INTRUSION DETECTION USING NAÏVE BAYESIAN AND DECISION TREE

MS Research Thesis

By

Summuyya Munib

(585-FBAS/MSCSF09)

Supervised By:

Prof. Dr Muhammad Sher

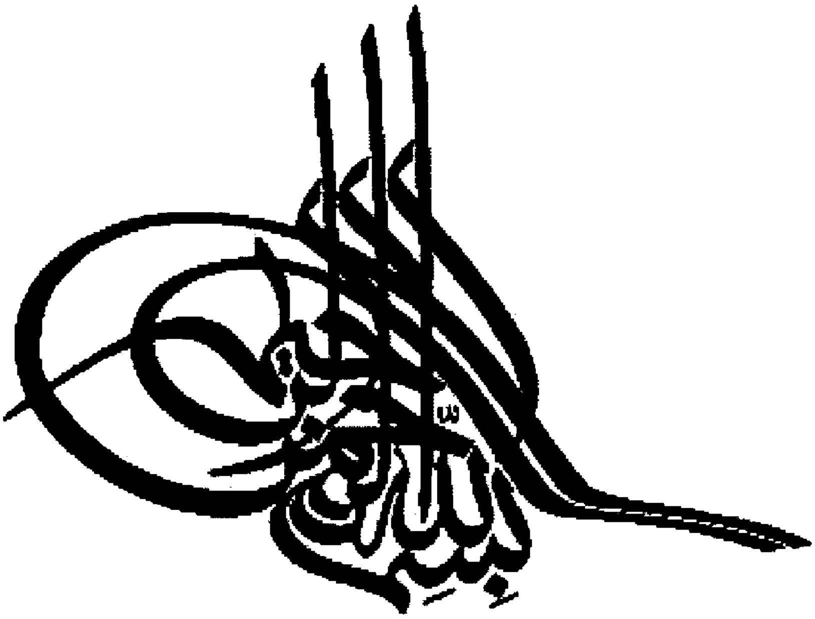
Department of Computer Science& Software Engineering

Faculty of Basic and Applied Sciences

International Islamic University, Islamabad

Application Software

computer software



A Dissertation Submitted to the

Department of Computer Science& Software Engineering

International Islamic University Islamabad

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

MS in Computer Science

International Islamic University, Islamabad

/16

Dated: March, 2012

Final Approval

It is certified that we have examined the thesis titled "Intrusion Detection using Naïve Bayesian and Decision Tree" submitted by Summuyya Munib, Registration Number 585-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

Supervisor:

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

16.3.12

Internal Examiner:

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

A Daud
21-03-12

External Examiner:

Dr. Sohail Ayubi
Manager (Technical)
National Engineering & Scientific Commission,
Islamabad.

16/3/12

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 Muhammad 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.

Summuyya Munib

(585-BAS/MSCS/F09)

Dedicated to my
Family for their
immense love,
patience and
support

Acknowledgements

All thanks and gratitude goes to Allah for all the blessings and knowledge he has given to us. He has given us everything we have and often we forget about the bounties we enjoy. First of all, I am grateful to the Almighty Allah for fortitude and courage he gave me to complete this project. All respects for our dear Holy Prophet Muhammad (SAW) who enlightened our minds to recognize our Creator and thyself as the last Prophet of Allah & great benefactor of mankind.

Project work could not be completed without the help and support of a number of people. I would like to express my gratitude to my Supervisor Dr. Muhammad Sher for the persistent guidance, support and the encouragement. I would also like to express my thanks to Ms Sadia Khan, for discussing issues and sharing ideas throughout the project. This project could not be completed without the constant encouragement and support of my family. In the last but not the least I would like to acknowledge my friends for constantly helping and encouraging me throughout the project.

Project in Brief

Project Title:	**Intrusion Detection using Naïve Bayesian and Decision Tree**
Undertaken By:	**Summuyya Munib**
Supervised By:	**Prof. Dr Muhammad Sher**
Start Date:	**January 2011**
Completion Date:	**Feburary 2012**
Tools and technologies:	**Wireshark, Matlab 2007**
Documentation Tools:	**MS Word**
Operating System:	**MS Windows 7**
System used:	**Intel core I 3**

Abbreviation

IDS	Intrusion Detection System
IP	Internet Protocol
IMS	IP Multimedia Subsystem
VoIP	Voice over IP
IPTv	IP based Television
3GPP	Third Generation Partnership Project
IETF	Internet Engineering Task Force
SIP	Session Initiation Protocol
UA	User Agents
K-NN	K-Nearest Neighbor
SVM	Support Vector Machine
CART	Classification and Regression Tree
MARS	Multivariate Adaptive Regression Spline
DoS	Denial of Service
PSTN	Public Switched Telephone Network

Table of Contents

List of Figures

List of Tables

Abstract

Network anomaly intrusion detection is vital to provide the security and protection. SIP is an application layer signaling protocol which is widely used in VoIP, IMS and IPTv. SIP possesses various threats; Denial of Service (DoS) is one of the serious threats among them. The project is to detect anomalies of the network. A DoS attack prevents the legitimate users to use the services. Thus, detection of this security threat is essential. Therefore, our work focuses on the detection of SIP Invite Flood attacks. An anomaly based approach will be used for detection of malicious behavior. Attack detection has been carried out using Naïve Bayes, CART, K-NN, and MARS. MARS had higher detection accuracy among them.

Chapter 1 Introduction

Chapter 1 provides the background knowledge needed for the issue in hand. Section 1.1 gives an overview of IP based Multimedia Subsystems and Voice over IP. Section 1.2 discusses Session Initiation Protocol, its network entities and methods. Section 1.3 defines intrusion and Section 1.4 defines the Intrusion Detection System and its general architecture. Section 1.5 provides an outline of thesis.

1.1 IP Multimedia Subsystem and Voice over IP

Traditionally, the telephony services are provided by circuit switched networks; known as Public Switched Telephone Networks (PSTN). Now, the technology of telephony services is evolving. The new technologies are emerging are based on IP networks.

As compared to other communication technologies, Internet and IP are continuously developing and growing in infrastructure, supporting numerous applications and devices. In the beginning, IP Multimedia Subsystem (IMS) was defined by the Third Generation Partnership Project 3GPP and 3GPP2. The aim was to present a new mobile network architecture that would facilitate the convergence of data, speech and mobile network technology over an IP based infrastructure. The intention was to overcome the variance between the existing traditional technologies of telecommunication and Internet technology. The outcome came in the form of IMS that supports new and innovative services. It provides the architectural umbrella for convergence of wireline and wireless. Due to the ability to preserving the important qualities of PSTN with the flexibility of Internet, IMS architecture has acquired attention from well known organizations like ITU, ESI and some others [1] [2].

IMS defines the basic architecture that provides voice over IP (VoIP) and multimedia services. IP telephony or Voice over IP is cheaper/cost saving for long distance calls. Because carrying voice traffic over data networks is less expensive. Apart from the voice services, customers can also be provided with the additional services.

1.2 Session Initiation Protocol

SIP is an application layer text based control protocol defined by Internet Engineering Task Force (IETF). It uses UTF-8 encoding. This protocol provides control and can handle call signaling. SIP can establish, manage and terminate the calls and multimedia sessions among participants. It offers features like call conference, call hold, call and media transfer. Also, SIP allows users to add more participants in the ongoing session. SIP operates over numerous transport protocols [3] [4]. A session can be a multimedia conference or a two way telephone call. Session is created using SIP invitations allowing the use of compatible media types among the participants during the session [4] [5].

Some of the features of SIP are

- ✓ Name Translation and User Location
- ✓ Feature Negotiation
- ✓ Call Participant Management
- ✓ Call feature changes
- ✓ Media negotiation

Because of these features this protocol is considered for call and multimedia communications over Internet.

1.2.1 Comparison of SIP and H.323

SIP is widely used for IP telephony services and has become a de-facto standard. IP Telephony acceptance lies in achieving at least the same level of services and ease of operation to the client as of PSTN. A signaling protocol is required to offer such features as that of PSTN. The two standards of signaling protocol that are competing in the field are SIP and H.323 but now from few years SIP has become dominant protocol. The primary advantages provided by SIP are flexibility in terms of new features and is relatively easy to debug and implement.

1.2.2 SIP Methods

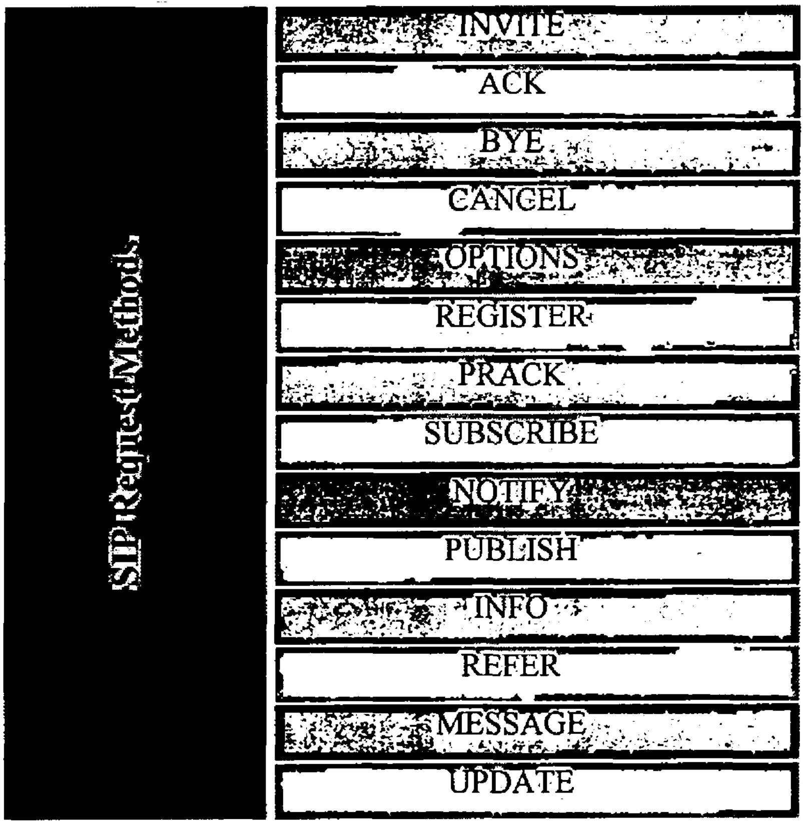
SIP is a text based protocol like HTTP. It uses Methods for communication. It has several methods which can be mainly characterized as request methods and corresponding response methods. These methods are defined in RFC 3261 [4][6]. Some other SIP Methods Extensions are also available defined in other RFC's. These methods can be divided into two groups.

1. SIP Requests
2. SIP Response

SIP Request Methods

User Agents places requests to get a service which is received by the SIP network server. SIP request Methods are shown in Table 1-1.

Table 1-1 SIP Request Methods



SIP Request Methods	INVITE
	ACK
	BYE
	CANCEL
	OPTIONS
	REGISTER
	PRACK
	SUBSCRIBE
	NOTIFY
	PUBLISH
	INFO
	REFER
	MESSAGE
	UPDATE

SIP Response Methods

When SIP network server receives a request, it acknowledges it by sending it a response. There are six families of responses

1xx Informational (e.g. 100 Trying, 180 Ringing)

2xx Successful (e.g. 200 OK, 202 Accepted)

3xx Redirection (e.g. 302 Moved Temporarily)
4xx Request Failure (e.g. 404 Not Found, 482 Loop Detected)
5xx Server Failure (e.g. 501 Not Implemented)
6xx Global Failure (e.g. 603 Decline)

SIP is a transaction based protocol where a SIP transaction is formed by a request and corresponding one or more responses; and SIP dialog consists of one or more transactions.

1.2.3 SIP Network Entities

SIP architecture consists of many connected entities. The two major components of SIP architecture are User Agent (UA) and network server. User Agent is a logical end point that can perform role of a user agent client and makes or receive SIP requests. It can also act as user agent server to receive and return response to a request. The server has three elements:

1. **Proxy Server**

   It mainly acts as a router as they implement call routing policies. Also, it can receive requests from the clients and makes requests on their behalf. In other words, proxy server accepts the session requests from the user agents then obtains the address of the requested destination.

2. **Registrar**

   Registrar is also a logical element, mostly located with proxy server. It registers the user's contact address. It is basically the database containing the locations of users within the domain of network. It accepts the request methods and places it in the location service.

3. **Redirect Server**

   As the name indicates, it generates redirectional responses to the requests received. It allows the proxy server to forward its requests to other domain.

4. **Location server**

   It provides the location details of user.

5. **Application server**

   Application server is used to provide advance services to users.

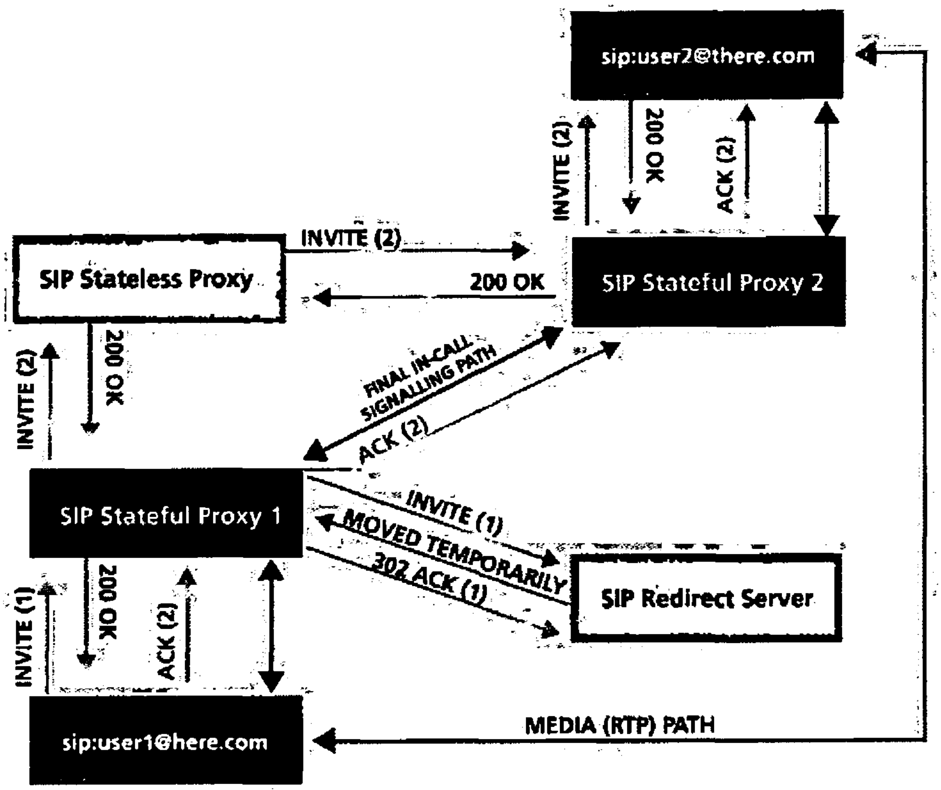


Figure 1-1 SIP Network Entities and exchange of messages [45]

According to domain, a session establishment between the user agents can be divided into two categories:

1. Session establishment within the domain
2. Session establishment with a different domain

Session establishment within the domain

In this case, both user agents are registered with the SIP Registrar Server. A user agent, let's say User-A, requests the SIP Proxy Server to initiate a call with another user agent, User-B. Proxy server checks with the Registrar server the address and location of User-B. After, checking the availability of User-B and negotiation of supported features, the call is established. Figure 1-2 shows the procedure of the within Domain call establishment.

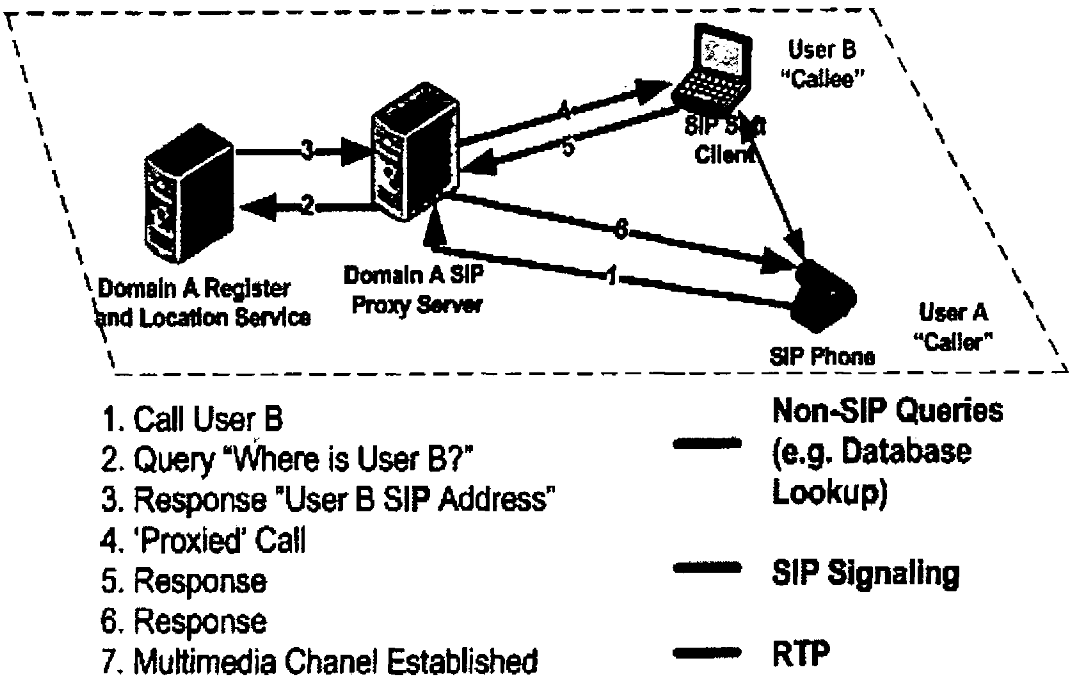
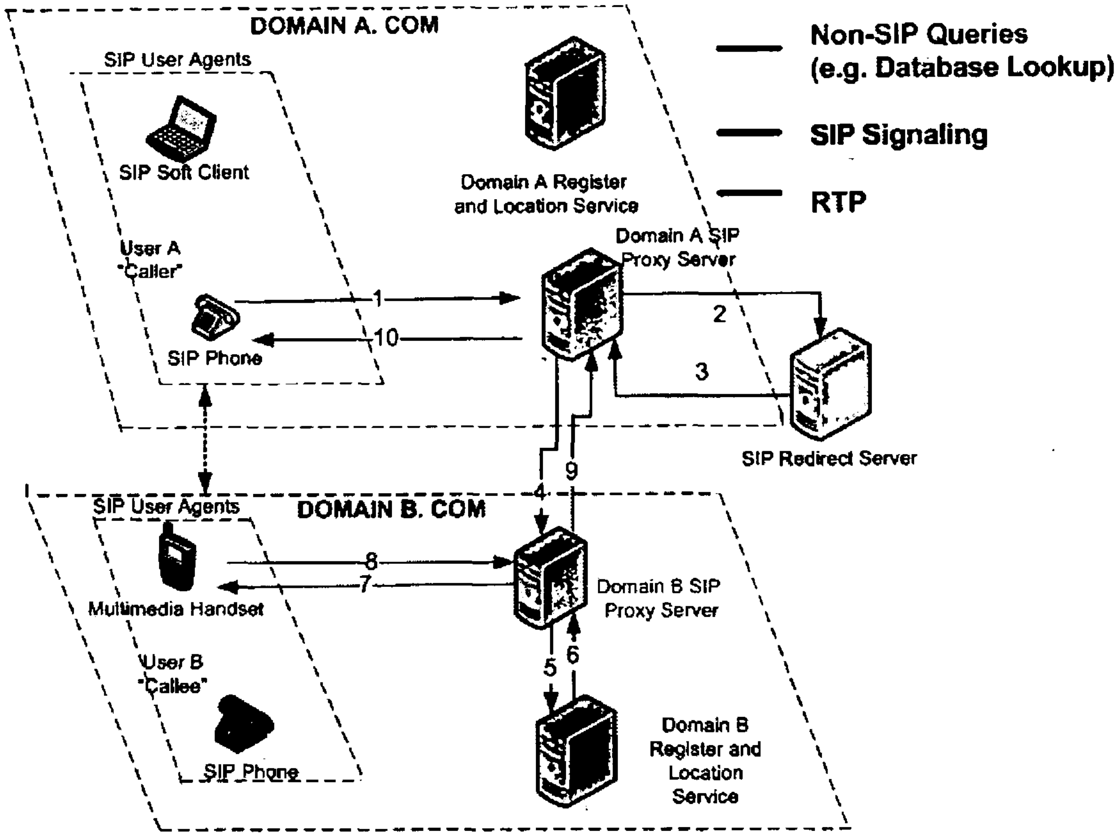

User B
"Callee"
SIP Soft Client
3
2
4
5
6
1
Domain A Register and Location Service
Domain A SIP Proxy Server
SIP Phone
User A
"Caller"
1. Call User B
2. Query "Where is User B?"
3. Response "User B SIP Address"
4. 'Proxied' Call
5. Response
6. Response
7. Multimedia Chanel Established
Non-SIP Queries (e.g. Database Lookup)
SIP Signaling
RTP

Figure 1-2 User Agents within the same domain [7]

Session establishment with a different domain

Contrary to the above case, the user agents establishing a session are located in different domains. Let's assume the User-A, user agent in domain A, wants to initiate a call with user agent User-B located in domain B. User-A will contact with the SIP Proxy Server. Proxy server will contact ISP Registrar Server to get the location, IP and status of User-B. After, checking the availability of User-B and negotiation of supported features, the call is established. Figure 1-3 shows the procedure of the within Domain call establishment.



1. Call User B
2. Query "How to get to User B?"
3. Response "Address of Proxy Controller for Domain"
4. Call "Proxied" to SIP Proxy for Domain B
5. Query "Where is User B"
6. User B's Address
7. Proxied Call
8. Response
9. Response
10. Response
11. Multimedia Channel Established

Figure 1-3 User Agents in different domains [7]

1.2.4 SIP-Call Example

In Figure 1-4, a typical example (taken from RFC3261) of exchange of SIP messages between two users is shown. The two participants in the dialog are Alice and Bob. Alice initiates the dialog by sending INVITE request to Bob. The messages following in response to the INVITE message are shown below. In order to negotiate the media description among the two corresponding parties; Session Description Protocol (SDP) is used. SDP messages are inserted in the INVITE message from the sender and receiver embeds it in the 200 OK message.

```
                     atlanta.com  . . . biloxi.com
                 .      proxy              proxy     .
               .                                       .
       Alice's  . . . . . . . . . . . . . . . . . . . .  Bob's
      softphone                                        SIP Phone
         |                |                |                |
         |    INVITE F1   |                |                |
         |--------------->|    INVITE F2   |                |
         |  100 Trying F3 |--------------->|    INVITE F4   |
         |<---------------|  100 Trying F5 |--------------->|
         |                |<-------------- | 180 Ringing F6 |
         |                | 180 Ringing F7 |<---------------|
         | 180 Ringing F8 |<---------------|     200 OK F9  |
         |<---------------|    200 OK F10  |<---------------|
         |    200 OK F11  |<---------------|                |
         |<---------------|                |                |
         |                       ACK F12                    |
         |------------------------------------------------->|
         |                   Media Session                  |
         |<================================================>|
         |                       BYE F13                    |
         |<-------------------------------------------------|
         |                     200 OK F14                   |
       |------------------------------------------------->|
```

Figure 1-4 SIP Call Example [6]

The INVITE message in the above Figure 1-4 may look like:

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
   Max-Forwards: 70
   To: Bob <sip:bob@biloxi.com>
   From: Alice <sip:alice@atlanta.com>;tag=1928301774
   Call-ID: a84b4c76e66710@pc33.atlanta.com
   CSeq: 314159 INVITE
   Contact: <sip:alice@pc33.atlanta.com>
   Content-Type: application/sdp
   Content-Length: 142

(Alice's SDP not shown)
```

1.2.5 SIP REGISTER Example

A user agent needs to register itself with the Registrar Server. Because, as we discussed earlier, a SIP Proxy server needs the location, status and IP address of a user agent so that it can forward the request made by a sender.

We assume that Bob wants to register itself with the Registrar Server of his VoIP domain. He will send Register request message to the Registrar Server. It maintains a location database, where it will store the logical and physical address of Bob. Proxy server access the database, by using the information it can then route the incoming calls to Bob. Figure 1-6 shows the example of SIP Register.

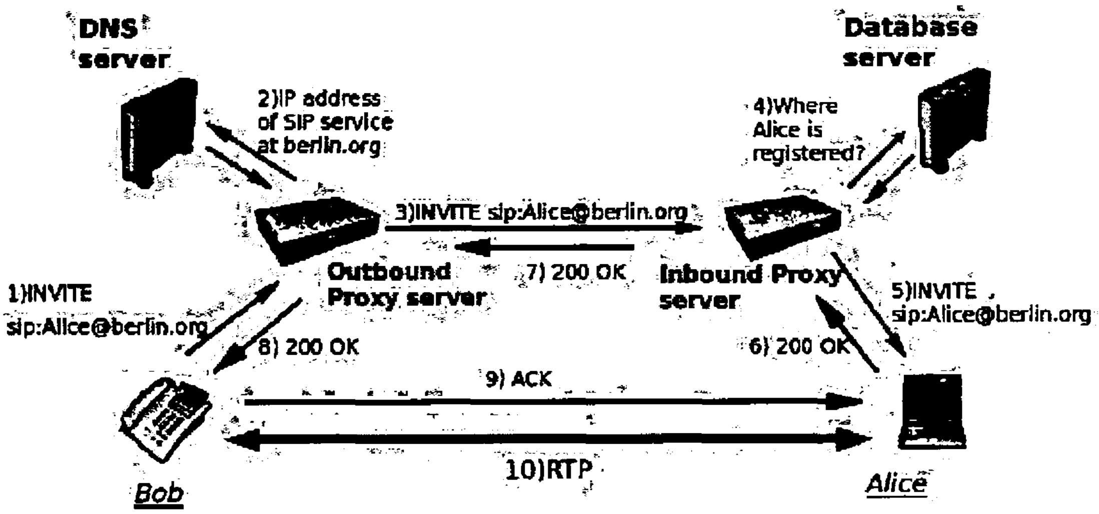

DNS server
Database server
2)IP address of SIP service at berlin.org
4)Where Alice is registered?
3)INVITE sip:Alice@berlin.org
7) 200 OK
Outbound Proxy server
Inbound Proxy server
1)INVITE sip:Alice@berlin.org
5)INVITE sip:Alice@berlin.org
8) 200 OK
6) 200 OK
9) ACK
10)RTP
Bob
Alice

Figure 1-5 SIP Trapezoid [8]

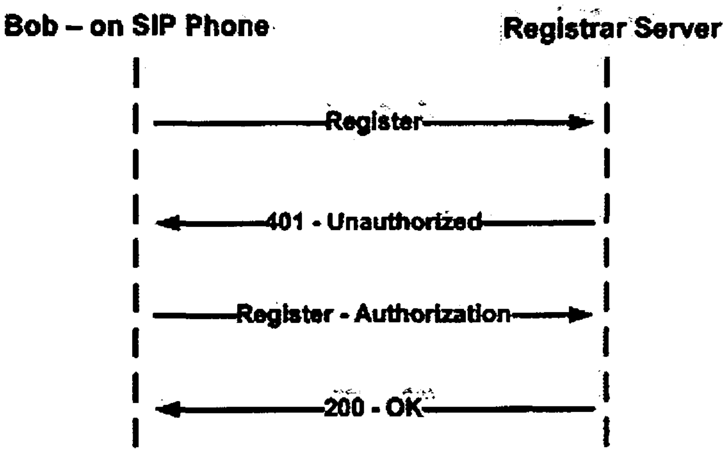


Figure 1-6 SIP Register example

1.3 Intrusion

Intrusion is an attempt to break into or misuse the system. An intrusion is an on purpose, unauthorized attempt to access or manipulate information or system and to render them unreliable or unusable. They can be legal users of the network or from outside the local network.

1.4 Intrusion Detection System

IDS are security tools whose function is to strengthen the security information and communication systems. IDS can determine legal and illegal acts of users within and out of the local network. IDS is defined by International Computer Security Association (ICSA) as:

"The detection of intrusions or intrusions attempts either manually or via software expert systems that operate on logs or other information available from the system or the network."

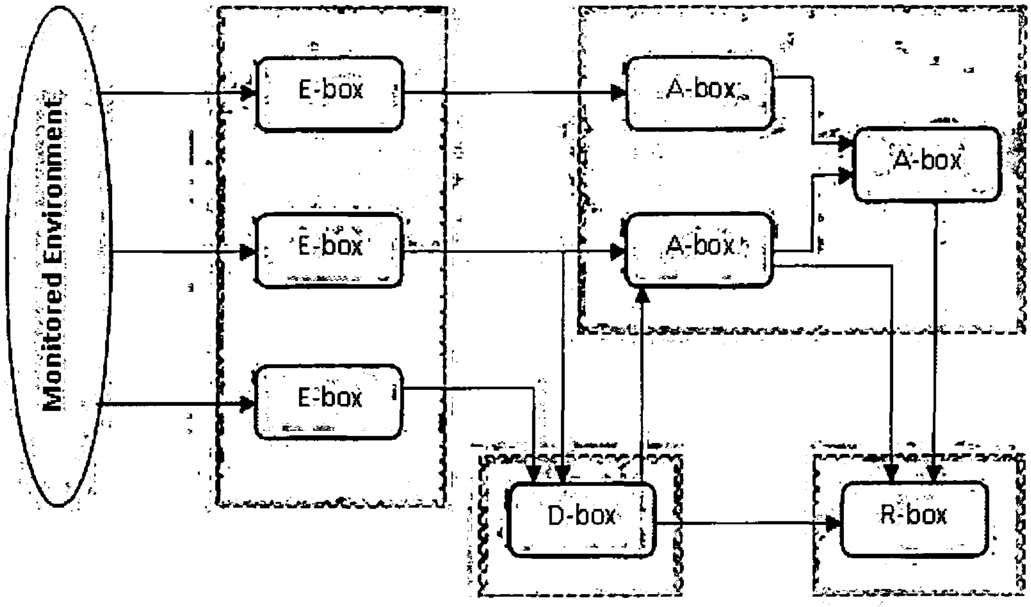


Figure 1-7 General Architecture for IDS System

IDWG has defined the general architecture of IDS [9]. The architecture is based on four functional modules as shown in Figure 1-7.

1. Event Blocks (E-box): It is composed of sensor elements which monitors the target system and collects the information events. These events are then analyzed by other blocks.
2. Database Blocks (D-box): Stores information from Event blocks for further processing.
3. Analysis Blocks (A-box): It processes the information to analyze events and identify the aggressive behavior.
4. Response Blocks (R-box): it executes a response if an intrusion is detected.

1.5 Thesis Organization

Chapter-2 presents literature survey carried out its limitations. In Chapter-3 the requirement analysis of intrusion detection is carried out. Chapter-4 introduces the architecture to carry out intrusion detection and the proposed solution. Performance measures used are also defmed. Chapter 5 gives an account of classifiers used. Chapter 6 presents classification results and their comparative analysis. Chapter 7 presents the conclusion and future work.

Chapter 2 Literature Survey

Chapter 2 presents a summary of the survey carried out during our course. Section 2.1 discusses the various characteristics of IDS. On basis of these characteristics IDS is categorized. Section 2.2 presents the literature review that is conducted; the objective is to review critical points of current knowledge or approaches on a certain issue and to identify their limitations. It provides the basis for problem domain.

2.1 Characteristics of Intrusion Detection System

The characteristics of the Intrusion Detection System are shown in Figure 2-1[10]. According to the detection method applied IDS can be divided into two categories [9] [10] [11].

1. **Misuse detection**

   It seeks defined patterns within analyzed data. It identifies intrusions by matching observed data with pre-defined descriptions of intrusive behavior. Therefore their false alarm rate is low but incapable to detect unknown attacks. In order to detect new attacks the database needs to be updated regularly.

2. **Anomaly Detection**

   It estimates the normal behavior model of the system and detects anomaly in observed data by noticing deviations from these models. As a result can detect previously unobserved intrusion attacks. FP are usually higher than the previous technique.

According to the information source/audit data source IDS can be categorized as Host based IDS which analyzes events related to Operating System e.g. system call and Network based analyzes information related to the network traffic data. A Host based IDS system can protect only the system on which it is installed. It will check for the intruder's attacks on the system. In Network based IDS, it will monitor the entire network or a subset of it. This type of IDS does not add any load on the systems connected to the network.

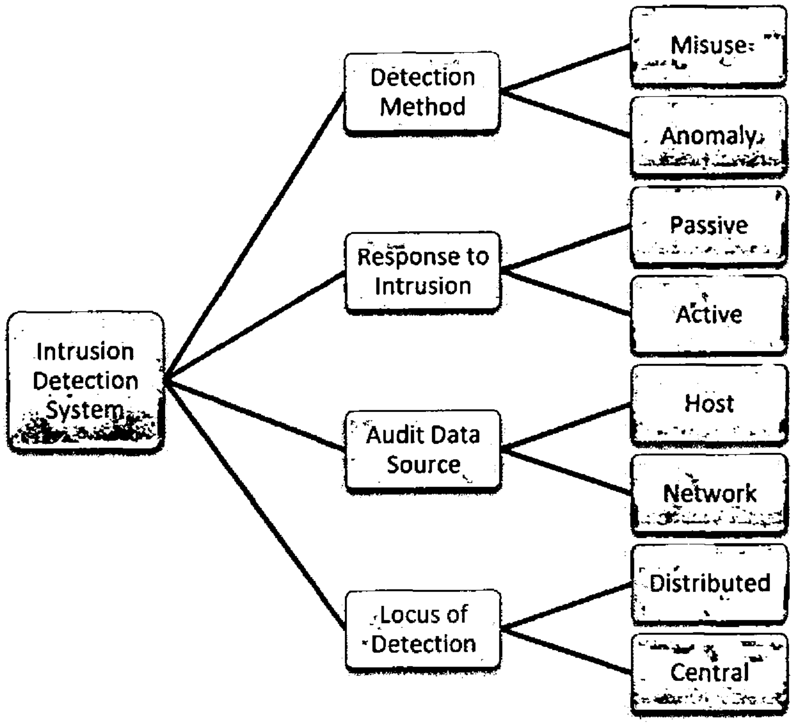


Figure 2-1 Characteristics of Intrusion Detection System

In a case of distributed intrusion detection, sensors distributed across the enterprise reports to central management system. These sensors monitor the network; gathers the information and sends the attack logs to the central monitoring system. The central system can then save the information in a database.

Anomaly detection techniques can be divided into three main classes according to the processing involved in modeling the behavioral model as shown in Figure 2-2 [9][11].

- **Statistical based**

In this approach, system behavior is represented from a random viewpoint. A profile of network traffic activity representing its stochastic behavior is created.

- **Knowledge based**

These techniques try to capture the claimed behavior from the available system data.

➢ Machine Learning

They establish an explicit or implicit model which allows categorization of analyzed pattern. These methods can capture interdependencies.

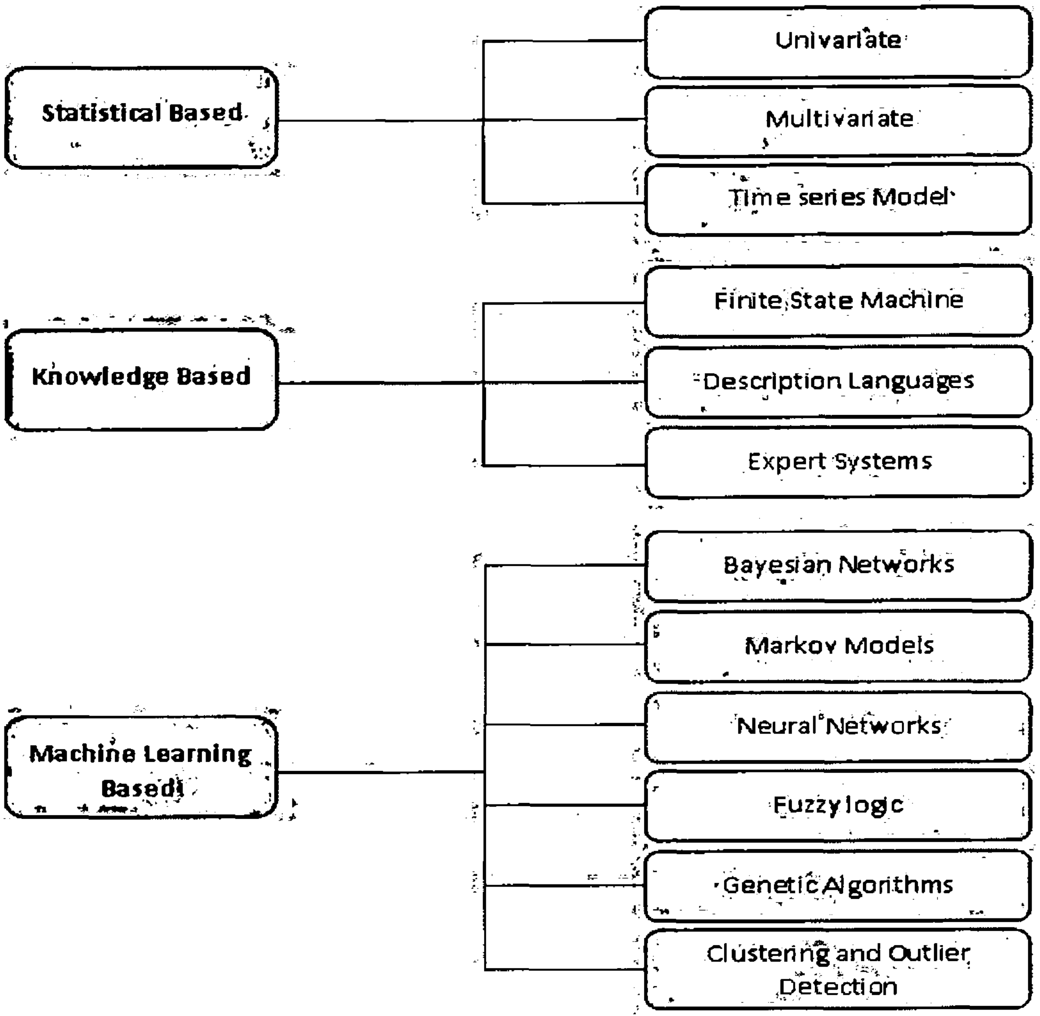


Figure 2-2 Classification of Anomaly detection techniques according to behavior modeling methodology

When an event is analyzed by a classifier, four types of scenarios arise corresponding to the results of detection [9].

1. False Positive (FP): Clean event but is classified as an intrusion
2. False Negative (FN): Malicious event but classified as normal/clean
3. True Positive (TP): Correctly classified as intrusion/attack
4. True Negative (TN): Event is correctly classified as normal/clean

Low FP and FN rates and high TP and TN rates results in good competence values.

2.2 Literature Overview

In paper [12], author has analyzed different neural network methods used for intrusion detection. They used the signature based approach for intrusion detection. They have proposed Back Propagation Neural Networks with Genetic Algorithm method for identifying attacks. Genetic algorithm is used to select the optimal parameters for Back Propagation Neural Networks. These weights are then used by Back Propagation Neural Networks to classify the traces as normal or attack.

The authors have identified intrusions using signature based approach which can only detect the attacks for which it is trained and cannot identify the new attacks. Although by using Genetic Algorithm, the generalization problem of Back Propagation Neural Networks has been dealt but the method has become computationally intensive.

In paper [13] authors have carried out experimental study of applying Naïve Bayes in intrusion detection. Bayes networks are powerful tools for decision and reasoning under uncertainty in the probability theory framework. Naïve Bayes are useful for inference purpose. This study shows although they have a simple structure and despite their strong assumption provides competitive results. Experiments were carried out on KDD'99 dataset. Experiments were performed on three levels of attack granularities. Naive Bayes have a number of advantages as they have a simple structure. Its construction is very simple and incremental. Classification is achieved in linear time although in Bayesian network with general structure is known to be NP complete. Naïve Bayes is based on strong independence relation assumption which may result in as a negative influence on the results.

Authors of paper [14] shows anomaly detection using machine learning techniques have the advantage of low false positives rate and faster testing speed. Bayesian inference is a statistical inference method in which observations are used to calculate the probability that a hypothesis may be true, or else to update its previously-calculated probability. Bayesian statistical inference in machine learning anomaly detection has improved the detection and predictive ability thus increasing security of the system.

In [15] paper authors have used a hybrid approach for anomaly based network intrusion detection. They have proposed to use Naïve Bayesian Tree to improve the detection for adaptive networks. It makes use of advantages of both the Bayesian classifier and decision trees. Decision tree contains Bayesian classifier in leaf nodes. Dataset is divided into subsets using decision tree. Experiments are carried on KDD 99 dataset. This method has achieved high detection rates, 99% and low false positives. The detection rate of R2L attacks needs improvement and needs to be modeled for real world IDS.

In above papers, a common limitation is that methodology has not been tested for real time intrusion detection and also has been not evaluated for application layer protocol.

In paper [16], Genetic Algorithm is used to select a subset of features that can give high detection rates on intrusion attacks and lower the false alarms. These features are given to a classifier. In this investigation, classifier chosen is decision tree. Experiments are performed on the KDD 99 dataset for TCP/IP attacks. The error rate of the mentioned experiment is under 3. The proposed method takes longer execution time than a decision tree. And also because of Genetic Algorithm, the algorithm is computationally intensive.

In paper [17], authors have proposed a methodology based on Artificial Neural Networks. The technique proposed is Boosted Subspace Probabilistic Neural Network (BSPNN) which is inspired by Vector Quantization-General Regression Neural Networks (VQ-GRNN). The technique is to combine VQ-GRNN and Adaptive Boosting (Adaboost). In boosting, a base classifier learns iteratively on several distributions of data. The proposed methodology is tested on KDD 99 dataset. The detection rate achieved for Denial of Service attacks is 98.1% and false alarms are 0.06%. The proposed technique provides good generalization but demands additional processing power because of the boosting. Also, boosting is not beneficial when the classifiers used are correlated.

Session Initiation Protocol (SIP) [18] has established itself as the de-facto standard for user's session control. A session can be any network connection a user initiates that lasts for some time, e.g. a voice call or a live video stream. Initially specified in 1999, SIP can be used for any session control between multiple participants. It is the foundation for Voice-over-IP (VoIP), IP Multimedia Subsystem (IMS)[19], and IP Television (IPTV). SIP is a text based protocol. Nowadays, it is the governing protocol for VoIP and the main building block of NGN. It is the core protocol for establishing, modification, and termination of the actual sessions between users. Few years ago, the dominant VoIP signaling protocol was H.323, however in 2008 SIP usage has surpassed H.323 usage [19][20].

Due to increasing popularity, SIP is becoming a viable target for attackers. As SIP is based on free, open standards, malicious users can easily launch attacks by exploiting weaknesses using commonly available tools [20]. There exist three basic classes of SIP attacks, i.e.

1. SIP message fraud

2. Unsolicited messages, i.e. spam

3. Denial of Service

In paper [21], authors have tried to identify the different possible security threats on SIP infrastructure and their effect on the services. Also it provides a few methods to mitigate such attacks. Attacks faced by SIP are: Denial of Service Attacks, SIP Injection Attack, SIP Spoofing Attack, SIP Authentication attack, SIP traffic capturing, Message modification attack, SIP VoIP SPAM (SPIT) attacks. Denial of Service attacks takes place when a high volume of traffic is sent by an attacker. This causes the resources of the system fully consumed and system is unable to answer the valid requests. DoS attacks have further classification that is SIP Register flooding, Call Flooding. In order to register with SIP registrar, user needs to send Register request. SIP Register attack occurs when attacker sends such a high stream of Register requests that Registrar becomes unable to handle the valid requests for a call. In case of call flooding attacks, end device continuously receives Invite request by attacker and when the request is acknowledged, the attacker hangs up. DoS attacks can easily occur because for signaling and data transfer same channels are used.

Thus, need for detection of attacks for SIP infrastructure arises. In this field, a lesser amount of work has been done so far. Some work for the detection of SIP based DoS attack is listed below.

In this paper [22], a neural network based approach is used to detect the intrusions. The proposed architecture for IDS and algorithm adapts to classify correctly a new normal traffic and an attack not represented during the training phase of classifier. The analysis carried out shows that when presented with a normal traffic pattern that was considerably different from the presented training normal traffic patterns, it couldn't be classified it with decent accuracy. The same is true when a new attack was presented.

In paper [23], authors have proposed a probabilistic graphical model, multidimensional Bayesian network classifier for handling multi–dimensional classification problem. It defines a unified framework. It allows a Bayesian network structure in the three sub graphs of an MBC. The proposed framework has been extended to general loss functions.

The proposed technique does not take into account both discrete and continuous variables to be predicted. Also, the proposed technique cannot handle missing data.

Authors of paper [24] have analyzed the role of SIP based DoS attacks on the IMS and proposed a framework for detection. On this framework classification accuracy of different classifiers has been analyzed. Analysis has been carried out on a traffic containing injected SIP floods of varying intensities. These algorithms are analyzed on ten synthetic SIP traffic datasets with different levels of attack intensities and durations. Results depict decision tree C4.5 can detect harmonic flood attacks of 25 calls per second with 90% accuracy.

Specification based approach has been presented in the paper [18]. A framework for detection of attacks is proposed that recognizes deviation from the normal behavior. A state model of proxy's server is developed. Implementation of transaction state machine has been carried out into VoIP Defender security architecture. The devised approach can detect DoS attacks towards the SIP infrastructure with low false error rate.

Although attacks are detected but the development of high quality knowledge is difficult and time consuming task.

In paper [27], authors have proposed an online monitoring approach and used Support Vector Machines for classification in order to distinguish between normal activity and attacks in SIP based VoIP environments. A set of 38 features in VoIP has been monitored. They have evaluated their approach over a mix of real world traces from a large VoIP provider and attacks locally generated on their own testbed. Support Vector machines can deal with a large dimensionality of data. The vectors created by SVM are non-linearly mapped into a high dimensional space. Each vector is labeled with a certain class. Support vectors which outline a hyper-plane in the feature space are calculated and used to classify the data. SPIT and flooding attacks have been detected with good accuracy.

In paper [28], authors have analyzed the robustness and reliability of generic SIP severs under DoS attacks. Analysis is carried out using a customized analysis tool that has the ability to synthesize and launch different types of attacks. From this study it is deduced that existing well known SIP servers can crash by launching simple INVITE flood attacks. Therefore, there is great need to implement SIP Intrusion Detection System (IDS), which can protect a SIP VoIP infrastructure from emerging SIP threats.

In paper [29], authors have carried out comparative analysis of various techniques has been carried out. Advantages and disadvantages of classification based approach are discussed. Some advantages are that they can make great use of algorithm to discriminate between examples of different classes, the testing phase requires small amount of time for classification. Because, it only needs to compare the example with a pre-computed model. The drawback is it needs a labeled dataset.

Statistical based techniques for intrusion detection do not require prior knowledge of attacks but are susceptible to be trained by an attacker in such a way that generated network traffic to accept abnormal behavior as normal. Also, parameters setting are difficult. Difficult to determine the threshold point that balances the likelihood of false positives and of false negatives.

Expert system based methodologies are robust and flexible but difficult and time consuming efforts are required for development of high quality knowledge.

Artificial Neural Networks designing is a complex procedure and are difficult to use. Also improvement of performance is dependent on sample size; performance gets better with the increase of training set. Training takes more time for noisy data. Necessary level of training needs to be determined otherwise results in overfitting which results in inaccurate predictions. They find solutions on their own, neural networks are a "black box"; the manner in which they find a given solution is unknown to the user.

Support Vector Machines approach limitation lies in choice of the kernel, speed and size, both in training and testing. Discrete data presents another problem.

2.3 Summary

In this chapter, we have discussed different categories of Intrusion Detection Systems. It gives an overview of the various types of IDS and some details are omitted to make things simpler. There are many ways in which IDS detects an attack. Although the technology is getting better day by day but it cannot be fitted for all situations. Also, the new technologies have some new limitations resulting in different attacks. A literature survey has been carried out to get to know the various approaches and techniques used for the Intrusion Detection Systems. On the basis of this literature survey, we formulated our problem.

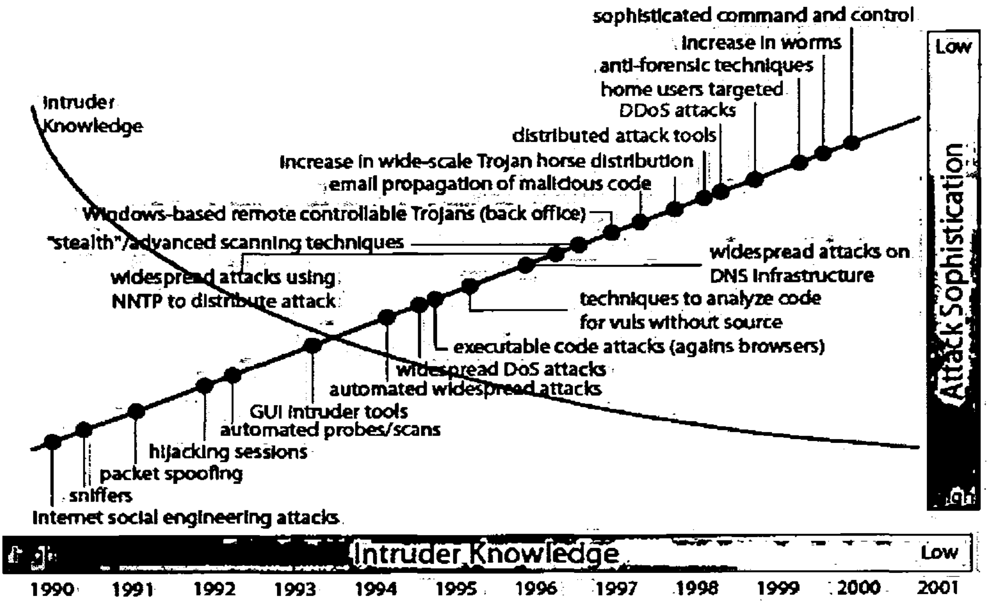
Chapter 3 Problem Domain

In this chapter, the motivation behind this work is discussed and later the domain of our problem is mentioned. section 3.1 carries out requirement analysis to gain an insight of the requirements of the system. Section 3.2 discusses the problem domain which is essential for proposing the solution of a problem.

3.1 Requirement Analysis

With the passage of time, Internet users are growing day by day. This increase is making the cyber world vulnerable to security threats. Also the number of attacks plus severity is increasing substantially. The number of incidents reported to Computer Emergency Response Team/Coordination Center (CERT/CC) is depicted in Figure.

The knowledge of attack and skill required by users has decreased while the attacks have grown sophisticated with time as shown in Figure 3-1.



Source: CERT

Figure 3-1 Number of incidents reported to CERT [26]

Nowadays, global telecommunications is in a phase of transition. Our telecommunication industry is moving towards voice and data convergence. This convergence has resulted in VoIP and IMS. The standard signaling protocol used by VoIP and IMS is Session Initiation Protocol.

IMS and VoIP are based on open standard network architecture and protocol technologies. It inherits the security issues of the underlying protocols. This makes it highly susceptible to a number of attacks resulting in interruption of provided services.

As said before, SIP is used by many enterprises for VoIP and IMS services which is a new technology. There are many related security problems and risks posed by these technologies; as the servers used by them can be reached through internet. Some of the threats faced by them are mentioned below.

- ✓ Message Interception and Modification
- ✓ Fraudulent Usage
- ✓ Call Hijacking and Man in the Middle Attack
- ✓ Denial of Service Attacks
- ✓ SIP Billing Attacks
- ✓ Social Threats

Denials of Service Attacks pose a great threat to the system. In DoS attacks, the attacker attempts to overload computing or memory resources. In this way, server cannot handle the legitimate requests and users are denied the service. Invite Flood Attack occurs when attacker sends a stream of Invite requests to the end device as a result it is unable to make or receive the calls.

3.2 Problem Domain

According to the literature survey, the intrusion detection systems based on signature approach cannot detect new attacks. The signatures need to be updated for new attacks. Also in deploying signature there is substantial latency. Also there exist various problems with existing techniques that induce the complexity of detection systems like low detection accuracy, unbalanced detection rates for different attack types and high false positives. Analysis of large volume of network data also poses a problem. SIP is deployed in an open environment which makes it more complex and vulnerable to the attacks. DoS Flood attacks can force service providers to reduce its capabilities or go out of service totally [27]. It can target network bandwidth, CPU processing power, memory usage with the aim to render the offered service unavailable.

There is a need for an intrusion detection methodology to detect the DoS Flood attacks for SIP infrastructure, in order to provide services to the legitimate users.

3.3 Summary

VoIP and IMS are vulnerable as they are deployed in an open environment contrary to PSTN. This technology not only inherits the limitations of their underlying protocols but voice and data communication makes them more complex and vulnerable. In this chapter, we have discussed the security issues faced by these technologies. Therefore, need arises to identify these attacks in order to make appropriate measures.

Chapter 4 Proposed Solution

In this chapter, a solution is proposed of the problem as discussed in the previous chapter. The approach used to monitor the traffic and technique employed for detection of attack has been discussed in detail. Section 4.2 discusses the proposed monitoring approach for anomaly based intrusion detection and proposed methodology for detection of an attack. Section 4.2 discusses various classifiers used in our study.

4.1 Proposed Technique

The architecture for carrying out intrusion detection is show in Figure 4-1. As we are considering Invite flood attacks for SIP therefore, the network traffic flow will be first filtered for SIP data flow. A queue is used to store SIP packets. Size of the queue is proportional to window size. When the queue is full, the data is presented to feature extractor and a feature vector will be calculated. A number of features like number of requests, number of responses, time duration etc are calculated. These features are then presented to a trained classifier that identifies it as either normal or an intrusion.

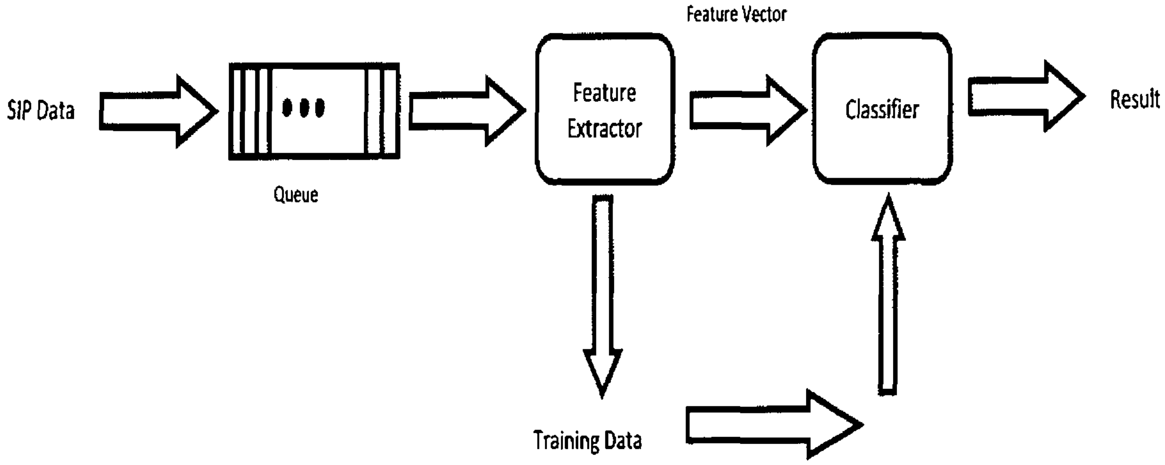


Figure 4-1 Architecture for Intrusion Detection

Classifier is trained during the training phase. Normal and attack features are presented to the classifier on which its parameters are estimated. These parameters are then used to classify the feature vector presented, calculated from the incoming SIP messages.

In order to overcome the limitations discussed in previous section, first we need to calculate features that can model the important attributes of the traffic. We must also take into account the correlations present among the messages. A dialog between the users consists of requests and response. There exists a certain relationship between the request and the response generated that needs to be considered. Therefore, we have introduced the ratio of individual response messages rather than calculating the family responses ratio. We have calculated overall twelve features; like duration of the segment, average inter-arrival of request and responses, number of requests, responses and SDP messages in the segment. Features giving more detail of the request and response distributions are number of invites, acknowledgements, ok, bye and busy. The ratio of number of senders and receivers can give us an insight to the number of participants. These features will be generated by the feature extraction module.

Considering classifiers, a non parametric regression analysis method will be carried out. Method is based on spline known as Multivariate Adaptive Regression Spline (MARS). The main reason to use this model is it can model non-linearity over different intervals. They are more flexible than linear regression model. They are sufficiently flexible to model non linearity and interactions of variable. MARS can estimate the functions themselves even though it has severe constraints on the function nature while nonlinear regression techniques are used to estimate the parameters of the underlying function which are known. Also, they require little or no data preparation. Outlier effect is contained by the use of hinge functions in the model. They have a good bias variance tradeoff.

MARS approximates the model by using a combination of linear truncated basis functions. Multivariate Adaptive Regression Splines model can be represented by

$$f_M(x) = c_0 + \sum_{i=1}^{k} c_i B_i(x) \tag{4.1}$$

where c_i and c_0 are coefficients and $B_i(x)$ are basis functions.

A hinge function is defined by a variable and a knot. A hinge function is of the form

$$max(0, x - k) \quad or \quad max(0, k - x) \qquad (4.2)$$

where k is a constant called knot. The algorithm comprises of two stages

1. **Forward Pass**

   It starts with a model consisting only of intercept term. Then, adds a pair of basis functions with minimum sum of squares residual error, repeatedly. This pair is identical but uses a different side of a mirrored hinge function. Variable or in our case we can say features/attributes are used to select a new basis function. The values of attributes are searched for selection of knots. This stage continues unless the change in the residual error is too small or maximum number of terms has reached.

2. **Backward Pass**

   During backward pass a more generalized model is created from the model built during forward pass. The model built in forward pass is usually an over-fitted model which is then pruned. A submodel is obtained by removing the terms one at a time and deletes the least effective term. Submodels are compared using Generalized Cross validation criteria.

Figure 4-2 shows the flowchart of the algorithm of MARS. It is used to detect the attack and results are compared with the work in literature and some other classification techniques described below in detail.

4.2 Classification Techniques

4.2.1 K-NN

K-NN was first introduced by E. Fix and J. Hodges [31]. It is a supervised learning method used for classification purpose. An object is classified by majority vote of its neighbors. That object is assigned to the class most common amid its k- nearest neighbors. This method is based on the Euclidean distance between the training and testing data.

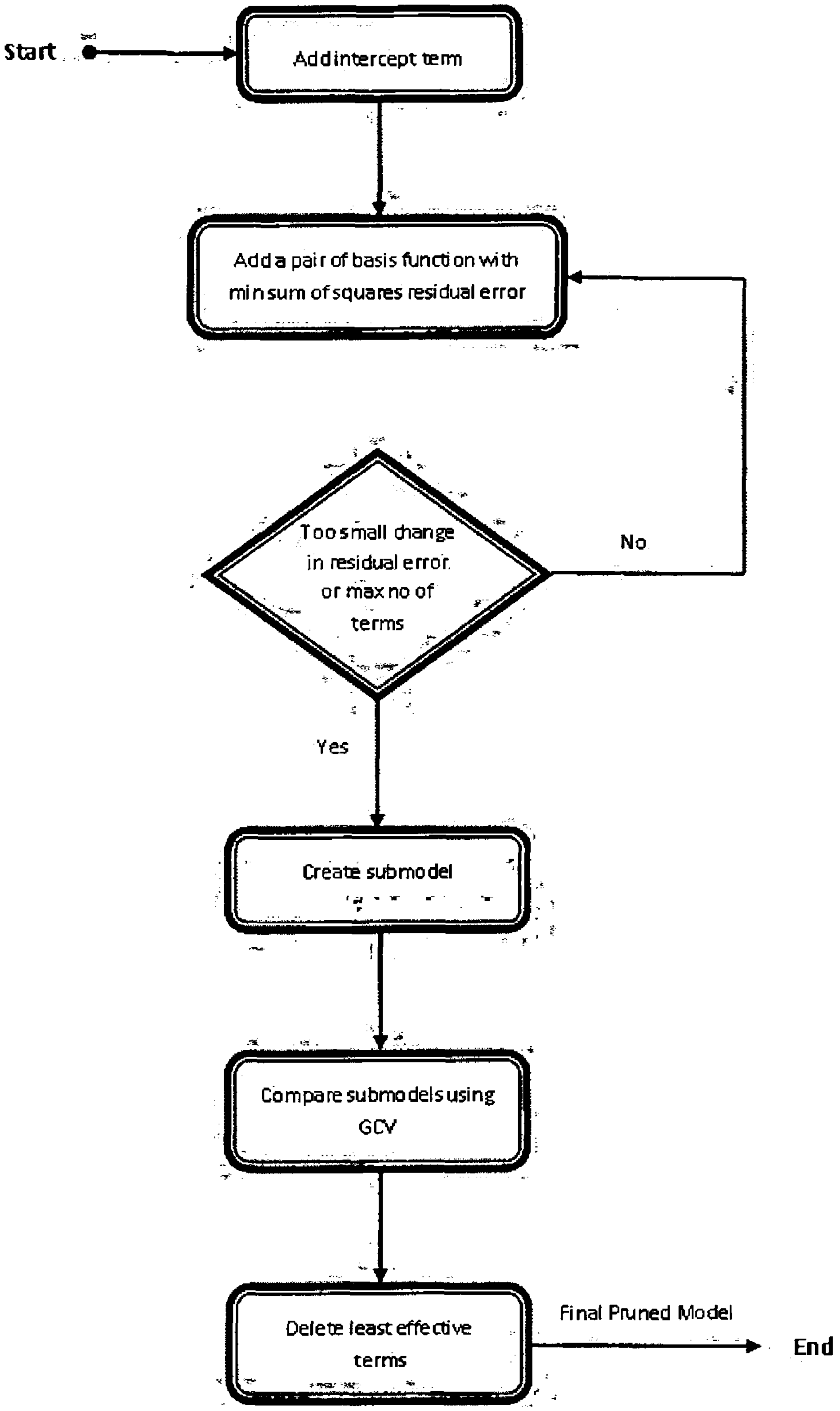

Start
Add intercept term
Add a pair of basis function with min sum of squares residual error
Too small change in residual error or max no of terms
No
Yes
Create submodel
Compare submodels using GCV
Delete least effective terms
Final Pruned Model
End

Figure 4-2 Flow chart of Multivariate Adaptive Regression Spline Algorithm

Method

The basic aim of this clustering method is to separate the data based on the resemblances among the different classes. For each point in the datasets, a distance measure is assigned. The distance metric applied is the Euclidean Distance which is given by

$$d = \sqrt{\sum_{j=0}^{n}(x_j - y_j)^2} \tag{4.3}$$

A distance matrix is computed from the calculated distances between the all possible combinations of the points (x, y). Each data point within the data set has a class label in the set, $L = \{l_1, l_2, \ldots l_n\}$. The distance matrix is then analyzed to determine the k-closest neighbors, where k is the number of neighbors. The most common class label among the set is then searched by examining the k-closest data points and that label is assigned to the data point being analyzed [32].

If for a particular data point two or more classes appear for an equal number of times, the test is run for $k-1$. If there is again a draw, K-NN is run on $k-2$. It is a recursive process. In case of the tie it will continue until $k=1$, and then there will be only one class that will represent the testing data point.

In Figure 5-1, the green circle data point has to be classified among the blue squares class or to the red triangles class. For $k=3$, it will be classified to the triangles class as inside the inner circle there is only one square and two triangles [33].

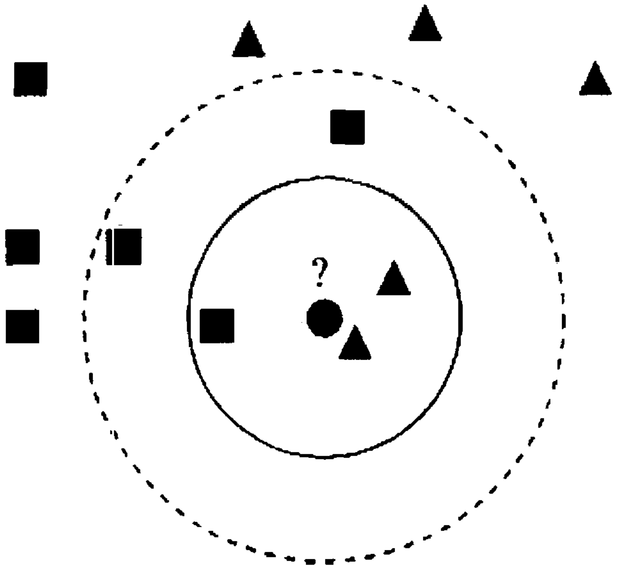


Figure 4-3 K-NN Classification [33]

Parameter Selection

A good choice of k depends upon the data. It can be selected by using cross validation method. By using the large values of k, the effect of noise is reduced on the classification but the drawback is that boundaries between the classes become less distinct [34].

The accuracy of the K-NN is degraded by the noisy data or the irrelevant features. It also becomes computationally intensive when the size of data becomes large. The size of k also affects the efficiency of the K-NN.

4.2.2 Naïve Bayes

Bayes theorem was developed by Thomas Bayes in 18thcentury, who did a lot of research in probability and decision theory.Bayes' theorem is used to calculate the probability that a certain event will occur or that a certain proposition is true, given that a related piece of information is already known [33].

Naive Bayes classifier is a versatile machine learning algorithm. It uses probabilistic approach based on bayes theorem assuming strong (naive) independence.It is a supervised learning algorithm possessing the advantage of requiring small amount of training data for parameters estimation. The algorithm supposes that a certain feature of a class presence is unrelated to the presence of any other feature. Classification data consists of a set of attributes where each attribute can take on a number of possible values. Then, data is classified into a single classification [35] [36].

Given the features calculate the probability that the given specimen belongs to a particular class. Given x it chooses the class with highest posteriori class probability.

The Baye's theorem is stated as

$$P(y|x)P(x) = P(x|y)P(y) \tag{4.4}$$

$$P(y|x) = \frac{P(x|y)P(y)}{P(x)} \tag{4.5}$$

where P(x) and P(y) are prior probabilities of x and y respectively. P(y|x) is the conditional probability also known as posterior probability of y.

To identify the best classification for an instance of data $D = (d_1, \dots d_n)$. The posterior probability of each class is calculated:

$$P(c_i | d_1, \dots d_n) \qquad (4.6)$$

where c_i is the ith class among a set of |C| classes. Class with the highest posterior probability known as *maximum posteriori* is selected as a correct classification.

Bayes theorem can be used to calculate the posteriori probability and can be written as

$$\frac{P(d_1, \dots d_n | c_i).P(c_i)}{P(d_1, \dots d_n)} \qquad (4.7)$$

As $P(d_{1,}.. d_n)$ is a constant independent of c_i, it can be eliminated and aimed to find the classification c_i for which the following is maximized:

$$P(d_1, \dots d_n | c_i). P(c_i) \qquad (4.8)$$

The naïve Bayes classifier assumes that each of the attribute is independent of the others, in that scenario $P(c_i | d_1, \dots d_n | c_i)$ can be rewritten as

$$P(c_i). \prod_{j=1}^{n} P(d_j | c_i) \qquad (4.9)$$

The naïve Bayes classifier picks a class for a data set by finding the classification c_i for which the value of above equation is a maximum.

$$max(P(c_i). \prod_{j=1}^{n} P(d_j | c_i)) \qquad (4.10)$$

4.2.3 Decision Tree

A decision tree is tree-like graph or model of decisions and their possible outcome. They are also known as classification trees or regression trees. In a decision tree, leaves represent classifications and branches represent sequence of features that guide them to the classifications.

It splits data into subsets based on some rules. Initially, the data is split into a number of groups by first rule. The tree represents it as branches from a root node. Then another rule to a subset is applied, so a second generation of sunsets is formed by applying a different rule to a different subset. These following splits are represented as branches (edges) originating from older branches nodes. A final subset of data is formed by either splitting or leaving a subset as it is. The unsplit nodes take form of leaves in tree which must be analogous to some target measure [37].

Decision trees can accept categorical and interval variables (consists of values that can be averaged). They are robust in case of missing values and distribution assumptions. There is some disadvantage of decision tree too like when input data and output targets contain no simple relationship, tree constructed is too simple. Even though it is accurate, it may not be the only one accurate description.

CART

CART uses recursive partitioning to create a tree. The important features of this method are surrogate splits used for missing values of input data prior probabilities incorporated during splitting, heuristic search for a split on linear combination of variables. It can be used to analyze either continuous or categorical data [37].

Regression tree can be created by using subsequent approach. Initially, a variable is selected which can split best. It creates a binary split on input data. Maximum splitting measure is obtained by performing an exhaustive search. Splitting criteria can be described as a rule to maximize the sum of squares subsets. For each variable X, a subset S that minimizes the sum of node impurities in the two child nodes and choose the split $\{X^{*} \square S^{*}\}$ that gives minimum overall X and S.CART uses GINI index as impurity function. It is generalization of binomial variance. During calculation of split measure, if a missing value in the input data case occurs then it is excluded. In such cases, surrogates rule are applied for assigning them to a branch. Before analyzing data, an appropriate threshold value to stop the tree building process cannot be identified, thus a retrospective cost complexity pruning is applied. First a large tree is built then, a subtree is found among it, then from this subtree another subtree is found. This process goes on until the smallest subtree consisting only of the root node is formed. A subtree among the sequence of subtrees with the same number of leaves has the smallest overall cost [38] [39] [40].

By using the costs calculated from cross validation or an independent validation dataset, a final pruned tree is selected.

Impurity function can be defined as the proportions of the learning sample data belonging to the possible classes of the response variable. If these proportions are denoted by$r_1, r_2, \dots, r_{j-1}, r_j$, then Gini Index can be defined as

$$g(r_1, \dots, r_j) = 2\sum_{j=1}^{J-1}\sum_{j'=j+1}^{J} r_j^2 \tag{4.11}$$

C4.5

The algorithm was developed by Quinlin, which is an improvement to ID3 also developed by him. It also uses heuristic approach to build the tree just like CART. But the impurity function used for splitting criteria is based on entropy. The entropy function can be expressed as

$$h(r_1, \dots, r_j) = -\sum_{j=1}^{J} r_j log r_j \tag{4.12}$$

where $r_1, r_2, \dots, r_{j-1}, r_j$ are proportions of the learning sample data belonging to the possible classes of the response variable [38].

4.2.4 Multivariate Adaptive Regression Splines

Multivariate adaptive regression splines (MARS) was developed by Jerome Friedman which is a multivariate non-parametric technique of regression analysis. It models non linearities and interactions. It does not assume or impose a particular functional relationship between the independent and dependent variables but creates it from a set of coefficients and basis functions. Methodology uses divide and conquer approach to find the regression equations.

Splines are defined as piecewise polynomial functions of degree $p > 0$. Knots are the breakpoints indicating the transition from one polynomial to the next. A MARS model considers polynomial degree, knots and the location of knots for creation of a model. Basis functions are linear truncated power functions. Some basis functions are numerically more stable than others, thus permits fit computation with high accuracy. Also fit computed by the model, is not affected by the change of basis functions. MARS approximates the model by using a combination of linear truncated basis functions. Multivariate Adaptive Regression Splines model can be represented by

$$f_M(x) = c_0 + \sum_{i=1}^{k} c_i B_i(x) \tag{4.13}$$

where c_i and c_0 are coefficients and $B_i(x)$ is basis function [33][42]. The function is a product of two or more of hinge functions to allow for the interactions.

Initially, MARS algorithm builds model consisting of large number of basis functions. This model overfits the data. Then, pruning is carried out; basis functions with lesser contribution are removed. MARS model building begins with a constant basis function which is mean of response values. Then one by one it adds a pair of basis function that gives small residual error by considering all pairs of new basis functions[42][43]. It finds all likely knot value for each variable. This procedure ends when a minimum value of error or specific model size is reached. This model is then pruned. During pruning, basis functions that do not contribute adequately are deleted from the model function. For this purpose generalized cross validation (GCV) is used.

$$GCV(S) = \frac{\sum_{i=1}^{N}[y_i - f_S(x_i)]^2}{N[1-(C(S)/N)]^2} \tag{4.14}$$

where *C(S)* is the cost complexity of *S* basis functions and N is the number of observations. Missing values are handled by dummy variables. They can reliably track complex data structures.

4.3 Summary

In this chapter, we have proposed the solution for the problem identified from literature survey. The SIP network traffic flow is stored in queue, from which we calculate a feature vector. This feature vector is presented to classifier for classification. We have used four classifiers in our study; K-NN, Naïve Bayes, Decision Tree and MARS. The working of these classifiers is discussed briefly.

Chapter 5 Experimental Results

Chapter 5 discusses the various parameters of our experiments and results of our investigation. Section 5.1 gives an overview of the dataset used. Section 5.2 defines the performance measures. Section 5.3 discusses the window size used. Section 5.4 defines the features extracted from the SIP network trace. Section 5.4 depicts the results of various classifiers used.

5.1 Dataset

In order to evaluate the results of techniques based on learning, there is need of labeled dataset. To obtain data from the service providers is difficult as they are bound by user privacy agreements. SIPp is a tool mostly used by researchers to generate the SIP traffic. In a XML routine, call flow scenarios are expressed. According to this XML file SIP traffic is generated. Thus, it is a convenient practice for evaluating stress conditions at servers and benchmarks. In spite of this, SIPp tool is yet not able to emulate the real SIP traffic. Because, it is more oriented towards the transaction layer rather than the call layer. In [44] generated a labeled dataset to be used to compare different detection techniques. VoIP traffic is generated in a controlled environment. Profiled emulated users based on a social model are used to generate the normal traffic and the Inviteflood tool is used to launch SIP flooding attacks and Spitter to generate the SPIT attacks. In our experiment dataset of Asterisks SIP network is considered. Three types of files are provided, network traffic, server logs and call detail record.

5.2 Performance Metrics

Performance is measured using detection accuracy and false positive rates. Accuracy is defined as

$$Accuracy = \frac{Number\ of\ correctly\ classified\ instances}{Total\ number\ of\ attack\ instances} * 100 \qquad (5.1)$$

$$Detection\ Accuracy = \frac{Number\ of\ correctly\ classified\ attack}{Total\ number\ of\ attack\ instances} * 100 \qquad (5.2)$$

$$False\ Positive\ Rate = \frac{Number\ of\ instances\ classified\ as\ attack}{Total\ number\ of\ normal\ instances} * 100 \quad (5.3)$$

We need to consider both detection accuracy and false positives because if all the data is classified as attack we may get 100% detection accuracy but also very high false positive rate and the accuracy achieved will be above or below 50 depending on percentage of normal and attack data. Similarly, if all data is classified as normal, detection accuracy will be zero and false positive rate will be zero.

5.3 Benchmark

Results achieved using the proposed approach will be compared with the work presented by authors in [27]. They have proposed Support Vector Machine for identification of flood attacks of various intensities. Detection Accuracy achieved by the author for different level of intensity attacks is shown in Table 5-1.

Table 5-1 Benchmark Detection accuracy

Attack Intensity	Detection Accuracy
1	1.48
10	60.13
100	88.82
1000	98.24

5.4 Window Size

The window for evaluating features can be either fixed or variable. In this experiment, fixed window will be used. In online monitoring, the window size plays an important role. A window size of 30 packets is proposed in [27]. We have carried out our own analysis as well. We performed experiments using 20, 30 and 40 window size. The classifiers used in the study are decision tree and Multivariate Adaptive Regression Spline (MARS). Results obtained are shown in Table 5-2.

Table 5-2 Accuracy for different window size

		Accuracy		Detection Accuracy		False Positive Rate	
Intensity/ Sec	Window	Decision Tree	MARS	Decision Tree	MARS	Decision Tree	MARS
1	20	79.11	89.55	38.93	69.40	0	0
	30	76.47	90.19	31.03	71.26	0	0
	40	76.56	84:89	31.81	56.06	0	0
10	20	98.94	99.25	100	100	1.89	1.26
	30	95.35	100	89.55	100	0.95	0
	40	96.89	99.22	100	100	5.06	1.26
100	20	100	100	100	100	0	0
	30	98.15	100	88.13	100	0	0
	40	100	100	100	100	0	0
1000	20	96.64	96.64	0	0	0	0
	30	99.90	100	100	100	0.10	0
	40	98.86	100	68.67	100	0	0

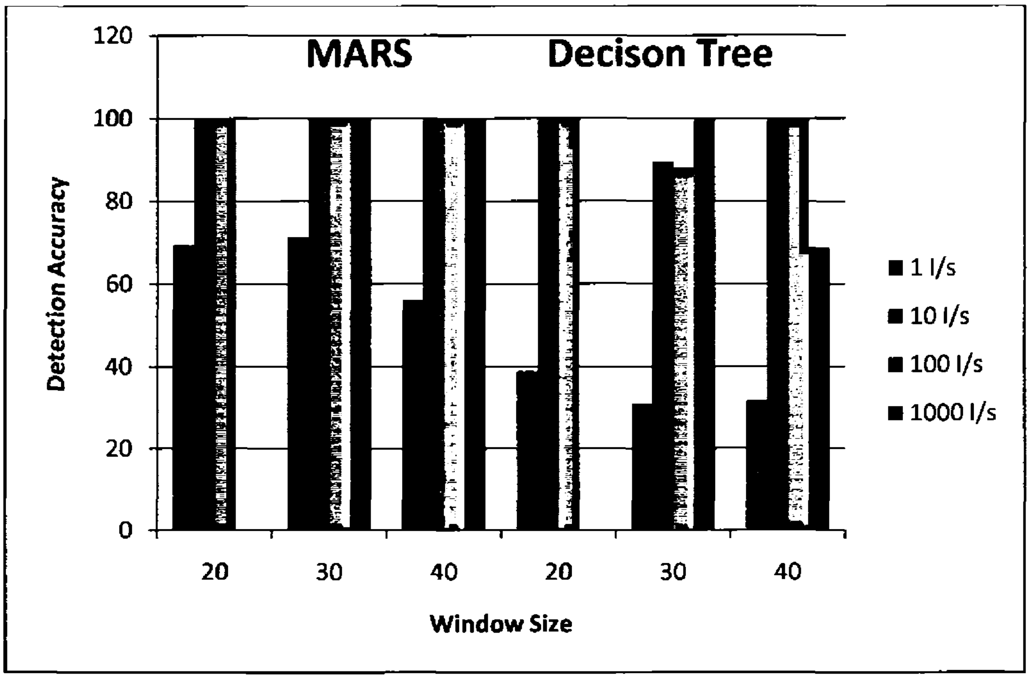


Figure 5-1 Detection Accuracy achieved using different window size

We can see that detection accuracy for low intensity attacks increases with smaller window size. But using small window size, detection accuracy of high intensity attacks is decreasing. Although with larger window size, stealthy attacks does not show same level of detection accuracy but high intensity attacks are detected with good accuracy.

5.5 Feature Extraction

A set of features is used to analyze the incoming SIP messages. A feature vector is calculated from a window. The features are based on general statistics. They give us an insight on the type of messages received and their ratio. These features are shown in Table 5-3. The energies of these features are normalized between -1 and 1.

Table 5-3 Features of SIP

Name	*Description*
Duration	Total time of the slice
NbReq	Number of requests/ Total number of messages
NbResp	Number of response/ Total number of messages
NbSdp	Number of sdp/ Total number of messages
AvInterReq	Average inter-arrival of requests
AvInterResp	Average inter-arrival of requests
NbInv	Number of Invites/ Total number of requests
NbBye	Number of Bye/ Total number of requests
NbAck	Number of Bye/ Total number of requests
NbBusy	Number of Busy/ Total number of responses
NbOk	Number of Ok/ Total number of responses
NbRatio	Number of Senders/Number of Receivers

5.6 Classification Results

Feature Extraction phase is followed by Classification phase or Detection Phase. As previously stated, in this phase classifier is trained by using the extracted features as data. After training phase, the testing is carried on. Some features are presented to the classifier and it attempts to recognize the attack.

5.6.1 Results for KNN

Results for KNN were obtained using different number of clusters. KNN is trained on 10 invites/sec data; half of the data is used for training. The remaining half is used for testing 10invites/sec intensity attack. The results are shown in Table 5-4.

Table 5-4 Results of K-NN for 100 Invites/sec

Clusters	Accuracy	Detection Accuracy	False Positives Rate
3	85.75	55.93	8.75
5	85.48	54.24	8.75
7	86.02	52.54	7.81

Results for 1000 invites/sec using different number of clusters is shown in Table 5-5.

Table 5-5 Results of K-NN for 1000 Invites/sec

Clusters	Accuracy	Detection Accuracy	False Positives Rate
3	97.72	33.33	0
5	97.81	36.11	0
7	97.72	33.33	0

When presented with 10 invites/sec for testing, results obtained are depicted in Table 5-6.

Table 5-6 Results of K-NN for 10 Invites/sec

Clusters	Accuracy	Detection Accuracy	False Positives Rate
3	83.72	62.68	2.8
5	82.55	61.19	3.81
7	83.14	59.70	1.90

Results for 1 invite/sec testing are shown in Table 5-7.

Table 5-7 Results of K-NN for 1 Invites/sec

Clusters	Accuracy	Detection Accuracy	False Positives Rate
3	76.07	31.03	0.59
5	75.29	29.88	1.19
7	74.51	25.28	0

Figure 1-1 shows the combined result for different intensity attacks.

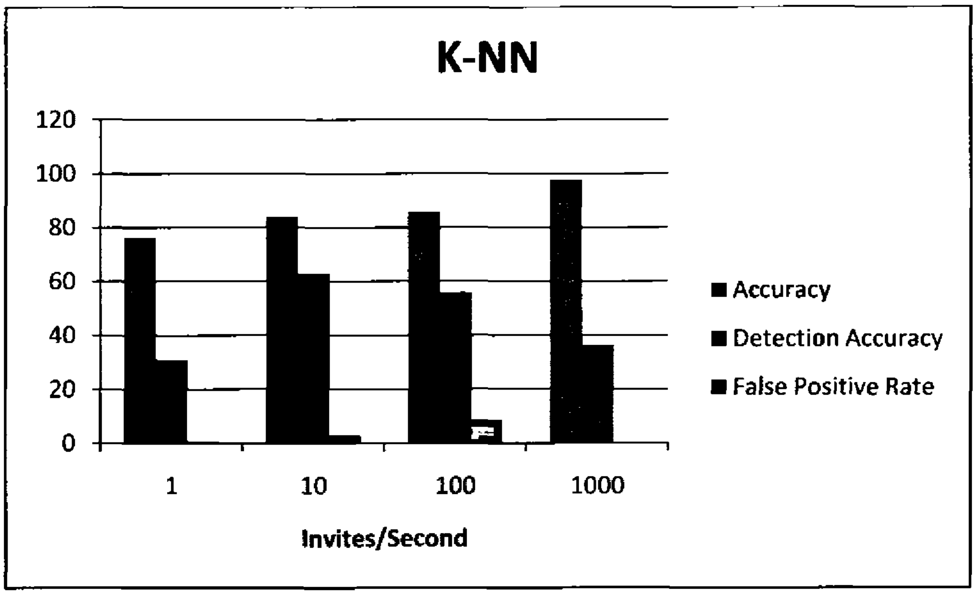


Figure 5-2 Results of K-NN classifier

5.6.2 Results for Naïve Bayes Classifier

The data was of 10 invites per second data was split into two halves; one was presented for training the classifier while other half for evaluation. In this case results for Invite Flood attacks of different intensities were as shown in Table 5-8.

Table 5-8 Results with Naïve Bayes Classifier

Invites/sec	Accuracy	Detection Accuracy	False Positives Rate
1	50.19	100	75.59
10	59.88	94.02	96.15
100	49.34	74.58	55.31
1000	82.91	72.22	16.71

5.6.3 Decision Tree Results

The classification and regression tree is used with GINI index as splitting criteria. Invite flood attack with 100 intensity is chosen as critical point and thus classifier is trained on it. The results obtained are given in the Table 5-9.

Table 5-9 Results using CART

Invites/sec	Accuracy (%)	Detection Accuracy (%)	False Positives (%)
1	76.47	31.03	0
10	95.35	89.55	0.95
100	98.15	88.13	0
1000	99.90	100	0.10

5.6.4 MARS

Multivariate Adaptive Regression Spline can model non linearities. First training of classifier was carried out and then it was tested for various intensity attacks. Results are shown in Table 5-10. The model was created in less than 3 second.

Table 5-10 Results with MARS

Invites/sec	Accuracy	Detection Accuracy	False Positive Rate
1	90.19	71.26	0
10	100	100	0
100	100	100	0
1000	100	100	0

5.7 Comparison

Results obtained for accuracy using above classifiers are compared in Figure 5-3. In case of 10,100, 1000 invites per second intensity attacks MARS achieves the highest accuracy and K-NN has the lowest. In case of 1 invite per second intensity attacks, although Naïve Bayes shows the best results among other classifiers but when we take into account other factors, accuracy results don't please us.

Decision tree shows good results on the 10 intensity per second attacks on which it is trained and on higher than that. While the performance on low intensity attacks, is not very good.

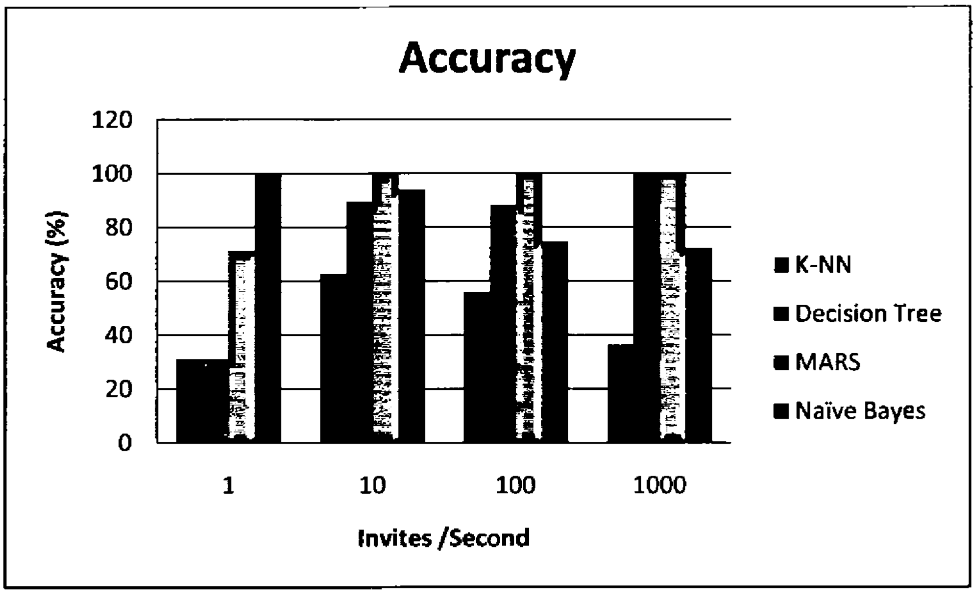


Figure 5-3 Accuracy of classifiers

Detection Accuracy of the classifiers is depicted in the below Figure 5-4. Except Naïve Bayes, other classifiers show promising detection accuracy. Decision tree and MARS have nearly same detection accuracy for 10, 100 and 1000 intensity attacks. But in case of low intensity attack, MARS performs much better while k-nn and decision tree achieves nearly same detection accuracy.

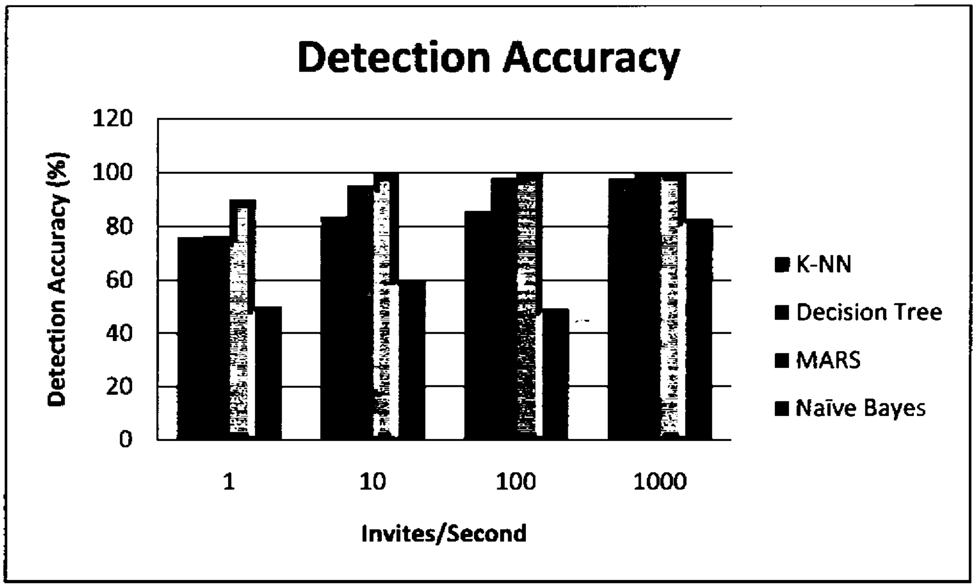


Figure 5-4 Detection Accuracy of classifiers

When we compare false positives, Naïve Bayes has the highest false positive rate which is not acceptable. MARS generates zero positive alarms. Decision tree shows very low false alarms. Figure 5-5 shows comparison of False Positive rates of classifiers used in this study.

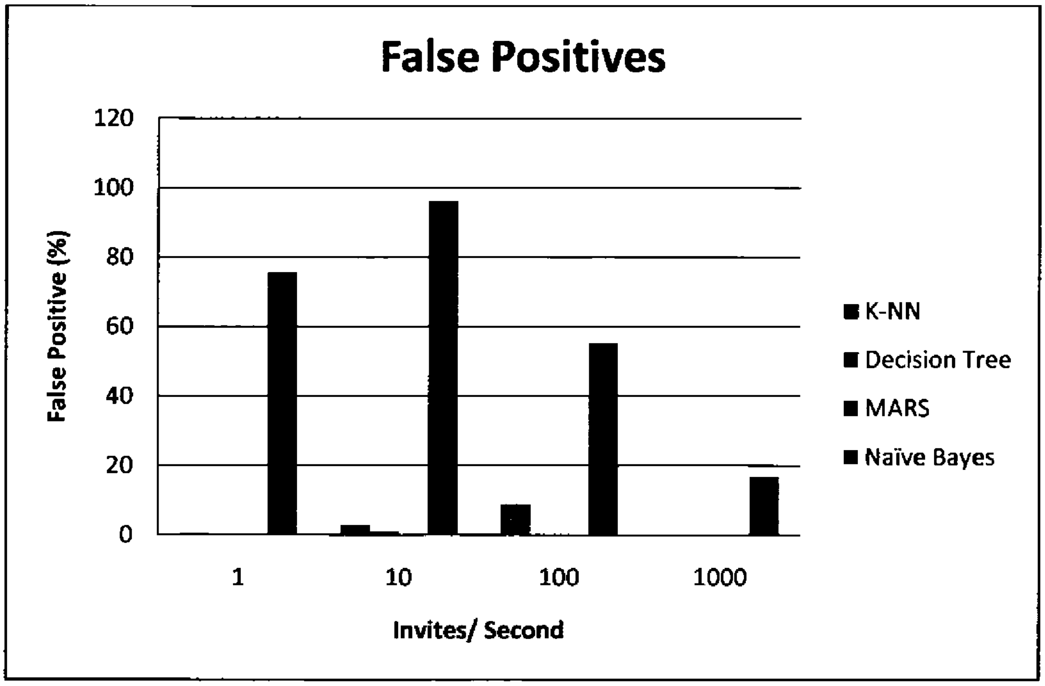


Figure 5-5 False Positive Rate of Classifiers

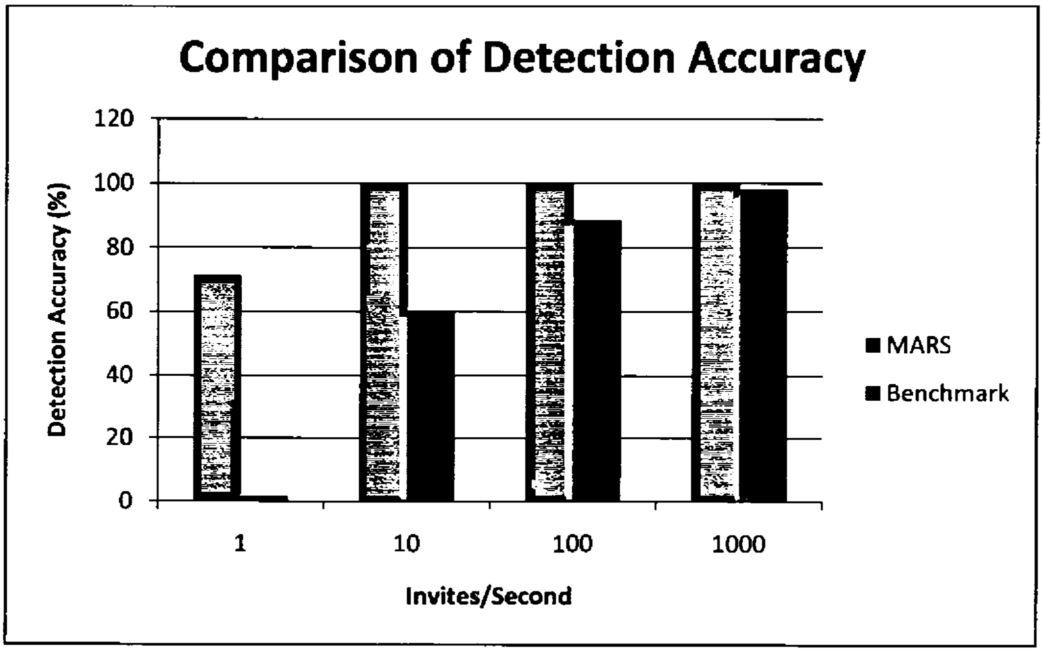


Figure 5-6 Comparison of detection accuracy of proposed approach with Benchmark

Figure 5-6 shows comparison of the detection accuracy of proposed classification approach, MARS, with the benchmark. Multivariate Adaptive Regression Spline performs far well in case of low intensity attacks than the benchmark. It also performs better in other cases as well.

False Positive Rates are not provided by the author therefore; comparison of false positive rate with the benchmark could not be performed.

5.8 Summary

In this chapter, the dataset used and the features extracted for the experiments is discussed. Then, we have presented the results of the experiment carried out and compared the results. K-NN performs well with low false alarms generated. Naïve Bayes performance, in terms of false alarms generated, is not acceptable. Techniques based on regression have shown good results; high detection rate low false alarms.

Chapter 6 Conclusions and Future Work

6.1 Conclusions

With the passage of time, network intrusion attacks are increasing. Thus, intrusion detection has become a vital task. Denial of Service attacks on SIP is a major issue. Our work deals with different low and high intensity of attacks. The labeled dataset used consists of normal data and invite flood attacks of 1, 10, 100 and 1000 invites per second.

SIP packets are stored in a queue from which feature vector is computed later on. A feature vector is computed from a window of 30 packets by feature extractor. The window size was selected after performing experiments. This feature vector was presented to a trained classifier which identifies it either as a normal or an attack. Results are obtained using different classifiers for invite flood attack detection.

Classifiers are trained with a mixed trace of 10 invites per second. The data is divided into two halves; one is used for training and other was used for testing the performance of the classifier. Also, the trained classifier is tested on 1, 100 and 1000 invites per second intensity data.

Naïve Bayes performance was not acceptable although the detection rate is sufficient but the false positive rate is very high. It assumes that features are independent and in intrusion detection case it is not true. The correlation among the features degrades the performance of Naïve Bayes. Results obtained using K-NN has very low false positives but the detection accuracy percentage is approximately 50.Theoretically, classification time is zero.

Performance of classification and regression is fairly good. The tree correctly detects the attacks of certain threshold on which it is trained and higher than that. The attacks lower than the certain threshold on which it is trained have a detection accuracy of 43.67%. The false positives are very low. Multivariate Adaptive Regression Spline showed excellent results. It identifies different intensity attacks and without any false positives. As this classifier can model non linearity without considering any underlying relation, it shows promising results.

The time to create a classification and regression tree and Multivariate Adaptive Regression Spline is about 30 seconds. The classification time is less than 1 second.

6.2 Future Work

Our work deals with the Invite flood attacks of different intensities and shows promising results. In future, some other features of SIP can be analyzed. Also, a feature selection technique can be applied, for picking those features that contributes more in the detection of malicious activity. The work can be carried out on SPAM and other SIP attacks using these techniques. Also, the work on a standard database for other SIP attacks should be carried out. So that, researchers are able to perform analysis on a standard dataset and their results can be compared.

References

[1].Neil Kinder, *"IMS-IP Multimedia Subsystem IMS Overview and the Unified Carrier Network"*, Published by *Sonus* Networks, 2005.

[2].Ericsson, "IMS-IP Multimedia Subsystem, The value of using the IMS architecture", White Paper, Oct 2004.

[3].I. Dalgic, H. Fang, *"Comparison of H.323 and SIP for IP Telephony Signaling"*, Published by 3Com Corporation, Technology Development Center, M/S 3219, Santa Clara, CA 95052.

[4].SIP, VoIP-info.org, A reference guide to all things VOIP, http://www.voip-info.org/wiki/view/SIP, Nov 2011.

[5].Intoduction to SIP (Session Initiation Protocol) A made easy tutorial, http://www.siptutorial.net/SIP/, July 2009.

[6].J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson,R. Spark, M. Handley, and E. Schooler, *"Session Initiation Protocol"*, RFC 3261, 2002.

[7].SIP Signaling. SIP Center, Available: http://www.sipcenter.com/sip.nsf/html /SIP+Signaling, Jan, 2007.

[8].A. Johnston *"SIP: Understanding the Session Initiation Protocol"*, Second Edition. Artech House, Inc., Norwood, MA, USA, 2003.

[9].P. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandz, E. Vazquez, *"Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges"* ScienceDirect Computers & Security, Volume 28, Issues 1-2, pp 18-28, February-March 2009.

[10]. S. Xiaonan Wu, W. Banzhaf, *"The use of computational intelligence in intrusion detection systems: A review"*, Applied Soft Computing, Vol. 10, Issue 1, pp 1–35, January 2010.

[11]. M. A. Faysel, and Syed S. Haque, *"Towards Cyber Defense: Research in Intrusion Detection and Intrusion Prevention Systems"*, International Journal of Computer Science and Network Security (IJCSNS), Vol.10, Issue 7, pp. 316-325, July 2010.

[12]. Xiao H. Yao, *"A Network Intrusion Detection Approach combined with Genetic Algorithm and Back Propagation Neural Network"*, International

Conference on E-Health Networking, Digital Ecosystems and Technologies, pp 402-405, IEEE 2010.

[13]. N.B. Amor, S. Benferhat, Z. Elouedi, *"Naive Bayes vs Decision Trees in Intrusion Detection Systems"*, In Proc. Of 2004 ACM Symposium on Applied Computing, pp 420-424, 2004.

[14]. Ying Zhao, Zhigao Zheng, Hong Wen, *"Bayesian Statistical inference in machine Learning Anomaly Detection"*, 2010 International Conference on Communications and Intelligence Information Security, Issue Date: 13-14 Oct, pp 113-116, IEEE 2010.

[15]. D. Md. Farid, Nguyen Huu Hoa, J. Darmont, N.Harbi, and M. Z. Rahman, *"Scaling Up Detection Rates and Reducing False Positives in Intrusion Detection using NB Tree"*, International Conference on Data Mining and Knowledge Engineering (ICDMKE 2010), Rome, Italy, 2010.

[16]. G. Stein, B. Chen, A. S. Wu and Kien A. Hua, *"Decision Tree Classifier for Network Intrusion Detection with GA-based Feature Selection"*, proceedings of the 43rd annual Southeast regional conference. Kennesaw, Georgia, 2005.

[17]. T. Phuoc Tran, L. Cao, D. Tran and Cuong Duc Nguyen, *" Novel Intrusion Detection using Probabilistic Neural Network and Adaptive Boosting"*, International Journal of Computer Science and Network Security (IJCSIS), Vol 6, pp 83-91, 2009.

[18]. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson,R. Spark, M. Handley, and E. Schooler. *Session Initiation Protocol, RFC 3261*, 2002.

[19]. G. Camarillo and M.-A. Garcia-Martin, *"The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds"*, John Wiley & Sons, 2006.

[20]. S. Ehlert, C. Wang, T. Magedanz and D. Sisalem, *"Specification-based Denial-of-Service Detection for SIP Voice-over-IP Networks"*, The Third International Conference on Internet Monitoring and Protection, pp 59-66, IEEE 2008.

[21]. F. Al-Moussa, P. Mudhar and A. Jones, *"Overview of SIP attacks and Countermeasures"*, Lecture Notes of the Institute for Computer Sciences,

[35]. Ben Coppin, *Artificial Intelligence Illuminated,* 1st Edition, Jones and Bartlett Publishers, ISBN 0-7637-3230-3, United States of America, April 2004.

[36]. George F. Lugar, *"Artificial Intelligence Structures and Strategies for Complex Problem Solving"*, Pearson Addison Wesley, Edition 4, ISBN-13: 978-0-321-54589-3, July 2001.

[37]. Padraic G. Nevill, *"Decision Trees for Predictive Modeling",* SAS Institute Inc., 4 August 1999.

[38]. Clifton D. Sutton, *"Classification and Regression Trees, Bagging, and Boosting"*, Handbook of Statistics, Vol. 24, pp. 303-329, Elsevier, 2005.

[39]. T.Bartz–Beielstein, S. Markon, *"Tuning Search Algorithms for Real-World Applications: A Regression Tree Based Approach",* Evolutionary Computation Congress, Vol 1, pp. 1111 - 1118, June 2004.

[40]. Wei-Yin Loh, *"Classification and regression trees"*, John Wiley & Sons, Inc. WIREs Data Mining Knowledge Discovery, Vol 1 pages 14-23, jan/feb 2011.

[41]. Jerome H. Friedman, *"Multivariate adaptive Regression splines"*, The analysis of Statistics, Vol 19, pp. 1-67, 1991.

[42]. T. Lee, C. Chiu, Y. Chou and Chi-Jie Lu, *"Mining the Customer Credit Using Classification and Regression Tree and Multivariate Adaptive Regression Splines"*, Computational Statistics & Data Analysis, Volume 50, Issue 4, pp. 1113–11304 February 2006.

[43]. Issa F. Zakeri, Anne L. Adolph, Maurice R. Puyau, Firoz A. Vohra and Nancy F. Butte, "Multivariate adaptive regression splines models for the prediction of energy expenditure in children and adolescents", Appl Physiol 108, pp. 128-136, 2010.

[44]. M. Nassar, R. State, and O. Festor, *"Labeled VoIP Data-set for Intrusion Detection Evaluation"*, In Proceedings of the 16th EUNICE/IFIP WG 6.6 conference on Networked services and applications: engineering, control and management, pp. 97-106, 2010.

[45]. Absolute Astronomy, http://www.absoluteastronomy.com/topics/Session_Initiation_Protocol, 2011.