ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique

Deepika P Vinchurkar, Alpa Reshamwala
M. Tech Student, Assistant Professor, Department of Computer Engineering
MPSTME, SVKM's NMIMS University Mumbai, India

Abstract*—In the recent years, Intrusion Detection materializes the high network security. Thus tries to be the most perfect system to deal with the network security and the intrusions attacks. Monitoring activity of the network and that of threats is the feature of the ideal Intrusion Detection System. Intrusion Detection System is classified on the basis of the source of Data and Model of Intrusion. There are some challenges faced by the Intrusion Detection System. Neural Network amd Machine Learning are the approaches through which the challenges can be overwhelmed. Anomaly in the Anomaly based Intrusion Detection System can be detected using various Anomaly detection techniques. Dimension Reduction can be done using Principle Component Analysis. Support Vector Machine can be used to specify the classifier construction problem. The paper describes the various approaches of Intrusion detection system in briefly.

***Keywords*- Intrusion Detection system, Anamoly Based intrusion., Neural Network, Machine Learning, Principle ComponentAnalysis, Support Vector Machine.**

I. INTRODUCTION

Malicious users and crackers seek weak targets such as unpatched systems, systems infected with Trojans, and networks running insecure services The assurance of integrity and safety should be applied to computer systems and data. The Internet has made the information flow to the large extent. Also at the same time it has to face many threats and attacks. Thus the security alert is required to control the attacks and threats. A notification must be sent to the administrators and security team members about the various threats and attacks which has occurred so that they can respond in real-time to the threat. The paper describes the challenges in IDS. In this paper we discuss various techniques for anomaly detection techniques and focus on the machine learning based techniques. Principle Component Analysis algorithm to reduce dimensionality is described in the paper. The paper also focuses on classification using Support Vector Machines.

A. Intrusion Detection Systems (IDs)

An intrusion detection system (IDS) is an active process or device that analyzes system and network activity for unauthorized and nasty activity. Intrusion Detection System (IDS) is any hardware, software, or a combination of both that monitors a system or network of systems against any malicious activity. The ultimate goal of any IDS is to catch perpetrators in the act before they do real damage to resources. An IDS protects a system from attack, misuse, and compromise. It also monitor network activity, audit network and system configurations for vulnerabilities, analyze data integrity, and more. IDS, these days, have become vital component in the security toolbox An IDS provides three functions: monitoring, detecting and generating an alert. IDS are often considered as the functionality of firewall. But there is a difference between them. A firewall must be regarded as a hedge that protects the information flow and prevent intrusions where as IDS detects if the network is under attack or if the security imposed by the firewall has been penetrated. Together firewall and IDS enhance the security of network.

B. What is Not An IDs?

Contrary to popular market belief and terminology employed in the literature on intrusion detection systems, not everything falls into this category. In particular, the following security devices are NOT IDS:

- Network logging systems used, for example, to detect complete vulnerability to any Denial of Service (DoS) attack across a congested network.
- Anti-virus products designed to detect malicious software.
- Security/cryptographic systems, for example VPN, SSL, S/MIME, Kerberos, Radius etc.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

II. RELATED WORK

This concept has been around for nearly twenty years but only recently has it seen a dramatic rise in popularity and incorporation into the overall information security infrastructure. Beginning in 1980, with James Anderson's paper, *Computer Security Threat Monitoring and Surveillance*, the notion of intrusion detection was born. In 1983, SRI International, and Dr. Dorothy Denning, began working on a government project that launched a new effort into intrusion detection development. One year later, Dr. Denning helped to develop the first model for intrusion detection, the Intrusion Detection Expert System (IDES). The intrusion detection market began to gain in popularity and truly generate revenues around 1997. In that year, the security market leader, ISS, developed a network intrusion detection system called realsecure. The first visible host-based intrusion detection company, Centrax Corporation, emerged.. Furthermore, government initiatives, such as the Federal Intrusion Detection Network, (fidnet) created under Presidential Decision Directive 63, are also adding impetus to the evolution of IDS. Advancements in IDS will ultimately push security technology into a whole new arena of automated security intelligence.

III. STRUCTURE AND ARCHITECTURE

An intrusion detection systems always has its core element - a sensor (an analysis engine) that is responsible for detecting intrusions.. Sensors receive raw data from three major information sources (Figure.1):

- Own IDS knowledge base,
- Syslog and
- Audit trails.

The syslog may include, for example, configuration of file system, user authorizations etc. This information creates the basis for a further decision-making process. The sensor is integrated with the component responsible for data collection (Fig.2) — an event generator. The collection manner is determined by the event generator policy that defines the filtering mode of event notification information. The event generator (operating system, network, application) produces a policy-consistent set of events that may be a log (or audit) of system events, or network packets.

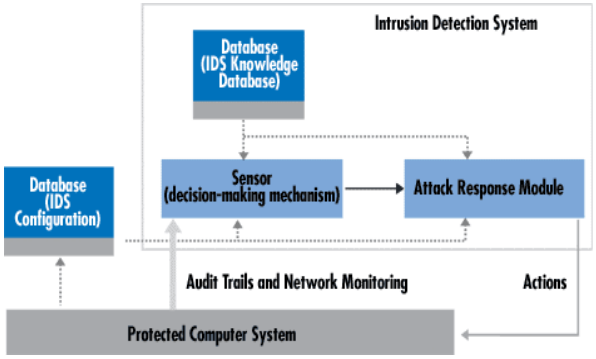

Fig 1.A Sample IDS. The Arrow Width is Proportional to the Amount of Information Flowing between System Components

The role of the sensor is to filter information and discard any irrelevant data obtained from the event set associated with the protected system, thereby detecting suspicious activities. The analyzer uses the detection policy database for this purpose. In addition, the database holds IDS configuration parameters, including modes of communication with the response module. The sensor also has its own database containing the dynamic history of potential complex.

A. Working Of Intrusion Detection System

The working of the intrusion detection system is quite similar as that of the other programs used to prevent the computer system from dangerous threats like malware, spyware, spam and many more. The job of the intrusion detection system starts from the recording the information about the problem and check the occurrence and the nature of the threat. When the system monitors the problem and collects the data about it, then it sends this information to the administration department of the intrusion detection system which makes several preventive

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

measures to protect the system and keep the system in the safe hands. Intrusion detection system can work in the specific manner by monitoring some important things. These important things are as follows.

1. Monitoring the activity of the network and activity of the threat in the network.
2. This system has ability to detect the viruses, malware, spyware and different form of viruses and the important thing about this it can also locate their restore point.
3. Intrusion detection system can work by observing the unauthenticated and unauthorized use of different programs of networking.

So, the whole working of the intrusion detection system based on the examination of such events of networking.

B. Ideal Intrusion Detection System

An ideal intrusion detection system [1] should address the following issues, regardless of mechanism it is based on:

1. The system must **run continually** without human supervision. It must be reliable enough to allow it to run in the background of the system being observed.
2. It should not be a "**black box**". That is, its internal workings should be examinable from outside.
3. It must be **fault tolerant** in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.
4. It must **resist subversion**. The system can monitor itself to ensure that it has not been subverted.
5. It must impose **minimal overhead** on the system. A system that slows a computer to a crawl will simply not be used.
6. It must **observe deviations** from normal behavior.
7. It must be **easily tailored** to the system. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.
8. It must deal with changing **system behavior** over time as new applications are being added. The system profile will change over time.
9. It must be **difficult to fool**.

All the above listed are the features that an ideal Intrusion Detection System must have. So that the system becomes perfect to defend the attacks and the intrusions.

IV. CATEGORIZATION OF INTRUSION DETECTION

An intrusion detection system (IDS) reviews all arriving and outbound network activity and recognizes guarded patterns that indicate a network or system attack from someone attempting to break into or compromise a system. Various classification[5] of the Intrusion Detection System are possible as per the different criteria. Initially the categorization can be done as follows as shown in figure 2:-

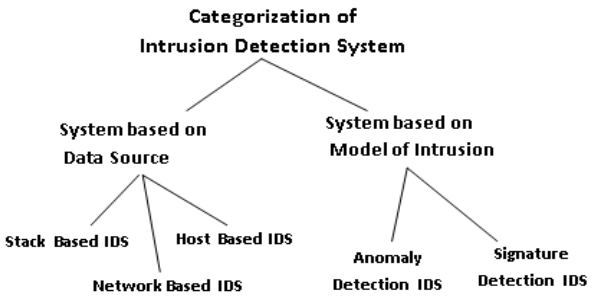

Fig 2. Categorization of Intrusion Detection System

A. Stack Based Intrusion Detection System (SIDS) :-

Stack based Intrusion Detection System (SIDS) is latest technology, which works by integrating meticulously with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers. Watching the packet

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

in this way allows the IDS to pull the packet from the stack before the OS or application has a chance to process the packets.

B. Network Based Intrusion Detection System (NIDS):-

Network based Intrusion Detection System (NIDS) monitors the traffic as it flows to other host. Monitoring criteria for a specific host in the network can be increased or decreased with relative ease. NIDS should be capable of standing against large amount of network traffic to remain effective. As network traffic increases exponentially NIDS must grab all the traffic and analyze in a timely manner.

C. Host Based Intrusion Detection System (HIDS):-

Host based Intrusion Detection System (HIDS) keeps record of the traffic that is originated or is projected to originate on a particular host.. HIDS controls the privileged access of the host to monitor specific components of a host that are not readily accessible to other systems.. HIDS has limited view of entire network topology and they cannot detect attack that is targeted for a host in a network which does not have HIDS installed

D. Anomaly Based Intrusion Detection System:-

Anomaly based Intrusion Detection System examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies. It works on the notion that "attack behavior" differs enough from "normal user behavior" such that it can be detected by cataloging and identifying the differences involved. The system administrator defines the baseline of normal behavior. Anomaly-based IDS systems are very prone to a lot of false positives .Anomaly-based IDS systems can cause heavy processing overheads on the computer system.

E. Signature Based Intrusion Detection System :-

Signature based Intrusion Detection System use a set of rule to identify intrusions by watching for patterns of events specific to known and documented attacks. It is typically connected to a large database which stocks attack signatures. These types of systems are able to detect only attacks "known" to its database. Thus, if the database is not updated with regularly, new attacks could slide through. Signature based IDS's affect performance when intrusion patterns match several attack signatures. In such cases, there is a noticeable performance lag. Signature definitions stored in the database need to be specific so that variations on known attacks are not missed. This can lead in building huge databases which eat up a chunk of space.

V. THREE PERSPECTIVES OF CHALLENGES IN IDSS

The performance of current IDSs [12] does not defend increasing number of attack types as many current IDS are still based on expert rules that are manually constructed by human experts and only describe known attack signatures. In this section, we analyze three perspectives of technical challenges in IDSs based on machine learning, which are feature extraction, classifier construction and sequential pattern prediction. To explain the three perspectives of technical challenges, a general framework for IDSs based on machine learning is presented in Figure 3. The framework is composed of three main parts. The first one is for data acquisition and feature extraction. Data acquisition is observes network flow data or process execution trajectories from host computers. A feature extraction module is used to convert the raw data into feature vectors. The real-time detection part, determine whether an observed pattern or a sequence of patterns is normal or abnormal. The third part is the machine learning part, in which audit data for training are stored in databases which are dynamically updated either by human analysts or by machine learning algorithms.

A. Feature Extraction

As illustrated in Fig.3, feature extraction is the basis for high-performance intrusion detection. If the features are improperly selected, the ultimate performance of detection models will be influenced a lot. This problem has been studied during the early work of W.K. Lee [3] and his research results lead to the benchmark dataset of KDD99, where a 41-dimensional feature vector was constructed for each network connection.

B. Classifier Construction

The classification precision of most existing methods needs to be improved since it is very difficult to detect lots of new attacks by only training on limited audit data. Using anomaly detection strategy can detect novel attacks but

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

the false alarm rate is usually very high since to model normal patterns very well is also hard. Thus, the classifier construction in IDSs remains another technical challenge for intrusion detection based on machine learning.

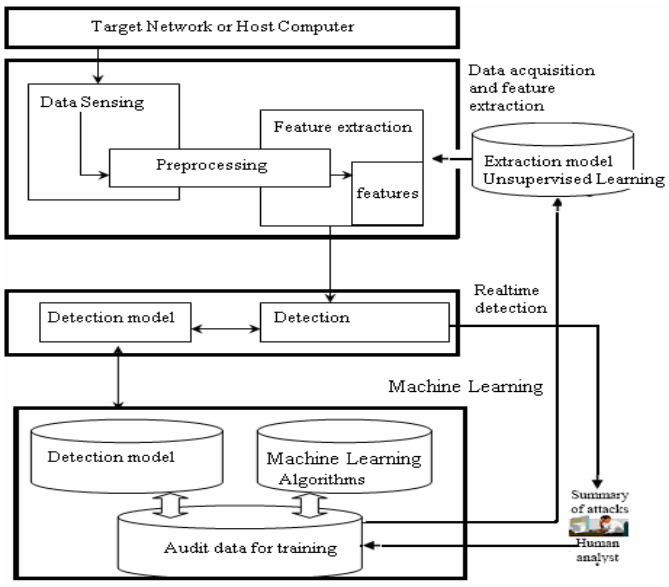

Fig.3.A Framework for IDS Based On Machine Learning

C. Sequential Pattern Prediction

The host-based intrusion detection problem can be considered as a sequential prediction problem since it is hard to determine a single short sequence of system calls to be normal or abnormal and there are intrinsic temporal relationships between sequences. Although we can still transform the above problem to a static classification problem by mapping the whole trace of a process to a feature vector, it has been shown that dynamic behavior modeling methods, such as Hidden Markov Models (HMMs), are more suitable for this kind of intrusion detection problem.

VI. NEURAL NETWORKS

An artificial Neural Network is a collection of treatments which provides the desired output by doing certain simple processing on the set of input. The processing task is performed in the hidden layer. Hidden layer is the intermediate layer between input set and the output set of the application. Thus the actual application of the neural network is done in the Hidden layers. The most important property of a Neural Network is to automatically learn / retrain coefficients in the Neural Network according to data inputs and data outputs Architecture of Neural Networks can be classified in the following two types:-

Supervised training algorithms, here learning is done on the basis of direct comparison of the output of the network with known correct answers. This is sometimes called as learning with a teacher. The well-known architecture of supervised neural network is the Multi-Level Perceptron (MLP).

Unsupervised training algorithms, here the learning goal is not defined at all. The only available information is in the co-relations of input data on signals. The network is expected to create categories from these co-relations and to produce output signals corresponding to input category. Self-Organizing Maps (SOM) are popular unsupervised training algorithms.

Neural Network Approach for Intrusion Detection

Applying the Neural Network (NN) approach to Intrusion Detection, we first have to expose NN to normal data and to attacks to automatically adjust coefficients of the NN during the training phase. Performance tests are then conducted with real network traffic and attacks. . In order to apply this approach to Intrusion Detection, we would have to introduce data representing attacks and non-attacks to the Neural Network to adjust automatically coefficients of this Network during the training phase. In other words, it will be necessary to collect data

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

representing normal and abnormal behavior to train the Neural Network. After training is accomplished, a certain number of performance tests with real network traffic and attacks were be conducted .

VII. MACHINE LEARNING

Machine learning is a system capable of acquiring and integrating the knowledge automatically. The capability of the systems to learn from experience, training, analytical observation, and other means, results in a system that can continuously self-improve and thereby exhibit efficiency and effectiveness. A machine learning system usually starts with some knowledge and a corresponding knowledge organization so that it can interpret, analyze, and test the knowledge acquired.

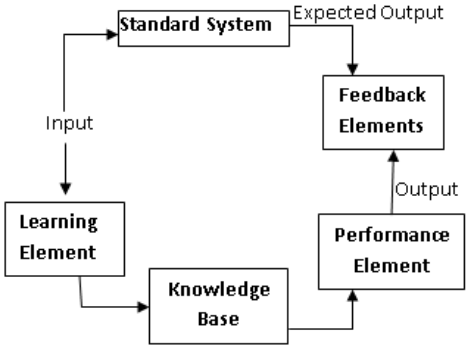

Fig 4. Learning System Model

The figure shown above is a typical learning system model. It consists of the following components.

a) ***Learning element: -*** It receives and processes the input obtained from a person (i.e. a teacher), from reference material like magazines, journals, etc, or from the environment at large.
b) ***Knowledge base: - This*** is somewhat similar to the database. Initially it may contain some basic knowledge. Thereafter it receives more knowledge which may be new and so be added as it is or it may replace the existing knowledge.
c) ***Performance element: -*** It uses the updated knowledge base to perform some tasks or solves some problems and produces the corresponding output.
d) ***Feedback element:-*** It is receiving the two inputs, one from learning element and one from standard (or idealized) system. This is to identify the differences between the two inputs. The feedback is used to determine what should be done in order to produce the correct output.
e) ***Standard system:-*** It is a trained person or a computer program that is able to produce the correct output. In order to check whether the machine learning system has learned well, the same input is given to the standard system. The outputs of standard system and that of performance element are given as inputs to the feedback element for the comparison. Standard system is also called idealized system. There are several factors affecting the performance. They are,

- Types of training provided
- The form and extent of any initial background knowledge
- The type of feedback provided
- The learning algorithms used.

Machine Learning Approach for Intrusion Detection

Intrusion Detection system could not distinguish between normal and abnormal behavior of system using the audit data due to the ineffective behavior model system. Thus has to rely on the human for detection of the behavior. Involvement of Human in the detection system reduces the performances of the IDS as it become the tedious job with increasing data and network traffic. Due to the above deficiencies of IDSs based on human experts, intrusion detection techniques using machine learning have attracted more and more interests in recent years. Machine learning is based heavily on statistical analysis of data and some algorithms can use patterns found in previous data to make decisions about new data.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

VIII. ANOMALY DETECTION TECHNIQUES

Anomaly detection [4] is based on a host or network. Many distinct techniques are used based on type of processing related to behavioral model. They are: Statistical based, Operational or threshold metric model, Markov Process or Marker Model, Statistical Moments or mean and standard deviation model, Univariate Model, Multivariate Model, Time series Model, Cognition based, Finite State Machine Model, Description script Model, Adept System Model, Machine Learning based, Bayesian Model, Genetic Algorithm model, Neural Network Model, Fuzzy Logic Model, Outlier Detection Model, Computer Immunology based, User Intention based. Here in this paper, only the few Machine Learning Techniques are discussed.

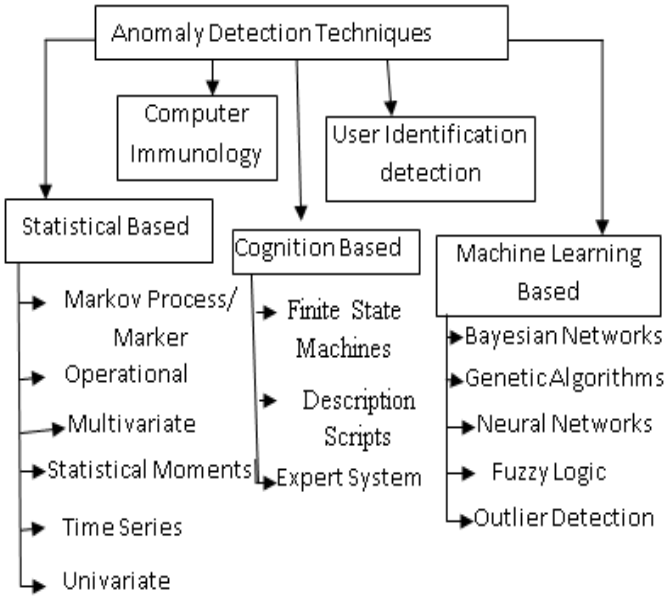

Fig 5. Various Anomaly Detection Techniques

A. Machine Learning Based Anomaly Detection Techniques

Machine learning techniques to detect outliers in datasets from a variety of fields were developed by Gardener (use a One-Class Support Vector Machine (OCSVM) to detect anomalies in EEG data from epilepsy patients [16]) and Barbara (proposed an algorithm to detect outliers in noisy datasets where no information is available regarding ground truth, based on a Transductive Confidence Machine (TCM) [14]).Unlike induction that uses all data points to induce a model, transduction, an alternative, uses small subset of them to estimate unknown attributes of test points. To perform online anomaly detection on time series data in [15], Ma and Perkins presented an algorithm using support vector regression.

a. *Bayesian Networks*

Bayesian methods provide a probabilistic approach to learning. They combine prior knowledge of probability distributions of the candidate hypotheses with the observed data to determine the posterior probability of target hypotheses. Thus they can be applied inherently to problems whose output requires probabilistic predictions. They also provide a framework for analyzing the bias of other algorithms that do not deal directly with probabilities. The naive Bayes classifier is an effective algorithm that uses Bayesian reasoning.

b. *Genetics Algorithms*

Genetic algorithm is a family of computational models based on principles of evolution and natural selection. These algorithms convert the problem in a specific domain into a model by using a chromosome-like data structure and evolve the chromosomes using selection, recombination, and mutation operators. The process of a genetic algorithm usually begins with a randomly selected population of chromosomes. These chromosomes are representations of the problem to be solved. The set of chromosomes during a stage of evolution are called a

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

population. An *evaluation function* is used to calculate the "goodness" of each chromosome. Applying genetic algorithm to intrusion detection seems to be a promising area. Genetic algorithms can be used to evolve simple rules for network traffic. These rules are used to differentiate normal network connections from anomalous connections.

IX. DIMENSION REDUCTION USING PRINCIPAL COMPONENT ANAYSIS

In this section, we will see the application of PCA[2 6 7] for dimensionality reduction of network connection data consisting of forty two features, for making the classification problem more efficient.

Algorithm:--

- Consider the network data corresponding to each connection record after mapping. Thus each column represents a dimension of the input data.
- Compute the mean for each dimension, and subtract it from each data value.
- Compute the covariance matrix C of the input data matrix.
- Calculate the Eigen values and the corresponding eigenvectors for this covariance matrix, and the principal components are computed by solving the eigenvalues problem of covariance matrix C.
- To find the principal components, choose the eigenvectors corresponding to K largest eigenvalues, where K<<N.

Dimensionality reduction step keep only the terms corresponding to the K largest eigenvalues. Hence obtain a new feature vector consisting of eigenvectors of principal components. The final data computed using this feature vector and the mean adjusted original input data using the given equation

$$Final\ Data = RowFeatureVector \times RowDataAdjust$$

Row Feature Vector is the matrix in which eigenvectors in the columns transposed and Row Data Adjust is the mean adjusted input data. The obtained subspace is spanned by the orthogonal set of eigenvectors which reveal the maximum variance in the data space. PCA helps in improving the efficiency of the analysis and reduces the dimensionality of the 42 dimensions. In PCA data from higher data space is projected to lower data space such that less number of errors are experienced. Thus the input provided to SVM well-organized with maximum change hence the classification by discriminating plane which considers minimum variance becomes more accurate. When viewed from an informative point of view, PCA provides SVM with the features that provide efficient classification.

X. CLASSIFICATION USING SUPPORT VECTOR MACHINE

In this section, we will apply multi-class Support Vector Machines (SVMs) to classifier construction in IDSs and evaluate the performance of SVMs on the KDD99 dataset. Compared with the winner's performance in KDD-Cup99, where a bagged boosting C5.0 classifier was used, the multi-class SVMs can obtain comparable results only by making use of a very small portion of the training data. The promising results clearly illustrate the learning efficiency and generalization ability of SVMs based on statistical learning theory.

Multi-Class SVMs for Intrusion Detection

Based on the idea of constructing optimal hyper-planes to improve generalization abilities, SVMs were originally proposed for binary classification problems. Nevertheless, most real world pattern recognition applications are multi-class classification cases. Thus, multi-class SVM algorithms have received much attention over the last decades and several decomposition-based approaches for multi-class problems have been proposed [9-10].

The idea of decomposition-based methods is to divide a multi-class problem into multiple binary problems, i.e., to construct multiple two-class SVM classifiers and combine their classification results. There are several strategies for the implementation of multi-class SVMs using binary SVM algorithms, which include one-vs-all, one-vs-one, and error correcting output coding (ECOC) [10], etc. Among the existing decomposition approaches, the one-vs-all strategy has been regarded as a simple method with relatively low precision when compared with other multi-class SVMs. However, a recent work in [9] demonstrated that one-vs-all classifiers are also extremely powerful and can produce results that are usually at least as accurate as other methods..

XI. CONCLUSION

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

In recent years, research on neural network methods and machine learning techniques to improve the network security by examining the behavior of the network as well as that of threats is done in the rapid force. The large volume of database is increasing rapidly resulting in gradual rise in the security attacks. The current IDS is ineffective to update the audit data rapidly it involves human interference thus reduces the performances. The paper elaborates the architecture of the Intrusion Detection System along with features of an ideal intrusion detection system. The study also describes the categorization and challenges if the IDS. In this paper we analyzed the neural network approach and the machine learning approach in overcoming the challenges of the IDS. We also studied the dimension reduction using PCA. We discussed the Support Vector Machine to deal with the classifier construction problem. Further there is need to design the system which will overcome the current challenges of IDS and also the system must provide a high performance in detecting the threats and security attacks.

REFERENCES

[1] http://www.cerias.purdue.edu/about/history/coast_resources/idcontent/detection.html.

[2] Annie George, 'Anomaly Detection based on Machine Learning: Dimensionality Reduction using PCA and Classification using SVM', International Journal of Computer Applications (0975 – 8887) Volume 47– No.21, June 2012.

[3] W.K. Lee, S.J.Stolfo. "A data mining framework for building intrusion detection model", In: Gong L., Reiter M.K. (eds.): Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, pp.120~132, 1999.

[4] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, 'A Review of Anomaly based Intrusion Detection Systems' International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011.

[5] Neethu B, 'Classification of Intrusion Detection Dataset using machine learning Approaches' International Journal of Electronics and Computer Science Engineering 1044 ISSN- 2277-1956. Available Online at www.ijecse.org.

[6] Lindsay I Smith, "A tutorial on Principal Components Analysis".

[7] CHEN Bo, Ma Wu, "Research of Intrusion Detection based on Principal Components Analysis", Information Engineering Institute, Dalian University, China, Second International Conference on Information and Computing Science, 2009.

[8] T. J.Hastie, R. J.Tibshirani, and J. H.Friedman. The elements of statistical learning: Data mining, inference, and prediction, Springer-Verlag, 2001.

[9] R.Rifkin, A.Klautau. "In defense of one-vs-all classification", Journal of Machine Learning Research, 5, pp.143-151, 2004.

[10] T. G.Dietterich, G.Bakiri. "Solving multiclass learning problems via error-correcting output codes", Journal of Artificial Intelligence Research, 2, pp. 263-286, 1995.

[11] B. Pfahringer. "Winning the KDD99 Classification Cup: Bagged Boosting", SIGKDD Explorations, 1(2), pp.65-66, 2000.

[12] Xin Xu*, 'Adaptive Intrusion Detection Based on Machine Learning: Feature Extraction, Classifier Constructionand Sequential Pattern Prediction,' International Journal of Web Services Practices, Vol.2, No.1-2 (2006), pp. 49-58.

[13] A. Gardner, A. Krieger, G. Vachtsevanos, and B. Litt, "One-class novelty detection for seizure analysis from intracranial EEG," J. Machine Learning Research (JMLR), vol. 7, pp. 1025–1044, Jun. 2006.

[14] Dayu Yang, Alexander Usynin, and J. Wesley Hines, "Anomaly-Based Intrusion Detection for SCADA Systems" IAEA Technical Meeting on Cyber Security of NPP I&C and Information systems, Idaho Fall, ID, Oct.2006.

[15] J. Ma and S. Perkins, "Online novelty detection on temporal sequences" ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Washington, DC, Aug. 2003.

[16] Dayu Yang, Alexander Usynin, and J. Wesley Hines, "Anomaly-Based Intrusion Detection for SCADA Systems" IAEA Technical Meeting on Cyber Security of NPP I&C and Information systems, Idaho Fall, ID, Oct.2006.

AUTHOR BIOGRAPHY

Deepika Vinchurkar, pursuing M.Tech CS at Mukesh Patel School of Technology Management and Engineering from NMIMS Mumbai, areas of interest are Network Security, Neural Netwoks.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 1, Issue 2, November 2012

Ms. Alpa Reshamwala is currently an Asistant Professor in the Department of Computers at MPSTME, NMIMS University. She received her B.E degree in Computer Engineering from Fr. CRCE, Bandra, Mumbai University in 2000 and M.E degree in Computer Engineering from TSEC, Mumbai University in 2008. Her area of Interest includes Artificial Intelligence, Data Mining, Soft Computing – Fuzzy Logic, Neural Network and Genetic Algorithm. She has 17 papers in National/International Conferences/ Journal to her credit. She is also associated as an International Expert of International Journal of Electronics Engineering and Mobile Computing. She has a membership of International Association of Computer Science and Information Technology (IACSIT) and is also a student member of UACEE (Universal Association of Computer and Electronics Engineers).