Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 11; April-June, 2015 pp. 16-19
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Intrusion Detection System using Soft Computing: A Survey

Jyoti Kumari[1] and Ashwani Kumar[2]

[1]M.Tech. Student K.R. Managalam University Gurgaon, India
[2]K.R. Managalam University Gurgaon, India
E-mail: [1]jyotisingh5333@yahoo.com, [2]ashwani.kumar@krmangalam.edu.in

Abstract—*Now a day's as the computer technology evolves and the use of internet is increased, it is very important to provide a high level security to protect highly sensitive and private information. So we use Intrusion Detection System to provide high level security. The main task of Intrusion Detection System (IDS) is to identify between intrusive activity and normal behavior. In order to detect the intrusion various approaches have been developed and proposed over the last decade. This paper includes an overview of Intrusion Detection System, some fundamental concept and various soft computing techniques like: Neural Network (NN), Fuzzy Logic, Support Vector Machine (SVM) and Genetic Algorithm (GA) to determine Intrusion over the computer Network. A robust IDSs system lays a foundation to build an efficient Intrusion Detection System.*

Keywords*: IDS(Intrusion Detection System), NN(Neural Network),GN(Genetic Algorithm), SVM(Support Vector Machine*

1. INTRODUCTION

As the computer technology is evolves and the threat of computer crime increases the apprehension and preemption of such violation become more and more difficult and challenging. Many security systems are designed to prevent unauthorized access to system resources and data. Everybody knows that it is unrealistic to completely prevent security breaches. So must try to prevent these security breaches as they occur so that action may be taken to repair the damage and prevent further harm.

An IDS is a tool, method or a process that monitoring the events occurring in a computer system or network and analyzing them for the sign of intrusion. This complete process is known as Intrusion Detection System. Intrusion Detection function includes:

- Monitoring and analyzing both user and system activity.
- Analyzing system configurations and vulnerabilities.
- Analysis of abnormal activity patterns.
- Tracking user policy violations.
- Accessing system and file integrity.
- Ability to recognize typical attack pattern.

Three Types of IDS are

- Host based IDS.
- Network based IDS.
- Distributed based IDS.

Host Based IDS: Host based IDS runs on individual host or device on the network. It is piece or piece of software on the host system to be monitored. It can monitor:

- Incoming packets.
- Login Activities
- Root activities.
- File systems.
- Wired and wireless network traffic; System log.
- Running process: File access/Modification.

The drawback of this system is that we have to install it on every individual computer which we want to monitor.

Network Based IDS: Network based IDS are placed on the network and the system attached with the network are monitored. It can monitor all the network traffic for the particular network segments or devices.

Advantages

- Identify intrusions by monitoring network traffic
- Need to place only on underlying network.
- Can monitor multiple systems at a time.

Limitation

- Difficult to detect intrusions from encrypted traffic.
- It helps only for detecting external intrusions.

Distributed Based IDS: A Distributed IDS consist of multiple IDS over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis and instant attack date.

2. INTRUSION DETECTION TECHNIQUES

Two Types of IDS techniques are Signature Based IDS and Anomaly Based IDS

2.1 Signature Based Detection Technique

Rule-based detection, also referred to as signature detection, pattern matching and misuse detection, is the first scheme that was used in early intrusion-detection systems. Rule-based detection uses pattern matching to detect known attack patterns. A signature is a pattern or string that corresponds to occurred attack, which is compared with already stored attack pattern. It also known as a knowledge-based or misuse based. It is Simple and effective method to detect known attacks. And this technique is ineffective to detect unknown attacks, Hard to keep database update and very Time Consuming.

2.2 Anomaly Based Detection Techniques

It will monitor the network traffic and compare it against the network traffic and compare it against an established baseline. The baseline will identify what is normal for the network, what sort of bandwidth is generally used, what protocols are used and alert the administrator or user when traffic is detected which is anomalous, or different then the baseline. It is basically effective to detect unknown attacks and unforeseen vulnerabilities. And its Weak profiles accuracy due to observed events being constantly changed and Unavailable during rebuilding of behavior profile.

2.3 Types of Errors in IDS

DOS (Denial of service): Denial of service (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.

R2L (Remote to Local): Unauthorized access from a remote machine. A remote to 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.

U2Su (User to Super User): Unauthorized access to local super user (root)User to root (U2Su) 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.

Probing: Surveillance and other probing. 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.

3. SOFT COMPUTING IN IDS

Soft computing is an innovative approach to construct computationally intelligent system [1].

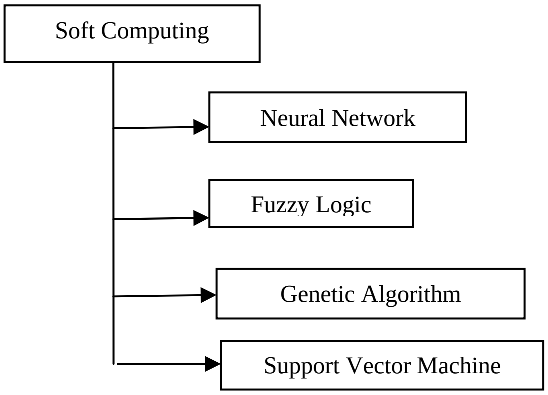

Fig. 1: Soft Computing Techniques

There are many soft computing techniques such as Artificial Neural Network (ANN), Fuzzy logic, Association rule mining, Support Vector Machine (SVM), Genetic Algorithm (GA), etc. that can be used to improve detection accuracy and efficiency of signature based IDS or anomaly detection based IDS[2]. The main Purpose of using Soft computing in IDS are: The ability of soft computing techniques to deal with uncertain and partially true data makes them attractive to be applied in intrusion detection. Soft Computing Techniques can be used here to train the network for better performance and enhancing the accuracy of the system. Moreover, soft Computing tools are used to decrease false positive rates of Intrusion Detection.

4. NEURAL NETWORK BASED IDS

An artificial neuron is a computational model inspired by the biological nervous systems such as the brain process information. Natural neurons receive signals through synapses located on the dendrites or membrane of the neuron. When the signals received are strong enough (surpass a certain threshold), the neuron is activated and emits a signal though the axon. This signal might be sent to another synapse, and might activate other neurons. Two types of architecture of Neural Network can be distinguished- Supervised training algorithm and Un-supervised training algorithm.

- **Supervised Training Algorithm**: Where in the learning phase, the network learn the desired output for a given Input or pattern. The well-known architecture of supervised neural network is the multilayer perceptron (MLP). MLP is employed for Pattern Recognition problems.
- **Unsupervised Training Algorithm**: where in the learning phase, the network learn without specifying desired output.

Applications of neural networks to intrusion detection: The Center for Education and Research in Information Assurance and Security (CERIAS) has produced a review of IDS research prototypes [4], and a few are now commercial products. Approaches for the misuse detection model are:

- Expert Systems: Containing a set of rules that describe attacks.
- Signature verification: Where attack scenarios are translated into sequences of audit events.
- Petri nets: where known attacks are represented with graphical Petri nets.
- Sate-Transition Diagrams: Representing attacks with a set of goals and transitions. The common approach for misuse detection concerns « signature verification », where a system detects previously seen, known attacks by looking for an invariant signature left by these attacks. This signature is found in audit files, in host-intrudes machine, or in snuffers looking for packets inside or outside of the attacked machine.

5. GENETIC ALGORITHM BASED IDS

Genetic Algorithms are search algorithms based on the principles of natural selection and genetics. GA evolves a population of initial individuals to a population of high quality individuals, where each individual represents a solution to the problem to be solved. Each individual is called chromosome and is composed of predetermined number of genes.

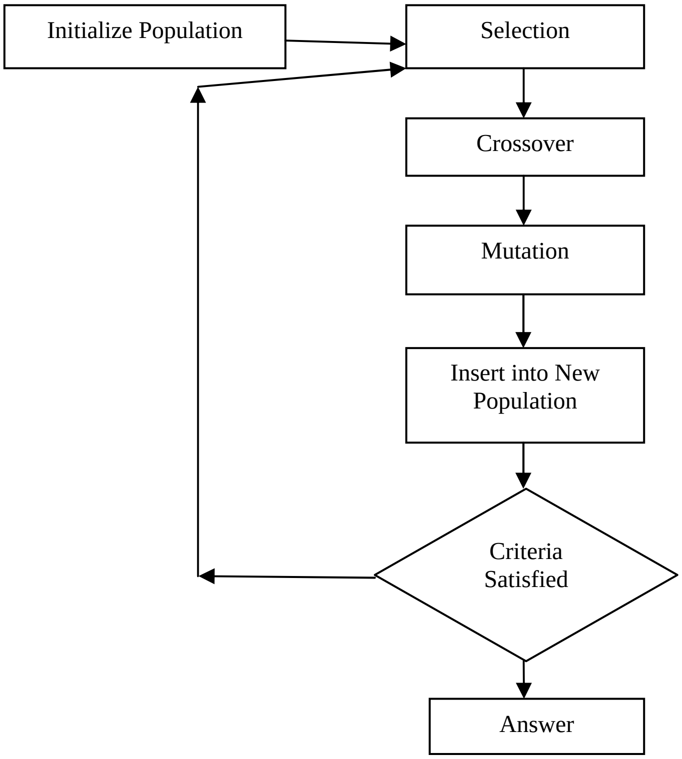

Fig. 2: Fundamental Mechanism of Genetic algorithm

The quality of each rule is measured by a fitness function as the quantitative representation of each rule's adaptation. The procedure starts from an initial population of randomly generated individuals. Then the population is evolved for a number of generations while gradually improving the qualities of the individuals in the sense of increasing the fitness value as the measure of quality. During each generation, three basic genetic operators are sequentially applied to each individual i.e. Selection, Cross over and Mutation. Those chromosomes with a higher fitness value are more likely to reproduce offspring. If the new generation contains a solution that produces an output that is close enough or equal to the desired answer then the problem has been solved. If this is not the case, the new generation will go through the same process. This will continue until a solution is reached.

6. FUZZY LOGIC BASED IDS

Fuzzy logic is very appropriate for using on IDS because there is no clear boundary between anomaly and normal events. The fuzzy logic part of the system is responsible for both i.e. dealing with the inaccuracy of the input data and handling the large number of input parameters. The fuzzy expert system consists of following types of entities: fuzzy variables, fuzzy sets and fuzzy rules. The process of a fuzzy system has three steps they are fuzzification. Rule based evaluation and Defuzzification. Fuzzification means adding fuzziness to data in fuzzy logic. In the fuzzification step, input crisp values are transformed into degrees of membership in the fuzzy sets [6]. In the rule based evaluation, strength value is associated with each fuzzy rule. The strength value is determined by the degree of memberships of the crisp i/p values in the fuzzy sets of antecedent (antecedent variables, that are assigned with the input data of the fuzzy expert system) part of the fuzzy rule. The Defuzzification stage converts the fuzzy outputs into crisp values [9]. The different stages in the fuzzy logic based intrusion detection system are as follows:

- Classifying the training data
- Generation of fuzzy rules
- Fuzzy decision module
- Identifying the appropriate classification for test input.

As an example for the fuzzy logic based approach, Dickerson et al. [10] report a research based on the fuzzy logic concept. His paper reports a Fuzzy Intrusion Recognition Engine (FIRE) for detecting malicious intrusion activities. In the reported work, the anomaly based Intrusion Detection System (IDS) is implemented using both the fuzzy logic and the data mining techniques. The fuzzy logic part of the system is mainly responsible for both handling the large number of input parameters and dealing with the inexactness of the input data.

7. SVM BASED IDS

SVM is an essential technique for IDS. It is machine learning algorithm which is used for binary classification, general pattern recognition and regression analysis of both linear and non-linear data. The main goal of SVM is to find the best classification function to distinguish between members of the two classes in the training data. An SVM maps linear algorithms into non-linear space. It uses a feature called, kernel function, for this mapping. Kernel functions like polynomial, radial basis function are used to divide the feature space by constructing a hyper-plane [5]. The kernel functions can be used at the time of training of the classifiers which selects support vectors along the surface of this function. SVM classify data by using these support vectors that outline the hyper-plane in the feature space SVM performs classification by constructing hyper-plane in a multidimensional space that separates two classes. And a good separation is achieved by the hyper-plane.

There are other reasons that we use SVMs for intrusion detection. The first is speed: as real-time performance is of primary importance to intrusion detection systems, any classifier that can potentially run “fast” is worth considering. The second reason is scalability: SVMs are relatively insensitive to the number of data points and the classification complexity does not depend on the dimensionality of the feature space [6], so they can potentially learn a larger set of patterns and thus be able to scale better than neural networks. Once the data is classified into two classes, a suitable optimizing algorithm can be used if necessary for further feature identification, depending on the application . SVMs can learn a larger set of patterns and be able to scale better, because the classification complexity does not depend on the dimensionality of the feature space. SVMs also have the ability to update the training patterns dynamically whenever there is a new pattern during classification [7].

7.1 Limitations of SVM:

It can only handle binary-class classification whereas intrusion detection requires multi-class classification.

Training of SVM is time-consuming for IDS domain and requires large dataset storage .Thus SVM is computationally expensive for resource-limited ad hoc network [8].Moreover SVM requires the processing of raw features for classification which increases the architecture complexity and decreases the accuracy of detecting intrusion.

8. CONCLUSION

IDS play an important role in computer security. It provides reliable and continuous detection service. In this paper, we present the techniques of IDS including NN, GA, SVM, and Fuzzy logic. This paper present two types of IDS techniques-Misuse and Anomaly. Misuse is not sufficient to prevent the intrusion. Hence, Anomaly detection can gives a wide range of novel attacks and finds the intrusion. However, it also generates high false positive and negative. So we need a Intrusion Detection System that has the ability to identify new and unseen attacks with reduced false negative and positive rate with the help of best soft computing technique.

REFERENCES

[1] Rashid Husain and Saifullahi Muhammad, “A survey on soft computing techniques in network security,” ISSN 2276-8947 © 2013 Scholarly-Journals.

[2] ShilpaBatra, PankajKumar, SapnaSinha, “SoftComputing Techniques (Data-Mining) On IntrusionDetection”, *International Journal of Computational Engineering Research,* Vol 03Issue, 4.

[3] Guang-Bin Huang, Dian Hui Wang and Yuan Lan, “Extreme learning machines: a survey”, Published: 25 May 2011_ Springer-Verlag,2011.

[4] Cramer, M., et. al (1995), “New Methods of Intrusion Detection using Control-Loop Measurement”, *In Proceedings of the Technology in Information Security Conference (I'ISC),* 95, pp. 1-10.

[5] Snehal A. Mulay, “ Intrusion Detection Using Support Vector Machine and Decision Tree”, *International Journal Of Computer Applications(0975-8887),*Volume 3-No.3, June2010.

[6] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu NaserBikas, “An Implementation of Intrusion Detection System Using Genetic Algorithm”, *International Journal of Network Security & Its Applications (IJNSA),* Vol.4, No.2, March 2012.

[7] Sandya Peddabachigari, Ajith Abraham, CrinaGrosan, Johanson Thomas (2005), ”Modeling Intrusion Detection Systems using Hybrid Intelligent Systems”, *Journal of Network and Computer Applications, Intrusion Detection System using Support Vector Machine Jayshree Jha International Conference & workshop on Advanced Computing* ,2013 (ICWAC 2013).

[8] J.F Joseph, A. Das,B.C. Seet, (2011), “Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA”, *IEEE Transaction on dependable and securecomputing,* Vol. 8, No. 2, MarhApril 2011.

[9] Mostaque Md. Morshedur Hassan, “Current Studies On IntrusionDetection System, GeneticAlgorithm And Fuzzy Logic”, *International Journal of Distributed and Parallel Systems (IJDPS),* Vol.4, No.2, March 2013.

[10] JingTao Yao, Songlun Zhao, and Li sa Fan, ”An Enhanced Support Vector Machine Modelfor Intrusion Detection”, *Department of Computer Science, University of Regina Regina, Saskatchewan, Canada* S4S 0A2.