CHAPTER 1

INTRODUCTION

The information stored in the organization plays a vital role in determining the success rate of the organization. When information stored in the computer is targeted for attack, the network in which the computer lies and the computer itself becomes the victim of the attack. Some of the major assets that are focused for attack are financial planning and design data, information related to the company's competitive position in the market, company's top secrets including shares and predicted share prices, company's yearly predicted benefits and the financial forecasting, intellectual properties including the baseline processes, methods and proprietary data and other intangible assets, personal identification and authorization information.

Intrusion detection is the most effective way to detect intrusions by using the audit data generated by the operating system. Since almost all activities are logged in a system, it is possible that a manual inspection of these logs would allow intrusions to be detected. A very important entity of the intrusion detection is the audit data used for analysis. It is essential to analyse the audit data even after an attack has occurred to determine the extent of damage occurred. This analysis also helps in tracking down the attacks and in recording the attack patterns for future detection. A good Intrusion Detection System (IDS) that can be used to analyse audit data becomes a valuable security tool for information systems.

Intrusion Detection Systems are defined as (Carl endorf et al 2006) tools, methods and resources help to identify, assess and report unauthorized and unapproved network and host or do both due to insider and outsider threats. The placement of IDS in the network can be done after the firewall and before the router. Another place of IDS may be before the firewall to completely stop external intrusions. On every system of the network the Host IDS can be placed along with the Network IDS to have more effective protection.

The audit data used for analysis in intrusion detection systems are host level audit files, event log entries, real time process lists, key press sequences, system call sequences (Animesh Patcha and Jung-Min Park 2007), command sequences, sniffed network traffic, application log files, file system states, system service scripts, output of statistical or protocol analyser and IDS sensor alerts, mails and messages (Mohammad et al 2001). Based on the method of applying the audit data there are two variants of intrusion detection, namely Misuse detection (Ajith Abraham et al 2007) and Masquerader detection (Zhou Jian et al 2007). Misuse detection systems detect intrusions by comparing with the previously detected intrusions database with the present detection through pattern matching technique (Tzu-Fang Sheu et al 2010). Anomaly Intrusion Detection Systems are capable of detecting both known and unknown intrusions applying more sophisticated statistical techniques or Machine learning techniques (Mukkamala and Sung 2005, Dima Novikov 2010).

A main issue concerning misuse detection is to develop signatures that include all possible attacks that avoid false negatives, and to develop signatures that do not match non-intrusive activities to avoid false positive. Though false negatives are frequently considered to be more serious, the selection of threshold levels is important so that neither of the above problems

is unreasonably magnified. There are two types of IDS based on the data sources. Host-based intrusion detection systems attempt to detect computer intrusions by monitoring audits process which tracks all system calls (Animesh Patcha and Jung-Min Park 2007). Many modern operating systems provide audit trails for processes that run on the machine. On the other hand, Network-based system analyses data packets that travel over the actual network domains. These packets are examined and compared with empirical data and verify their nature to check whether it is malicious or benign.

A masquerade attack in which one user impersonates another is one type of computer abuse. Such attacks are often mounted by insiders and can be very difficult to detect. The idea behind masquerader detection is to establish each user's normal activity profile which is used as a baseline for detecting possible intrusion attempts. Automatic discovery of masqueraders is sometimes undertaken by detecting significant departures from normal user behaviour, as represented by user profiles based on users command histories. Masquerading is the act of substituting oneself for another. Masquerading is to disguise by assuming the appearance of someone or not. Sometimes it is furnished with a false appearance or an assumed identity or obscure the existence or true state or character of something. The computer masquerade problem can be explained in the following scenario. A legitimate user takes a break, leaving the terminal open, an interloper logged in during the users absence, and assumes the control of the keyboard, enters commands, taking advantage of the legitimate user's privileges and access to programs and data (Jian Zhou et al 2008).

1.1 METHODS OF INTRUSION

The methods of intrusion may be physical intrusion, system intrusion and remote intrusion. The intruders may get into the systems using software implementation bugs, buffer overflows, unexpected combinations of

commands, unhandled input sequences, improper system configuration, known default system configuration settings, lack of administrator attention to the initial attempts, creation of holes and honeypots, password cracking, sniffing unsecured network traffic, design flaws, unsecured network, TCP/IP protocol flaws and OS design flaws.

1.2 CHALLENGES FACED BY IDS

One of the major problems faced by IDS is huge number of false positive alerts that are mistakenly classified as normal traffic due to security violations. A perfect IDS does not generate false or irrelevant alarms. In practice, signature based IDS found to produce more false alarms than expected. This is because of the overly general signatures and lack of built in verification tool to validate the success of the attack. The huge amount of false positives in the alert log makes the process of taking remedial action for the true positives, i.e. successful attacks, delayed and labor intensive.

Same intrusion event can trigger hundreds of similar alerts. For example, a single network scan may cause to generate several alerts which differ by a small amount of time. These alerts can be fused together before passing on to human analyst. Also, different types of alert are having same underlying event as the root cause. Each attribute of all alerts can be generalized to find out the correlated alerts. This can help in the process of root cause analysis and hence eliminates more number of false positives. Alert generalization also helps to speed up alert verification some times. For example, suppose a large number of IIS exploit attack comes to port 80 of a particular machine which is running an Apache web server and Linux, obviously all of these can be marked as irrelevant since they are not successful.

An IDS inspects all inbound and outbound network traffic. When intrusive activity occurs, IDS let you know about that by making an alarm. It can generate false positives or false negatives. False Positive (FP) occurs when an alarm is generated for a normal activity. False Negative (FN) occurs when no alarm is there for an abnormal activity. Misuse detection is different from anomaly detection under IDS categories. In misuse detection it analyzes the information that it gathers and then it compares to large databases of attack signatures. In anomaly detection it monitors network segments to compare their state to normal baseline and look for anomalies. Misuse detection is particularly a difficult problem because of the extensive vulnerabilities of computer systems and the creativity of attackers.

1.3 DOS AND DDOS ATTACKS

Computer Security relies on three major characteristics confidentiality, integrity and availability. The threats compromising the availability of the resources are termed as Denial of Service (DoS) Attacks. Since the term Denial of Service expresses **'**Service Unavailability**',** it is often used in security research. Basically DoS attacks are targeting a single victim. The targeted victim may be a Server or a node. The targeted victims are usually compromised and controlled by the software such as Trinoo, Tribe Flood Network, TFN2K, Stacheldraht, Shaft and Mstream. DoS attacks may also be used to bring down all the nodes offering a particular service. DoS attack involving more than one computer or more than one network to mount an attack on a target in a coordinated manner is called Distributed Denial of Service (DDoS) attack (Malliga Subramanian and Tamilarasi Angamuthu 2010).

DDoS attacks pose serious threats to Computer and Network Security, in which victim networks are bombarded with a high volume of attack packets or traffic originating from a large number of machines

(Dong Seong Kim and Jong Son Park 2003). The aim of such attacks is to overload the victim with a flood of packets and make it incapable of performing normal services for legitimate users. In a typical three-tier DDoS attack, the attacker first compromises relay hosts called agents, which in turn compromise attack machines called zombies that transmit attack packets to the victim. Packets sent from zombie machines may have spoofed source IP addresses to make tracing difficult.

An Intrusion Detection System (IDS) is used to monitor network and system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable user policies, or standard security practices.

A DDoS attack is characterized by the explicit attempt by the attackers to bring down the service of the particular server using hundreds and thousands of machines all over the network. Then the attacker installs DDoS software on them, allowing them to control all these vulnerable machines to launch coordinated attacks on victim sites. These attacks usually exhaust bandwidth, router processing capacity, network stack resources or break network connectivity. Some examples are the attack attempt to flood a network, thereby preventing legitimate network traffic, disrupt connections between two machines, preventing access to a service, prevent a particular individual from accessing a service and disrupt service to a specific system or person (Jinu Kurian and Kamil Sarac 2010)

1.3.1 Real DDoS Attack Incidents

DDoS attacks are a real threat to all the servers and websites. The attacks are launched using the three tire framework towards a particular server. Hence the server fails to serve the legitimate users and the service from the server is not available throughout the world for some specific period of time. This section highlights some of the DDoS attacks that happened in real time and the effect of those attacks.

The first DoS attack occurred against Panix, (Prashant Kulkarni 2010) the New York City area's oldest and the largest Internet Service Provider (ISP), on September 6, 1996, at about 5:30 p.m. The next high level DDoS attacks occurred in 7^{th} – 11^{th} February 2000, on the famous websites CNN, Yahoo, E-bay, Datek. The first major attack involving DNS servers as reflectors occurred in January 2001. In February 2007, more than 10,000 online game servers in games such as Return to Castle Wolfenstein, Halo, Counter-Strike and many others were attacked by ”RUS” hacker group. On June 25, 2009, the day Michael Jackson died, the spike in searches related to Michael Jackson was so big for about 25 minutes, when some people searched Google News they saw a ”We’re sorry” page before finding the articles they were looking for. On August 6, 2009 several social networking sites, including Twitter, Facebook, Livejournal, and Google blogging pages were hit by DDoS attacks, apparently aimed at Georgian blogger ”Cyxymu.

1.3.2 Phases of DDoS Attack

DDoS attacks are done in two phases. First the attacker tries to compromise the vulnerable machines in the network. The attacker or master forms his own network with the compromised hosts of other networks and call them slaves. This is called ‘**intrusion phase’.** The attacker then selects the victim server/node and starts sending packets towards the victim machine. The speciality of DDoS attacks is that it is not from a single host/network like

DoS but are launched from different dynamic networks which are already compromised. This is called '**DDoS attack phase'**.

1.3.3 Method of launching the DDoS attacks

When an attacker wants to launch the DDoS attack towards a particular website or victim, some basic procedures have to be performed to break into the system and launch the attack. The **network scanning** is done to infer the vulnerabilities in the network like proxy server points, vendor – specific default passwords, poor configuration of deployed routers, special Software used in the Operating Systems, and default Open ports.

Once the perpetrator found a point of entry to a system then administrator/root access to the system is targeted in a hidden way. The access is hidden and it is ensured that the actions done in the machine are not listed in the default running processor list or in any of the process or event log entries. Then the access and information obtained from the system is tested, to check if any other log entry is made about the initiated actions. The privileges are used to gather information in the machine. The configuration of the machine is changed in a way to **allow access** for the attacker at anytime.

The attacker now gained access to the machine. Some malicious software or scripts written in any programming language are installed in the machine to **conceal the fact of break-in** and to hide the traces of subsequent activity. For example the versions of history and process commands are replaced with attacker's own versions. The new versions are designed in such a way not to show the commands executed or processes and forks created and run by the attacker. These replacement tools are called "*Rootkit*". Once they are installed the root is broken and with this "*broken root*" system administrator privileges are taken over to keep other root users and ordinary users of the system to find the attacker.

The slave node which is physically located in a distant network can now be **remotely controlled** by the attacker. Then more nodes are compromised in the same way and they are configured to hide the activity of the attacker in a skilled way. All these compromised nodes are called *zombies* or *slaves*. All these machines are used to launch the attack in a coordinated way. These networks of attacking nodes are geographically distributed in nature and form the attacking network of zombies and called *DDoS Network*. Earlier the attacking scripts installation and forming a network of compromised systems was done mostly in manual means. Overtime Intruders have acquired good knowledge and developed and employed a higher degree of automation in multiple aspects of DDoS technology.

The attack is initiated from the attacker and propagates through the compromised zombies and targets the victim. Hence the zombies in the DDoS *Network* now accept commands from the attacker over the Internet and in response to those commands it sends unlimited number of packets over the Internet to the victim machine or website. The victim machine or the main server of the website now responds to these fake requests and by doing this the network bandwidth is filled and the legitimate user does not get reply from the victim. The numbers of packets received by the victim machine or main server of website are very large in the order of GBs. So naturally the main server or local proxy server of the website is bombarded with unusual and huge traffic and becomes inactive.

The attack thus uses the three tier framework to launch the attack. Attacker first sends a single command to the compromised host which in turn sends commands to the larger number compromised zombies in the *DDoS* Network and instructs them to launch attack towards the main server of the website or victim machine. The single command sent by the attacker is not known outside and sometimes encrypted also. When the attacker wants to stop the attack again a single command is sent to the compromised host which

in turn sends commands to all the zombies in the *DDoS* Network to stop the attack. All these processes are done automatically with sophisticated tools like Stacheldraht (Yang Li and Bin-Xing Fang 2007).

The attacker now makes note of the addresses of the machines they have taken over. All the observed IP addresses are noted in a separate file of the control system of the attacker. These IP addresses can be again used if the attacker wants to launch the attack again or if some IP addresses are needed for spoofing. The list of IP addresses of the compromised hosts also give the information about class of IP address used in a particular network and the range of IP addresses used in the network. The range can be very useful to the attacker. If the compromised host is protected by the administrator then another machine in the same range can be tried for launching the attack.

The attacker has a list of compromised hosts in his machine and now the activities of the hosts are remotely monitored by the attacker. The attacker can now restart the same procedure when the previous attack was not monitored or given less care by the system administrator. If the attack is found and the compromised hosts are now protected well than some other machines in the same network can be tried for attack.

1.4 STATISTICAL METHODS FOR DETECTION

Intrusion detection is done using the statistical (Zheng Zhang et al 2001), probabilistic (Kok-Chin et al 2008), rule based and distance based methods (Daniel Yeung et al 2007). State transition analysis (Ilugun et al 1995), Petri nets, and Finite State Automata Methods, Deterministic Finite State Automata models (Joel Branch et al 2002) are also adopted for intrusion detection (Zhou-Jun Xu et al 2003). These rule based methods do not provide flexibility for the new data that are not present in the training set. They suffer from the drawback of late detection and less classification accuracy.

1.5 RULE BASED SYSTEMS FOR DETECTION

Most current approaches to the process of detecting intrusions utilize some form of rule based analysis (Komviriyavut et al 2009). Rule based analysis relies on a set of predefined rules that are provided by an administrator, automatically created by the system, or both (El-Hajj et al 2008). Expert systems are the most common form of rule-based intrusion detection approaches. An Expert system consists of a set of rules that encode the knowledge of a human "expert". These rules are used by the system to make conclusions about the security-related data from the intrusion detection system. But these systems are found to be inefficient in identifying the network breaches (Joong-Hee Lee et al 2008, Jun-feng Tian et al 2005).

1.6 MACHINE LEARNING ALGORITHMS FOR DETECTION

In intrusion detection, machine learning has so far been primarily used to build systems that classify network connections or system call sequences into one of several predefined classes. This task has been proved to be very difficult because it aims at building IDSs only from training examples. Christine Dartigue et al (2009) have developed a methodology to apply data mining for intrusion detection. The importance of domain-specific knowledge in constructing such IDSs is also given. The key advantage of this work is that it employs the models built by data mining methods and classifies the attacks (Wenke Lee et al 1999). So the possibility of new attacks and their recognition can be easily accomplished by this research work. Neil Rowe and Sandra Schiavo (1998) have developed intelligent IDS for detection of intrusions.

1.7 LITERATURE SURVEY

Intrusion Detection problem opens up many research issues. There are numerous methods for detection and classification of intrusions such as traffic collection, traffic monitoring, profiling and usage of both hardware and

software based tools. Some techniques are used such as statistical, rule based and learning based methods. But when it comes to real time detection, the challenge lies in detecting the novel attacks which are launched through the latest automated tools and methods with brand new signatures which do not exists in the literature.

Development of Rule based, Learning based techniques and their combinations as Ensemble Design are highlighted in this thesis for detection and classification of Real Time intrusions. Tools and techniques that are used to detect and classify the attacks using the standard available data such as *kddcup 99* and *Shonlau's Truncated Command Sequences (STCS)* are discussed in this section.

1.7.1 Related Works in Intrusion Detection Systems

Intrusion is basically an active sequence of related events that deliberately causes harm or attack, attempts both successful and unsuccessful such as rendering the system unusable, accessing unauthorized information or manipulating such information. The techniques and methods defined to detect and classify the intrusions are available individually or as tools. IDS research provides avenues for numerous research issues which are discussed in this section (Carl endorf et al 2006).

Hyunjin Kim et al (2009) have proposed an Aho-Corasick algorithm based parallel string matching for intrusion detection. The balance memory usage between homogenous Finite-State Machine (FSM) for each string matcher and an optimal set of bit position groups are determined and the target patterns are sorted by Binary-Reflected Grey Code (BRGC) which reduces the bit transmissions and are used for detection of intrusions.

Wanli Ma et al (2008) have investigated the feature selection of network traffic and the impacts on the detection rates. The *kddcup 99* dataset is used as experimental dataset. The detection rates are found by choosing the different combinations of these feature groups. The ineffectiveness of the approach is also shown in finding anomalies by looking at the host based features within the shorter time interval of 2 secs.

Jiankun Hu et al (2009) have elaborated simple data pre-processing approach which reduces the data upto 58% to speed up a Hidden Markov Model (HMM) training for system-call-based anomaly intrusion detection. This helps in reducing the training time by 50 % with performance degradation.

Wang Ling et al (2009) have employed a method to analyse attacker behaviour to improve the detection rate. A three phase system with phases like data preprocessing phase, fusion decision phase and data call back phase is developed. The rates of false alarms are very high.

Zhao Yueai and Chen Junjie (2009) have identified a novel approach for HNIDS by taking two-stage strategy with load balancing model. In the on-line phase, the network packets are captured and split according to the type of protocol, then intrusion are detected by each sensor. In the off-line, training dataset are used to build model, which can detect intrusion. It evaluates the SMOTE over-sampling approaches, AdaBoost and random forests algorithm.

Anazida Zainal et al (2008) have addressed the issue of continuous detection by introducing traffic monitoring mechanism. In traffic monitoring, a new recognition paradigm is proposed in which it minimizes unnecessary recognition. Empirical results show 30 to 40 % reduction of normal connections is achieved with *kddcup 99* datasets with a lengthy detection process.

Dit-Yan Yeung and Chow (2002) have illustrated a nonparametric density estimation approach based on Parzen-window estimators with Gaussian kernels to build an intrusion detection system using normal data only. The system is tested on *kddcup 99* dataset. Since only normal data is used in the attack traffic and its variations are not known to the system.

Yu Guan et al (2003) have developed a clustering heuristic for intrusion detection, called Y-means. The heuristic is based on the K-means algorithm and other related clustering algorithms. It overcomes two shortcomings of K-means that are number of clusters dependency and degeneracy. The result of simulations run on the *kddcup 99* data set shows that Y-means is an effective method for partitioning large data space. A detection rate of 89.89% and a false alarm rate of 1.00% are achieved with Y-means clustering.

Gupta et al (2010) have experimented with Conditional Random Fields and Layered Approach to address two issues namely accuracy and efficiency. The proposed system based on Layered Conditional Random fields outperforms other well-known methods such as the decision trees and the naïve Bayes. The improvement in attack detection is very high, particularly, for the U2R attacks (34.8% improvement) and the R2L attacks (34.5% improvement).

Dae-Ki Kang Fuller and Honavar (2005) have presented the use of a bag of system calls representation for intrusion detection in system call sequences and describe misuse and anomaly detection results with standard machine learning techniques on University of New Mexico (UMM) and MIT Lincoln Lab (MITLL) system call sequences with the proposed representation. Better results are obtained but the collection and processing of the system calls become very complex.

Comparing with all these approaches the real time detection and classification model discussed in this thesis is different in many aspects. Since the work combines rule based and machine learning algorithms, it takes cue from both the fields. The precise nature of rule based algorithms and the recognition of previously unseen things of the learning algorithms lead to more improved detection performance and lesser false alarms.

1.7.2 Related works in application of Fuzzy Logic for Intrusion Detection

Fuzzy Inference Systems and some variations of Fuzzy Logic is applied to the Intrusion Detection. Fuzzy Logic based systems are used in detection and classification of attacks based on the available data. Fuzzy Association Rules are also applied to detect the intrusions. Fuzzy Logic applied with other techniques such as SVM are briefed in this section

Ali et al (2009) have demonstrated the effect of input fuzzification. The input is applied to NN. Two types of experiments have been carried out with and without fuzzified inputs. The input fuzzification is found to improve the detection rate and the types of attack has been increased with high rate of false alarms

Gautam Singaraju et al (2004) have designed a testbed which allows the user to select the best IDS for a customized environment. Fuzzy logic is used to develop the quantitative analysis. Robust metrics for evaluation of IDS have also been proposed with increased overhead in processing

Ma Yanchun (2010) has proposed IDS to study the DoS attacks using fuzzy association rules mining. The system correctly identifies the DoS attacks with lowest number of false positives. Also the source of an attacker is

identified and informed to the firewall to block the packets from an attacker (Mabu Chen et al, 2010).

Spathoulas and Katsikas (2009) have constructed a model based on FIS for detection of attacks. The design of the system is based on meta-alerts and it carries special information about the nature of alerts. The system has been tested against the DARPA dataset and the false positives are reduced to 83%. The derived attributes used in the system are difficult to describe.

Ming-Yang Su et al (2008) have applied a fast algorithm to generate fuzzy association rules by incremental mining approach for which the transactions or data records are online instantly collected from live packets. As one data record is collected online, the latest fuzzy rules can be obtained immediately. But the weightage of the rules is not considered here.

Guiling Zhang et al (2010) have focused on the use of payload of network protocol and modelled a payload-based anomaly detector which can successfully detect outliers of network servers. It extends these works by applying a new noise-reduced Fuzzy Support Vector Machine to improve the detection rate. The new method named PAYL-FSVM employs reconstruction error based fuzzy membership function to reduce the noise of the data and to solve the sharp boundary problem. The effect of noisy data still takes part in reducing the accuracy

Orfila et al (2003) have illustrated an IDS model with high rate of false positives. The number of alerts that an IDS launch is clearly higher than the number of attacks. The prediction skill of IDS is then computed according to the false positives produced. The fraction of IDS over the total number of them that predicts a given event determines whether such event is predicted or not. The performance obtained from the application of fuzzy thresholds over such fraction is compared with the corresponding crisp thresholds.

The real time detection model using Fuzzy Inference System (FIS) proposed in this thesis explores the advantage of using the Automatic Rule Generation (ARG) module which actually reduces the time of inference by assigning weights for the rules based on the available attributes. The classification accuracy is also better. The ARG module proposed in this thesis is distinct and simplifies the process of framing the rules based on attributes and feeding the rules to the FIS rule editor and thus makes the human intervention lesser than the normal systems. Based on these advantages FIS-ARG is found to be more suitable than the available techniques.

1.7.3 Related works in application of Decision Trees (DT) for Intrusion Detection

Decision Trees (DT) are applied in detection of intrusions using its variations such as ID3 and C4.5. The DT classifier helps in classifying the intrusions based on their information gain value. The information gain value is calculated and the classes are assigned using the range of information gain value. DT and its combination methods are discussed in this section.

Nong Ye et al (2001) have conducted experiments such as decision tree, Hotelling's T2 test, chi-square multivariate test, and Markov chain based on probabilistic properties of activity data in an information system for detecting intrusions into the information system. The data is applied to the training set and the testing set of computer audit data for investigating the frequency property and the ordering property of computer audit data.

Zhen Ying Ma et al (2005) have implemented a multi-class SVMs and a new Decision Tree (DT-SVM) for intrusion detection. A new support vector (SV) reduction algorithm is applied and found that it decreases the training time dramatically while improving the detection rate.

Juan Wang et al (2009) have developed a C4.5 Decision Tree algorithm and converted it into rules. The rules are used to detect the intrusions from the normal data. The network behaviour is analysed and classified as normal or misuse. The complete processing of the network data is found to be an overhead in this case.

Xiaodan Wang et al (2006) have proposed Decision Tree based Support Vector Machine. The feature space of the Support Vector Machines is divided based on the decision tree structure. The structure of the tree is closely related to the performance. A new separability measure is defined based on the distribution of the training samples in the feature space. This measure is used in the formation of the Decision Tree. The performance is improved than the individual usage of Decision Tree or Support Vector Machines.

The real time intrusion detection model proposed in this thesis is based on the Decision Tree with Reduced Error Pruning (DT-REP) module. The REP module is found to be efficient over the other methods reported in the literature which actually increases the classification accuracy and reduces the time for classification by pruning unimportant nodes.

1.7.4 Related works in application of Neural Networks (NN) for Intrusion Detection

Neural Networks are applied to intrusion detection with its variations like Multi-layer Perceptrons (MLP), Back Propagation Networks (BPN), Self Organizing Maps and Radial Basis Function Networks (RBF). Learning is accomplished with training and the instances are actually classified using the model created during learning. This helps in improving the detection of novel attacks.

Fariba Haddadi et al (2010) have represented the two layer feed forward NN for detection of intrusions. Early stopping strategy is used in training to overcome the issue of over-fitting. DARPA dataset is used for the experiments. The pre-processed data is converted in the range [-1, 1] and given to the NN for classification of Intrusions.

Demidova and Ternovoy (2007) have demonstrated the use of Neural Networks for detecting network attacks. The Back-Prorogation Neural Network is used to find the attacks in the network traffic. The detection rate is increased whereas the false alarm rate is also very high.

AI Islam and Sabarina (2009) have devoted research efforts to model the detection system using Recurrent Neural Networks (RNN) which detects the flooding attacks such as DoS and DDoS attacks. Several index terms like Denial-of-service, Distributed-Denial-of-Service, IP spoofing, Flood attack, Zombie, RNN Ensemble are defined and they are used in detection rate of attacks but the detection of new attacks is found to be very low.

Yu-Ping Zhou et al (2009) have proposed an intelligent intrusion detection using Hierarchical Neuro-Fuzzy Classifier. Principal Component Analysis (PCA) is used to reduce the features and Fuzzy-C Means Clustering is used to create the Fuzzy rules. *kddcup 99* data is used for evaluation of the experiments. Genetic Algorithm is used in optimizing the results of the detection model.

Sang-Jun Han and Sung-Bae Cho (2005) have designed an intrusion-detection model using Evolutionary Neural Networks. The improvement is shown with respect to less time for detection because the structure of the network and weight of the network are discovered simultaneously. Experimental results with the 1999 Defence Advanced Research Projects Agency (DARPA) Intrusion Detection Evaluation data confirm that Evolutionary Neural Networks ENNs are effective for intrusion detection with little trade off with the training time.

Chavan et al (2004) have studied about two machine learning paradigms, Artificial Neural Networks and Fuzzy Inference Systems that are used to design an Intrusion Detection System. *Snort* is used to perform real time traffic analysis and packet logging on IP network during the training phase of the system. In 1998 DARPA Intrusion Detection Evaluation Data and TCP dump raw data are used for detection.

Idris and Shanmugam (2005) have discussed about the AI techniques applied for IDS and proposed a dynamic model of Intelligent Intrusion Detection System. Using the network profiling data the Neural Network with Self Organizing maps and Fuzzy Logic are used for detection of misuse and anomaly intrusions.

Sung-Bae Cho et al (2002) have presented a novel intrusion detection system (IDS) that models the normal behaviours with hidden Markov models (HMM) and attempts to detect intrusions. Soft computing techniques such as Neural Network and Fuzzy Logic are incorporated into the system to achieve robustness and flexibility. Self-Organising maps (SOM) determines the optimal measure of audit data and reduce them into appropriate size for efficient modelling by HMM (Selvakani Kandeepan and Rengan Rajesh 2010, Srinivasan and Vaidehi 2008).

The Neural Network (NN) Model proposed in this thesis which can change the number of hidden layer neurons to improve the detection rate of the new intrusions is adaptive. When compared with the work in the literature this thesis proposes a novel technique using ADNN which improves the classification rate of new attacks.

1.7.5 Related works in application of Naïve Bayes Classifiers (NBC) for Intrusion Detection

Naïve Bayes Classifiers (NBC) are used for detection of intrusions and masqueraders based on the probability distributions of the users and attacks. The NBC is used both in misuse and anomaly detection. NBC are very successful in text categorization which proves the performance in detection of intrusions also.

Qin Zhao et al (2004) have designed a new detection paradigm using hybrid and hierarchical NIDS. The network payload data is monitored and the network based attacks are analysed. Application layer attacks are detected using NBC after statistical pre-processing.

Kok-Chin Khor et al (2010) have the employed the use of single and multiple Bayesian classifier approach using variations of Bayes Network such as Naïve Bayes Classifier, Bayesian Networks, and Expert-elicited Bayesian Network, since only Bayes classifiers are involved in the combination technique and this approach offers less detection results with standard available data like *kddcup 99*

Panda et al (2010) have developed a discriminative multinomial Naïve Bayes Classifier for NIDS with filtering analysis. The variation of the kddcup 99 dataset namely NSL-kddcup 99 is used. Two class classification which gives high classification rate and better accuracy with low false alarms is performed.

Panda and Patra (2008) have designed IDS to protect the systems against unauthorised attacks. The performance of other tree based algorithms such as ID3, J48, Naïve Bayes Classifier is evaluated and found that the Naïve Bayes Classifier is one of the most inductive learning algorithms for intrusion detection research.

Chou et al (2007) have proposed a method to reduce the dimensionality of features using the correlation based feature selection mechanism. Six datasets are derived from the UCI_KDD archive and used for experiments. The results show that feature selection with C4.5 and Naïve Bayes classifiers are well suited for experiments (Ye Zhu et al 2010).

Naïve Bayes Classifiers with Multi-Variate Bernoulli Model proposed in this thesis have unique characteristics to classify the newer types of attacks in the standard and real time data. The new attacks are recognized with better classification accuracy compared with the existing approaches

1.7.6 Related works in Support Vector Machines (SVM) for Intrusion Detection

Support Vector Machines are used for detection and classification of the intrusions using the standard available data or using the real time data. There are some variations of SVM like one class SVM, c-SVM which are used for detection of intrusions. The SVM is used in detection of masqueraders a specific type of intruders who are actually the insiders of the organization.

Fang Liu and Zhen-Guo Chen (2004) have presented a method to improve the limited performance of Minimax Probability Machine in training time and a new multi-layer classifier model based on MPM ensemble with boosting to intrusion detection. After illustrating the model with a representative dataset and applying it to the real-world network datasets like *kddcup 99,* the effectiveness of the approach is shown. Experiments have shown that the intrusion detection system based on Multi-Layer Minimax Probability Machine achieves the comparative performance with the Support Vector Machine and with less training time.

Wenjie Tian and JiCheng Liu (2009) have demonstrated an integrated Intrusion detection model based on Support Vector Regression and principal components analysis (PCA).It reduces the size of original dataset which are calculated and used to train individual SVR classifier for ensemble, to increase the detection accuracy.

Qiao Pei-li and Chen Shi-Feng (2009) have explained the BP neural network and Support Vector Machine (SVM) based on the theory of neural network integration, applying fuzzy clustering technology to cluster data, choosing data from the cluster centre to train ensemble individuals, then selecting and integrating those individuals of significant diversity.

Zhang Hongmei (2009) have proposed an intrusion detection model of SVM ensemble using rough set feature reduction. Utilizing the character that Rough set algorithm can keep the structure of original dataset after reduction, the reduction of the original dataset are calculated and used to train individual SVM classifier. To validate the effectiveness of the proposed method, simulation experiments are performed based on the *kddcup 99* dataset.

Perdisci et al (2006) have identified a new approach to construct high speed payload. A feature clustering algorithm is originally proposed for text classification problems to reduce the dimensionality of the feature space. Accuracy and hardness of evasion is obtained by constructing anomaly-based IDS using an ensemble of one-class SVM classifiers that work on different feature spaces.

Zong-Hua Zhang and Hong Shen (2004) have implemented an adaptive intrusion detection system with incremental learning ability. A generic framework, including several important components is proposed. One-class support vector machine is modified as the kernel algorithm of AID, and the performance is evaluated using reformulated 1998 DARPA BSM data set.

Kunlun Li and Guita Teng (2006) have proposed an unsupervised learning method for anomaly detection. This is to introduce a new kind of kernel function, a simple form of p-kernel, to one-class SVM. Comparison of this method with standard SVM and several other existing machine learning algorithms shows that the approach is very effective.

Latifur Khan et al (2007) have given an idea about detection of intrusions using support vector machines and hierarchical clustering. A Dynamically Growing Self Organizing Tree (DGSOT) algorithm for clustering is proposed which overcomes the drawbacks of the existing clustering algorithms. With these variations the SVM is proved with high generalization accuracy

Zhanchun Li et al (2006) have presented a masquerade detection system based on Correlation Eigen Matrix and support vector machine (SVM). The system first creates a profile defining a normal user's behaviour by Correlation Eigen Matrix, and then compares the similarity of a Current behaviour with the created profile to decide whether the input instance is a valid user or masquerader. In order to avoid over fitting and reducing the computational burden, user behaviour principal features are extracted by the PCA method. SVM is used to distinguish valid user or masquerader for user behaviour after training procedure has been completed by learning.

Min Yang et al (2007) have studied and designed a new method for masquerade detection based on string kernel. String kernel is an inner product in the feature space generated by all subsequences of length k. By using string kernel, OCSVM (one-class support vector machine) algorithm can directly process the UNIX command sequences, which are the input data of masquerade detection.

Shu-Xia Lu and Xi-Zhao Wang (2004) have compared four methods based on SVM listed as BIP Lagrangian Support Vector Machine, Finite Newton Lagrangian Support Vector Machine, Smooth Support Vector Machine and Finite Newton Support Vector Machine. The study provides some guidelines for choosing an appropriate one from four SVM classification methods in a classification problem.

Compared with the existing approaches the work done in this thesis is distinguished in many aspects. The Multi-Level Support Vector Machine (MLSVM) used in this research uses more than one level to classify the attack with more improved accuracy. The SNMP-MIB data used for detection helps in improving the accuracy of the real time attacks

1.7.7 Related works in Ensemble of Algorithms for Intrusion Detection

Ensemble Design of machine learning algorithms is used in detection of intrusions using the standard available data and real time data. Many algorithms are combined based on the combination techniques used. To fuse the output of the classifiers the basic need is there should be diversity among classifiers.

Parikh and Tsuhan Chen (2008) have applied a method to have a finer balance between misdetections and false alarms than the more conventional intrusion detection approaches, namely misuse detection and anomaly detection. One benefit is that intrusion detection is significantly more effective by using multiple sources of information. Different errors in intrusion detection have different costs associated with them. A pattern recognition approach is proposed that addresses both of these issues. It utilizes an ensemble of a classifiers approach to intelligently combine information from multiple sources and is explicitly tuned toward minimizing the cost of the errors as opposed to the error rate itself.

Ming-Guang Ouyang et al (2002) have identified a new data mining based technique for intrusion detection using an ensemble of binary classifiers with feature selection and multiboosting simultaneously and it improves the detection of attacks that occur less frequently in the training data. It provides better performance in the *kddcup 99* cup challenge.

Te-Shun Chou and Tsung-Nan Chou (2009) have discussed about a hybrid design for intrusion detection that combines anomaly detection with misuse detection. It includes an ensemble feature selecting classifier and a data mining classifier (Taeshik Shon and Jongsub Moon 2007).

Dartigue et al (2009) have illustrated a data mining based technique for intrusion detection using an ensemble of binary classifiers with feature selection and multi boosting simultaneously. It improves the detection of attacks that occur less frequently in the training data. This model applies a new ensemble approach which aggregates each binary classifier's decisions for the same input and decides which class is most suitable for a given input (Panda and Patra 2008, Sekeh and Bin Maroof 2009).

Fangfei Weng et al (2007) have studied the use of unsupervised anomaly detection system based on the clustering ensemble. The system is based on the multiple runs of K-means to accumulate evidence to avoid the false classification of anomalistic data. Then single link is used to construct the hierarchical clustering. The *kddcup 99* test data is used to show that this system is greatly effective.

DeLooze et al (2006) have discussed about the ensemble of SOMs to identify computer attacks and characterize them appropriately using the major classes of computer attacks (Denial of Service, Probe, User to Root and Remote to Local).The procedure produces a set of confidence levels for each connection as a way to describe the connection's behaviour.

Te-Shun Chou et al (2009) have applied a three layer hierarchy with multi-classifier intrusion detection architecture to promote the overall detection accuracy. The *kddcup 99* intrusion detection data set is chosen as the evaluation tools (Hui Lu and Jinhua Xu, 2009).

Zainal et al (2008) have designed an ensemble of one class classifiers where each uses different learning paradigms Linear Genetic Programming (LGP), Adaptive Neural Fuzzy Inference System (ANFIS) and Random Forest (RF). Empirical results have shown an improvement in detection accuracy for all classes of network traffic; Normal, probe, DoS, U2R and R2L.

Chan et al (2005) have proposed a Multiple Classifier System to solve problems in Network Intrusion Detection System (NIDS). The MCS is one of the approaches that has been adopted in the detection of DoS attacks recently. Majority vote, average, weighted majority vote, neural network and Dempster -Shafer combination are the fusion strategies that have been widely adopted.

Compared with all these approaches the Threshold based Ensemble Design (TBED) model proposed in this thesis is unique in many aspects. The TBED combines both rule based and learning based classifiers. The output of the Ensemble Design model is better compared to all the other previous models and found that the detection accuracy is greatly improved than the existing literature for new and known attacks.

1.8 THESIS CONTRIBUTIONS

Compared with all the works in the literature, the proposed methods discussed in this thesis are unique in many aspects. The new methods proposed in this thesis provide the real time detection of

intrusions in three layers such as Network, Transport and Application layer attacks. The latest application layer attacks are generated, detected and classified along with other types of attacks. In this thesis machine learning algorithms are applied for classification of intrusions. They are the enhanced and improved versions of the original algorithms. They are designed to meet the needs of the real time detection and classification of the attacks with new modules like ARG of FIS, REP of DT, Adaptive NN, MVB of NBC, more levels of SVM. In this research the rule based methods such as Fuzzy Inference System with Automatic Rule Generation (FIS-ARG) and Decision Trees with Reduced Error Pruning Module (DT-REP) are used to have more precise output. The learning based methods such as Adaptive Neural Networks (ADNN) and Naive Bayes Classifiers with Multi Variate Bernoulli Model (NBC-MVB) are used to detect the new types of intrusions. Multilevel Support Vector Machines (MLSVM) used in this research improves the classification using the SNMP-MIB data. A new threshold based ensemble design classifier is designed and implemented. Threshold Based Ensemble Design Classifier (TBED) proposed in this research provides best classification for all the attacks both known and unknown. The algorithms proposed in this thesis are evaluated against standard and real time datasets and found to be more suitable for both. Hence this research provides promising tools for real time detection and classification models.

1.9 ORGANIZATION OF THE THESIS

Chapter 1 provides a solid basis for real time detection of attacks. The related work in this field is surveyed and compared with the proposed work.

Chapter 2 explains the methods of collecting the real time data using the packet generation, capturing and attack detection strategies. The

detection mechanisms are customized and the detection of attacks is explored. Two rule based techniques Fuzzy Inference System (FIS) and Decision Trees (DT) with an Automatic Rule Generation and Reduced Error Pruning (REP) are proposed to classify the attacks. The Automatic Rule Generation Module (ARG) greatly reduces human workload of generating rules.

Chapter 3 proposes a method of classification with Adaptive Neural Networks and Naïve Bayes Classifier with Multi-Variate Bernoulli Model for classification of new attacks.

Chapter 4 proposes Multilevel Support Vector Machines for attack classification. The MLSVM provides better detection accuracy when compared with the rule based and learning techniques.

Chapter 5 proposes the development of a Ensemble IDS Tool with Threshold based Ensemble design classifier which is a combination of rule based techniques and learning algorithms. The Ensemble Design classifier helps in reducing the false positives to a considerable percentage.

Chapter 6 presents the conclusions arrived from this work and directs some suggestions for future extension of this work.