Asian Journal of Information Technology 13 (12): 755-760, 2014
ISSN: 1682-3915

Quantification of Network Security Situational Based Awareness on Neural Networks

[1]R. Mohan Raj and [2]S. Anbu
[1]Department of CSE, St. Peter's University, Avadi, Chennai-54, India
[2]Department of CSE, St. Peter's College of Engineering and Technology, Avadi, Cehnnai-54, India

Abstract: Network security systems are now mainly employed to secure company networks. An Intrusion Detection System has the capacity to detect in real-time all intrusions and to execute work to stop the attack. With the growth of computer networking, electronic commerce and web services, security of networking systems has become very important. Many companies now rely on web services as a major source of revenue. Computer hacking poses significant problems to these companies as distributed attacks can render their cyber-store front inoperable for long periods of time. This happens so often that an entire area of research, called intrusion detection has been devoted to detecting this activity. We show that evidence of many of these attacks can be found in a careful analysis of network data. We also illustrate that the learning abilities of neural networks can serve to detect this activity. Intrusion detection is an essential mechanism to protect computer systems from many attacks. Besides the classical prevention security tools, Intrusion Detection Systems (IDS) are nowadays widely used by the security administrators. In this study, we present Intrusion Detection Systems using neural networks.

Key words: Intrusion detection, neural networks, network security, SOMs, attacks

INTRODUCTION

Recent advances in computers and computer networks have brought many challenges to the modern society. Internet has put the connectivity of people and organizations at a high position that has never been reached before. Now-a-days, internet is largely used in government, military and commercial institutions. The new emerging protocols and new network architectures permit to share, consult, exchange and transfer information from any place all over the world to any other one situated in a different country, continent, sea or ocean. New infrastructures including DSL (Digital Subscriber Line) lines have largely permitted the exchange of information between individuals. They created community networks of interest that are strongly distributed, dynamic and are "superimposed" to the current network infrastructures. Network traffic analysis is an important part of computer security, yet it grows more challenging each day: network traffic grows in volume and complexity, hosts on the internet grow in number and diversity and attacks grow in variety and sophistication. Identifying patterns of normal and anomalous traffic automatically and using these patterns to monitor unseen traffic is therefore of prime importance.

The attack detection tools are very important for providing safety in computer and network system. These tools fully depend on accuracy of attack detection. Moreover, the detection is also must for prevention of any attack. Therefore, accurate detection of attack is very important. A number of attempts have been done in the field of attack detection but they suffered many limitations such as time consuming statistical analysis, regular updating, non adaptive, accuracy and flexibility. Therefore, it is an artificial neural network that supports an ideal specification of an attack detection system and is a solution to the problems of previous systems. As a result, an artificial neural network inspired by nervous system has become an interesting tool in the applications of attack detection systems due to its promising features. Attack detection by artificial neural networks is an ongoing area and thus interest in this field has increased among researchers. Let us review to some basic concepts and terminologies regarding our research. An unauthorized user who tries to enter in network or computer system is known as intruder. A system that detects and logs in appropriate activities is called as Intrusion Detection System. The Intrusion Detection Systems can be classified into three categories as host based, network based and vulnerability assessment

Corresponding Author: R. Mohan Raj, Department of CSE, St. Peter's University, Avadi, Chennai-54, India

based. A host based IDS evaluates information found on a single or multiple host systems, including contents of operating systems, system and application files. While, network based IDS evaluates information captured from network communications, analyzing the stream of packets traveling across the network. Packets are captured through a set of sensors. Vulnerability assessment based IDS detects vulnerabilities on internal networks and firewall. Moreover, intrusion detection is further divided into two main classes such as misuse and anomaly detection. First is the general category of intrusion detection which works by identifying activities which vary from established ptterns for users or groups of users. It typically involves the creation of knowledge bases which contain the profiles of the monitored activities. The second technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse detection also utilizes a knowledge base of information. Mostly attack detection tools use the evaluation parameters such as false positive, false negative and detection rate. A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. While, a false negative occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.

LITERATURE REVIEW

Dorothy Denning proposed an intrusion detection model in 1987 which became a landmark in the research in this area. The model which she proposed forms the basic core of most intrusion detection methodologies in use today. After this a lot works had been done in this field of intrusion in the form of statistical approaches, rule based, graphical and hybrid system. All of these approaches have limitations as described previously in the background section. Presently, we are taking much interest in the application of attack detection tools by using neural networks due to its features. An artificial neural network consists of a group of processing elements (neurons) that are highly interconnected and convert a set of inputs to a set of preferred outputs. The first artificial neuron was formed in 1943 by the neurophysiologist Warren McCulloch and the logician Walter Pits. Artificial neural networks are alternatives. The first advantage in the use of a neural network in the attack detection would be the flexibility that the network would provide. A neural network would be capable of analyzing the data from the network, even if the data is incomplete or unclear. Similarly, the network would possess the ability to conduct an analysis with data in a non-linear fashion. Further, because some attacks may be conducted against the network in a coordinated attack by multiple attackers, the ability to process data from a number of sources in a non-linear fashion is especially important. The problem of frequently updation of traditional attack detector is also minimized by ANN. It has generalization property and hence able to detect unknown and even variation of known attacks. Another reason to employ ANN in probing attack detection is that ANN can cluster patterns which share similar features, thus, the classification problem in attack detection can be solved by ANN. The natural speed of neural networks is another advantage.

Performance comparison between backpropagation algorithms is presented by Ahmad *et al.* (2007, 2009) in which different supervised algorithms are benchmarked. They proposed an optimized solution with respect to mean square error after making many experiment on the standard dataset in the field of attack detection. The focus was to find best training neural network among Back Propagation algorithms. A systematic review in the field of intrusion detection by using artificial neural networks is also presented by Ahmad *et al.* (2007, 2009) in which they analyzed different approaches in terms of development, implementation, NN architecture, dataset and testing parameter details. They also point out many issues in current traditional as well as intelligent attack detection systems. There are many works in the literature that deal with attack detection in networks but the application of artificial neural networks is a new area in this field. One of the major challenges for present intrusion detection approaches is to reduce false alarm rates. The false alarm rate is still high for recent neural intrusion detection approaches because they have not sufficient ability to attacks. Aikaterini Mitrokotsa worked on attack detection by using ESOMS that is widely used in this field but the problem is performance accuracy as false positives and false negatives increases. Another work on intrusion detection is done by Stefano Zanero. They also used the SOMS in their experiments with 75% detection rate and but it also suffered increase in false positives. Rajeswari and Kannan (2008) worked on intrusion detection and their developed model showed 83.59% accuracy with 16.41% false alarm in terms of attacks. Yao Yu worked to improve false positive rate using their hybrid MLP/CNN neural network but still suffered with a false positive rate. Morteza Amini tried to present a real-time solution using unsupervised neural nets like ART and SOM to detect known and unknown attacks in network traffic. Rhodes *et al.* (2000) proposed

MSOMS that used unsupervised learning and is best for data analysis collected from network and overflow detection. Therefore, supervised neural network suffered training overhead while the others are not efficient in accuracy. In this study, we have reworked of the previous work and focused on probing attacks by using different learning parameters, activation functions and layered nature of the proposed system.

INTRUSION DETECTION SYSTEMS

The timely accurate detection of computer and network system intrusion has always been an exclusive goal for system administrators and information security researchers. While, the complexities of host computers already made intrusion detection which is a difficult endeavor to increasing prevalence of distributed network based systems and insecure networks such as the need for intrusion detection is very necessary has the internet is greatly increased.

Classification of Intrusion Detection Systems: Intrusion Detection Systems can be classified into three categories:

Host-based IDS: Evaluate information found on a single or multiple host systems including contents of operating systems, system and application files.

Network-based IDS: Evaluate information captured from network communications, analyzing the stream of packets traveling across the network. Packets are captured through set of sensors.

Vulnerability-assessment: Vulnerable attacks are to detect on internal networks and firewalls. There are two primary models to analyze events to detect attacks:

Anomaly detection typically involves the creation of knowledge bases that contain the profiles of the monitored activities. The second approach to intrusion detection is to misuse detection. This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Anomaly detection utilizes threshold monitoring to indicate when a certain established metric has been reached misuse detection techniques frequently utilize a rule-based approach. When applied to misuse detection, the rules become scenarios for network attacks. The intrusion detection mechanism identifies a potential attack if a user's activities are found to be consistent with the established rules. The use of comprehensive rules is critical in the application of expert systems for intrusion detection (Fig. 1).

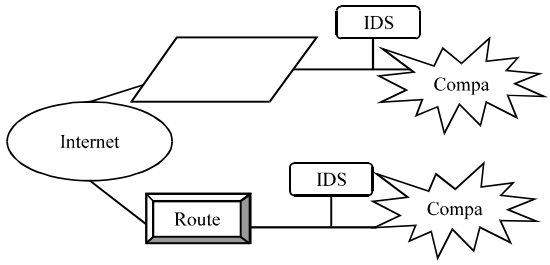

Fig. 1: Intrusion detection systems placed in typical locations

NEURAL NETWORKS FOR INTRUSION DETECTION

A limited amount of research has been conducted on the application of neural networks to detecting computer intrusions. Artificial neural networks offer the potential to resolve a number of the problems encountered by the other current approaches to intrusion detection. Artificial neural networks have been proposed as alternatives to the statistical analysis component of anomaly detection systems. Statistical analysis involves statistical comparison of current events to a predetermined set of baseline criteria. The technique is most often employed in the detection of deviations from typical behavior and determination of the similarly of events to those which are indicative of an attack. Neural networks were specifically proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior.

Neural network approach for intrusion detection: One promising research in intrusion detection concerns the application of the neural network techniques for the Misuse Detection Model and the Anomaly Detection Model. Performance evaluations presented in this study all refer to the DARPA intrusion data base neural network approach an artificial neural network consists of a collection of treatments to transform a set of inputs to a set of searched outputs, through a set of simple processing units or nodes and connections between them. Subsets of the units are input, output nodes and nodes between input and output form hidden layers; the connection between two units has some weight used to determine how much one unit will affect the other. Two types of architecture of neural networks can be distinguished:

Supervised Training algorithms: Where in the learning phase, the network learns the desired output for a given input or pattern. The well known architecture of

supervised neural network is the Multi-Level Perceptron (MLP); the MLP is employed for pattern recognition problems.

Unsupervised Training algorithms: Where in the learning phase, the network learns without specifying desired output.

ARTIFICIAL NEURAL NETWORKS (ANNS) IN INTRUSION DETECTION

The ability of soft computing techniques for dealing with uncertain and partially true data makes them attractive to be applied in intrusion detection some studies have used soft computing techniques other than ANNs in intrusion detection. For example, Genetic algorithms have been used along with decision trees to automatically generate rules for classifying network connections. However, ANNs are the most commonly used soft computing technique in IDSs. An ANN is a processing system that is inspired by the biological nervous systems such as the brain process information. It is composed of a large number of highly interconnected processing elements (neurons) working with each other to solve specific problems. Each processing element (neuron) is basically a summing element followed by an active function. Some IDS designers exploit ANN as a pattern recognition technique. Pattern recognition can be implemented by using a feed-forward neural network that has been trained accordingly. During training, the neural network parameters are optimized to associate outputs with corresponding input patterns. When the neural network is used, it identifies the input pattern and tries to output the corresponding class. When a connected record has no output associated with it is given as an input. The neural network gives the output that corresponds to a taught input pattern that is least different from the given pattern. It is to be considered as a part of soft computing techniques for intrusion detection are two kinds in the artificial neural networks:

- Multi layer feed forward neural networks
- Kohonen's self-organizing maps

Multi-layer feed forward neural networks: Multi-layered feed forward Neural Networks (ANNs) are in non-parametric regression methods which approximate the underlying functionality in data by minimizing the loss function. The common loss function used for training an ANN is a quadratic error function. ANNs use supervised learning for adaptation. The database forms a training set. During the training, specified items of data records are put on the input of the neural network and its weights are changed in such way, so that its output would approximate values in the data set. After finishing the learning process, the learned knowledge is represented by the values of neural network weights. Back propagation of error algorithm is used for training. ANNs are able to efficiently decide in situations which do not occur in the training set, these are best for decision making applications. Three layer ANNs network, i.e., input layer, output layer and hidden layer shown in Fig. 2.

Kohonen's self-organizing maps: Self-organizing maps are also called as Kohonen's Self-Organizing Maps (SOMs). SOMs have become a promising technique in cluster analysis. Self-Organizing Maps (SOM) are popular unsupervised training algorithms a SOM tries to find a topological mapping from the input space to clusters. SOM are employed for classification problems. The unsupervised learning process in SOM can be described as in Fig. 3. The connection weights are assigned with small random numbers at the beginning. The income input vectors presented by the sample data are received by the input neurons. The input vector is transmitted to the output neurons via connections. In the learning stage, the weights are updated following Kohonen's learning rule. The weight update only occurs for the active output neurons and its topological neighbors. The neighborhood

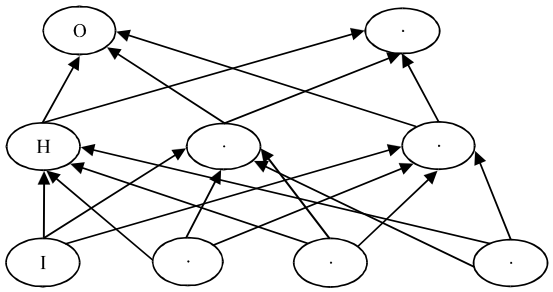

Fig. 2: Multi-layer feed-forward neural network; O: Output layer; H: Hidden layer; I: Input layer

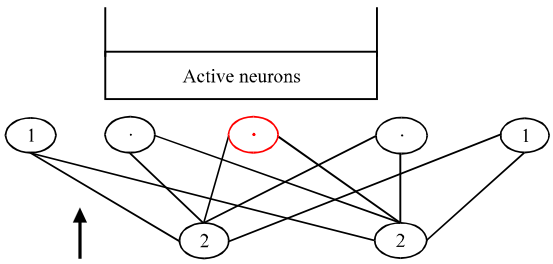

Fig. 3: Kohonen's self-organizing map; 1: output layer 2: input layer

starts large and slowly decreases in size over time. Because the learning rate is reduced to zero, the learning process eventually converges. After the learning process, similar sets of items active the same neuron. SOM divides the input set into subsets of similar records. Therefore, SOM is a method of cluster analysis and is often used for vector quantization.

MISUSE IDS WITH NEURAL NETWORKS

Misuse systems are based on expert knowledge of the usual attacks. It spends more time doing compression of the system activity with database of attack signatures. Some signatures are simple to define and check the database directly. However, the signatures difficult to define in port scan. Port scan is an attempt to intrude the system usually via internet. An intruder tries to find out a vulnerable server reading on some port but does not do direct damage and treats a port scan as an attack due to its malicious implications. Therefore, the misuse system should look for such events. Here, a problem to define signatures of this event. Misuse system has to analyze the incoming packets which could be in some items modified by intruder to overcome revealing. However, the intruder can change the source address and source port in packets and send packets over a long time. In this situation neural networks can be used. SOM classifies each input y1 into 1 of one of clusters which it represents. Numbers are assigned to the clusters or i.e., each neuron of SOM into which the incoming packets were classified form a trace which is fed into the back propagation network. Numbers are assigned to SOM nodes of SOM lattice which are near neighbours do not differ a lot. The sequence x1, ..., xn which fed into system, consists of the last several hundred packets. The SOM block of the system must be trained beforehand by unsupervised learning and back propagation by supervised learning.

ANOMALY IDS WITH NEURALNETWORKS

Anomaly detection is the model of normal behaviour of the system and they look for derivations from the normal behaviour as potential intrusions. The main difficulty is to build an anomaly system lays in defining normal behaviour of the system. To describe the normal behaviour of the system is usually possibly only certain extent. To define a normal activity of the system in general is a very difficult task. For this purpose, one can use neural networks the ability to learn the system with examples or trained with learning and their capability of abstraction. The learning ability means that is not necessary to define normal behaviour of the system explicitly. Generalization allows the anomaly system to recognize when an attack has been muted slightly. The neural network should be able to recognize a variant of an attack that might be missed by a misuse system. Also, generalization may allow the anomaly system to recognize conditions that are typical of an attack in general.

Advantages of neural network-based misuse detection systems: The first advantage in the utilization of neural networks in the detection of instances of misuse would be the flexible. Neural network would be capable of analyzing the data from the network, even if the data is incomplete or distorted. Both, these characteristics are very important in a network environment where the information is received subject to the random failings of the system. The benefit of this approach is inherent speed of neural networks. Because, the resources of the system to identify the attacks immediately to protect the computer. The neural network provides a predictive capability to the detection of instances of misuse detection would identify the probability that a particular are event or series of events. The neural network gains experience to improve the ability to determine where these events are likely to occur in the attack process. This information could then be used to generate a series of events that should occur is in fact an intrusion attempt. By tracking the subsequent occurrence of these events the system would be capable of improving the analysis of the events and possibly conducting defensive measures before the attack is successful. However, most important advantage of neural networks in misuse detection is the ability of the neural network to "learn" the characteristics of misuse attacks and identify instances that are unlike any which have been observed before by the network.

Disadvantages of neural network-based misuse detection systems: There are two primary reasons why neural networks have not been applied to the problem of misuse detection in the past. The first reason relates to the training requirements of the neural network. Because, the ability of the artificial neural network to identify indications of an intrusion is completely dependent on the accurate training of the system, the training data and the training methods are used critical. The training routine requires a very large amount of data to ensure that the results are statistically accurate.

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 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

CONCLUSION

Research and development of Intrusion Detection Systems has been ongoing since the early 80's and the challenges faced by designers increase as the targeted systems because more diverse and complex. Misuse detection is a particularly difficult problem because of the extensive number of vulnerabilities in computer systems and the creativity of the attackers. Neural networks provide a number of advantages in the detection of these attacks. Many methods have been employed for intrusion detection. However, modeling networking trends for a simple representation to a neural network shows great promise, especially on an individual attack basis.

REFERENCES

Ahmad, I., A.B. Abdullah and A.S. Alghamdi, 2009. Artificial neural network approaches to intrusion detection: A review. Proceedings of the 8th Wseas international conference on Telecommunications and informatics, May 30-June 1, 2009, Istanbul, Turkey, pp: 200-205.

Ahmad, I., S.U. Swati and S. Mohsin, 2007. Intrusion detection mechanism by resilient back propagation (RPROP). Eur. J. Scient. Res., 17: 523-531.

Rajeswari, L.P. and A. Kannan, 2008. An inrusion detection system based on multiple level hybrid classifier using enhanced C045. Proceedings of the IEEE International Conference on Signal Processing, Communications and Networking, January 5, 2008, Madras Institute of Technology, Anna University Chemai, India, pp: 75-79.

Rhodes, B., J. Mahaffey and J. Cannady, 2000. Multiple self-organizing maps for intrusion detection. Proceedings of the 23rd National Information Systems Security Conference, October 16-19, 2000, Baltimore, Maryland.