A Survey: Importance of ANN based NIDS in Detection of DoS Attacks

Sonali D.Tangi
Affiliated to Pune University, Pune
Jayawantrao Sawant College of Engineering

M.D.Ingale
Affiliated to Pune University, Pune
Jayawantrao Sawant College of Engineering

ABSTRACT

Today's world i.e. either private or public (government) sector totally influenced by Internet and networking for their business, entertainment purpose. But black side of an internet cannot be ignored .Internet makes the door open to the intruders and hackers. Any successful attempt made by intruders in capturing data causes a big loss of confidential data or digital money. This forces organizations to adopt serious security policy. It may include either use of an encryption methodology or firewall .Now a days as preventive security organization may use an Intrusion detection system. An Intrusion detection system classifies incoming data as normal data and attack data and if attack pattern is recognized it gives alarm to the network administrator .There are various algorithms and methods are proposed for IDS. In this paper we proposed the importance of ANN in developing NIDS for detecting denial of service attacks. The proposed ANN based NIDS will make classification of input packets into 4 categories DoS, U2R,R2L, PROBING in the first step .In the second step NIDS system can be enhanced to detect the DoS attack as Smruf, Teardrop, Neptune, Land, Pod, Back. This developed NIDS can minimize false positive and false negative rate by increasing number of hidden layers in the construction of ANN.

General Terms

Network Security, Artificial Neural Network .Network Intrusion Detection System, Intrusion Detection System. Denial of service .

Keywords

Artificial Neural Network (ANN) .Network Intrusion Detection System (NIDS), Denial of service (DoS).

1. INTRODUCTION TO IDS

Today as dependency on computer networks and internet by public, private organization, and people is increasing tremendously for business, education, enjoyment purposes which brought a revolution in computer world. But this also has a black side. The attackers and intruders are always trying to break the security of your intranet and make the entrance into your network or computer system. The costs of temporary or permanent damages caused by unauthorized access of the intruders to computer systems have forced different business and public as well as private organizations to adapt serious security policy. The security policy adapted includes software packages such as an antivirus system, firewalls, cryptography and intrusion detection system.

1.1 Intruders

No matter how much secure a system is made there would be loopholes found by attackers who are called Intruders, because they are always trying to compromise privacy of the network. Whether the network itself is private or (LAN) or public (the Internet), matter is the intent of the intruder. Regardless of how the intruder gets into system we need to detect it, prevent it from his/her destructive purpose. The main intention of an intruder is to compromise the security of the network in terms of integrity, confidentiality, availability.

1.2 What is an Intrusion Detection System?

An unauthorized user that can access network assets and play something disaster is known as an intruder. Intrusion detection systems are the `burglar alarms' (or rather `intrusion alarms') to the computer security guard .The main aim of this system is to secure the network by giving signal to network administrator if network 's security has been compromise, so that he can respond to such alarm by taking quick actions against intruder's attempt. An IDS is used to detect illegal access to a computer or network system. There are various methods of responding to a network intrusion, but they all require the exact and suitable recognition of the attack. The Intrusion detection system is not new concept but **Dr. Dorothy Denning** proposed an intrusion detection model in 1987 which is a landmark in this area. An intrusion detection system (IDS) is a **device** or **software application** that monitors network and system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may try to stop an intrusion attempt but this is neither required nor expected from a monitoring system. Intrusion detection system (IDS) is primarily concentrates on recognizing possible incidents, logging information about them, and reporting attempts. Its main role in a network is to help network administrator to prepare and deal with the network attacks. [8] Intrusion detection system performs various functions such as,

1. Monitoring and analyzing both user and system activities.
2. Analyzing system configurations and vulnerabilities.
3. Assessing system and file integrity.
4. Ability to recognize patterns typical of attacks.
5. Analysis of abnormal activity patterns.
6. Tracking user policy violations.

The purpose of IDS is to help computer systems on how to deal with attacks, and for that IDS is collecting information from several different sources within the computer systems and networks and compares this information with pre existing patterns of discrimination as to whether there are attacks or weaknesses. [5]Traditional IDS are capable to just classify the data as normal data or attack data while modern IDS can have ability to classify the incoming attacks in to following main four categories.

1. DOS: denial of service

2. R2L: unauthorized access from a remote machine

3. U2R: unauthorized access to local super user (root) privileges

4. Probing: surveillance and other probing

1.3 Need of using new technology

The attackers and intruders are quite intelligent and finding new sophisticated techniques for penetrating the organizations intranet. So our defending system should also use new methodology for detecting new emerging attack patterns, vulnerabilities. Then only we can say our network is quite secure. So we should design and implement an ids based on Genetic algorithm, Artificial neural network , Fuzzy logic ,Support vector machine, data mining or decision tree any one of the machine learning algorithm .This paper proposed to use an artificial neural network to develop a NIDS.

2. SURVEY

2.1 Classification of IDS

The researchers are proposed different types of intrusion detection system depending upon their behavior, use, and their detecting technique as follows.

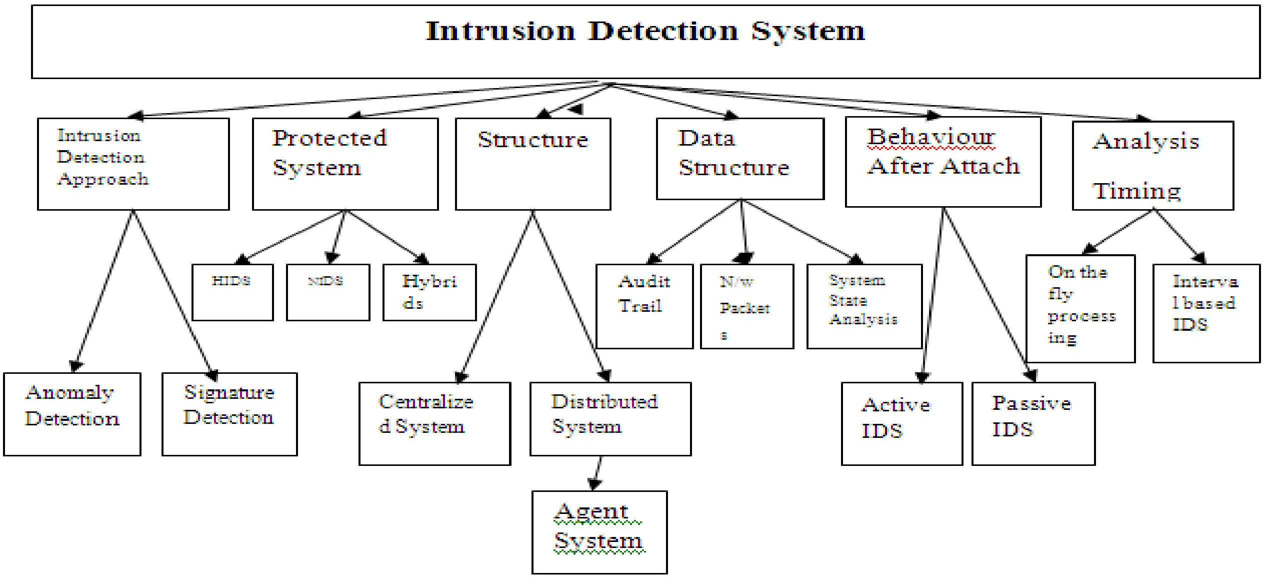

Fig 1: Classification of IDS

1. Misuse detection based or Signature based IDS:-[1] A misuse detection based IDS also called as Signature based IDS. It contains a database of known attack patterns called as signatures. It examines going traffic, activity of the user and system, transaction or behavior for matches with known patterns and it raises alarm only when it founds the match. It works similar as virus scanner. It can be placed on network or host to monitor the vulnerabilities. This type of IDS gives less false positive alarms.

2. A**nomaly detection based or Heuristic or Behaviors based IDS**: - Anomaly based IDS analyzes the traffic patterns and determine normal activities. After that, it applies statistical or heuristic measures to event to determine if they match with this normal behavior. Events which do not match with the accepted normal behavior or patterns are considered as attacks. These types of IDS may detect any type of attacks. As a slight change in behavior can be considered as attack so this type of IDS give high false alarm.

3. Host-based systems: - Host Based IDS can be installed locally on any host machines. A host-based IDS examines the activity on each computer or host. It works on information collected from within an individual computer system. It utilizes information sources like operating system audit trails, C2audit logs and system logs. HIDS can be installed on different types of machines namely servers, workstations and the host. It can also determine which process or users are involved in illegal activity.

4. Network-based or NIDS:-A network-based system, or NIDS, analyzes the individual packets flowing through a network or its entire network segment. This is generally achieved by placing the network interface card in promiscuous mode to capture all network traffic segments. These network traffic packets are checked by the IDS to find the attacks. Network based IDS can reassemble packets, looks at headers; determine if there are any predefined patterns or signature match. NIDS not only monitor the incoming and outgoing network traffic, but also NIDS server scan system files looking for unauthorized activity to maintain data and file integrity. Depending on this pattern or signature matching, IDS decides about the attacks. They are easy to install, undetectable to attackers, operating system independent and used on existing network.

5. Passive system IDS: - A passive system IDS detects security violation and logs the information also signals an alert.

6. R**eactive system IDS**:-A reactive system IDS also known as Intrusion Prevention System responds to any doubtful activity by logging off a user or by reprogramming the firewall and blocks the network traffic from the malicious source.

7. Offline IDS:- The offline IDSs analyze connection data from the logs after the connection has established. This can happen just after the connection has started, so that further access could be denied if the connection was classified as an intrusion.

8. Online IDS:-The online IDSs, if possible, analyze data before connection is allowed. They also monitor the connections so that a connection can be dropped if it starts to seem like an intrusion.

2.2 Different AI Types

Various techniques have been utilized in designing NIDS such as Genetic algorithm, Fuzzy logic, Probabilistic reasoning, artificial neural network, support vector machine, decision tree .Combinations of these can also be used. For example genetic algorithms can be used to build a neural network and probabilistic reasoning can be built on fuzzy logic. Neural networks are the most common AI type for IDS [3].

1. Genetic algorithms can be used to keep the number of iterations as small as possible. Genetic algorithms first randomize values for each set. Then they select a few of the best sets and mix and differentiate values from each of these. This is continued until the desired result is reached or the maximum number of generations has passed.

2. A Probabilistic reasoning based IDS uses Bayesian networks to assess the probability of an intrusion. They had multiagent system in which agents in separate computers could communicate and tell each other threat estimates from each one's point of view. The agents concentrated on detecting different intrusions on separate domains. The system offers a possibility to select the percentage that an event must reach in order to be shown. The multiagent approach adds redundancy to the IDS and increases efficiency. Bayesian networks are also widely used in learning spam filters for e-mail.

3. A SVM based IDS uses supervised learning method which can able to classify the data into the binary form: Attack or Normal. It cannot be able to classify the attack data in to the specific category like DoS, R2L, U2R and Probing.

Let's discuss the comparative analysis of all AI techniques that are used for designing and implementing an IDS. Table 1 gives each positive and negative sides of different techniques used for implementing an IDS.

Table 1 Comparative analysis of AI techniques.

Sr. No.	Technique	Dataset	Advantages	Disadvantages
1.	Decision Tree	KDD99	1.Simple to use 2.works with several Databases 3.Low misclassification rate	1.Pattern finding process is time consuming
2.	Genetic Algorithm	KDD99	1. Classification rules are derived from network audit data. 2.Technique is independent on dataset	1. Low detection rate for unknown attacks.
3.	SVM	KDD99	1. 41 features reduced to 29. 2. Insignificant features are removed.	1. Unable to process entire training dataset. 2. Can' classify into specific category.

This paper proposed NIDS which is based on an artificial neural network because of its following advantages.

2.2.1 Advantages of ANN [8]:

1. It has self learning capability.

2. When an element of the neural network fails, it can continue without any problem due to their parallel nature.

3. A neural network learns and does not need to be reprogrammed.

4. High speed, flexibility while detecting attacks.

5. Use of ANN in detection of dos attacks as it can cluster patterns which share similar features.

6. Classification of attack problem can be solved using ANN.

3. ARTIFICIAL NEURAL NETWORK

The first artificial neuron was formed in 1943 by the neurophysiologist Warren McCulloch and the logician Walter Pits. [1]An artificial neural network is an information processing system has some similar performance characteristics as biological neural networks. A Neural net consist of a large number of simple processing elements called neurons, units, cells or nodes. Each neuron is connected to other neurons by means of directed communication links, each with an associate weight. The weights represent information being used by the net to solve the problem, such as storing and recalling data or patterns, performing general mappings from input patterns to output patterns. The output of each neuron is fed as the input to all of the neurons in the next layer. To detect the attacks from network an artificial neural network has to be trained with known attack patterns. There are two different learning methods for the neural network: supervised and unsupervised .In supervised learning method the network learns the desired output for a given input or pattern. The popular example of supervised learning is a Multilayer or Level Perceptron (MLP) which is used for pattern reorganization. In unsupervised learning neural network learns without specifying output. A self organizing Maps (SOM) neural network is its popular example. To classify the packets in the network as normal or attack using ANN following steps are used

1. Present the neural network with number of inputs.

2. Check how closely the actual output generated for a specific input matches the desired output.

3. Change the neural network parameters to better approximate the output.

To classify attack into specific DoS attack following are the steps to be followed.

1. Designing a simple ANN with few inputs and outputs for NIDS.

2. Training the ANN based NIDS with synthetic inputs.

3. Testing the ANN based NIDS for representative DoS attacks with synthetic inputs.

4. Expanding the NIDS for other DoS attacks.

5. Developing Feature Extraction algorithm and integrating with the NIDS.

6. Total testing and Validation.

This paper presents importance of ANN based NIDS which will detect the denial of service attacks such as Smurf, Teardrop, Neptune, Land, Back ,Pod etc.

4 CONCLUSIONS

The Network Intrusion Detection System developed will become an integral part of Computer Defense System. NIDS based on ANN can be used for detecting various types of DoS attacks such as Shrub, Teardrop, Neptune, Land, Pod, Back within negligible time. For the implementation of NIDS based on ANN MATLAB's Neural Network Toolbox can be used. The proposed NIDS can have low error rate, high learning rate and quick response rate. If better training is done than unknown attacks can also be detected using same NIDS.

5. ACKNOWLEDGMENTS

The author would like to thank to his guide Prof.M.D.Ingale for his valuable suggestions, guidance and support at each moment while preparation of this research paper .The author would also like to thank to IJCA team for giving opportunity to publish this research work. Last but not least the author would like to express her gratitude to all his friends, and individuals, who have directly and indirectly helped, and supported in the completion of her work.

6. REFERENCES

[1] Mohammad Reza Norouzian*, Sobhan Merati "Classifying Attacks in a Network Intrusion Detection System Based onArtificial Neural Networks", ISBN 978-89-5519-155-4, Feb. 13~16, 2011 ICACT2011

[2] Iftikhar Ahmad, Azween B Abdullah, Abdullah S Alghamdi, "Application of Artificial Neural Network in Detection of DOS Attacks"

[3] TaraporeN.Z., Kulkarni D.B. and Kamakshi P.V., "Application of artificial intelligence based techniques for intrusion Detection systems: a review", Journal of Artificial Intelligence ISSN: 2229-3965 & E-ISSN: 2229-3973, Volume 3, Issue 3, 2012, pp.-111-116.

[4] Dilip Kumar Barman, Dr.Guruprasad Khataniar, "design of intrusion detection system based on artificial neural network and application of rough set" , ISSN:2249-5789, International Journal of Computer Science & Communication Networks,Vol 2(4), 548-552

[5] Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung,"Intrusion Detection: Support Vector Machines and Neural Networks "Department of Computer Science New Mexico Institute of Mining and Technology

[6]. Matti Manninen "Using Artificial Intelligence in Intrusion Detection Systems", Helsinki University of Technology.

[7]Mehdi Moradi and Mohammad Zulkernine "A Neural Network Based System for Intrusion Detection and Classification of Attacks".

[8]. Bhavin Shah , Bhushan H Trivedi , "Artificial Neural Network based Intrusion Detection System: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 39– No.6, February 2012.