CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

Computer networks and their related applications have become an attractive source in the era of information society [Huy and Deokjai 2008]. Similarly, in recent years, the potential thread to the global information infrastructure has also increased greatly. In order to guard against several cyber attacks and computer viruses, numerous computer security approaches have been extensively researched in the recent years. The major security techniques proposed are cryptography, firewalls, anomaly, intrusion detection, etc. Among the available standard techniques, intrusion detection techniques have been considered to be one of the most significant and competent techniques for protecting complex and dynamic intrusion attacks.

An intrusion is a violation of the security policy of the system and thus intrusion detection mainly refers to the methods that detect violations of system security policy. Since the cruelty of attacks in the network has increased radically then the Intrusion Detection System (IDS) has become an essential factor to the security infrastructure of several companies. It facilitates companies to defend their systems from various attacks that come with rising network connectivity and dependence on information systems [Liberios and Alzebeta 2004]. Several information security techniques are available today to protect information systems against unauthorized use, duplication, alteration, destruction and virus attacks. An IDS is a program that analyzes what happens or has happened during an execution and tries to find out the indications that the computer has been misused.
Intrusion Detection is one in all the key parts of network management. IDS examines a host or network to spot the potential intrusions or attacks. It is often either network based or host based, whereas network primarily based intrusion detection systems are common. Network based intrusion detection systems examine all the packets flowing through the network for the signs of attacks. Host based systems explore user and method activity on the local machine for the signs of intrusions.

Intrusions discuss with the network attacks against vulnerable services, data-driven attacks on applications, host-based attacks like privilege escalation, unauthorized logins and access to sensitive files, or malware like viruses, worms and Trojan horses. These actions attempt to compromise the integrity, confidentiality or availability of a resource. Intrusions lead to services being denied, system failing to reply or data taken or being lost. Intrusion detection suggests that detection of unauthorized use of a system or attacks on a system or network Intrusion. IDS facilitate data systems to be prepared for, and handle attacks. They accomplish this by aggregation data from a spread of systems and network sources, so analyzing the data for attainable security issues.

IDS is a software or hardware product that monitors, analyzes, and tracks network traffic or hosts audit logs to determine whether any violations of an organization’s security policy have taken place. IDS can detect intrusions that have circumvented or passed through a firewall or that are occurring within the Local Area Network (LAN) behind the firewall.

IDSs perform variety of functions:
- Monitoring users and system activity
- Auditing system configuration for vulnerabilities and misconfiguration
- Assessing the integrity of critical system and data files
- Recognizing known attack patterns in system activity
• Identifying abnormal activity through statistical analysis
• Managing audit trails and highlighting user violation of policy or normal activity
• Correcting system configuration errors
• Installing and operating traps to record information about intruders

An Intrusion Detection System usually operates behind the firewall as shown in Figure 1.1, looking for patterns in network traffic which may indicate malicious activity. Thus, IDSs are used because the second and the final level of defense in any protected network against attacks that breach alternative defenses. The necessity for this second layer of protection is questioned like “Is there a need of an IDS once there is a firewall?”. To reply for the question, it is needed to grasp what a firewall will and have to do, associate degree what an IDS does and does not do. This can facilitate in realizing the necessity for each IDS and firewall to assist in securing a network. The standard network security solutions, together with firewall, were not designed to handle network and application layer attacks like Denial of Service, worms, viruses, and Trojans. Along with the drastic growth of the internet, the high prevalence of the threats over the internet has been the reason for the safety personnel to think about IDSs.

The unauthorized activities on the internet are not only by the external attackers however also by internal sources, like fraudulent employees or people abusing their privileges for private gain or revenge. These internal activities cannot be prevented by a firewall that sometimes stops the external traffic from coming into the internal network. Firewalls are created to prevent spare network traffic into or out of any network. Packet filtering firewall generally can scan a packet for layer 3 and layer 4 protocol information. They are not noticeably dynamic defensive abilities to most of the firewall. The traffic approaching the
firewall either matches up to the applied rule and is allowed through or the traffic is stopped and therefore the firewall logs the blocked traffic.

An IDS provides much greater visibility to detect signs of attacks and compromised hosts. There is still the need for a firewall to block traffic before it enters the network; but, an IDS is also needed to make sure that the traffic that gets past the firewall will be monitored. So an IDS is to supervise and control all cases happening to computer system or network system, analyze any signal arising from related safety problems, send alarms when safety problems occur, and inform related personnel or units to take relevant measures to reduce possible risks. Its framework includes three parts:

1. Information collection / Data collection: The source of these collected data can be separated into host, network and application, according to the position.

2. Analysis engine: Analysis engine is able to analyze whether there are symptoms of any intrusion or not.

3. Response: Takes actions after analysis, records analysis results, sends real-time alarm, or adjusts intrusion detection system and so on.

IDSs, as originally introduced by Anderson [1980] and later formalized by Denning [1987], have received increasing attention in the recent years. The IDSs

---

*Figure 1.1 A Typical Security Scenario of IDS*
along with the firewall form the fundamental technologies for network security. IDSs can be categorized into two classes, anomaly based IDSs and misuse based IDSs. Anomaly based IDSs look for deviations from normal usage behavior to identify abnormal behavior. Misuse based, on the other hand, recognizes patterns of attack. Anomaly detection techniques rely on models of the normal behavior of a computer system. These models may focus on the users, the applications, or the network. Behavior profiles are built by performing statistical analysis on historical data [Helman 1993 and Javitz 1994] or by using rule based approaches to specify behavior patterns [Ko 1997, Wagner 2001 and Warrender 1999]. A self-evident truth of anomaly detection is that attacks dissent from traditional behavior in sort and quantity. By process what is traditional, any violation is identified, whether it is a part of threat model or not. However, the advantage of detecting previously unknown attacks is paid for in terms of high false positive rates in anomaly detection systems. It is additionally tough to train an anomaly detection system in extremely dynamic environments. The anomaly detection systems are intrinsically advanced and conjointly there are some issues in determinative that specific event triggered the alarms.

On the other hand, misuse detection systems essentially contain attack descriptions or signatures and match them against the audit data stream, looking for evidence of known attacks. The main advantage of misuse detection systems is that they focus analysis on the audit data and generally produce few false positives. The most disadvantages of misuse detection systems are that they will detect only familiar attacks that they need a defined signature. As new attacks are discovered, developers should model and add them to the signature database. Additionally, signature based IDSs are a lot of vulnerable to attacks aimed towards triggering a high volume of detection alerts by injecting traffic that has been specifically crafted to match the signatures employed in the analysis method.
1.1.1 Challenges and Limitations of IDS

Current cyber security capabilities have evolved largely as trivial patches and add-ons to the Internet, which were proposed on the principles of open communication and implicit mutual trust. It is now recognized that it is no longer sufficient to follow such evolutionary paths and that security must be considered as a sophisticated research and design part of the information infrastructure. With all the progress that IDS have made over the last few years, it still has some major difficulties. The analysis is most probably slow and often computationally intensive. Hence, intrusion detection programs used to detect intrusions after the intrusions have occurred. There is still a little hope to detect an attack in progress.

The attackers continue to find ingenious ways to compromise remote hosts and frequently make their tools publicly available. Also, the increasing size and complexity of the Internet along with the end host operating systems make it more flat to vulnerabilities. Further, there is only a slight broad understanding of the intrusion activity due to many privacy issues. Because of these challenges, current best practices for the internet security rely on the reports of new intrusions. Another well recognized fact is that false positives are one of the biggest problems when working with IDS. Also, a large amount of false alerts mean a lot in terms of acceptability of IDSs if the incidence of attacks is considerably less in comparison to the normal traffic. It is very difficult to integrate firewall logs, router logs, system logs and host based IDS alerts, with alerts from a network based IDS. The last main challenge is the need for well skilled IDS analysts. In order to monitor and evaluate the alerts forces, the analyst has to stay on top of all the newest attacks, worms, virus, different operating systems and network changes on the internal network to keep rule list accurate.

In the last two decades, a range of commercial and public domain intrusion detection systems have been extended. These systems use various approaches to
detect intrusions. As a result, they show distinct preferences in detecting certain classes of attacks with improved accuracy while performing moderately for the other classes. The analysis of these IDSs have given us some insight into the problems that still have to be solved before intrusion detection systems that are useful and reliable for detecting a wide range of intrusions.

1.2 TYPES OF IDS

There are several ways to categorize the types of IDS that are available. Depend on the kind of activities, transactions and traffics or systems they monitor, Instruction Detection System can be categorized into Network based (NIDS) and Host based (HIDS).

1.2.1 Network based Intrusion Detection System (NIDS)

NIDS are best suited to alert generation of intrusion from outside the perimeter of the enterprise. The NIDS are inserted at numerous points on LAN and observe packets traffic on the Network information is assembled into packets and transmitted on internet or LAN. Network based IDS are valuable if they are placed simply outside the firewalls, thereby alerting personals to incoming packets which may circumvent to the firewall. Some NIDS take or permits taking input of custom signatures taken from user security policy which allows restricted detection security policy violation. This limitation is attributable to packets traffic information that does not work well nowadays in switched and encrypted environments wherever packets analysis is weak in detecting, attacking or originating from approved network users. NIDS use raw network packets because of the information supply, the NIDS generally uses a network adapter in promiscuous mode that listens and analyses all traffic in time period as it travels across the network.
Figure 1.2 Network Intrusion Detection System

Advantages

*Lower price of ownership:* NIDS are often deployed for every network section. An IDS monitors network traffic destined for all the systems in an exceedingly network section. This nullifies the need of loading package at software hosts within the network section. This reduces management overhead, as there is no need to maintain detector software at the host level.

*Easier to deploy:* NIDS is easier to deploy because it does not have an effect on standard systems or infrastructure. These systems are operating system independent. A network based IDS sensor will monitor all the attacks on a network segment regardless of the type of the software the target host is running.

*Detect network based attacks:* NIDS checks for all the packet headers for any malicious attack. Several IP-based denials of service attacks like TCP SYN attack, fragmented packet attack etc. are often identified only by looking at the packet headers as they travel across a network. NIDS detector will quickly notice this kind of attack by staring at the contents of the packets at the real time.

*Retaining evidence:* NIDS use live network traffic and does real time intrusion detection. Thus, the attacker cannot remove evidence of attack; these data can be used for forensic analysis. On the other hand, a host based sensor
detects attacks by looking at the system log files. Many hackers have the capacity of making changes in the log files so as to remove any evidence of an attack.

*Real Time detection and quick response:* NIDS monitors traffic on a real time. Therefore, network based IDS can detect malicious activity when they occur. Based on how the sensor is configured, such attack can be stopped even before they can get to a host and compromise the system. On the other hand, host based systems detect attacks by looking at changes made to system files.

*Detection of failed attacks:* NIDS sensor deployed outside the firewall can detect malicious attacks on resources behind the firewall; still the firewall may reject these attempts. This information can be much useful for forensic analysis.

**Disadvantages**

- NIDS may fail to recognize attack when network volume becomes over-whelming.
- NIDS cannot analyze encrypted packets, making some of the traffic invisible to the process and reducing the effectiveness of NIDS.
- Attacks involving fragmented or malformed packets cannot easily be detected.

**1.2.2 Host based Intrusion Detection System (HIDS)**

HIDS monitors the incoming and outgoing activity on a specific system within the network. Specifically, it monitors the dynamic behavior and state of the computer system. The administrator is going to be notified once an intrusion has been detected. Host based IDS places monitoring sensors also called agents on network resources nodes to watch audit logs that are generated by Network OS or application. Audit logs contain records for events and activities going down at individual network resources. As a result of this HIDS will find attacks that cannot be seen by NIDS and might be misused by trustworthy insider. Host based system
utilize signature rule base that springs from site-specific security policy. Host based will overcome the issues related to NIDS immediately when alarming the security personnel who will find the supply provided by website security policy. HIDS may verify if any attack was unsuccessful, either attributable to immediate response to alarm or the other reason however this can be not accessible at packet level. HIDS may maintain user login and user logoff action and every one activity that generates audit records.

**Advantages**

*Verifies success or failure of an attack:* Since a HIDS uses system logs containing events that have actually occurred, they can determine whether an attack occurred or not with greater accuracy and fewer false positives than a network based system. NIDS sensors although quicker in response than HIDS sensors, generate more false positives because of the very fact that it detects malicious packets on the real time and some of these packets will be from a trusted host.

*Monitors System Activities:* HIDS sensor monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executables etc. HIDS sensor can also monitor all user logon and logoff activity, user activities while connected to the network, file system changes, activities that are normally executed only by an administrator. Operating systems log any event where users accounts are added, deleted or modified to any extent. The HIDS can able to detect an improper change as soon as it is executed. A network based system cannot give so much detailed information about system activities as compared with host based.

*Detects attacks that a NIDS fail to detect:* HIDS can detect attacks that NIDS sensors fail to detect. For example, if an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the
network sensors. So, host based sensors can be very useful in protecting hosts from malicious internal users in addition to protecting systems from external users.

*Near real time detection and response:* Although HIDS does not offer true real-time response, it can come extremely close if implemented correctly. Unlike older systems, which use a process to check the status and content of log files at predefined intervals, many current host based systems receive an interrupt from the operating system when there is a new log file entry. This new entry can be processed immediately, significantly reducing the time between attack recognition and response.

*Does not require additional hardware:* HIDS sensors reside on the host systems. Thus they do not require any additional hardware for deployment, thus they reduce the cost of deployment for the system.

*Lower entry cost:* Host based IDS sensors are far cheaper than the network based IDS sensors.

**Disadvantages**

- More management efforts are required to install configuration and manage HIDS.
- Both direct attacks and attacks against the host operating system results in compromise and/or loss in functionality of HIDS.
- Host OS audit logs occupy large amounts of disk space and disk capacity needs to be added, which may reduce system performance.
1.3 INTRUSION DETECTION TECHNOLOGIES

Intrusion Detection technologies can be categorized into two major groups: Misuse detection and Anomaly detection.

1.3.1 Misuse Based Detection

A misuse detection system traces intrusion activities that follow recognized patterns. These patterns explain a suspect collection of sequences of activities or operations that can possibly be dangerous. The major drawback of this detection is that it does not have the capability to trace or detect any new kind of intrusions, i.e., certain events that have never occurred in the past.

The misuse detection is also known as signature based detection because alarms are generated based on specific attack signatures. This type of signatures attack encompass specific traffic or activity that is based on known intrusive activity.

Expression matching

The simplest form of misuse detection is expression matching, which searches an event stream for occurrences of specific patterns or signatures. Signatures can be very simple to make, however especially when combined with protocol.

State transition analysis

In state transition analysis model, attacks are of network states and transitions (matching events). Every observed event is applied to finite state machine instances (each representing an attack scenario), possibly causing transitions. Any machine that reaches its final (acceptance) state indicates an attack. This type of approach allows complex intrusion scenarios to be modeled in
a simple way and is capable of detecting slow or distributed attacks, but may have difficulty expressing elaborate scenarios.

**Target Monitoring**

Any change or modification in the target objects are reported by the Target Monitoring Systems. This is usually done through cryptographic algorithm that computes a crypto checksum for each target file [Carl et al 2003]. Changes such as file modification or program logon which would cause changes in the crypto checksum are reported by the IDS. This type of system is the easiest to put for implementation, because it does not require any constant monitoring by the administrator. Integrity checksum can be computed at whatever intervals user wish, and on either all files or just the system critical files. Tripwire software will perform target monitoring using crypto checksum by providing instant notification of changes to configuration files and enabling automatic restoration.

**Stealth Probes**

Stealth probes collects and correlates data to detect attacks made over long period of time, often referred to as “low and slow” attacks [Carl et al 2003]. Attackers, for example, will check for system vulnerabilities and open ports over a two months period, and wait another two months to actually launch for the attacks. They take a wide area sampling and attempt to discover any correlating attacks.

**Advantages**

- Misuse detectors are very effective at detecting attacks without generating an overwhelming number of false alarms.
- Misuse detectors can quickly and reliably diagnose the use of a specific attack tool or technique. This can help security managers prioritize corrective measures and track security problems on their systems.
Disadvantages

- Misuse detectors can only detect those attacks they know about therefore they must be constantly updated with signatures of new attacks.
- Many misuse detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks. State based misuse detectors can overcome this limitation, but are not commonly used in commercial IDSs.

1.3.2 Anomaly Based Detection

Anomaly based detection relies on process of the network behavior. Behavior of the network is in accordance with the predefined behavior then it is accepted alternatively it triggers the event within the anomaly detection. Behavior of the accepted network is ready or learnt by the specifications of the network directors. An anomaly detection system examines event data and identifies pattern of activities that appear to be ordinary. If an event lies outside of the patterns, it is considered as a possible intrusion [Kyaw 2010].

The network behavior is that the IDS engine is capable capability to cut through the assorted protocols in any respect levels. The engine should be ready to process the protocols and perceive its goal. Although this protocol analysis is computationally expensive, the advantages it generates like increasing the rule set helps in less false positive alarms.

The major disadvantage of anomaly detection is process its rule set. The potency of the system depends on however well it is enforced and tested on all protocols. Rule defining method is additionally suffering from numerous protocols employed by varied vendors. Except for these, custom protocols also build rule process a troublesome job. For detection to occur properly, the elaborate
knowledge concerning the accepted network behavior ought to be developed by the administrators. However once the principles are outlined and protocol is constructed then anomaly detection systems work well.

If the malicious behavior of the user falls below the accepted behavior then it goes unobserved. An activity like directory traversal on a targeted vulnerable server to that complies with network protocol and it simply goes unobserved because it does not trigger any out of protocol, and payload or bandwidth limitation flags.

The major advantage of anomaly based mostly detection over signature based engines is that a unique attack that a signature does not exist will be detected if it falls out of the conventional traffic patterns. It is discovered once the systems find new machine driven worms. If the new system is infected with a worm it always starts scanning for alternative vulnerable systems at an accelerated rate filling the network with malicious traffic, therefore inflicting the event of a TCP connection or bandwidth abnormality rule.

Anomaly detection technique is intended to uncover the patterns of behavior that are far from traditional and something that wide by deviates from it gets flagged as a possible intrusion. Anomaly detection will be categorized into static and dynamic [Jones and Sielken 2000].

In static anomaly detector it is assumed that some of the monitored system remains constant or static. The static portion of a system consists of two parts: the system code and the portion of system data that is still constant. Static parts of the system will be described as a binary bit string or a group of such strings (such as files). If this portion ever deviates from its original kind, either a mistake has occurred or associate intruder has altered the static portion of the system. Static anomaly detectors are a unit to visualize for data integrity.
In dynamic anomaly detector the definition of behavior is enclosed. System behavior is outlined as a sequence (or partially ordered sequence) of distinct events. For instance, audit records created by the operating system area unit employed by IDS to define the events of interest. During this case, the behavior will be discovered only if audit records are created by OS. Events could occur in a very strict sequence.

The system parameters that are set throughout initialization to reflect behavior if it is unsure whether the behavior is abnormal or not. Initial behavior is assumed to be traditional. It is measured then used to set parameters that describe correct or nominal behavior. There is usually an unclear boundary between normal and abnormal behavior. If uncertain behavior is not considered anomalous, then intrusion activity might not be detected. If uncertain behavior is taken into account anomalous, then a system administrator is also alerted by false alarms once there is no intrusion [Jones and Sielken 2000].

Anomaly Detection Techniques

Anomaly detection is based on a host or network and some of the distinct techniques are used based on the type of processing related to behavioral model.

Protocol Anomaly Detection

Protocol anomaly refers to all exceptions related to protocol format and behavior with respect to common practice on the internet and standard specifications. The network and transport layer protocol anomalies are included in layers 3 and 4 and application layer protocol anomalies in layers 6 and 7. Unusual conditions are checked for in the process of IP defragmentation, TCP reassembly. When the IDS are in line, many exceptions leading to ambiguous interpretation by the end host can be averted. When an IDS is monitoring application protocol behavior, it must be able to perform deep application protocol parsing, which is also known as decoding. The subsequent anomalies are examples of protocol
anomalies that could be detected when application protocol behavior is being observed:

- Illegal field values, command usage and combinations
- Unusually long or short field lengths, which can indicate an attacker is attempting to introduce a buffer overflow
- Unusual number of occurrences of particular fields or commands
- Running a protocol or service for a non-standard purpose

**Application Payload Anomaly**

Application anomaly must be supported by detailed analysis of application protocols to define accurate behavior constraints for them. Application anomaly also requires understanding of the application semantics in order to be effective. One needs to know what type of encoding is legal for a given field, and what other applications can be embedded within it. One best example of application level anomaly is the presence of shell code in unexpected fields. A reliable anomaly profile allows shell code execution attacks to be detected without knowing what particular exploit code is involved, or even the existence of exploit code.

**Statistical Anomaly Based Intrusion Detection**

A normal TCP traffic follows a well defined three way handshake process for connection setup, data transfer phase, and then completes with the connection tear down. There is a stable balance among different types of TCP packets in the absence of attacks which is compared against short term observations that will be affected by attack events. Statistical anomaly based IDS captures this behavior and differentiates between the long term and short term observations in a given protected environment to avoid generating false alarms on normal traffic variations.
1.4 DATA MINING AND INTRUSION DETECTION SYSTEM

Data mining refers to extracting or mining knowledge from large amounts of data. Cluster analysis is the process of grouping the objects (usually represented as a vector of measurements, or a point in a multidimensional space) so that the objects of one cluster are similar to each other whereas objects of different clusters are dissimilar. Clustering is the unsupervised classification of objects (observations, data items, instances, cases, patterns, or feature vectors) into groups, clusters. From a machine learning perspective, clusters correspond to hidden patterns, the search for clusters is unsupervised learning, and the resulting system represents a data concept. Therefore, clustering is unsupervised learning of a hidden data concept. The applications of clustering often deal with large datasets and data with many attributes.

Data mining techniques can be differentiated by their different model functions and representation, preference criterion, and algorithms [Fayyad et al 1996]. The main function of the model is classification, as normal, or malicious, or as a particular type of attack. Additionally, data mining systems provide the means to easily perform data summarization and visualization, aiding the security analyst in identifying areas of concern. The models must be represented in some form. Common representations for data mining techniques include rules, decision trees, linear and non-linear functions, instance based examples, and probability models [Fayyad et al 1996]. The use of data mining techniques in IDSs usually implies analysis of the collected data in an offline environment. There are important advantages in performing intrusion detection in an offline environment, in addition to the real time detection tasks typically employed. The most important advantages are:

- In offline analysis, it is assumed that all connections have already finished and, therefore, we can compute all the features and check the detection rules one by one [Lee and Stolfo 2001].
The estimation and detection process is generally very demanding and, therefore, the problem cannot be addressed in an online environment because of the various the real time constraints [Singh and Kandula 2001]. Many real time IDSs will start to drop packets when flooded with data faster than they can process it.

An offline environment provides the ability to transfer logs from remote sites to a central site for analysis during off peak times.

Data mining techniques can also be used to enhance IDSs in real time. Lee et al. [Lee and Xiang, 2001] were one of the first to address important and challenging issues of accuracy, efficiency, and usability of real time IDSs. They implemented feature extraction and construction algorithms for labeled audit data. They developed several anomaly detection algorithms. Recently intrusion detection techniques through data mining approaches have attracted several researchers. As an essential application area of data mining intrusion detection focus to lessen the burden of examining vast volumes of audit data and recognizing the performance optimization of detection rules. Number of researchers suggested numerous techniques in various groups from Bayesian techniques to decision trees. These techniques have improved the efficiency of the detection to a certain extent.

In the present day situation data mining approaches have taken valuable steps towards solution of several issues in different intrusion detection issues. There are various benefits in utilizing the data mining approaches for solving the problem of network intrusion [Xue & Zhu 2009]. It can process huge amount of data and easy to detect the unobserved and hidden information. A classification based IDS attempts to classify all traffic as either normal or malicious. The challenge in this is to minimize the number of false positives (classification of normal traffic as malicious) and false negatives (classification of malicious traffic
as normal). Furthermore data mining systems easily performs data summarization and visualization that facilitate the security analysis in various research areas [Bloedorn et al 2001].

1.5 TYPES OF ATTACKS IN PROTOCOLS

There are various attacks associated in Intrusion Detection. The main attacks which normally occur in protocols are as follows:

Probe Attacks

Probing is a class of attack where an attacker scans a network to gather information or find known vulnerabilities. An attacker with a map of machines and services that are available on a network can use the information to look for exploits. Aimed at acquiring information about the target network from a source that is often external to the network. Then the basic connection level features such as the “duration of connection” and “source bytes” are significant while features like “number of files creations” and “number of files accessed” are not expected to provide information for detecting probes.

DoS Attacks

The Denial of service (DoS) attacks also called the Distribution Denial of Service (DDoS) attacks are meant to force the target to stop the service that is provided by flooding it with probes illegitimate requests. The DoS attack to be detected that the traffic features such as the “percentage of connections having same destination host and same service” and packet level features such as the “source bytes” and “percentage of packets with errors” are significant. Detecting the DoS attacks is not being important to know whether a user is “logged in or not”. DoS is a class of attack where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate users access to a machine.
DoS attack is an attempt to make a computer resource unavailable to its intended users in computer security. Typically the targets are high profile web servers and the attack attempts to make the hosted web pages unavailable on the internet. There are two main types of DoS attacks: flooding and flaw exploitations. Flooding attacks can be simply implemented. For example for this one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. Then if the attacker has access to greater bandwidth than the victim and this will easily and quickly overwhelm the victim. A Denial of Service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- Flooding a network, thereby preventing legitimate network traffic.
- Disrupting service to a specific system or person.
- Attacks can be directed at any network device, including attacks on routing devices and web, electronic mail, or Domain Name System Servers.
- Consumption of computational resources, such as bandwidth, disk space, or CPU time.

R2L Attacks

Unauthorized access from a remote machine. A Remote to Local user (R2L) attack is a class of attack where an attacker sends packets to a machine over a network, then exploits the machine’s vulnerability to illegally gain local access as a user. The R2L attacks are one of the most difficult to detect as they involve the network level and the host level features. Therefore select both the network level features such as the “duration of connection” and “service requested” and the host level features such as the “number of failed login attempts” among others for detecting R2L attacks.
U2R Attacks

Unauthorized access to local super user (root). User to Root (U2R) exploits are a class of attacks where an attacker starts out with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system. The U2R attacks involve the semantic details that are very difficult to capture at an early stage. Applications of these attacks are content based and target. Thus for U2R attacks features such as “number of file creations” and “number of shell prompts invoked” are selected while features such as “protocol” and “source bytes” are ignored.

The main protocols in which normally above discussed attacks occurred are described below:

ICMP

Internet Control Message Protocol (ICMP) is used by the IP layer to send one way informational messages to a host. No verification in ICMP which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets. Some of the few types of attacks that are associated with ICMP are as follows: ICMP DoS attack: this type of attacker could use either the ICMP “Time exceeded” or “Destination unreachable” messages. Together these ICMP messages can cause a host to immediately drop a connection link. An attacker can make use of this by simply forging one of these ICMP messages and sending it to one or both of the communicating hosts.

The ICMP redirect message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network. If an attacker forges an ICMP Redirect message then it can cause another host to send packets for certain connections through the attacker’s host. Ping of death means an attacker sends an ICMP echo request packet that is larger than the maximum IP
packet size. Since the received ICMP echo request packet is larger than the normal IP packet size then it is fragmented. The target cannot reassemble the packets and so the OS crashes or reboots. ICMP nuke attack means nukes send a packet of information that the target OS cannot handle then which causes the system to crash. ICMP ping flood attack means that the broadcast storm of pings overwhelms the target system so it cannot respond to legitimate traffic.

TCP

Transfer Control Protocol (TCP) provides the higher layer application reliable connection oriented service. Each TCP connection requires an establishment procedure and a termination step between communication peers. TCP also provides sequencing and flow control. Without any option, a TCP header occupies 20 bytes as shown in Figure 1.3. The sequence number is essential in keeping the sending and receiving datagram in proper order.

<table>
<thead>
<tr>
<th>Source Port Number</th>
<th>Destination Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Acknowledge Number</td>
<td></td>
</tr>
<tr>
<td>Header</td>
<td>Reserved</td>
</tr>
<tr>
<td>URG,ACK,PSH,RST,SYN,FIN</td>
<td>Window Size</td>
</tr>
<tr>
<td>TCP Checksum</td>
<td>Urgent Pointer</td>
</tr>
<tr>
<td>Options (If Any)</td>
<td></td>
</tr>
<tr>
<td>Data (If Any)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1.3 TCP Header

There are six flag bits within a TCP header, namely URG, ACK, PSH, RST, SYN and FIN, each of which has a special meaning in connection establishment, connection termination or other control phases. Window size, which specifies how many bytes of data can be accepted each time by the
receiving side, is advertised between the two communication peers for the purpose of flow control.

If one application wants to communicate with another via TCP then it sends a communication request. Exact addresses are received by this type of request. TCP will set up a full duplex communication between the two applications after a handshake between the two applications are received; the full duplex communication will occupy the communication line between the two computers until it is closed by one of the two applications.

Attack begins as a normal TCP connection the client and the server exchange information in TCP packets. The TCP client continues to send ACK packets to the server and these ACK packets tells the server that a connection is requested. Then the server responds to the client with an ACK packet and the client is supposed to respond with another packet accepting the connection to establish the session. The clients continually send and receive the ACK packets but it does not open the session in this type of attack. The server holds these sessions open and awaiting the final packet in the sequence. This cause the server to fill up the available connections and denies any requesting clients access. TCP sequence number attack means when the attacker takes control of one end of a TCP session. TCP message is sent the client or the server generates a sequence number each time. The attacker intercepts and then responds with a sequence number similar to the one used in the original session. This attack can then disrupt a session. The attacker can place himself between the client and the server at that time of valid sequence number is guessed.

**UDP**

User Datagram Protocol (UDP) uses a simple transmission model without implicit handshaking dialogues for providing reliability and ordering or data integrity. UDP provides an unreliable service and datagram may arrive out of
order and appear duplicated or go missing without notice. It assumes that error checking and correction is either not necessary or performed in the application avoiding the overhead of such processing at the network interface level [Postel 1980]. UDP flood attack is one of the attacks in UDP it is similar to the ICMP flood attack. This type of UDP flood attack sends a large number of UDP messages to the target in a short time so that the target gets too busy to transmit the normal network data packets. The port numbers in UDP header identify the sending process and the receiving process, while the checksum provides a limited ability for error detection (Figure 1.4).

<table>
<thead>
<tr>
<th>Source Port Number</th>
<th>Destination Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Length</td>
<td>UDP Checksum</td>
</tr>
<tr>
<td></td>
<td>Data</td>
</tr>
</tbody>
</table>

*Figure 1.4 UDP Header*

However, due to its simplicity and low overhead compared to connection-oriented protocols, UDP is suitable for the design of simple request/reply application protocol, such as DNS (Domain Name System), SNMP (Simple Network Management Protocol), and so on.

1.6 **SVM CLASSIFICATION**

Support Vector Machines (SVM) are an effective method to solve pattern recognition and regression problems such as handwritten recognition, face image recognition and time series prediction. At present, SVM has become a research hotspot of machine learning. In the applications of SVM, researchers pay much attention on its learning efficiency and generalization performance, and proposed novel approaches to improve the learning efficiency of SVM. Although some achievements have been made, the data size in real world applications is often
large and the generalization performance is largely depended on kernel function. Therefore, the researches on how to improve learning efficiency and generalization performance of SVM combining with other artificial intelligence methods still have important theoretical and practical value.

SVM are new machine learning methods based on statistical learning theory which is proposed by Vapnic and co-workers [N. Cristianini and J. Shawe-Taylor, 2000]. A SVM are the classifiers which were originally designed for binary classification [Xiaodan Wang et al, Pang Ning Tan et al, 2006], can be used to classify the attacks. Binary classification problems can be solved using SVM. It belongs to the family of generalized linear classifier and can be interpreted as an extension of the perceptron. A special property is that they simultaneously minimize the empirical classification error and maximize geometric margin and hence they are also known as maximum margin classifiers.

This learning machines that plot the training vectors in high dimensional feature space and labeling each vector by its class. It classify data by determining a set of support vectors and which are members of the set of training inputs that outline a hyper plane in the feature space. Reasons for the use of SVMs for intrusion detection is the speed is one of the reasons, as a real-time performance is of primary importance to IDS and any classifier that can potentially run fast is worth considering. Scalability is the second reason that the SVMs are relatively insensitive to the number of data points and the classification complexity does not depend on the dimensionality of the feature space [Joachims 1998], so they can potentially learn a larger set of patterns and thus be able to scale better than neural networks. If the data is classified into two classes then suitable optimizing algorithm can be used if necessary for further feature identification, depending on the application [Joachims 1998].
Applications of SVM

Support Vector Machines are finding many uses in pattern recognition and classification tasks. The task of text categorisation refers to the classification of natural text documents into a fixed number of predefined categories based on their content. This is important in email filtering, web searching, sorting documents by topic and classification of news stories. The automatic categorisation of images is gaining importance in medical applications. Hand-written digit recognition was one of the real world tasks on which Support Vector Machines were tested. The problem on which the test was carried is used a benchmark for classification schemes.

Support Vector Machines did as well on the problem as other classification algorithms that were designed specifically for this problem. It is remarkable that SVM performed as well as these other systems without any detailed prior knowledge. Bioinformatics is another area where SVMs are being applied in many different ways. One important area of research in bioinformatics is to predict the features of a protein based on its amino acid sequence. One approach involves relating new protein sequences to proteins whose properties are already known. Similarity between proteins is called protein homology. An SVM based protein homology detection system handily outperformed state-of-the art protein homology detection systems.

SVMs are being used in the automatic categorization of gene expression data from DNA microarrays. As the volume of genomics data grows, it is becoming important to have automated means of assigning functions to genes. SVMs are being applied very successfully in gene expression data for classifying unseen genes and have outperformed various systems that use Fisher's Linear Discriminant or decision trees techniques.
1.7 GRANULAR COMPUTING

Granular computing focuses on problem solving based on the common sense concepts of granule, granulated view, granularity, and hierarchy. They are interpreted as the abstraction, generalization, clustering, levels of abstraction, levels of detail, and so on in various domains. The granular computing is taken as a study of a general theory of problem solving based on different levels of granularity. Granular computing can be studied by applying its principles and ideas. It can be investigated in different levels or perspectives by focusing on its philosophical foundations, basic components, fundamental issues, and general principles. Granular Computing consists of components by which it is constructed. The basic components and their interactions by which any granular computation is constructed discussed below:

Granules

A granule may be interpreted as one of the numerous small particles forming a larger unit. Collectively, they provide a representation of the unit with respect to a particular level of granularity. That is, a granule may be considered as a localized view or a specific aspect of a large unit. Granules are regarded as the primitive notion of granular computing. Its physical meanings become clearer when dealing with more concrete models. For example, in set-theoretic setting, such as rough sets, quotient space theory and cluster analysis, a granule may be interpreted as a subset of a universal set [Pawlak 1991]. In planning, a granule can be a sub-plan. In programming, a granule can be a program module [Ledgard et al 1979]. The size of a granule is considered as a basic property. Intuitively, the size may be interpreted as the degree of abstraction, concreteness, or detail. In the set-theoretic setting, the size of a granule can be the cardinality of the granule. Connections and relationship between granules can be represented by binary
relations. In concrete models, they may be interpreted as dependency, closeness, or overlapping.

**Hierarchies**

Granules in different levels are linked by the order relations and operations on granules. The order relation on granules can be extended to granulated views (levels). A level is above another level if each granule in the former level is ordered before a granule in the latter level, and each granule in the latter level is ordered after a granule in the former level, under the order relation. The ordering of levels can be described by the notion of hierarchy. The theory of hierarchy provides a multi-layered framework based on levels. A granule in a higher level can be decomposed into many granules in a lower level, and conversely many granules in a lower level can be combined into one granule in a higher level. A granule in a lower level may be a more detailed description of a granule in a higher level with added information.

**Granular Structures**

The internal structure of a granule provides a proper description, interpretation, and characterization of the granule. A granule may have a complex structure itself. For examples, the internal structure of a granule may be a hierarchy consisting of many levels. The internal structure is also useful in establishing linkage among granules in different levels. All granules in a level may collectively show a certain structure. This is the internal structure of a granulated view.

A hierarchy represents the overall structure of all levels. In a hierarchy, both the internal structure of granule and the internal structure of granulated views are reflected, to some degree, by the order relations. In a hierarchy, not any two granulated views can be compared based on the order relation. In the special case, the hierarchy is a tree.
Granular computing is a new concept and computing paradigm in the domain of information processing. It covers all the research about theories, methods, techniques and tools of granulation, and it can be used to process large scale information. The essence of granular computing is to find an approximate solution, which is simple and low-cost, to replace the exact solution through using inaccurate and large scale information to achieve the tractability, robustness, low cost and better describing the real world of intelligent systems or intelligent control. In a word, the combination of granular computing with intelligence computing approaches is becoming a hotspot to constitute efficient algorithms for complex problems. To improve the performance of traditional SVM, granular support vector machine, which combines statistical learning theory and granular computing is used in this work.

1.8 KDD DATASET

*KDD Cup’99 dataset*

The Knowledge Discovery and Data Mining (KDD) Cup 1999 dataset [KDD Cup 2007] used for benchmarking intrusion detection problems is used in our experiment. The first important deficiency in the KDD data set is the huge number of redundant records. Since 1999, KDD’99 has been the most wildly used data set for the evaluation of anomaly detection techniques. This data set is built based on the data captured in DARPA’98 (Defense Advanced Research Projects Agency) IDS evaluation program [Lippmann et al., 2000]. DARPA’98 is about 4 gigabytes of compressed raw (binary) tcpdump data of 7 weeks of network traffic. It can be processed into about 5 million connection records and each with about 100 bytes. Two weeks of test data have around 2 million connection records. Training dataset of KDD consists of approximately 4,900,000 single connection
vectors each of which contains 41 features and is labeled as either normal or an attack and with exactly one specific attack type.

**KDD Cup’99 Features**

- Basic features: Type of this category encapsulates all the attributes that can be extracted from a TCP/IP connection and most of these features leading to an implicit delay in detection.
- Traffic features: Type of this category includes features that are computed with respect to a window interval and is divided into two groups:
  - “Same host” features: It examine only the connections in the past 2 seconds that have the same destination host as the current connection and calculate statistics related to protocol behavior and service etc.
  - “Same service” features: It examine only the connections in the past 2 seconds that have the same service as the current connection.
- Content features: Unlike most of the DoS and Probing attacks the R2L and U2R attacks do not have any intrusion frequent sequential patterns. Because of the DoS and Probing attacks involve many connections to some host in a very short period of time. But R2L and U2R attacks are embedded in the data portions of the packets and normally involve only a single connection. To detect these kinds of attacks need some features to be able to look for suspicious behavior in the data portion example number of failed login attempts. This type of features are called content features.
**NSL-KDD dataset**

The new version of KDD data set is NSL-KDD. NSL-KDD dataset is a reduced version of the original KDD Cup’99 dataset. NSL-KDD consists of the same features as KDD Cup’99. This dataset consists of 41 features and one class attribute. The class attribute has 21 classes that fall under four types of attacks: Probe attacks, User to Root (U2R) attacks, Remote to Local (R2L) attacks and Denial of Service (DoS) attacks. This dataset has a binary class attribute. Also, it has a reasonable number of training and test instances which makes it practical to run the experiments on. The following are the advantages compared with the original KDD data set:

- It does not include redundant records in the train set, so the classifiers will not be biased towards more frequent records.
- There is no duplicate record in the proposed test sets; therefore, the performances of the learners are not biased by the methods which have better detection rates on the frequent records.
- The number of selected records from each difficulty level group is inversely proportional to the percentage of records in the original KDD data set. As a result, the classification rates of distinct machine learning methods vary a wider range, which makes it more efficient to have an accurate evaluation of different learning techniques.
- The numbers of records in the train and test sets are reasonable, which makes it affordable to run the experiments on the complete set without the need to randomly select a small portion.
1.9 PROBLEM SPECIFICATION

Several studies regarding machine learning methods are extensively used in network security. The network security industry is still evolving, adapting and responding to the persistent pressure exerted by cyber criminals. SVM is much suitable for solving pattern classification problems, suits for high dimensional data and error can be controlled explicitly. Therefore this research examines the SVM algorithms and explains the application domain Network Intrusion Detection System for each one.

NIDS tries to identify security attacks of intruders by investigating several data records observed in process on the network. The process of identifying and responding to intrusion activities is a tough process. Unknown anomalies or intrusions recognition is also tough. Detection of suspected intrusion is tedious, to provide a comprehensive overview of significant Support Vector Machine algorithms and discuss their suitability for these kinds of systems.

This research will use SVM based algorithms to produce a prediction model capable of classifying normal and abnormal traffic. The observed network flow data will contain traffic features, as well as a classification of whether each network flow instance (each of which is comprised of multiple behavioral features) is normal, or an anomaly.

Using the constructed hypothesis model, previously unobserved network flow data instances will be presented to the model for prediction. The model will attempt to predict whether or not the instance is normal or anomalous, and the result recorded. This will be repeated for all instances in the unobserved set to determine how closely the created model represents reality, and thus the overall usefulness for traffic classification.
1.10 OBJECTIVES OF THE RESEARCH

The main goal of the research is to propose new techniques for NIDS and it includes:

- To use data mining techniques for intrusion detection in communication networks.
- To identify intrusions based on a known pattern for the malicious activity.
- To identify malicious traffic based on deviations from established normal network traffic patterns.
- To develop a NIDS system using SVM that increases the detection performance with faster convergence.
- To make the system to process a large set of dataset and for decreasing the chance of misclassification of attacks.

The proposed methodology aims to effectively for NIDS and to decrease misclassification of attacks. It consists of three phases:

- Network Intrusion Detection using Kernelized SVM
- Network Intrusion Detection using Granular SVM

1.11 ORGANIZATION OF THE THESIS

The thesis is organized as follows: Chapter I deals with the overview of Network Intrusion Detection System, its importance, overview of techniques and also discusses the objectives of the research. Chapter II analyses the previous work done in the areas of Network Intrusion Detection System. Chapter III deals with the brief description of the “Research Methodology” of the proposed approaches. Chapter IV describes the first proposed approach namely, “Network Intrusion
Detection using Kernelized SVM”. Chapter V describes the second proposed methodology namely, “Network Intrusion Detection using Granular Support Vector Machines”. Chapter VI deals with the improved methodology namely, “Network Intrusion Detection using GSVM-Repetitive Under Sampling”. Chapter VII gives the Experimental Results and Chapter VIII concludes the thesis with the findings. The works of several researchers are quoted and used as evidence to support the concepts explained in the thesis. All such evidences used are listed in the reference section of the thesis.

1.12 SUMMARY

This chapter completely deals with the brief explanation of Intrusion Detection and their data attacks. And this gives introduction for various techniques of support vector machines and granular computing which are going to be implemented further in this research work.