NEURAL NETWORKS FOR INTRUSION DETECTION AND ITS APPLICATIONS

Saswati Sahoo[1] Vikas Ranjan[2]

[1] Computer Science & Engineering, Gandhi Engineering College(GEC, Bhubaneswar)

2 Electronics & Communication Engineering, Gandhi Engineering College(GEC, Bhubaneswar)

Abstract: **With rapid expansion of computer networks during the past decade, security has become a crucial issue for computer system. Different soft-computing based methods have been proposed in recent years for the development of intrusion detection system. Different neural network structures are analyzed to find the optimal neural network with regards to the number of hidden layers. Misuse detection is the process of attempting to identify instances of network attacks by comparing current activity against the expected actions of an intruder. Most current approaches to misuse detection involve the use of Rule-based expert systems to identify indications of known attacks. These techniques are less successful in identifying attacks which vary from expected patterns. Artificial neural networks provide the potential to identify and classify network activity based on limited, incomplete, and nonlinear data sources.**

Key Words**: Intrusion Detection, Misuse Detection, Neural Networks, Computer Security.**

I. INTRODUCTION

The rapid development and expansion world wide web and local network systems have changed the computing world in the last decade. The highly connected computing world has also equipped the intruders and hackers with new facilities for their destructive purposes. The costs of temporary or permanent damages caused by unauthorized access of the intruders to increasingly implement various systems to monitor data flow in their networks. These systems are generally referred to as Intrusion Detection Systems (IDSs).

There are two main approaches to the design of IDSs. In a misuse detection based IDS, intrusions are detected by looking for activities that correspond to known signatures of intrusion or vulnerabilities. On the other hand, anomaly detection based IDS detects intrusions by searching for abnormal network traffic. The abnormal traffic pattern can be defined either as the violation of accepted thresholds for the legitimate profile developed for his/her normal behavior.

One of the most commonly used approaches in expert system based on intrusion detection is a rule-based analysis using Denning's profile model. Soft computing is a general term for describing a set of optimization. Processing techniques for this are Fuzzy Logic (FL), Artificial Neural Networks (ANNs), Probabilistic reasoning (PR), and Genetic Algorithms (GAs). It is a capable of disclosing the latent patterns both abnormal and normal connection to audit records and generalize the patterns to new connection records of the same class**.** In the previous studies, the neural networks have been implemented with the capability to detect normal and attack connections.

II. 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.

A. 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 [9] and [10].

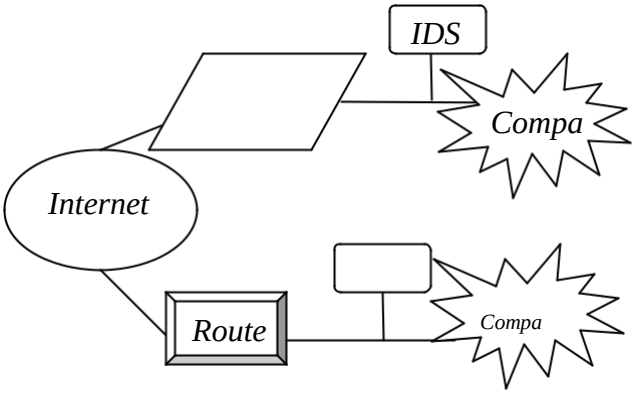
Anomaly detection utilizes threshold monitoring to indicate when a certain established metric has been reached misuse detection techniques frequently utilize a rule-based approach.

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.

B. Locations of Intrusion Detection Systems in Networks

Intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Depending upon the network topology, the Proceedings of the World Congress on Engineering 2013 Vol II, WCE 2013, July 3 - 5, 2013, London, U.K.

type of intrusion activity (i.e. internal, external or both), and our security policy (what we want to protect from hackers), IDSs can be positioned at one or more places in the network. For example, if we want to detect only external intrusion activities, and we have only one router connecting to the Internet, the best place for an intrusion detection system may be just inside the router or a firewall. On the other hand, if we have multiple paths to the internet, and we want to detect internal threats as well, we should place one IDS box in every network segment. Intrusion detection systems placed in typical locations shown in the figure below



IDS

Fig.1.Intrusion Detection systems placed in typical locations.

C. Current Approaches to Intrusion Detection

Most current approaches to the process of detecting intrusions utilize some form of rule-based analysis. Rule-based analysis relies on sets of predefined rules that are provided by an administrator, automatically created by the system or both. Expert systems are the most common form of rule-based intrusion detection approaches

[5] and [13].The use of expert system techniques in intrusion detection mechanisms was a significant milestone in the development of effective and practical detection-based information security systems[1],[5],[11] and [13].

Rule-based systems suffer from an inability to detect attacks scenarios that may occur over an extended period of time. While the individual instances of suspicious activity may be detected by the system, they may not be reported if they appear to occur in isolation. Intrusion scenarios in which multiple attackers operate in concert are also difficult for these methods to detect because they do not focus on the state transitions in an attack, but instead of concentrating on the occurrence of individual elements. Any division of an attack either over time or among several unrelated attackers is difficult for these methods to detect.

Rule-based systems also lack flexibility in the rule-to audit record representation. Slight variations in an attack sequence can effect the activity-rule comparison to a degree that the intrusion is not detected by the intrusion detection mechanism. While increasing the level of abstraction of the rule-base does provide a partial solution to this weakness, it also reduces the granularity of the intrusion detection device. A number of non-expert system- based approaches to intrusion detection have been developed in the past several years. [2], [3], [4], [6], [14], and [14]. While many of these have shown substantial promise, expert systems remain the most commonly accepted approach to the detection of attacks.

III. 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, [5] [6], [10], [23] and [26]. 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 [8]. Neural networks were specifically proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior.

A. 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 paper 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 nodes, 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.

IV. 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.

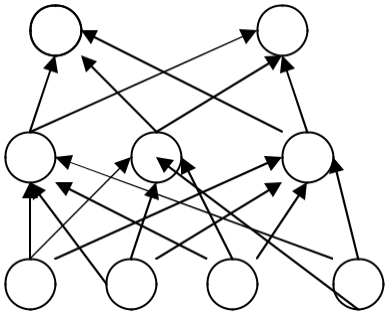
An ANN is a processing system that is inspired by the biological nervous systems, such as the brain process information. It is composed of a large number of highly interconnected processing elements (neurons) working with each other to solve specific problems. Each processing element (neuron) is basically 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.

1. Multi layer feed forward neural networks.
2. Kohonen's Self-Organizing Maps.

A. Multilayered feed forward neural networks

Multilayered feedforward 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 the below figure 2.



O-Output Layer; H-Hidden Layer; I-input Layer Fig.2. Multi layer feedforward neural network

(ANN)

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 the figure 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 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.

V. 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. For example the signatures are defined simple in the Unix operating system for processing with new file to root ownership. But 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.

The income packets $x_1 \ldots\ldots x_n$ Feature Extraction block. The output of the Feature Extraction block $y_1 \ldots\ldots y_n$ is the point of input of SOM neural network. SOM classifies each input y_1 into one 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 $x_1 \ldots\ldots x_n$, 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 backpropagation by supervised learning.

ANOMALY IDS WITH NEURAL NETWORKS

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. The Neural Network Intrusion Detection (NNID) system is implemented in the UNIX environment is the best example for above s7ystem.

B. 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. A neural network might be trained to recognize known suspicious events with a high degree of accuracy. The network would also gain the ability to apply this knowledge to identify instances of attacks which did not match the exact characteristics of previous intrusions. The probability of an attack against the system may be estimated and a potential threat flagged whenever the probability exceeds a specified threshold

B.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. The training of a neural network for misuse detection purposes may require thousands of individualattacks sequences, and this quantity of sensitive information is difficult to obtain.

C. 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 [2], 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.

VI. 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

REFERENCES

[1] Anderson, D., Frivold, T. & Valdes, A (May, 1995). Next-generation Intrusion Detection Expert System (NIDES):

[2] 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.

[3] Debar, H., Becke, M., & Siboni, D. (1992). A Neural Network Component for an Intrusion Detection System. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy.*

[4] Debar, H. & Dorizzi, B. (1992). An Application Recurrent Network to an Intrusion Detection System. In Proceedings of the International Joint Conference on Neural Networks. pp. (11)478-483.

[5] Denning, Dorothy. (February, 1987). An Intrusion-Detection Model. IEEE Transactions on Software Engineering, Vol. SE-13, NO.2.

[6] Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990). A Neural Network . Approach Towards Intrusion Detection. In Proceedings of the 13th National Computer Security Conference.

[7]Frank, Jeremy. (1994). Artificial Intelligence and Intrusion Detection: Current and Future Directions. In Proceedings of the 17th National Computer Security Conference.

[8] Helman, P. and Liepins, G., (1993). Statistical foundations of audit trail analysis for the detection of computer misuse, IEEE Trans. on Software Engineering, 19(9):886-901.

[9] Kumar, S. & Spafford, E. (1994) A Pattern Matching Model for Misuse Intrusion Detection. In Proceedings of the 17th National Computer Security Conference, pages 11-21.

[10] Kumar,S.&Spafford, E. Software Architecture to Support Misuse Intrusion Detection. Department of Computer Sciences, Purdue University; CSD-TR-95-009

[11] Lunt, T.F. (1989). Real-Time Intrusion Detection. Computer Security Journal Vol. VI, Number 1. pp 9-14.

[12] Ryan, J., Lin, M., and Miikkulainen, R. (1997). Intrusion Detection with Neural Networks. AI Approaches to Fraud Detection and Risk Management: MAl Workshop (Providence, Rhode Island), pp. 72-79.

[13] Sebring, M., Shell house, E., Hanna, M. & Whitehurst, R. (1988) Expert Systems in Intrusion Detection:

[14] Stanford-Chen, S. (1995, May 7). Using Thumbprints to Trace Intruders. UC Davis.

[15] Tan, K. (1995). The Application of Neural Networks to UNIX Computer Security. In Proceedings of the IEEE International Conference on Neural Networks, Vol.] Pp.476-481.