RESEARCH ON APPLICATION OF INTRUSION DETECTION SYSTEM IN DATA MINING

Shwetha Nayak B.

Dept of CSE, Canara Engineering College, Mangalore, shwetha.nayakb@gmail.com

Keywords: Intrusion Detection System (IDS), Data Mining, Firewall, Threat.

Abstract

Network security is a large and growing area of concern for every network. The more we invent for the good of humanity, humans try to negate the good factor and hence the fear of viruses and hacking. Research has to move in the direction of preserving and guarding network environments which today are facing an ever increasing number of security threats in the form of Trojan worm attacks and viruses that can damage the Computer systems and communication channel. Firewalls are used as a security check point in a network environment; nevertheless there are still various types of security issues which are on the rise. In order to strengthen the network from illegal access the concept of IDS (Intrusion Detection System) is gaining popularity around the world.

The applications of the data mining in the computer security field improves the development of IDS in order to work on these applications it is essential to classify the degree of attacks in IDS and use it through data mining. Despite the use of IDS we cannot be completely certain about its workability and results of IDS use have been uncertain. To plug the loopholes we need to adjust the detection strategy according to the degree of attack activities to ensure error free results.

1 Introduction

In the process of development, internet brings large profit increase in our industry and makes our life easier and more convenient, but along with this there are some serious security problems existing like hacking and computer viruses which spread quickly across the network. One of the main challenges in the security management of large-scale high-speed networks is the detection of suspicious anomalies in network traffic patterns due to Distributed Denial of Service (DDoS) attacks or worm propagation. A secure network must provide the following:

Data confidentiality: Data that are being transferred through the network should be accessible only to those that have been properly authorized.

Data integrity: Data should maintain their integrity from the moment they are transmitted to the moment they are actually received. No corruption or data loss is accepted either from random events or malicious activity.

Data availability: The network should be resilient to Denial of Service attacks.

The first threat for a computer network system was realized in 1988 when the first worm was launched which overid over 6000 PCs of the ARPANET network. These threats and others that are likely to appear in the future have lead to the design and development of Intrusion Detection Systems. According to webopedia an intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a net work or system attack from someone attempting to break into or compromise a system.

Data mining refers to extracting or “mining” knowledge from large amounts of data. It should have been more appropriately named “knowledge mining from data,” which is somewhat long so it was called “Knowledge mining”. Many other terms carry a similar or slightly different meaning to data mining, such as knowledge mining from data, knowledge extraction, Data / pattern analysis, data archaeology, and data dredging.

There are many data which made from messages flow in the networks. And the obvious feature of data mining technique is to recover novel and useful knowledge from mass data to forecast what will happen in the future. Data mining technology has gotten great success in some fields such as commerce, finance etc. The message in net and the audit information which remain in server and work station become analytical object of data mining technology, because the count of them are very large, we can imagine that there will be significant meaning if we handle these data under operate data mining technology effectively.

2 Intrusions

Intrusions are actions that attempt to bypass security mechanisms of computer systems. So they are any set of actions that threatens the integrity, availability, or confidentiality of a network resource. These properties have the following explanations:

Confidentiality – means that information is not made available or disclosed to unauthorized individuals, entities or processes.

Integrity – means that data has not been altered or destroyed in an unauthorized manner. Availability – means that a system or a system resource that ensures that it is accessible and usable upon demand by an authorized system user.

Availability is one of the core characteristics of a secure system.

Occasionally intrusions are caused by: Attackers accessing the system from Internet; Insider attackers − authorized users attempting to gain and misuse non-authorized privileges. Examples of intrusions:

Denial of service (DoS): DoS is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users access to a machine. Having network connectivity available through more than one service provider can be part of the answer to this problem. At least that way, when the main entrance is blocked, you can use the emergency exit to maintain at least minimal communications such as email. There are many varieties of DoS attacks. Some DoS attacks (like a mailbomb, neptune, or smurf attack) abuse a perfectly legitimate feature. Others (teardrop, Ping of Death) create malformed packets that confuse the TCP/IP stack of the machine that is trying to reconstruct the packet. Still others (apache2, back, syslogd) take advantage of bugs in a particular network daemon. User to Root Attacks (U2R): this is a class of exploit in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system. There are several different types of U2R attacks where the most common is the buffer overflow attack. Buffer overflows occur when a program copies too much data into a static buffer without checking to make sure that the data will fit.

Scan: it is the reconnaissance on the network or a particular host. The purpose of port scanning is to determine what ports are open, and hence what services that may be running on a system are available to the attacker. This result is utilized for good by network and system administrators as a part of network security audits, and for evil by attackers who wish to compromise a box by using an exploit for one of the discovered running services on its open port. Port scanning also provides a number of additional applications and the added bonus of possibly being able to determine what OS a system is using (due to inconsistent or peculiar responses each OS's implementation of the TCP/IP stack returns). Port scanning's additional applications can also tell us what hosts are up on a network and various other network topological details, such as IP addressing, MAC addressing, router and gateway filtering, firewall rules, IP-based trust relationships, etc.

Remote to Local (R2L): In this type an attacker who does not have an account on a victim machine, gains local access to machine, infiltrates files from the machine, or modifies data in transit to the machine.

3 Intrusion Detection System

Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, like unauthorized entrance, activity, or file modification. There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic.
- Identifying abnormal activities.
- Assessing severity and raising alarm.

Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Some DoS attacks are too complex for today's firewalls, e.g. if there is an attack on port 80 (web service), firewalls cannot prevent that attack because they cannot distinguish good traffic from DoS attack traffic. Additionally, firewalls are too deep in the network hierarchy. Your router may be affected even before the firewall gets the traffic. Nonetheless, firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall. We have to consider redundancy issues when building the local network. Critical components are not only the firewall and related hosts, but also servers (shadow file servers, shadow disks, surplus workstations, and hot spares). To protect against interrupted power supplies, backup power arrangements should be made. Firewalls are not the ultimate solution and must be supplemented by appropriate authentication and authorization throughout the network. To recognize attacks and possible breaches of security, adequate administration and control must be ensured. Firewalls are useless if, for example, log files are not regularly checked for suspicious activities (at least daily).

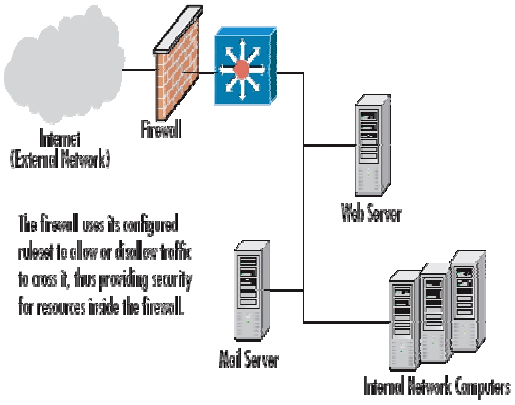

Figure 1: Basic Firewall Installation.

Intrusion Detection System (IDS) is software that automates the intrusion detection process and detects possible intrusions. Intrusion Detection Systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. An IDS is composed of several components:

- **Sensors** which generate security events;
- **Console** to monitor events and alerts and control the sensors;
- **Central Engine** that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

In many simple IDS implementations these three components are combined in a single device or appliance. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. IDSs use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain IDSs have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap. Many IDSs not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts. IDSs are an integral and necessary element of a complete information security infrastructure performing as "the logical complement to network firewalls". Simply put, IDS tools allow for complete supervision of networks, regardless of the action being taken, such that information will always exist to determine the nature of the security incident and its source. Ideally the team's network is separated from the outside world by a well-designed firewall. The outside world includes the team's host organization.

Firewalls protect a network and attempt to prevent intrusions, while IDS tools detect whether or not the network is under attack or has, in fact, been breached. IDS tools thus form an integral part of a thorough and complete security system. They don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack such as a DoS attack. IDSs remain the only proactive means of detecting and responding to threats that stem from both inside and outside a corporate network.

Intrusion detection tools use several techniques to help them determine what qualifies as an intrusion versus normal traffic. Whether a system uses anomaly detection, misuse detection, target monitoring, or stealth probes, they generally fall into one of two categories:

Host-based IDSs (HIDS) – examine data held on individual computers that serve as hosts. The network architecture of host-based is agent-based, which means that a software agent resides on each of the hosts that will be governed by the system.

Network-based IDSs (NIDS) – examine data exchanged between computers. More efficient host-based intrusion detection systems are capable of monitoring and collecting system audit trails in real time as well as on a scheduled basis, thus distributing both CPU utilization and network overhead and providing for a flexible means of security administration.

Each technique has a distinct approach to monitoring and securing data and each category has strengths and weaknesses that should be measured against the requirements for each separate target environment. The two types of intrusion detection systems differ significantly from each other, but complement one another well. But in a proper IDS implementation, it would be advantageous to fully integrate the network intrusion detection system, such that it would filter alerts and notifications in an identical manner to the host-based portion of the system, controlled from the same central location. In doing so, this provides a convenient mean of managing and reacting to misuse using both types of intrusion detection.

Ideally, the best IDS tools combine both approaches under one management console. That way, the user gets comprehensive coverage, making sure to guard against as

many threats as possible. As an organization introduces IDS into its network to augment its current information security strategy, the primary focus of the intrusion detection system should be host-based. Consequently, intrusion detection systems should rely predominantly on host-based components, but should always make use of network-based IDSs to complete the defense. In short, a truly secure environment requires both a network and host- based intrusion detection implementation to provide for a robust system that is the basis for all of the monitoring, response, and detection of computer misuse.

Now that we have examined the two basic types of IDS (HIDS and NIDS) and why they should be used together, we can investigate how they go about doing their job. For each of the two types, there are four basic techniques used to detect intruders: anomaly detection, misuse detection (signature detection), target monitoring and stealth probes.

- Anomaly detection: Designed to uncover abnormal patterns of behaviour, the IDS establishes a baseline of normal usage patterns, and anything that widely deviates from it gets flagged as a possible intrusion. What is considered to be an anomaly can vary, but normally, we think as an anomaly any incident that occurs on frequency greater than or less than two standard deviations from the statistical norm. It identifies anomalies as deviations from “normal” behaviour and automatically detects any deviation from it, flagging the latter as suspect. Thus these techniques identify new types of intrusion as deviations from normal usage. It is an extremely powerful and novel tool but a potential drawback is the high false alarm rate, i.e. previously unseen (yet legitimate) system behaviours may also be recognized as anomalies, and hence flagged as potential intrusions. If a user in the graphics department suddenly starts accessing accounting programs or compiling code, the system can properly alert its administrators.
- Misuse detection (Signature detection): here each instance in a data set is labelled as “normal” or “intrusive” and a learning algorithm is trained over the labelled data. These techniques are able to automatically retrain intrusion detection models on different input data that include new types of attacks; as long as they have been labelled appropriately. Unlike signature-based IDS, models of misuse are created automatically and can be more sophisticated and precise than manually created signatures. They have high degree of accuracy in detecting known attacks and their variants. Their disadvantage is that they cannot detect unknown intrusions and they rely on signatures extracted by human experts. This method uses specifically known patterns of unauthorized behaviour to predict and detect subsequent similar attempts. These specific patterns are called signatures. For host-based intrusion detection, one example of a signature is "three failed logins." For network intrusion detection, a signature can be as simple as a specific pattern that matches a portion of a network packet. For instance, packet content signatures and/or header content signatures can indicate unauthorized actions, such as improper FTP initiation. The occurrence of a signature might not signify an actual attempted unauthorized access. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response, or notification should be sent to the proper authorities.
- Target Monitoring – these systems do not actively search for anomalies or misuse, but instead look for the modification of specified files. This is more of a corrective control, designed to uncover an unauthorized action after it occurs in order to reverse it. One way to check for the covert editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the mission/system critical files.
- Stealth Probes – this technique attempts to detect any attackers that choose to carry out their mission over prolonged periods of time. Attackers, for example, will check for system vulnerabilities and open ports over a two-month period, and wait another two months to actually launch the attacks. Stealth probes collect a wide -variety of data throughout the system, checking for any methodical attacks over a long period of time. They take a wide-area sampling and attempt to discover any correlating attacks. In effect, this method combines anomaly detection and misuse detection in an attempt to uncover suspicious activity.

4 Drawbacks of intrusion detection system

Intrusion Detection Systems (IDS) have become a standard component in security infrastructures as they allow network administrators to detect policy violations. These policy violations range from external attackers trying to gain unauthorized access to insiders abusing their access.

Current IDS have a number of significant drawbacks:

- Current IDS are usually tuned to detect known service level network attacks. This leaves them vulnerable to original and novel malicious attacks.
- **Data overload**: Another aspect which does not relate directly to misuse detection but is extremely important is how much data an analyst can efficiently analyze. That amount of data he needs to look at seems to be growing rapidly. Depending on the intrusion detection tools employed by a company and its size there is the possibility for logs to reach millions of records per day.
- **False positives**: A common complaint is the amount of false positives IDS will generate. A false positive occurs when

normal attack is mistakenly classified as malicious and treated accordingly.

- **False negatives**: This is the case where IDS does not generate an alert when an intrusion is actually taking place. (Classification of malicious traffic as normal)

Data mining can help improve intrusion detection by addressing each and every one of the above mentioned problems.

5 Data mining

Data mining (DM), also called Knowledge-Discovery and Data Mining, is the process of automatically searching large volumes of data for patterns using association rules. It is a fairly recent topic in computer science but utilizes many older computational techniques from statistics, information retrieval, machine learning and pattern recognition.

Some of the basic KDD steps are:

1. Understanding the application domain: First is developing an understanding of the application domain, the relevant background knowledge, and the specific goals of the KDD endeavour.

2. Data integration and selection: Second are the integration of multiple (potentially heterogeneous) data sources and the selection of the subset of data that is relevant to the analysis task.

3. Data mining: Third is the application of specific algorithms for extracting patterns from data.

4. Pattern evaluation: Fourth is the interpretation and validation of the discovered patterns. The goal of this step is to guarantee that actual knowledge is being discovered.

5. Knowledge representation: This step involves documenting and using the discovered knowledge.

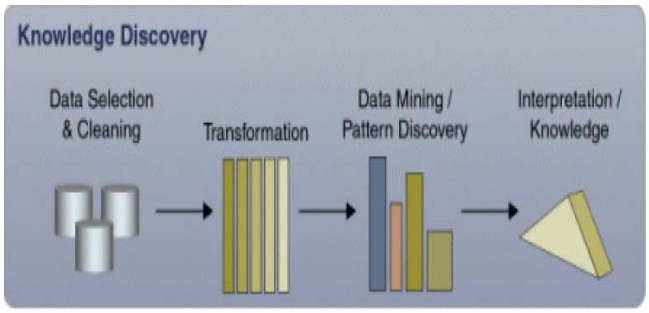

Figure 2: Data Mining process of Knowledge Discovery

Data Selection and Cleaning (Pre-processing): Selection of relevant items for representation

- Integrate data from different formats and heterogeneous sources.
- Verify correct ranges and limits.

Data cleaning of invalid data

- Use existing data to extrapolate.
- Compute the least noisy representation.

Transformation (pre-processing): Input-format related transformations.

Data Mining/ Pattern Discovery:

- Identify sets of information to be mined
- Technique selection: association mining, clustering, time-series analysis.
- Extend the patterns to larger selections.
- Pattern Evaluation.

Interpretation Knowledge (Post-processing):

- Documentation.
- Order patterns with metrics.
- Highlight most relevant patterns.
- Visualization.

Data Mining is used for wide variety of purposes both in private and in public sectors. Its areas of applications are:

Risk Analysis: Insurance Companies and Banks use Data Mining for Risk Analysis. An Insurance Company searches in its own insurants and claims databases for relationships between personal characteristics and claim behavior. The companies are mostly interested in the characteristics of insurants with a highly deviating claim behavior, premium policy etc.

Direct Marketing: Data Mining techniques are used to discover the relationship between one's personal characteristics.

Production Quality Control: Data Mining can be used to determine the combinations of production factors that influence the quality of the product. This information allows the process engineers to explain why certain products fail the final test and to increase the quality of the production process.

Surveillance: Data Mining techniques could be used by various public and private agencies to monitor the behavior, activities and/or changing information, usually of individuals or groups.

Science: The Data Mining techniques are used in Scientific and Engineering fields such as astronomy, bio-informatics etc., and in Medical field in the discovery of drugs.

Security: Data Mining techniques are mostly used in the Security and Fraud Detection applications. Many Financial organizations, Telecom companies have developed the applications based on Data Mining and to detect the frauds.

Criminal and Forensic Investigations: The data Mining technique has been used in the forensic department to identify the fingerprint, patterns, images taken from a crime scene, images taken from suspects or images to be used as control samples etc. Data mining techniques are used in the investigation of the domestic violence, death, threat to person or property, fraud or any other crimes that require complex detection.

Tax Administration: Data Mining techniques have been used by the Income Tax department to identify the audit targets to enforce the tax payment.

a.

b.

Aviation Safety: Discovery of the accidental trends in aviation, and precaution measure to ensure to prevent such type of event does not happen in future.

6 Intrusion detection system in data mining

Data Mining is also called Knowledge Discovery in Database. These data are usually numerous, incomplete, indistinct and random. Data as original information can also be called knowledge. In general, knowledge refers to concepts, rules and restraints. The method of finding knowledge can be mathematical or non-mathematical. It can be deductive or inductive. The known knowledge can be used to optimize enquiry, manage information, control progress and make intellectual decision. Data mining is a criss-cross subject. It helps people to apply data from low and simple inquiry to discover knowledge in data and support decision. For our understanding we divide intrusion detection into two categories:

- The Misapplication Detection Strategy
- The Abnormal Detection Strategy.

Both strategies have their own advantages and disadvantages. In Misapplication Detection Model, every entity in the data collection is marked as normal or invasive. We construct invasion model through machine study or the analytical technology of data mining from these data. This invasive model will bring rules and classify the given data according to the characteristics of the sample data. The advantage of adopting misapplication detection model is that the detection of known attack behavior is very effective. At the same time, invasive model has a favorable openness and it can use the data, which has new mark as training collection. Then add it to invasion model after learning, so that it includes new styles of attack. The disadvantage of invasion model is that the accuracy of data log influences the rationalization of the model very much, and incorrect log data will lead to the increased rate of misreport. Besides, the collect behavior of these log data also is quite a difficult task. The major limitation of misapplication detection model is that it cannot distinguish the attack behavior of unknown style because it just includes the description of known attack actions. Before the invasion behavior added to detection model, the system is totally open to this kind of attacks, and to some extent it is unsafe. At present, the abnormal detection model is the most widely used intrusion detection measure, and still there are lots of researches going on in this field.

In the analysis of intrusion detection system, the data circulating in network has the following characteristics:

Mass data, even if a small commercial website,

The number of data message sent and received are quite impressive and incomplete whose transportation is busy.

Data message that overweigh network carry will be discarded when network is unstable. Data information may get changed in the transportation of message. We can see that these data is in accordance with the feature of object of data mining. We want to apply data mining technology in the Intrusion Detection System. Figure-7 describes application of IDS with data mining. Both the Abnormal Detection Model and Misapplication Detection Model need to log data as training data whose accuracy will largely influence Intrusion Detection System. Because of density and accuracy of visit network, it is difficult to acquire completely the attack actions. In addition, it is also uneasy to log the attack behavior. Data mining techniques can reveal this problem.

The analysis of general network visit and isolated point is an invasive behavior which reduces the difficulty of acquisition of training data. Normally, we need to decide which feature is effective to express network and system action when we build intrusion detection system. Some characteristics can be extracted directly from audit data; others need to be taken from the statistics and are computed using the audit data, such as the quantity in TCP message in certain period of time. It is difficult to make these decisions, with the use of data mining techniques.

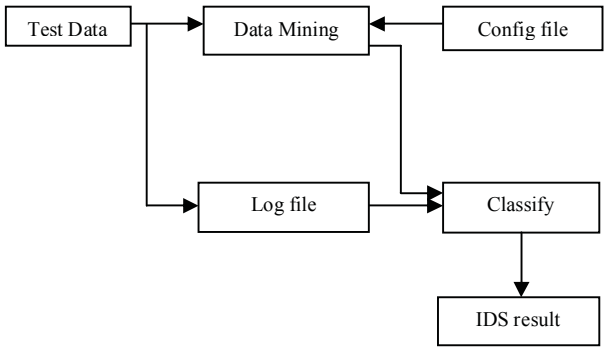

Figure 3: IDS with Data Mining

Intrusion Detection System is a passive method. It monitors information system and sends out warning when it detects intrusion, but data mining techniques can analyze these data when network information is acquired, it can forecast the visits on its own initiative, reduce the frequency of matching, and thus achieving the function of active defence. Data mining techniques, for instance, Clustering, Classification, Feature Summary, and Association Rules can be applied in the Intrusion Detection System. It has been proved that data mining techniques improves the property of intrusion detection system, the processing rate and reduces the rate of misreporting.

Audit log: It captures all system calls, all file opens, closes, read and writes and all new processes and their owners, process Ids, parent process Ids and arguments.

7 The distinction of attack degree

It is rare to define that one network behaviour is normal or invasive in intrusion detection system, in most cases, it is uncertain. More often than not, the majority of network behaviours may perform either normal or invasive, under this circumstance, the intrusion detection system cannot make sound judgment, thus, the rate of misreport is high. In order to resolve this problem, intrusion detection system needs to deal with this kind of uncertainty.

Adding confidence into the rule of intrusion detection system and the form of rule r is:

$f1 \wedge f2 \wedge \ldots \wedge fn \rightarrow fn+1\ \theta$, $0 <= \theta <= 1$

θ stands for Confidence.

TABLE 1: THE MEANING OF θ

θ	Meaning
$\theta = 0$	Sure for being normal.
$0 < \theta < 0.5$	May be normal, the lower number the stronger definition
$\theta = 0.5$	Know nothing about the conclusion
$0.5 < \theta < 1$	May be invasion of higher number, the stronger definition
$\theta = 1$	Sure for being invasive

Through the uncertainty, data mining technology break away from the limitation that "if not true then false" in the process of data training, we can give different number of θ according to distance, and its result is more exact and mere reasonable.

For uncertain distinction, we can simply give normality or possible normality, intrusion or possible intrusion and every number correspond to a region of θ. The attack distinction is helpful to integrate different intrusion detection system, some sensitive security organizations adopt multiple intrusion detection system to protect their network, while the attack detection degree is enhanced, it also increases the difficulty of distinguishing and the rate of misreporting. How to integrate these intrusion detection systems is a comparatively real problem. The integrated idea that has been mentioned before is to integrate middle result from multiple intrusion detection system. It is expressed by scene then the final result is got. This pattern is fairly difficult and it needs to learn internal structure of each intrusion detection system well. The method for the integration of dividing attack degree is to put results from different intrusion detection system into a unified standard and the process of integration is simple and easy.

Before integration, it is required that multiple IDS with certain behavior meet the conditions of consistent process.

Definition 1: for a certain behaviour A, multiple IDS have given judgments, and all absolute value about the difference between confidence judgment from any two IDS in the group are less than α($0< \alpha<p$) and all IDS about its confidence judgment belong to the region that [0,p], or $0<\alpha<p$ and all IDS about its confidence judgment to the region that [p,1] and $0<p<1$.

And then we can say multiple IDS system meets the condition of the consistent process. For a system that requires high safety, we can adopt the strategy that emulate the highest confidence and suppose that authoritative of each IDS is close.

There is only a IDS confidence judgment that is the highest in Cooperation group , in this case, other IDSs will close up to IDSi, that is to say ,they adjust their confidence judgment and make them close to IDSi confidence.

IDSA algorithm:

Supposed that there are K IDS in Cooperation group.

Set j=1

if j<>i and j<=k then $\Delta=\alpha*(CFi-CFj)$ /* CFi and CFj are the confidence of IDSi and IDSj */

else if j<k then j=j+1 repeat it

$CFj=CFj+\Delta$

if j<k then j=j+1 and go to 2

else return

The strategies mentioned above embody the conservative attitude toward the judgment for IDSs, which is suitable to be used in the high safety environment. In other situations, it is subject to appropriate adjustments.

In addition, the result from the distinction of attack degree in intrusion detection system can be tested and corrected in practical data in network behavior. In order to avoid putting in too much energy and being influenced by subjective factors. This process should use data mining technology to realize, the nature of self-adjustment of data mining can make the analytical results more exact.

8 Conclusions

As security incidents are increasing, use of Intrusion Detection System (IDS) has become necessary. In is very likely that IDS capabilities will become core capabilities of network infrastructure and Operating systems. Application of Data Mining Technology in Intrusion Detection System (IDS) is an emerging trend. The traditional Intrusion detection System had difficulty in acquiring training data collection and it could not extract characteristic sample and achieve defence against intrusions. All this can be achieved using Data Mining technology.

The application of Data Mining technology, the sequence representation of data in network traffic is not mature, there are barriers in the application of Intrusion detection technology and the elasticity of system is not good, the analysis of huge amount of data, the method of handling data are immature. Lot of research can be done in this area.

References

[1] Research of Data Mining in Intrusion detection System and uncertainty of Attack: Wei Liu, IEEE-2009.

[2] A survey of Intrusion detection and prevention techniques: Usman Asghar Sandhu, Sajjad Haider, Salman Naseer, Obaid Ullah Ateeb, 2011 International Conference on Information Communication and Management IPCSIT vol.16.

[3] A short survey of Intrusion detection systems: Vera Marinova-Boncheva, Information of Information Technologies.

[4] Data Mining And Its Significance In Industrial Applications: Alok Ranjan, Prasana Kumara, IJARCS- Vol.3, 2012.

[5] Emerging Trends in Data Mining for Intrusion Detection: Dr. Ravindra s Hegadi, Alok Ranjan, Prasana Kumara, IJARCS- Vol.3, 2012.

[6] Data Mining Techniques for (Network) Intrusion Detection Systems: Theodoros Lappas and Konstantinos Pelechrinis, Department of Computer Science and Engineering, UC Riverside CA 92521.

[7] Attack Development for Intrusion Detection Evaluation: By Kumar J. Das.

[8] DATA MINING FOR INTRUSION DETECTION-A Critical Review: Klaus Julisch, IBM Research, Zurich Research Laboratory.

[9] INTRUSION DETECTION SYSTEM (IDS)-PRODUCT SURVEY: Kathleen A. Jackson.

[10] Intrusion Detection Systems: A Survey and Taxonomy, Stefan Axelsson, Department of Computer Engineering, Chalmers University of Technology, G¨oteborg, Sweden.