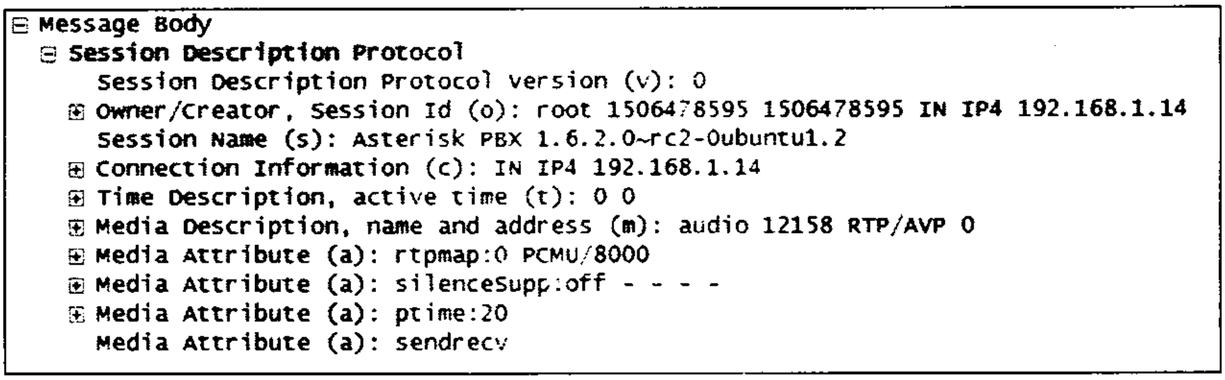


Figure 1-5 SIP Call flow example [9]

1.4.2 Session Description Protocol SDP

SDP was proposed by IETF in April 1998 as RFC2327, its revised addition was brought in 2006 as RFC4566. SDP is used for describing multimedia sessions for the purposes of multimedia session initiation [11]. SDP doesn't serves for end to end media delivery rather it is used for session initiation. SDP is designed to be extensible to support new media types and formats, and due to its extensible nature it is used in conjunction with various other protocols like SIP.

Figure 1-6 shows example of SDP body. It includes various fields namely, *Version:* it tells about the current version of SDP, *Owner/Creator, Session ID (o)* uniquely identifies the session, *Session Name (s)* tells the name of the session *.connection Information (c)* tells the connection type and address. *Time description (t)* tells describes start time and the stop time of the session. Media Attribute (a) describes media session type, port, protocol and the format-list.

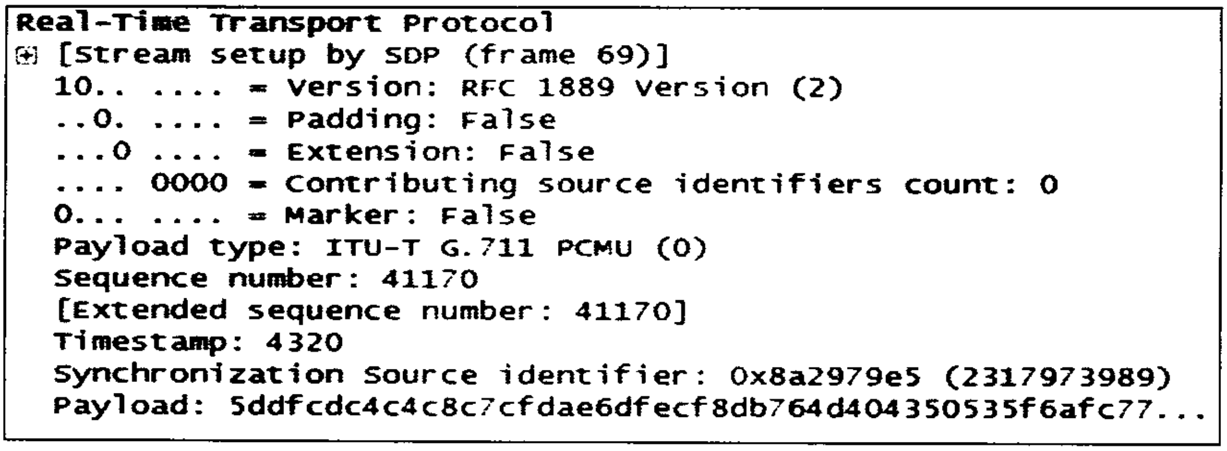


```
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol version (v): 0
    ⊞ Owner/Creator, Session Id (o): root 1506478595 1506478595 IN IP4 192.168.1.14
      Session Name (s): Asterisk PBX 1.6.2.0~rc2-0ubuntu1.2
    ⊞ Connection Information (c): IN IP4 192.168.1.14
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 12158 RTP/AVP 0
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): silenceSupp:off - - - -
    ⊞ Media Attribute (a): ptime:20
      Media Attribute (a): sendrecv
```

Figure 1-6 SDP Message body

1.4.3 Real-Time Transport Protocol RTP

RTP was originally designed by IETF in 1996 as RFC1889 [12], which was further superseded in 2003 by RFC 3550 [13]. RTP facilitates end-to-end transport of real-time data. RTP doesn't give any assurance about Quality of service for real-time services. RTP works independent of underlying transport protocol. For QoS assurance Real time control protocol RTCP has been employed which guarantee QoS and convey information about the participants in an on-going session. RTCP also provide mechanism to arrange received packets in correct order.



```
Real-Time Transport Protocol
⊞ [Stream setup by SDP (frame 69)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 .... = Extension: False
  .... 0000 = Contributing source identifiers count: 0
  0... .... = Marker: False
  Payload type: ITU-T G.711 PCMU (0)
  Sequence number: 41170
  [Extended sequence number: 41170]
  Timestamp: 4320
  Synchronization Source identifier: 0x8a2979e5 (2317973989)
  Payload: 5ddfcdc4c4c8c7cfdae6dfecf8db764d404350535f6afc77...
```

Figure 1-7 RTP header

RTP message header comprises of various fields. *Version* tells currents version of RTP, *padding* bit is set true in case of padding octets, *Extension* bit is set if the RTP header is extended, *contributing source identifier count* the number of contributing sources, *Marker* Indicates the start of a new frame, *Payload type* tells codec in use, *Sequence number* is incremented after each sent RTP packet, *synchronization source identifier payload* tells about the sender of the RTP packet

1.5 Thesis Outline

In this chapter we have tried to give an overview about what is an intrusion and types of attacks. Classification of intrusion detection systems on the basis of detection method and monitoring resources is discussed briefly in this chapter. Later in the chapter we gave introduction about VoIP protocol and then discussed various other protocols which are involved in VoIP like SIP, SDP. RTP and RTCP. Our main focus is on SIP protocol so it is discussed with more detail.

Rest of dissertation focuses on detailed discussion of intrusion detection methodologies. VoIP is emerging technology; it is offering lot of benefits to the user but along with this various security risks are associated. In the next chapter we will discuss these issues and also SIP specific security breaches. We will also discuss literature survey which will cover research work done already in the field of VoIP intrusion detection. In chapter 3 we will present requirement analysis of the system and also define our problem domain in chapter 4 we will demonstrate our proposed system design. Chapter 5 will focus on the result achieved through our proposed system design. Then we will conclude our work in the last chapter.

Chapter 2

2. Intrusion detection methodologies

There are two major categories of intrusion detection systems misuse detection systems and Anomaly detection systems which were discussed briefly in the section 1.2.1 of chapter 1. Most IDS technology uses one of these methods while some focus on the integration of both techniques in order to achieve more detection accuracy and to reduce false alarm generated by the system. Here we are going to discuss these methods in more detail.

2.1 Misuse Detection

Misuse detection system compares the system activity against set of signature or rules. Alarm is triggered when system activity matches some signature present in signature repository. Signatures are created using pattern of known attacks. Previously known attacks to the system are detected accurately by the system but ineffective against new attacks.

In this section we are going to discuss different ways to represent attack signatures

2.1.1 Rule Based Languages

Utilizing rule based languages to create rule of known attacks is most commonly used technique for misuse based intrusion detection. Known attack scenarios are specified as rule sets, and a forward chaining algorithm is used to find intrusion [14]. Common examples of rule based languages are rule-based sequence evaluation language RUSSEL [15] and production based system tool set (P-Best) [16].

2.1.2 State Transition Analysis Tool Kit

Though rule based languages as discussed previously provides flexibility but in general they are difficult to use. It has been utilized for attack detection in networks, distributed systems and UNIX systems. Unlike rule based languages it is a high level tool for misuse detection. Attack description in STAT is much easier and simpler as compared to rule based language.

2.1.3 Automatically Build Misuse Detection Models

Data mining techniques are used to automatically construct misuse detection module. Frequent episodes and Association rules are used to find hidden relationships among data which is used to represent a system's behavior, and the Meta classification is used to combine the results of different classifiers to get better classification results.

2.1.4 Abstraction-Based Intrusion Detection

Misuse detection technique has one common drawback, system is able to cater the requirements of a single system for which it has been designed and couldn't be used in any other environment even though they have some security concerns. Abstraction-based systems aim to addresses these issues.

2.1.5 Limitations of misuse detection systems

These systems perform better than anomaly based intrusion detection systems for known threats and produce fewer false alarms because they use obvious knowledge about security threats. The major limitation of misuse detection system is that it is unable to detect novel attacks and as the system requires explicit knowledge of attacks so, attack patterns should be precisely defined.

2.2 Anomaly Detection

2.2.1 Statistical methods

According to this approach intruder behavior is different from that of normal user. Statistical methods used to construct normal user profile and try to find out difference between normal user profile and attackers profile.

2.2.2 Machine Learning and Data Mining Techniques

Various techniques like Time based Inductive Machine, Instance based Learning, Neural Network, and Audit Data Analysis and Mining can be used for anomaly detection

2.2.3 Specification-Based Methods

Specification-based systems are based on manually developed specifications that capture valid operation sequence rather than previously seen. They are capable of detecting new attacks avoiding the high rate of false alarms caused by legitimate but unseen behavior in the anomaly detection approach.

2.2.4 Limitations of anomaly detection method

Although anomaly detection has the ability to detect new attack but same flaws are also associated with this technique. A common problem is normal user profile is created from audit data collected during normal operation of the system, if same attack data is found during this period it will considered as normal. Anomaly detection approaches also suffer from high rate of false alarms.

2.3 Related work

In this section we are going to discuss previous work done in the field intrusion detection.

2.3.1 Fuzzy network profiling for intrusion detection

Dickerson et al. [18] propose a fuzzy intrusion recognition engine (FIRE). It is anomaly base Intrusion detection system based on fuzzy logic concepts. Data mining techniques have been employed by the system to process the incoming network traffic. FIRE can detect wide range of common attacks.

The proposed system consists of three types of modules. The Network Data Collector (NDC) which acts as network data sniffer, it captures network packets 15min fixed time interval and give input to Network Data Processor (NDP). NDP places raw packet data in proper categories by applying some data mining technique and then it uses fuzzy logic to create fuzzy sets. These fuzzy sets are further given as input to fuzzy Threat Analyzer (FTA). Final output from FTA leads to alerts which are sent to security administrator for response.

After the data mining process NDP produces fuzzy sets. Input data is evaluated against three characteristics, UNIQUENESS, VARIANCE and COUNT. The author has used five fuzzy sets. Fuzzy rules are specified by the security administrator of the system. The system is tested against data gathered form local area network of College of Engineering at Iowa State University.

The reported results are descriptive rather numerical that's why it is difficult to evaluate the performance of the proposed system. This system is not able to fulfill the requirements of a real-time detection of intrusion. Attacks with shorter duration are likely to be diluted during the long period flow of packet information and thus went undetected.

2.3.2 Fuzzy Based Snort (FB-Snort)

Wassim El-Hajj et al. [19] propose a NIDS. The proposed system is capable of detecting port scanning attacks. It integrates snort, a famous NIDS with fuzzy logic controller for detecting port scanning attacks and they called resulting system as fuzzy based snort (FB-SNORT). The proposed system is aimed to increase the detection rate and to decrease false alarm rate for port scanning attack. The choice of using fuzzy logic is based on two major reasons a) no clear boundaries exist between normality and anomaly b) fuzzy logic helps to smooth abrupt separation between normality and abnormality [19].

FB-Snort works as a part of snort system; it improves Snort by adding ranks to alarms triggered by Snort and also benefits in decreasing false positive as well as false negative alarms generated by the Snort and also improve the accuracy of the system.

The designed system can only work for detecting some types of port scanning attack. It can't detect all variations of port scanning attack with no false positives and negatives and no experimental results are concluded for any type of attack like DoS etc.

2.3.3 Fuzzy Based IDS on Application Layer

S.Sangeetha and Dr.V.Vaidehi [20] present a host based intrusion detection which works at application layer of the network stack. The proposed IDS consist of two modules semantic IDS and Fuzzy based IDS which work in hybrid way. Semantic/Rule based IDS looks for the specific pattern which are defined as malicious. Alert is generated if attack pattern matches the rule present in the rule base. A non-intrusive pattern could be malicious if it occurs frequently in short time interval. To detect such patterns FASIDS uses fuzzy intrusion detection system (FIDS). The proposed system is intended to work for HTTP traffic. This system analyzes both header and payload for intrusion detection.

During first module, the semantic intrusion detection is performed on the basis of rules present in the rule base. An event that doesn't match any of the rules present in the rule is forwarded to FIDS for further investigation. FIDS normalize these non-intrusive patterns and then convert them into linguistic variable in fuzzy sets. These fuzzy sets are further analyzed with the help of Fuzzy Cognitive Mapping (FCM). It fires an alarm to the client/server if some intrusion is detected. Results achieved through FASIDS show better performance in case of the detection rate and time taken to identify intrusions. False positive rate is also decreased for a specific attack.

The system is designed just for single application layer protocol HTTP (Hyper-Text Transfer Protocol).

2.3.4 A Signature Database for Intrusion detection Targeting VoIP

Bazara Barry and H. Anthony Chan [21] present an Intrusion detection system that consists of a signature database that works in conjunction with a specification-based detection module specifically designed for VoIP. As a detection base line, specification-based module takes the specifications of VoIP applications and protocols. Any deviation from the protocol's normal behavior as described by its specifications is treated as intrusion.

Proposed system is hybrid hosed based IDS for signaling protocol (SIP) and media protocol (RTP). Both header and payload parts are analyzed by the system to find any sign of intrusion. The proposed system uses an Extended Finite State Machine (EFSM) for each of the protocols involved in a session to find any deviation from proper protocol behavior according to specifications. A state table is maintained to perform further checks on semantics violations. Thus the designed system supports the use of semantics aware signatures together with syntax-aware ones.

They have four types of attacks related with SIP and RTP to demonstrate the functionality of their proposed system. The attacks include BYE attack, Re-INVITE attack, Voice injection attack, and REGISTER flooding attack.

The proposed system doesn't consider abnormal/dynamic network condition into account. False alarms are raised by the system in the case of attacks launched by delaying RTP packets. The IDS designed here relies on strict specifications that do not consider implementation differences. Some flexibility in specification based module is required.

2.3.5 A Rule based Approach for detecting port scanning attack

Urupoj Kanlayasiri et al. [22] proposed an intrusion detection system for detecting port scanning attacks. The proposed system was a Host based IDS and it utilizes rule-based state diagram technique for detecting intrusion activities in the system. Proposed system consists of two main modules a) Feature selector FS b) Decision engine (DE).System uses a set of features extracted from network packet like source IP address, TCP flags etc. Decision engine perform analysis on the basis of these extracted features. It analyzes features with a set of detection rules. Proposed system is tested against various scanning tools such as PortScanner and exscan.

Major limitation of the proposed system is that it depends on threshold values. The Threshold values used by the system are static. In this case intrusion detection depends on correct setting of threshold values, as the network traffic varies in real time communication, sudden increase in traffic can happen which is not necessarily DoS attack. In this case false alarms are raised by the system

2.3.6 Framework for detecting anomalies in VoIP

Yacine Bouzida and Christophe Mangin [23] proposed a system to secure overlay networks by detecting anomalies in Voice over IP networks. It is Network based IDS designed especially for SIP protocol.

The designed system consists of three stages. The first collect network traffic. In the second stage features are extracted from captured traffic is either normal or attack. In the last stage classification process is performed that is based on a model able to differentiate between normality and anomaly. This model is constructed using a set of features on the bases of different statistical measures between current network flow and past flows.

Proposed system monitor network traffic state fully and extract useful attributes from it. These attributes are based on known VoIP attacks. Gathered attributes are message header fields and their values (To, From, Via etc.), or message reply codes (1xx, 2xx etc.) or collected statistical data e.g. the number of INVITE requests in certain time of interval. Once the profiles are completed, the detection process starts. In the detection stage these attributes are classified into one of three classes Normal, known Attack, new condition which could possibly be some new attack situation. Given feature can belong to one of the three possible classes. During the learning phase feedback method is employed to improve the detection accuracy. Decision trees induction algorithm is used for learning.

The designed system is tested against tcp dump data gathered from an operational test bed of 2 hours duration. Learning is done on data collected in the first hour while Testing is performed on the data captured in the second collection hour. They have achieved 99% detection accuracy.

In the proposed system features based on different statistical measures between current network flow and past flows. This implies that past network flow is also involved in the intrusion detection process. One important issue related to propose system is that it doesn't address poison traffic attack i-e attacker can slowly increase the traffic which serves as input to the system and thus manages to escape from the detection.

2.3.7 A Swarm-Intelligence-Based Intrusion Detection Technique

Zhou Lianying and Liu Fengyu [24] proposed Swarm-intelligence-based IDS which aims to decrease the misjudgment & misdetection and while at the same time increase the real-time response in the present IDS. The system is inspired from biology's swarm intelligence concept such that insects like bees and aunts have less intelligence and power when working as an individual but when they are in colony then they can solve their issues and show high *swarm intelligence.*

IDS proposed in this work is based on four properties 1) Simplifying system will help in improving efficiency 2) IDS should maintain server detection system it will help to improve synchronously of the system 3) separating data traffic for each unit this will help in reducing processing of data 4) information exchange among function units should be enhanced, it will help in detecting more complex attacks.

Two models of swarm intelligence are introduced in their work, Host based model and network based model. Both models use separate detection units e.g in network model there is detection unit of ftp services, detection unit for telnet services, detection unit for e-mail services etc. where as in host based models there are detection unit for password file, detection unit for audit and log file etc. Detection Units of both models have common structure but each element's data resource and processing logic is different [24]. A signature selecting module is used to extract variables and filter data sources according to the required detection unit. The abnormal event-processing in the system is used to detect abnormal events. With the help of uniqueness of detection unit's functionality the detection results are clear and there is no need of central controller. Due to independence and less interaction may apparently improve real time response of system.

The system discussed in this paper is not implemented for set of attacks or tested against attacks. Effectiveness of system against set of attacks is not known. Real time performance of the system can't be judged.

2.3.8 An EFSM-Based IDS for Ad Hoc Networks

Jean Marie Orset et al. [25] Propose an IDS based on extended finite state machines (EFSM). It is a specification based IDS designed to address security issues related to routing protocols of Mobile ad hoc networks (MANET). OLSR routing protocol has been chosen as a case study. Specifications of OLSR are extracted manually according to RFC 3626. As it is known that OLSR is link state routing protocol, the authors in this paper have decided to model the behavior of each routing node in accordance with its state and its connectivity with the neighbor nodes.

In designed system use of EFSM has facilitated to examine the message exchange among various nodes of the network. They have used a backward checking algorithm to identify any violations to specifications of protocol. Thus the technique benefits in terms of time taken for verification.

There proposed architecture is specification based and not supported with signature based module, which made it difficult to detect DoS attacks.

2.3.9 Progressive Multi Gray-Leveling

Dongwook Shin and Choon Shim [26] proposed a progressive multi Gray-leveling algorithm (PMG) for protecting VoIP infrastructure against Spam attacks. The proposed algorithm finds the grey level of the caller. Grey level determines whether caller is SPAM or not. The analysis is based on former call patterns.

A Spam caller tries to put large number of calls in short time interval hence the gray level of the caller increases. With the increase of grey level the chance of becoming a Spam caller increases. According to PMG algorithm, if grey level increases certain threshold value then caller is no more allowed to make calls. The status of the caller will change if the spam call is not initiated in the next time period, the grey level decreases below certain threshold caller is again allowed to make calls.

The algorithm has been implemented in Vovida Open Communication Application Library (VOCAL) and Cisco call manager. Various tests have been performed to check system accuracy. According to the test results PMG works well in spam voice protection and depends on correct setting of parameters.

The major limitation of the proposed system is that it cannot treat calls carrying new identities.

2.3.10 Monitoring SIP Traffic Using SVM

Nassar et al. [37] has presented Intrusion detection system for monitoring SIP-VoIP network, the system proposed in this research is anomaly based IDS and uses online monitoring approach. They used support vector machine for classification. The system performs analysis on a set of 38 features extracted from VoIP network flow.

System starts the Intrusion detection process by capturing SIP packets from network. These messages are trapped in a buffer of predefined size. After the queue is full features are extracted. SVM classifier decides whether the vectors/features represent anomaly. Alarm is triggered in case of anomaly.

Designed system detects High intensity attacks with good detection accuracy of about 98.24% but low intensity (stealthy) attack are detected with 1.24 % detection accuracy.

2.3.11 Snort

Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire [27]. It performs real time intrusion detection by utilizing its rule set.

Snort makes use of benefits offered by both signature based intrusion detection method and anomaly based intrusion detection method.

It works in three different modes namely packet sniffer mode packet logger mode, network intrusion detection and prevention mode. In packet sniffer mode it reads packets from network and displays them, the packet logger mode is responsible for logging data packets captured from network on to the disk while the third modules provides real time intrusion detection and prevention.

Snort rules are not aware of Sessions. It means that snort don't offer any mechanism for grouping SIP packets belonging to one session. Malicious patterns which are spread across SIP packets may get escape form detection mechanism. SIP and RTP are handled packet by packet in snort

Snort detection mechanism is simple yet efficient. It begins with capturing packets from network, then after decoding sends them to rule detection engine. Where rule matching is performed and alerts are generated if some attack is detected. The detection infrastructure provided by snort id efficient for various network based intrusions however it is not very effective against VoIP networks.

Stateful analysis of network packets becomes a requirement for intrusion detection systems. Various preprocessors are designed for this purpose. Preprocessor are used for reassembly of network packets belonging to same session. Snort is using *Stream5 preprocessor* for maintaining session state. It reassembles multiple TCP and UDP packets belonging to the same session and subsequently applies detection rules. To the best of my knowledge this preprocessor is only effective for Transport layer and couldn't fulfill the requirements for session maintenance of Application layer protocol like SIP and RTP. These are being handled packet by packet manner in Snort. So the malicious patterns which are spread across packets may get escape form detection mechanism. The could affect detection efficiency and accuracy

2.4 Summary

In this chapter we have discussed in detail the concept of intrusion detection and various methodologies used in this fields. Intrusion detection is a broad field with more and more innovations incorporating into it with time. Here in this chapter we have some research work done in this field. Numerous systems have been and tested for various types of networks. Every system has its own advantages and limitations associated with it.

Chapter 3

3. Requirement Analysis

VoIP is emerging technology in the field of telecommunication. It has come as a benefit from network convergence. It has open new dimensions for telecom services and is gaining popularity day by day due to it benefits in terms of cost and efficiency. Due to the architectural difference between traditional circuit-switched networks and VoIP there exist various security issues. VoIP inherits these security issues from the Internet layer and also offers set of its own. Unlike traditional PSTN, VoIP has open architecture so it is more easily accessed by attackers.

Internet protocol was designed for openness and scalability. With the help of these features IP has gain success and popularity. Along with these benefits some security threats are also introduced due to openness in the designed architecture. VoIP uses SIP as a signaling protocol for establishing multimedia sessions. SIP is also based on open IP Stack, so it is vulnerable to various security risks.

In this chapter we are going to discuss various issues related to VoIP security. Different types of attacks will be discussed briefly. Among all, main focus will be on attacks related to SIP specifically Denial of Service and Social threats. The rest of chapter is organized as follows:

3.1 VoIP Security Threats

Though VoIP is offering lot of benefits to the users, some security risks are also increased. These security risks are mainly divided into three main categories

- Supporting services threats
- Media protocol threats
- Signaling protocol threats

3.1.1 Supporting services threats

Various protocols are involved in VoIP communication e.g. DHCP, ARP, DNS etc. security risks are also associated with these security protocols. Domain Name Service (DNS) transforms a host name into IP addresses. DNS Spoofing and DNS Cache Poisoning are two common security threat related with DNS. ARP is Address resolution protocol it is used for resolution of network layer into link layer addresses. This protocol is also vulnerable to poisoning and spoofing attack.

3.1.2 Media protocol threats

Media protocols are used for real time transfer of voice and multimedia transfer over IP. Real Time RTP is most commonly used protocol for this purpose. After session establishment with the help of signaling protocol RTP is used for end-to-end transmission of data. VoIP is real time protocol so latency, jitter, delay are important issues to be considered for QoS. If RTP packets are transmitted in clear (i-e without encryption) than packets can be easily sniffed. The sequence number can be judged and some fake packets can be injected into the legitimate media flow. As a result some unexpected data packets received at the receiving side.

3.1.3 Signaling Protocol threats

The signaling protocol is the pillar of VoIP communication network. SIP is chosen as default signaling protocol by IETF. It is the focus of a wide range of security risks. Following are some categories of the risks associated with SIP.

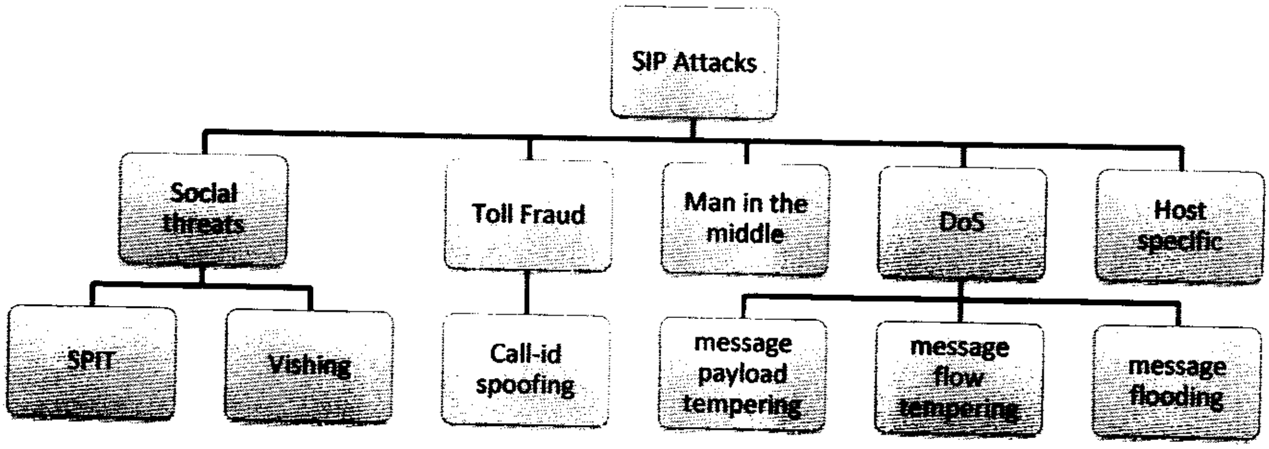


Figure 3- 1 Various types of attacks on SIP

Spam over Internet Telephony (SPIT)

In general, "spam" refer to some information, sent to numerous receivers without knowing their response. Spam is usually associated with some sort of marketing, fraud, or phishing messages. These types of messages are common in form of email, Short Text Messages, and phone calls over the traditional Public Switched Telephone Network (PSTN).

VoIP has gain popularity over traditional telephony, and can be considered as an alternative to PSTN in the near future. SIP has been established as a de-facto standard for VoIP. SIP services resemble much like traditional email. Hence the Spam attackers are likely to misuse services as they do with email systems. New threats are found which can target VoIP. One of them is SPIT which is quite similar to email spam. There are wide range of scenarios in which Spam attack can be launched on the internet telephony e.g. *Interactive marketing calls* in which caller (Spammer) tries to sell different things like insurance policies e.tc or it could be *Passive marketing* in which some prerecorded messages are used to sell products or services.

Although these types of attacks can also be launched over traditional PSTN but with help of VoIP it is more cheap, easy and efficient. These attacks can be launched with less cost in VoIP as compared to PSTN. As cost of making a call using VoIP is almost negligible, it just requires a high speed internet connection. A DSL line with 2 Mbits can make almost 30 calls simultaneously; whereas if PSTN is used for this case then this would be more costly. Botnets are specially designed with VoIP-directed software for launching these kinds of attacks.

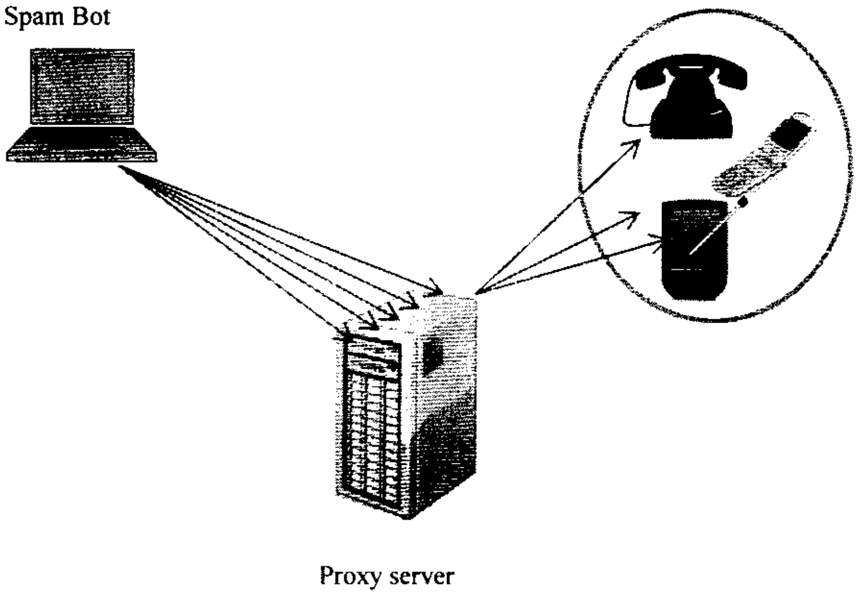


Figure 3- 2 Spam over internet telephony (SPIT)

Vishing

Another variant of Spam attack is VoIP Phishing or Vishing attack. Vishing in general is an attacker trying to acquire some confidential information from victim e.g. an attacker asking for entering bank account details in a fake web page. Similarly in VoIP spam an attacker can ask for dialing some expensive number in order to get some prize.

Toll Fraud

Attacker connected to the Internet tries to bypass the billing procedure. It is unauthorized use of paid long-distance communications services. It is a two-step procedure. In the first step the attacker perform scanning on the internet for finding suitable VoIP systems and then in the second step attacker connects to the selected system pretending as a remote extension and then tries to make calls through the victim system.

Call-id spoofing

Making fake caller-id is relatively easy in case of VoIP as compared to traditional PSTN e.g. *From* field in SIP header appears to be caller number in the recipient hand set, it can be set to anything as there is no check on its validity. Call-id spoofing can cause the system's reliability into question.

Man in the middle attack

VoIP is also vulnerable to man-in-the-middle-attack (MITM). To launch this type of attack attacker captures SIP traffic and masquerades as the calling party to the target. Once the attacker got access, he can then capture calls through a redirection server.

Denial of Service (DoS)

DoS is the most critical threat which affects the availability of resources held by a particular host on the network. The goal of DoS attack is to prevent legitimate user for accessing services offered by victim host.

The three main categories of SIP based DoS attacks are SIP message flow tampering SIP message payload tampering and SIP message flooding [28].

a) SIP Message Flow tampering

This type of flooding attack is used to disturb the ongoing transmission between entities of network. In VoIP communication between two entities happen in synchronous time model. A dedicated connection is established between the parties participating in the communication. Attacker targets this connection by sending bogus messages. Various types message flow tampering can be launched by using fake request messages e.g.

BYE Attack: attacker can send a fake BYE message with right credentials to terminate a existing session between two entities.

CANCEL Attack: CANCEL request can be used to cancel the call establishment request.

b) Message Payload tempering Attack

While launching this type of attack, attacker tries to mount harmful content with the message. Such type of attack may cause crash, buffer overflow, and remote code execution e.tc. Both user-agents and proxy server could be affected with such type of attacks.

c) SIP Message Flooding

This type of DoS attacks involves overwhelming the target with a number of valid and/or invalid requests [29]. Resources that are targeted in sip message flooding attack are [28]

Bandwidth: victim is flooded with more messages that it has ability to handle

CPU: victim is flooded with more messages than it can process

Memory: request create a state on the host, in the case of flooding several requests are directed towards victim that it will run out of memory

Flooding attack can be originated from single source or can be launched using multiple sources (also known as DDoS attack). Following are some categories of flooding attacks on SIP server

Register request Flooding

Register server is one of the critical elements in VoIP network. It is responsible for handling *register* request. It accepts these requests and places the information related with these request into location service of the domain which it handles. While launching flooding attack on register server several register requests are sent to the register server.

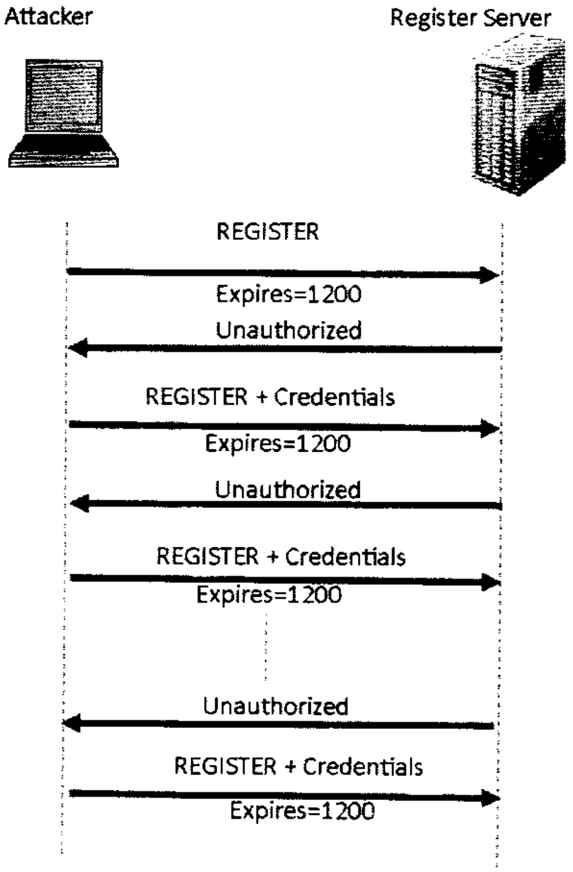


Figure 3- 3 Register Server flooding

This cause's victim register server to become paralyzed. The aim of Register server flooding attack could be a) guess legitimate user password, b) to cause a DoS at Register server [30].

Invite request flooding

An attacker can also launch invite flooding attack not only on the proxy server but also on the user-agents. User agents have a limited ability to handle invite request. Attacker exploits this ability by sending large number of INVITE requests without acknowledging the response of user-agent. Another scenario of launching this type of attack is INVITE flood with false IP domain address or INVITE flooding with false SIP URI in some another domain [37].

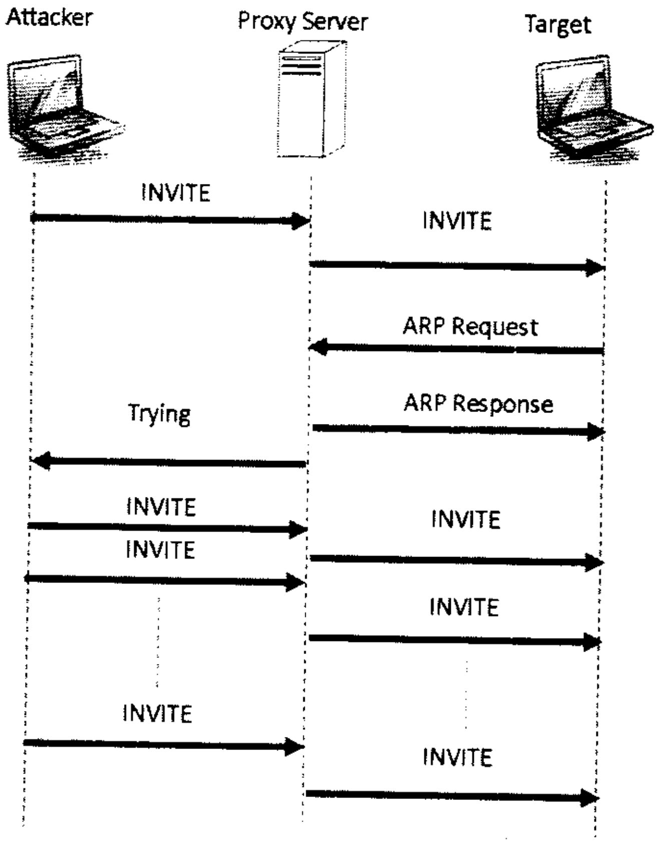


Figure 3- 4 Invite message flooding

3.2 Problem Definition

Voice over IP is emerging as a standard and attempts to replace old PSTN systems. As the use of VoIP in communication is increasing day by day the security threats associated with this protocol are diversifying. Due to distributed nature of VoIP network and real time characteristics it suffers from various security flaws. VoIP utilizes separate channels for signaling and media transmission. These channels run over IP and separate protocols are employed for each. Security risks are associated with each protocol involved in the communication e.g. Denial of service, spoofing, masquerading, eavesdropping, SPIT etc. Various security mechanisms have been proposed for intrusion detection in VoIP. But these techniques are not able to fulfill the requirement of intrusion detection in the distributed architecture of VoIP.

3.3 Research Objective

The key protocol for VoIP is SIP. SIP deployment is likely to increase in future; protecting SIP against various security threats is becoming essential. In this research our major focus will be:

1. To secure a SIP-based network against various Denial of service attacks and social threats
2. Improve the detection rate
3. To reduce false alarms generated by the intrusion detection system
4. To find the intensity of attacks detected by the system

3.4 Summary

VoIP is exposed to many security threats. Different protocols along with the security threats are discussed in this chapter. Focus of our research is intrusion detection for SIP protocol. In this chapter we have discussed SIP-VoIP security breaches. Later in this chapter we have formulated our problem definition and discussed research objective.

Chapter 4

4. Proposed Solution

In this chapter we shall describe our proposed architecture to counter threats like denial of service and social threats in SIP based VoIP network.

We have already discussed various intrusion detection systems in previous chapters. We shall discuss a method of intrusion detection implementation keeping in view the effectiveness and advantages of classic Signature based intrusion method along with the benefits of fuzzy logic based intrusion detection technique. We shall discuss how detection accuracy can be improved through the use of hybrid intrusion detection system. Our proposed system consists of two modules, in the first module network packets are analyzed for any suspicious events with the signature based IDS module. Alarm is triggered if some attack is detected otherwise the non-intrusive patterns are then further analysis with the second module. Second module makes use of fuzzy logic to detect intrusive patterns.

Rest of this chapter is arranged as follows in section 4.1 we are going to discuss fuzzy logic and how intrusion detection is done by using fuzzy logic. In Section 4.2 we will demonstrate the design features for our proposed system. Architecture of proposed system will be discussed in detail in Section 4.3. In Section 4.4 we will discuss how different attacks can be detected through our proposed system, In Section 4.5 general flow of the system will be discussed.

4.1 Fuzzy logic

Fuzzy logic was introduced by Dr. Lotfi Zadeh in the 1960's as a means to model the uncertainty of natural language [31]. It mimics human decision making capability because it has ability to work with imprecise data. Fuzzy logic system uses fuzzy membership functions and set of rules to reason about data. Membership functions are curves that map every input to a membership value in the range of 0.0 to 1.0. It is graphical representation of a given input and it associates weight with each input. This weighting factor determines the degree of membership (DOM) of each rule. There are various shapes of membership functions e.g. Gaussian, triangular, trapezoidal, bell etc. Fuzzy rules are defined by domain expert. Following is an example of fuzzy rule.

If *funding* is **sufficient** or *staff* is **small** then risk is **low**.

In this example sufficient, small and low are membership functions defined for input variable funding, staff and output variable risk.

4.1.1 Fuzzy Inference system (FIS)

Fuzzy inferencing is a process of transforming given input to an output with the help of fuzzy logic. In literature mainly two types of inference systems are discussed, these are Mamdani fuzzy inference system and takagi-sugeno-kang inferencing system. Among them Mamdani model is most commonly used. This model was developed by Mamdani and Assilian in 1975 for controlling steam machine by set of linguistic rules obtained by domain expert.

To compute the output of FIS given the inputs, it has five steps 1) Determining fuzzy rules 2) Fuzzification of input data 3) Application of fuzzy operators on Antecedents 4) Implication from antecedent to consequent part of rule 5) Aggregation of consequent across the rule 6) Defuzzification [32].

Determining fuzzy rules

Fuzzy rules are a collection of linguistic statements. These rules are used to define how the FIS should make a decision for classifying an input or controlling an output.

Fuzzification

This is the first step of fuzzy inferencing mechanism. It determines the degree to which the given input belongs to the fuzzy set via fuzzy Membership function. Membership functions are used to map given input to a value between 0 and 1. Where 1 represents absolute truth and 0 represents absolute falseness. The output of fuzzification is a degree of membership in the qualifying linguistic set.

Application of fuzzy operators on Antecedents

After fuzzification of inputs, degree of membership of all antecedents is found. If there is more than one antecedent in a given rule then fuzzy operators (*and, or*) are applied to obtain a single value which represents the result of rule's antecedents.

Implication from antecedent to consequent

Every rule has a weight i-e a number between 0 and 1. Before applying implication method rule weight is checked. Consequent is also a fuzzy set with corresponding membership function. Consequent is reshaped according to the single outcome of antecedent part of the rule. Implication is applied on each rule. Input to the implication process is single value from antecedent and out of implication is a fuzzy set.

Aggregation of consequent across the rule

Final decision depends on testing of all rules in Fuzzy inferencing system. In this step output from all rules is combined to get a single fuzzy set.

Defuzzification

The output of each rule is fuzzy it must be converted into some scalar output; the process of converting fuzzy input to scalar output is called Defuzzification. The aggregate output of fuzzy sets is given as input to Defuzzification module which gives a single output. There are various types of Defuzzification methods including centroid, middle of maximum etc.

4.1.2 Intrusion Detection using Fuzzy logic

Presently, security risks are increasing due to increasingly getting connected with public accessible networks e.g. internet. To counter these security risks various intrusion detection schemes are applied specifically data mining techniques, Artificial intelligence techniques, soft computing etc. data mining techniques like clustering, association rule mining and various others are used for detecting intrusive activities in the network. In the similar way many Artificial intelligence techniques including fuzzy logic, neural networks, decision trees etc. are also applied for this purpose. Among them Fuzzy logic techniques offer many advantages over other AI techniques.

Fuzzy logic has been extensively deployed now days in the field of intrusion detection. There are several reasons for using fuzzy logic in the field of intrusion detection. One reason is that alarm generation against attacks is often fuzzy, at what degree of attack alarm should be raised is also fuzzy because in some situations there is a very little difference between normality and anomaly.

4.2 Design Requirements

Various systems have been designed so far for detecting intrusion in VoIP networks which shows better results for various types of attacks but still there are security holes left behind. In this section we are going to discuss design requirements of Intrusion detection system for VoIP signaling protocol SIP. SIP is vulnerable to many security threats as mentioned in previous chapter. In order to get better detection accuracy intrusion detection system should have following features.

4.2.1 Stateful detection

Though Stateless analysis is useful and worked efficiently under heavy network traffic but Stateful analysis is required for networks like VoIP. Stateful detection involves performing analysis for an entire connection or session, capturing and storing certain pieces of relevant data seen in the session, and using these data to identify attacks that involve multiple requests and responses [33]. States presents system snapshot at a particular time interval. Stateful detection describes system penetration as sequence of actions that intruder tries to perform. In Stateful analysis, states from multiple packets are accumulated to get an aggregate state which is further used for intrusion detection. In our system we are going to use Stateful analysis for intrusion detection of SIP. It is very important to maintain SIP state while doing intrusion detection in VoIP as SIP is call management protocol and it is involved from call establishment till termination.

4.2.2 Hybrid intrusion detection

Signature based intrusion detection is most commonly used intrusion detection methodology. It looks for specific patterns which are defined as intrusive. This method shows good performance for detecting previously known attacks. Detection accuracy of the signature based IDS strongly depends on correct setting of threshold values. Any intrusion attempt which fell outside the range of threshold is not detected by signature based IDS regardless of its distance from intrusion threshold. In other words we can say that there exist an abrupt separation between anomaly and normality. In order to smooth down this abrupt separation we have integrated fuzzy IDS with the signature based IDS. Fuzzy IDS defines a range of values as intrusions and shows better detection accuracy as compared with signature based IDS.

4.3 Proposed Architecture

VoIP networks are distributed in nature. Various protocols are involved in VoIP communication. SIP which is call management is most vulnerable to security threats. Our designed system works at application layer and provides Stateful intrusion detection at application layer. The proposed system is a Network based intrusion detection system.

Packet Capture

Incoming VoIP network traffic is captured by this module. It reads network packets and stores them on the disk for further analysis.

Filter

Network packets captured previously are filtered by this module. Various protocols are involved in VoIP communication. Our system is designed for intrusion detection of signaling protocol. So SIP packets are separated from others in order to save the processing power of IDS modules.

Signature based IDS

Stateful intrusion detection is performed on the packets captured by the previous module. The input to this module is looked-up in Call record tables. In this module intrusion is detected if the incoming pattern matches with the signature present in the rule base otherwise it will be declared as non-intrusive by the signature based module. Fuzzy IDS module will help to detect these types of intrusions.

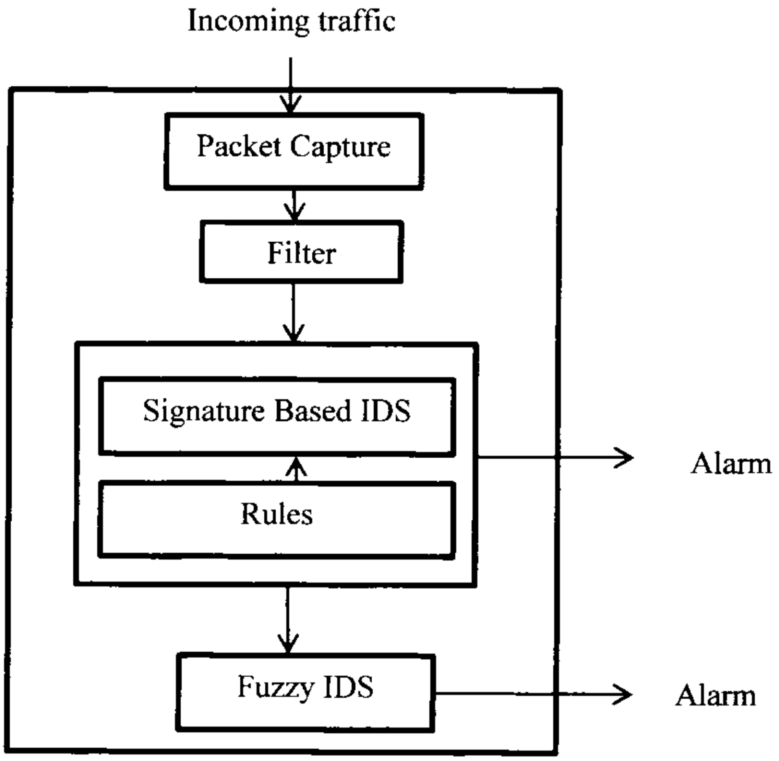


Figure 4- 1 Proposed system architecture

Fuzzy IDS

Non- intrusive patterns are given as input to this module. It performs further analysis to detect intrusions which are not detected by signature IDS module. Figure 4-2 shows basic flow of this module

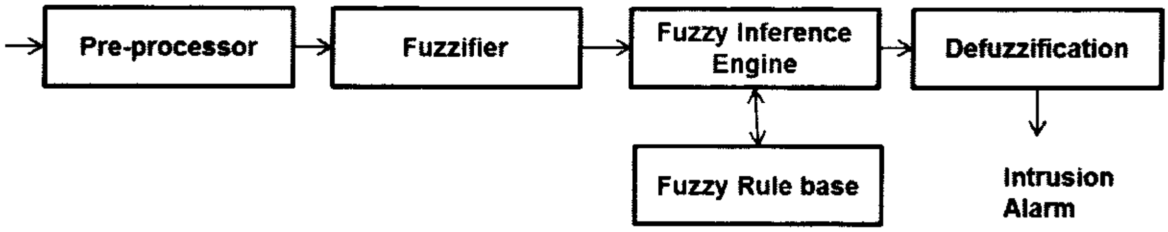


Figure 4- 2 Fuzzy IDS architecture

Preprocessor

Preprocessor is used to extract useful features from SIP packets buffer. Features are extracted from the network data captured using any one of two analysis methods; the memory-window or memory less window. In memory window analysis a time window a size n is moved over raw packets in Overlapping order and then features are extracted from the set of raw packets [34]. Some of these features memorize information from previous windows. While on the other hand in memory less window analysis method no information is memorized from previous windows. It shows information contained in the current window. This stage passes the extracted features to fuzzification module

Fuzzification

As in fuzzy logic manipulation is on linguistic values, the crisp data is normalized in the range of 0.0 to 1.0 and the converted into linguistic values of fuzzy sets. Fuzzy rules are constructed based on a map of multiple inputs to a single output.

Fuzzy inference engine

Fuzzy inference engine applies some reasoning to compute fuzzy outputs. Fuzzy inference engine make use of fuzzy rules built from expert knowledge to generate final response. In our system we are going to use Mamdani's inferencing model to generate final response. In Mamdani-type inference mechanism expects output membership functions in the form of fuzzy sets. After aggregation these output membership function are defuzzyfied to get crisp output value.

Defuzzyfication

Input to this module is fuzzy set and resulting output is single value. In our system we are going to use centroid method for defuzzyfication.

4.4 Attacks

We have implemented two types of attacks to demonstrate the functionality of our proposed IDS at application layer. These attacks are launched by exploiting various vulnerabilities of SIP. The implemented attacks are message flooding attack and Spam attack on internet telephony. The rest of this section discusses attacks and the method which we are going to use for detection.

4.4.1 INVITE message flooding

Flooding attacks falls in important categories of attacks in network security. Flooding attacks can target the signaling plane elements like proxy servers and gateway with the objective to take them down and produce havoc in the VoIP network [37]. These attacks can be launched in various ways like flooding the signaling plane with large number of request messages, by exploiting vulnerabilities of end device, sending malformed request messages etc.

4.4.1.1 Signature based IDS

In our prototype implementation we have taken INVITE message flooding to demonstrate the validity of our IDS. In this type of attack, attacker sends large number of INVITE request to the target host. As soon as the server receives INVIITE message it allocates some memory for the transaction. Normally few seconds are required for call setup, this makes proxy server vulnerable to flooding attack. Attacker flood the proxy server with large number of INVITE message request in short period of time without acknowledging any response from server. Following table maintains record for all user-agents sending INVITE requests.

Table 4- 1 User agent record table

Field	Description
SIP URI	URI of the user agent sending INVITE request
Invite Count	Number of INVITE messages send by a particular SIP URI
Start Time	Time when first INVITE request is received
Current Time	Time of current INVITE request

The pseudo-code for detecting INVITE message flood attack is as follows

```
If (current time-start time < Tsec)
Invite count > threshold
raise Alarm
else normal
```

This code generates alarm when number of invites messages send by a particular SIP URI exceeds certain threshold value in specific time period.

4.1.1.2 Fuzzy IDS

INVITE message flood attack aim to overload target proxy server with large number of (INVITE) Call request. As a result proxy server become unable to process other legitimate call request. To detect this type of attack, system maintains a call record table which provides information about every call request to the proxy server. It consist of following fields

Table 4- 2 Call-Record Table

Field	**Description**
Call-Id	Uniquely identifies a call
Call Start time	Start time of the call
Completion time	Ending time of the call
Call Duration	Duration of call
Inter Call arrival time	Time duration between call requests
Rejection time	Call rejection time

Call-id is the unique identifier which uniquely identifies the call. Whenever a new call id is received, system creates new record for the caller; otherwise if received request is from existing call-id, system updates that call record table entry. System maintains this table for certain time interval then it extracts useful call related parameters for detection purpose.

Under INVITE message flooding attack ***number of completed calls*** decreases and ***call rejection rate*** increases. Figure 4-3 shows the call rejection ratio and call completion ratio of normal traffic when there is no attack and when the network is under flood attack. Attacks are launched with different intensities (flood with 1, 10,100 and 1000 invite request per second).

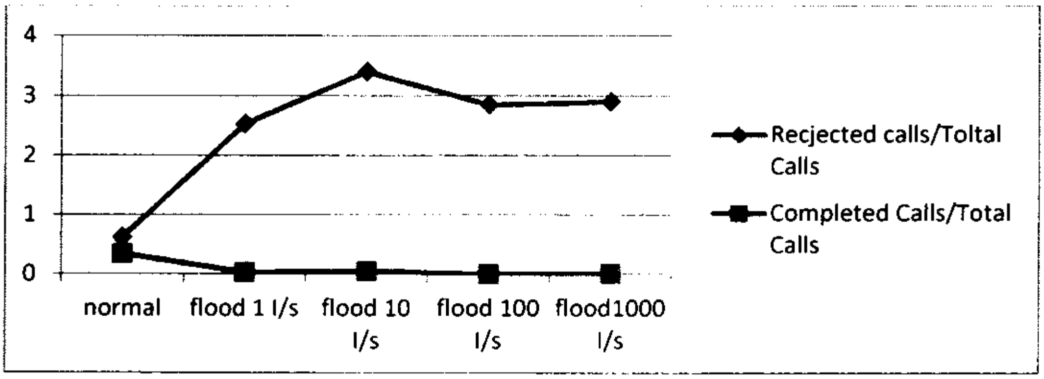


Figure 4- 3 Rejected call ratio and completed call ratio under normal and attack network traffic

As the target is flooded with large ***number of INVITE*** requests so, ***Inter Invite Arrival Time*** is also low as compared with normal network traffic. These four parameters are used by fuzzy IDS module to find out the intensity of INVITE message flooding attack.

Table 4- 3 Parameters for fuzzy logic IDS

Parameter	**Value**
Number of INVITES	High
Average Inter INVITE arrival time	Low
Call Rejection ratio (Rejected calls/total number of calls)	High
Call Completion ratio (Completed calls/total number of calls)	Low

Fuzzy rules for finding attack intensity depend on four parameters as discussed in table 4-3. Fuzzy inference engine is composed of membership functions for all these four parameter and set of rules.

The following section describes the steps involved in fuzzy logic intrusion detection.

a) Configuration Parameters

The attributes input to the system are mentioned in the table above. For each parameter three triangular membership functions are used: low, high and very high.

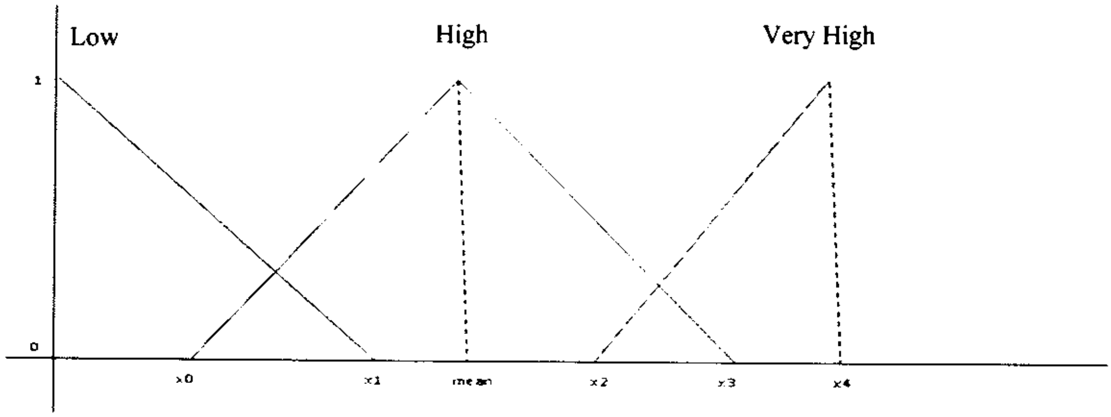


Figure 4- 4 Fuzzy sets

In order to obtain rules consistent with data, value of any parameter x is configured using following table.

Table 4- 4 Fuzzy set boundaries

X	Description
Mean	Average attribute value
x_0	90% of x_{min} (minimum value of x)
x_1	Average minus standard deviation
x_2	Average plus standard deviation
x_3	110% of x_{max} (maximum value of x)
x_4	x_3 plus Average

Figure 4-5 shows the membership functions for *Call Rejection Ratio* parameter. The out parameter also has three triangular membership functions distributed in the range [0.0, 1.0]

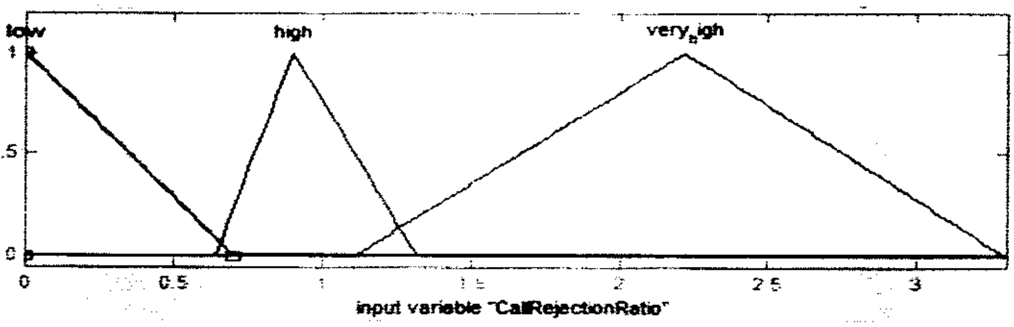


Figure 4- 5 CallRejectionRatio membership function

b) Rules

After defining fuzzy sets fuzzy rules are designed. These rules were formed depending on the knowledge of flooding attack and the relationship between theses parameters. We have developed twenty rules to find flooding attack intensity.

Here we are going to explain one rule out of them

If (CallRejectionRatio is high) and (CallCompletionRatio is low) and (NumberOfInvites is high) and (InterInviteArrivalTime is high) then (flood is high)

This rule shows that flood attack is high when Call Rejection ratio is high and Call completion ratio is low and at the same time number of invites received in the given time window is high and inter arrival of invite request is also high.

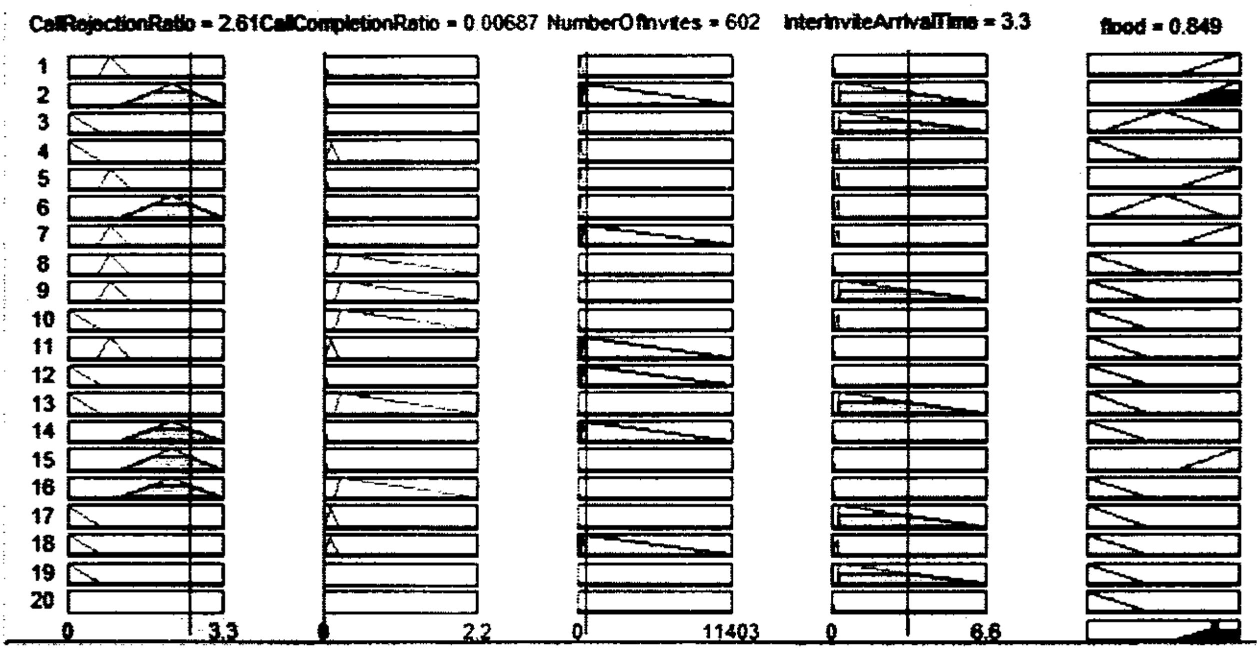


Figure 4- 6 fuzzy logic rules for detecting Invite message flooding attack

4.4.2 Spam over Internet Telephony (SPIT)

The second attack which we have implemented is a social threat. We have discussed this attack with much detail in previous chapters. VoIP Spam in not a serious problem yet but it is expected that it become a dilemma in near future as the use of VoIP is increasing day by day. Session Initiation Protocol (SIP) is the underlying technology behind this social threat. Similar to email Spam, VoIP Spammer sends bulk of unsolicited calls to target network. These calls are mostly pre-recorded and automatically dialed so, they follow some common pattern and have fixed duration of about 15 to 20 sec. in most cases specially programmed Spam bots are used to launch attack on the target network.

4.4.2.1 Signature based IDS

The signature based detection depends on following three parameters.

Call Rate: SPAM caller tries to put huge number of calls in small time duration. So the call rate is usually greater than normal call traffic

Inter Call Arrival time: As SPAM caller is making huge number of calls in small duration so time between the call requests is usually very low.

Call duration: Call duration of SPIT caller is usually very small as compared with normal call. Most of the time call is rejected by the recipient, once he found that call is spam. Sometimes SPAM caller plays some pre-recorded message like telemarketing calls, so in this case most the calls will have same duration.

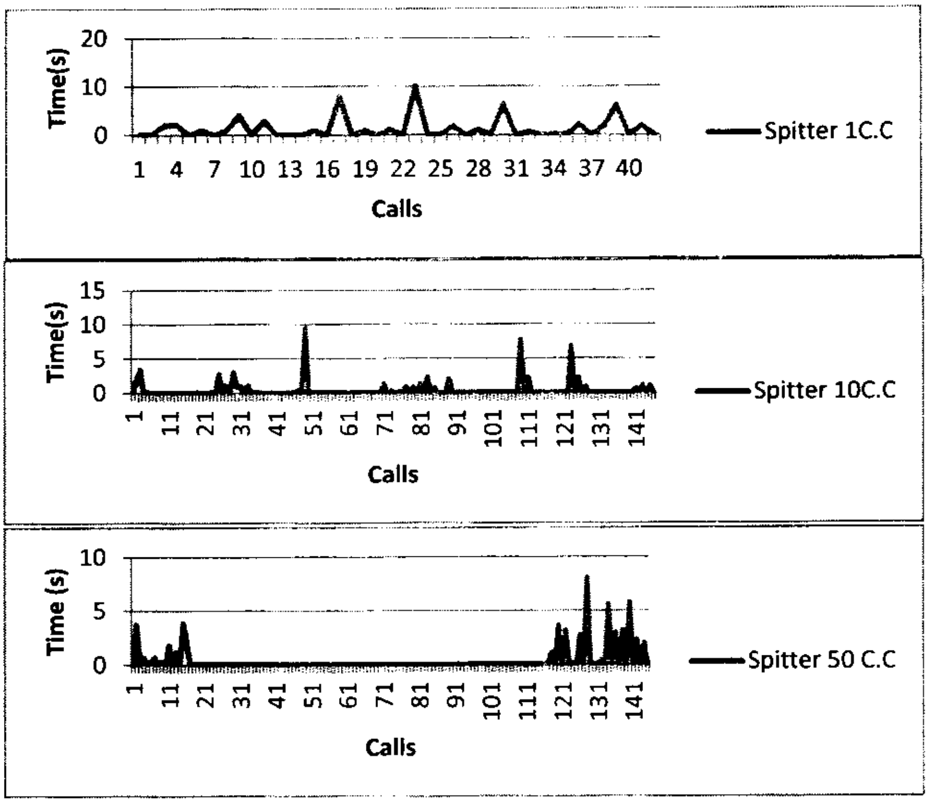


Figure 4- 7 Inter Call arrival time at various attack intensities

Graphs in figure 4-7 shows attack data of one min duration collected in three different attack rates (1 C.C, 10 C.C and 50 C.C). It can be noticed that as the attack intensity is increasing (from 1 to 50 concurrent calls) number of calls are increasing and at the same time inter call arrival time is decreasing.

With the help of Call-record table System calculates ***Avg inter Call Arrival Time*** (Average time between call requests), ***Avg Call duration*** (Average duration of calls) and total no of ***Calls*** in particular time duration for SPIT detection and matches them against rule present in the signature database, if the rule matches System will generate intrusion Alarm.

Pseudo-code for SPIT attack is mentioned below

```
If (time < t sec) && (Avg inter call arrival time<th1 && Avg Call duration < th2 &&
 Calls > th3)
Trigger Alarm
Else Normal
```

4.4.2.2 Fuzzy IDS

In order to improve detection accuracy network packets are analyzed through Fuzzy IDS module. This module again uses parameters mentioned in section 4.2.2.1 and one additional feature of call rejection ratio. During a SPIT attack call rejection rate increases due to unsolicited and unwanted communication. All these parameter are configured according to the method discussed previously. After defining membership functions fuzzy rules are designed. We have developed five rules for SPIT attack detection.

Here we are going to explain one rule out of them.

If (Calls is high) and (CallDuration is low) and (InterCallArivalTime is high) then (SpitAttack is veryHigh)

This rule shows SPIT attack intensity is very high when there high number of calls with low call duration and inter arrival time of call request is also very high.

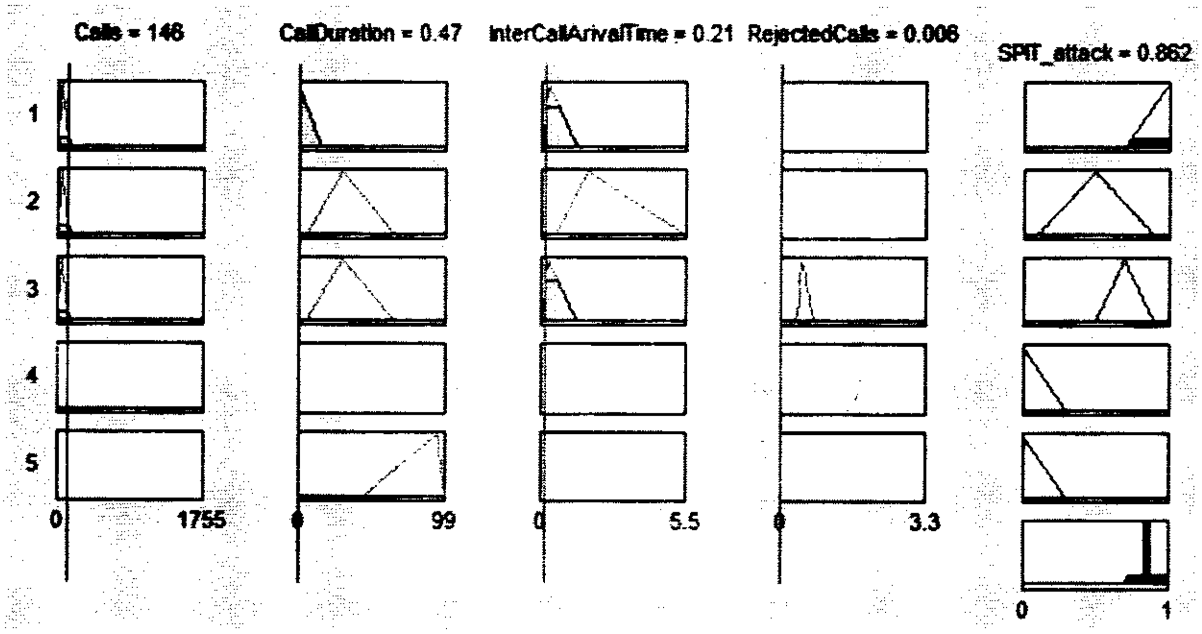


Figure 4- 8 the fuzzy logic rule to detect SPIT attacks

4.5 Flow chart

Figure 4-9 completely explains overall flow of the proposed system. System filters SIP packets from incoming VoIP traffic. After receiving SIP packets system updates its Call-Record table and User agent record table. These tables are then further used by Signature IDS module and Fuzzy IDS module to extract useful parameters about User agents involved in communication and Calls during a particular time interval.

First Signature based IDS module checks if an incoming traffic pattern matches some rule present in the rule base, if some match occurs it will generate intrusion alarm. Otherwise this traffic is declared normal. This normal or non-intrusive traffic is further analyzed with Fuzzy IDS module. If some traffic pattern matches rule present in fuzzy rule base alarm is triggered otherwise incoming traffic is declared normal.

With the help of hybrid intrusion detection architecture intrusion went undetected by Signature based IDS module are further detected by Fuzzy IDS module and as a result better detection accuracy can be achieved.

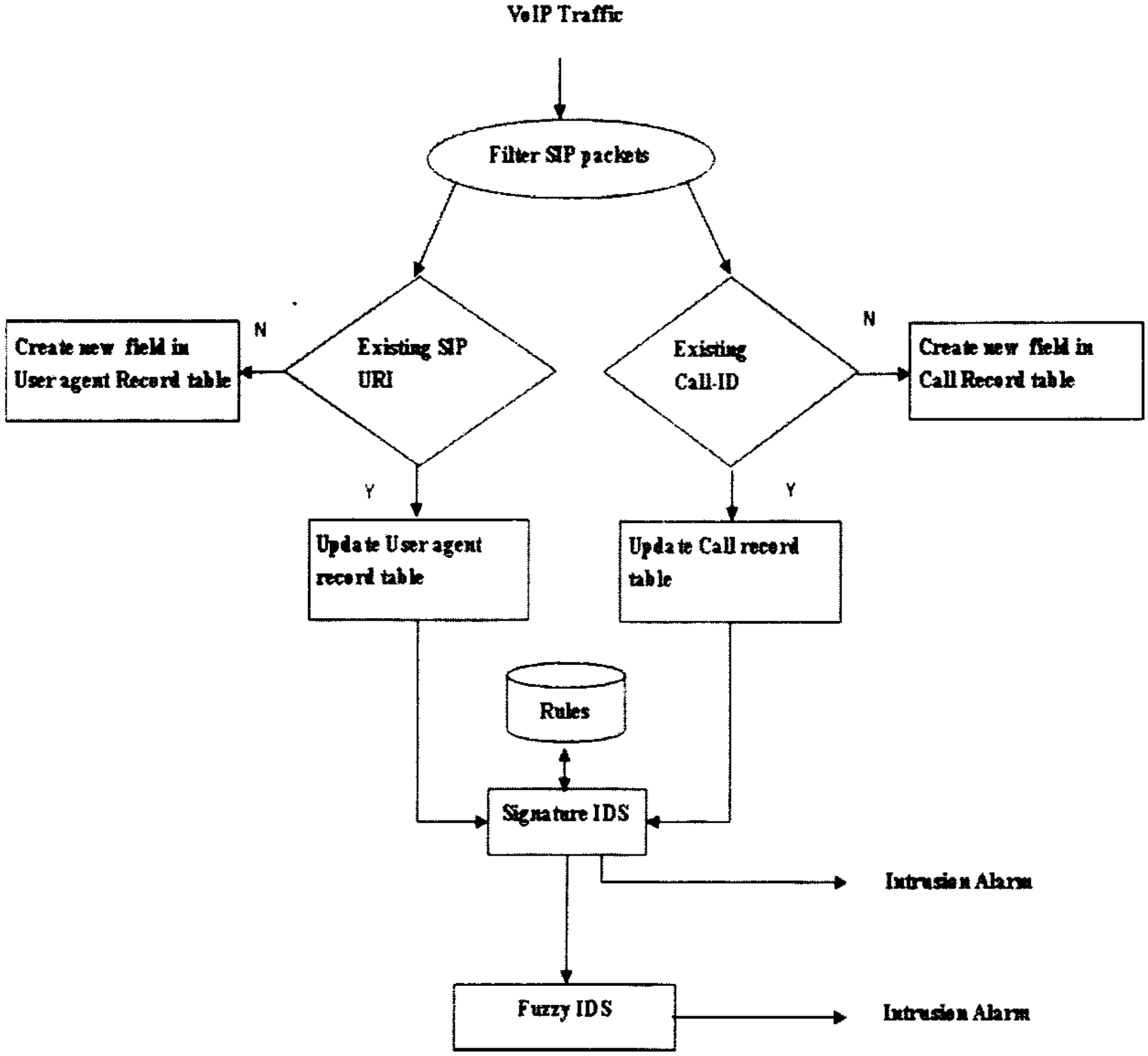


Figure 4- 9 Flow chart

4.6 Summary

In this chapter we have discussed intrusion detection using fuzzy logic in detail. Then we analyzed some important design requirements of our proposed system including hybrid intrusion detection method and Stateful detection method. The role and limitation of signature based IDS and fuzzy IDS are discussed and how they can be integrated to get better accuracy is also discussed in this chapter.

Chapter 5

5. Experiments and Results

In this chapter we will analyze result achieved by our system. Our discussion on result analysis focuses on two basic parameters namely, detection accuracy and False alarm rate. In this chapter we will show how are IDS detects both types of attacks and false alarm rate produced by the system. As we have designed a Hybrid IDS, we will also discuss performance achieved by modules if deployed separately and increase in performance when working together in hybrid fashion.

Intrusion detection algorithm is used to map incoming network traffic into attack and normal category. Effectiveness of intrusion detection system can be measured in terms of its ability to minimize false alarm rate. Detection accuracy of IDS depends mainly on hit rate and False alarm rate. We will discuss detection accuracy of our IDS w.r.t these parameters.

5.1 Data Set

We are going to use a common labeled data set available for intrusion detection evaluation. This data set is developed at INRIA research center, Nancy, France to perform quantitative evaluation of intrusion detection on SIP/VoIP networks. Nassar et al. [36] has mentioned completely test-bed for generating and customizing these VoIP traces. This labeled data-set is composed of normal, different kind of attacks and mixed normal/attack traces. Three different types of data sources are provided for Intrusion detection: *network traffic, Call Detail Record (CDR) and Server logs.*

5.2 SPIT attack

In our system Spit attack detection is based on four parameters namely, numbers of calls, average call duration, inter call arrival time and number of rejected calls.

5.2.1 Detection Accuracy

We have tested our proposed solution for SPIT attack detection on three different attack intensities. SPIT attack was launched using Spitter/Asterisk tool. Intensity of attack is determined by number of concurrent calls. Following table shows the results of individual modules of the system to detect attack rate at 1,10 and 50 Concurrent Calls. Detection accuracy can be found with the help of following equation.

$$DetectionAccuracy = \frac{Attack\ period\ classified\ as\ attack}{Overall\ attack\ period} * 100 \ldots\ldots\ldots (5.1)$$

Table 5- 1 Detection accuracy for SPIT attack

Attack rate (number of concurrent calls)	Detection Accuracy		
	Signature based IDS	Fuzzy IDS	Hybrid IDS
1	19.08%	85%	95.3%
10	100%	100%	100%
50	100%	100%	100%

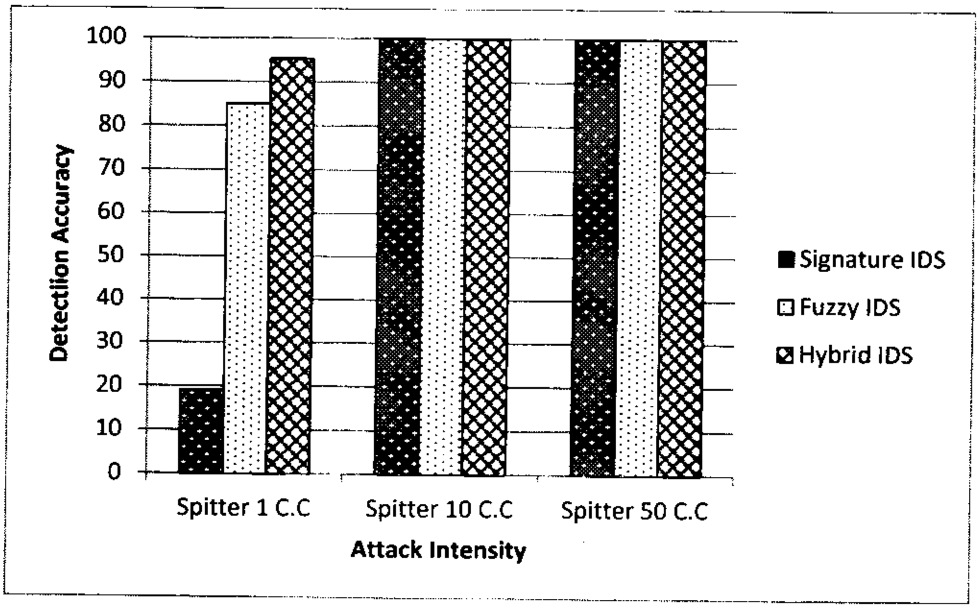


Figure 5- 1 Detection accuracy at various attack rates

It can be seen from the above graph that detection accuracy is improved with the use of Hybrid IDS. In case of Spitter 1C.C signature IDS provides just 19.08% accuracy while fuzzy IDS provides 85%. By combining both techniques we have achieved 95.3% accuracy.

Fuzzy attack detection example

Signature based IDS approach relies on static threshold values. Detection accuracy of signature based IDS depends on correct setting of threshold values. Any intrusion attempt which falls outside the range of threshold values is considered normal regardless of its distance from intrusion threshold. Fuzzy logic helps to smooth this abrupt separation between normality and anomaly. E.g. threshold value for Average call duration is set to 20, Spam attack can happen with little change in duration. Signature based IDS will not be able to detect this little change and generate false alarm. Fuzzy logic system works on range of values, thus provide flexibility for detection.

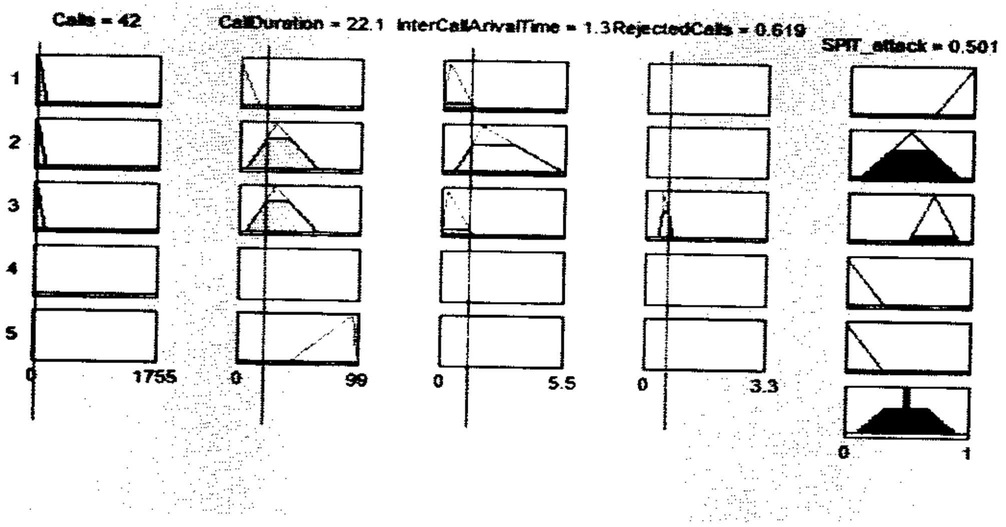


Figure 5- 2 Fuzzy logic attack detection example

Here in this example call duration is 22.1(s) Signature based IDS will declare this traffic pattern as normal but fuzzy logic has detected this with the intensity of 0.501.

5.2.2 Attack Intensity

Our designed IDS have the ability to detect these attacks. Beside this Fuzzy IDS also gave the idea about the severity of attack. In the first experiment when attack rate was 1C.C, the system detects the attack with intensity range 0.56 to 0.7, in the second experiment attack rate was 10C.C, and System detects these attacks with intensity range of 0.75 to 0.86. Again in the third experiment when attack rate was 50C.C, system detects this attack with intensity of 0.86. Greater the number of intensity, more severe the attack is.

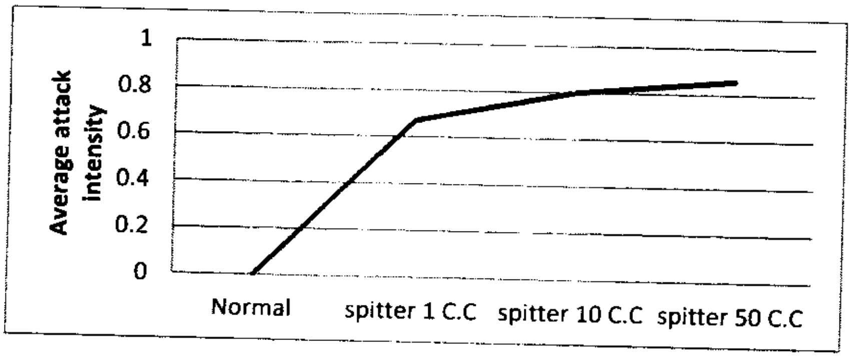


Figure 5- 3 SPIT attack intensity

5.2.3 False Alarms

Efficient IDS reports an intrusive activity as it happens and don't trigger any alarm when no intrusive activity found. The important measure of IDS is not how often it finds signs of intrusions, but how rarely it generates false alarms. There are basically two types of false alarms namely False positive and False negative. A False positive alarm is triggered when intrusion detection system identify normal data as attack whereas in case of False negative IDS fails to identify the attack. False Negative Alarms can be calculated with the help of following equations

$$False\ Negative\ accuracy = \frac{Number\ of\ instances\ classified\ as\ normal}{Total\ number\ of\ attack\ instances} * 100 \ldots\ldots (5.2)$$

No False positive alarm is produced by Signature and fuzzy IDS module. False negative alarms are produced by Signature based IDS module while detecting low intensity (stealthy) attacks. Fuzzy module also produced false negative alarm in detecting Spitter attack at the rate of 1 C.C. but these False alarms are reduced when we have used both techniques in Hybrid fashion.

Table 5- 2 False alarm generated by Signature based approach, Fuzzy IDS and Hybrid IDS

Attack rate	False Negative		
	Signature IDS	Fuzzy IDS	Hybrid IDS
1 C.C	81%	27.1%	9%
10 C.C	0%	0%	0%
50 C.C	0%	0%	0%

5.3 INVITE message Flooding attack

In invite message flooding attack target is flooded with large number of INVITE request so that it becomes unable to serve legitimate requests. Our signature based module not only detects this event but is also capable of locating Attacker. This module maintains a log file in which user agent profile is maintained, when some user tries to launch attack it generates alarm.

Similarly Fuzzy IDS make use of four parameters *call rejection rate, call completion rate, average inter invite arrival time* and last but not least *number of INVITE requests*

5.3.1Detection Accuracy

We have tested our proposed system against flooding attack at four different rates; flood 1 invites/sec, flood 10 invites/sec, flood 100 invites/sec, and flood 1000 invites/sec Detection accuracy is found using Equation 5.1

Table 5- 3 Detection accuracy for INVITE message flooding at four different Attack rates

Attack rate (Invites/sec)	Detection Accuracy		
	Signature based IDS	Fuzzy IDS	Hybrid IDS
1	49.3%	98.7%	98.7%
10	100%	85%	100%
100	58.9%	100%	100%
1000	100%	100%	100%

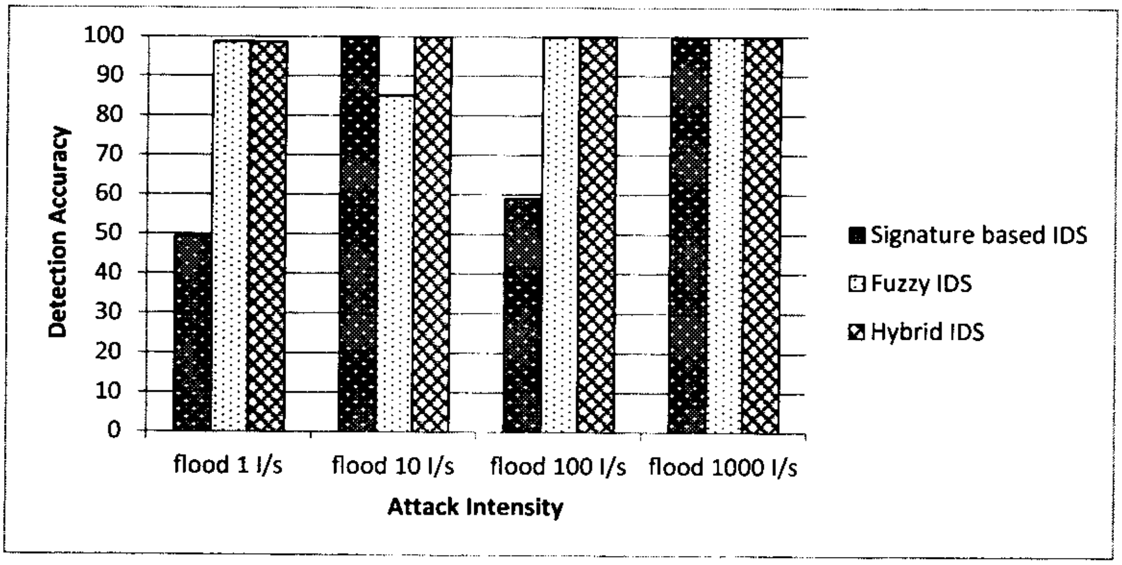


Figure 5- 4 Detection accuracy for flood attack detection

The signature based module show less detection accuracy for low intensity attack like flood at 1 invite/sec. this attack can be detected through fuzzy module. So, the detection accuracy has improved to 98.7% with the use of hybrid IDS.

5.3.2 Attack intensity

Fuzzy IDS module also provides information about attack intensity. In the first test case in which attack rate is 1 invite/sec, fuzzy module detect it with intensity of 0.55 to 0.81, in the second case attack rate of 10 invites/sec is detected with attack intensity of 0.82, similarly in flood attack of 100 and 1000 invites/sec , attack intensities are 0.84 and 0.83 respectively.

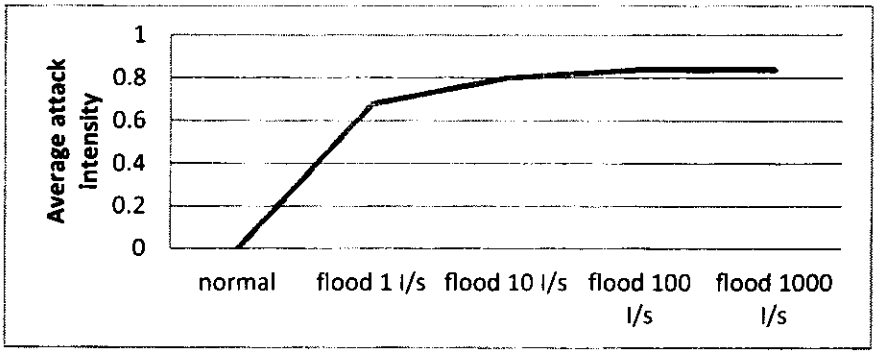


Figure 5- 5 INVITE message flood attack intensity

5.3.3 False Alarms

Again in the case of invite message flooding attack false alarm rate is very low. False negative alarm are produced by signature based module in case of flood attack of 1 invite/sec. but this attack is detected as our designed system is hybrid so, attack went undetected by signature module is further detected by fuzzy module therefore False alarm rate has been reduced considerably.

Table 5- 4 False alarm generated by Signature based approach, Fuzzy IDS and Hybrid IDS

Attack rate	False Negative		
	Signature IDS	Fuzzy IDS	Hybrid IDS
1 invites/sec	66%	33%	33%
10 invites/sec	50%	50%	50%
100 invites/sec	0	0	0
1000 invites/sec	0	0	0

5.4 Comparison

We have compared our results with the intrusion detection system for VoIP proposed in [37]. In their work they have used Support vector Machine for classification. They have also tested there system for Labeled VoIP dataset developed at INRIA research lab. It can be seen from table 5-5 our proposed Hybrid IDS shows better accuracy for detecting Stealthy attack (flood 1 invite/s, flood 10 invites/s) as compared with SVM.

Table 5- 5 Detection accuracy comparison

Attack Rate	SVM	Signature IDS	Fuzzy IDS	Hybrid IDS
1 Invite/s	1.48%	49.3%	98.7%	98.7%
10 Invite/s	60.13%	100%	85%	100%
100 Invite/s	80.82%	58.9%	100%	100%
1000 Invite/s	98.24%	100%	100%	100%

5.5 Summary

In this chapter we have seen that that our proposed technique constitutes hybrid methodologies. We have discussed detection accuracy of individual modules and also mentioned that detection accuracy can be significantly improved when modules are combined. Also false Alarm rate is reduced noticeably.

Chapter 6

6. Conclusion and Future work

VoIP is shaping the future of telephony. Due to its popularity VoIP security issues are also increasing day by day. In this thesis we studied VoIP in details and security risks associated with this protocol. We have proposed Hybrid intrusion detection system for SIP-VoIP. The hybridism of our proposed IDS is the result of combining Signature based IDS with Fuzzy IDS. These two detection methodologies worked together to detect attacks at application layer.

6.1 Conclusions

In the first chapter we have explained role and importance of intrusion detection system. Later in this chapter we have discussed VoIP technology and SIP which is the de-facto signaling protocol for VoIP. Various security threats associated with this application layer protocol are mentioned. Other protocols involved in VoIP communication like RTP, RTCP are also discussed. Basic intrusion detection methodologies are explained with detail in chapter 2. Rest of this chapter focuses on research work done previously in the field of intrusion detection and VoIP security. In this chapter we also mentioned the achievements and limitations of existing VoIP intrusion detection systems. With the help of literature survey we come to know that VoIP offers its own security threats along with other traditional risks. In the next chapter we discussed SIP specific threats, there purpose, the way they are launched and the effect they produce on VoIP network.

Considering all these facts we have proposed a Hybrid intrusion detection system for VoIP. Our proposed system consists of two modules in the first module detection is performed using signature based approach, network packets are captured and analyzed against attack signature, if some match occurs alarm is generated otherwise the captured data is forwarded to fuzzy inferencing engine. In this module network data is analyzed against fuzzy rules. If incoming traffic matches with the fuzzy rules intrusion alarm is generated and intensity of attack is found. Our proposed hybrid IDS helps in better detection because attack patterns that are not detected by signature based IDS module are further detected by fuzzy IDS.

Another important feature of our designed system is that it performs Stateful intrusion detection. Despite of the fact that Stateless protocol analysis is much more efficient under heavy traffic load, it is faster and easy to implement but still Stateful protocol analysis is essential and preferred for VoIP communication. Some attack patterns spread across various packets. Attack patterns which spread across SIP packets may get escape form detection mechanism. Stateful intrusion detection helps to group packets belonging to same session and hence improve intrusion detection mechanism. Our Signatures are Stateful, they can cause load on the underlying network but provide better performance in detecting intrusions.

We have tested our proposed system against VoIP data set gathered at INRIA research center. The data set is composed of real world attack-free and attack traces. We than tested our IDS modules (Signature based IDS and Fuzzy IDS) separately and in hybrid way. Results demonstrate that high detection accuracy is achieved for detecting Invite flooding and Spamming attacks when both techniques for intrusion detection are combined together.

6.2 Future work

In this thesis we have provide a basis for hybrid and Stateful intrusion detection system for SIP-VoIP system. There exist space for improvement and enhancement in our work. We have implemented two types of attack to demonstrate the effectiveness of our approach. The IDS can be enhanced by covering various other security threats as mentioned in chapter 3. Similarly our proposed system is considering only one application layer protocol that is SIP, as future enhancements we shall consider other protocol like RTP, RTCP etc. involved in VoIP communication to more effectively detect VoIP attacks.

References

[1] Mohamed Nassar, “VoIP Networks Monitoring and Intrusion Detection”. PhD dissertation, Dept. Computer Science, The Henri Poincare University – Nancy, France. March 2009.

[2] J. P. Anderson,“Computer Security Threat Monitoring and Surveillance”, Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.

[3] Patrick stuart wheeler, “Techniques for Improving the Performance of Signature-Based Network Intrusion Detection Systems” MS thesis, University of California, Davis, 2006.

[4] Bazara I. A. Barry, “A Hybrid and Cross-Protocol Architecture with Semantics and Syntax Awareness to Improve Intrusion Detection Efficiency in Voice over IP Environments”, PhD dissertation, Faculty of Engineering and The Built Environment University of Cape Town, August 2008.

[5] P. Mell, V. Hu, R. Lipmann, J. Haines, and M. Zissman, “An Overview of Issues in Testing Intrusion Detection Systems,” Technical Report, NIST IR 7007, National Institute of Standard and Technology, August 2003.

[6] H. Schulzrinne - Columbia University, G. Camarillo - Ericsson, A. Johnston - WorldCom, J. Peterson - Neustar, R. Sparks - dynamicsoft, M. Handley - ICIR, E. Schooler - AT&T. *"SIP : Session Initiation Protocol* – RFC 3261 ". June 2002.

[7] White Paper – “Understanding SIP – Today’s hottest communication protocol comes of age”. Ubiquity. (2010, May 12). [Online]. Available: http://www.cse.iitd.ernet.in/~pkalra/siv864/SIP-overview.pdf

[8] IETF Internet-Draft, *3GPP R5 requirements on SIP*, 2002. [Online] Available: http://tools.ietf.org/html/draft-ietf-sipping-3gpp-r5-requirements-00

[9] Dongwon Seo, Heejo Lee and Ejovi Nuwere, “Detecting More SIP Attacks on VoIP Services by Combining Rule Matching and State Transition Models”, IFIP International Federation for Information Processing,Volume 278, Pages 397-411, year 2008.

[10] IETF Internet-Draft, A Session Initiation Protocol (SIP) Event Package for Registrations,2004. [Online] Available: http://tools.ietf.org/html/rfc3680

[11] M. Handley, V. Jacobson and C. Perkins, "SDP: Session Description Protocol" RFC4566, 2006. [Online] Available: http://tools.ietf.org/html/rfc4566

[12] H. Schulzrinne and S. Casner,"RTP: Real Time Transport Protocol", RFC 1889 ,1996. [Online] Available: http://www.ietf.org/rfc/rfc1889.txt

[13] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, 2003. [Online] Available: http://tools.ietf.org/html/rfc3550

[14] Hossein Bidgoli, "The Internet encyclopedia", Volume 1,2004.

[15] Mounji, A., Charlier, B.L., Zampuniéris, D., and Habra, N. "Distributed audit trail analysis", Proceedings of the ISOC'95 symposium on network and distributed system security, pp. 102--112, Los Alamitos, CA,1995.

[16] Lindqvist, U. and Porras, P.A. "Detecting computer and network misuse through the production-based expert system toolset (PBEST)".In L. Gong & M. Reiter (Eds.), Proceedings of the 1999 IEEE symposium on security and privacy , pp. 146--161, IEEE Computer Socitey, Los Alamitos, CA,1999.

[17] Steve A.Hofmeyr, Stephanie A Forrest and Anil Buntwal Somayaji , "Intrusion detection using sequences of system calls", Journal of Computer Security, Vol 6, pp 151—180, August 1998.

[18] Dickerson J.E. and Dickerson J.A., "Fuzzy network profiling for intrusion detection", in Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, pp. 301–306, Atlanta, USA, July 2000.

[19] Wassim El-Hajj, Fadi Aloul, Zouheir Trabelsi and Nazar Zaki, "On Detecting Port Scanning using Fuzzy Based Intrusion Detection System", Wireless Communications and Mobile Computing Conference, pp 105 - 110, August 2008.

[20] S.Sangeetha and Dr.V.Vaidehi, "Fuzzy aided application layer semantic intrusion detection system - FASIDS" , International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010.

[21] Bazara Barry and H. Anthony Chan, “A Signature Database for Intrusion Detection Systems Targeting Voice over Internet Protocol”, Military Communications Conference, pp 1-8, San Diego, CA, November 2008.

[22] Urupoj Kanlayasiri and Surasak Sanguanpong and Wipa Jaratmanachot, “A Rule-based Approach for Port Scanning Detection”, 23nd Electrical Engineering Conference (EECON-23),Chiangmai November, 2000.

[23] Yacine Bouzida and Christophe Mangin. "A framework for detecting anomalies in VoIP networks", in *proceedings IEEE Computer Society the Third International Conference on Availability, Reliability and Security*, pp 204-211, Year 2008.

[24] Zhou Lianying and Liu Fengyu, “A Swarm-Intelligence-Based Intrusion Detection Technique”, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.7B. July 2006.

[25] J. M. Orset, B. Alcalde, and A. Cavalli, “An EFSM-Based Intrusion Detection System for Ad Hoc Networks”, Proceedings of The Third International Symposium, Automated Technology for Verification and Analysis (ATVA), Taipei, Taiwan, October 2005.

[26] Dongwook Shin and Choon Shim, “Progressive multi gray-leveling: A voice Spam protection algorithm”, IEEE Network. Vol 5, pp 18 - 24 , Sep/Oct 2006.

[27] Snort – The de-facto Standard for Intrusion Detection/Prevention. [Online] Available: http://www.snort.org

[28] Sven Ehlert , Dimitris Geneiatakis and Thomas Magedanz ,“Survey of network security systems to counter SIP-based denial-of-service attacks”, journal of computers &Security ,vol 29, pp 225–243, Year 2010.

[29] David Endler, Dipak Ghosal, Reza Jafari, Akbal Karlcut, Marc Kolenko, Nhut Nguyen, Wil Walkoe and Jonathan Zar, “VOIPSA VoIP Security and Privacy Threat Taxonomy ”, Public Release 1.0. October 24, 2005.

[30] Dimitris Geneiatakis, Tasos Dagiuklas, Georgios Kambourakis, Costas Lambrinoudakis, Stefanos Gritzalis , Karlovassi Sven Ehlert and Dorgham Sisalem, “Survey of Security Vulnerabilities in Session Initiation Protocol”, IEEE

Communications Surveys & Tutorials. The Electronic Magazine of Original Peer-Reviewing Survey Articles. Vol. 8, No. 3. pp 68-81. 3rd Quarter 2006.

[31] L.A. Zadeh , "Fuzzy Sets", Information and Control, Vol 8, pp 338-353, June 1965.

[32] Khalid Ateatallah Alsubhi, "A Fuzzy-logic based Alert Prioritization Engine for IDSs: Architecture and Configuration", MS thesis, University of Waterloo, Ontario, Canada, 2008.

[33] B. I. A. Barry and H. A. Chan, "A Hybrid, Stateful, and Cross-protocol Intrusion Detection System for Converged Applications" ,*Springer LNCS*, vol. 4804, OTM 2007, Part II, pp 1616-1633, November 2007.

[34] Aly M. El-Semary Mostafa Gadal-Haqq and M. Mostafa, "Distributed and Scalable Intrusion Detection System Based on Agents and Intelligent Techniques", Journal of Information Processing Systems, Vol.6, No.4, December 2010.

[35] https://gforge.inria.fr

[36] Mohamed Nassar, Radu State, and Olivier Festor , "Labeled VoIP Data-set for Intrusion Detection Evaluation", EUNICE'10 Proceedings of the 16th EUNICE/IFIP WG 6.6 conference on Networked services and applications: engineering, control and management,2010.

[37] Mohamed Nassar, Radu State, and Olivier Festor, "Monitoring SIP Traffic Using Support Vector Machines", 11th International Symposium on Recent advances in intrusion detection RAID 2008, Boston: United States, 2008.