ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

Neural Networks For Intrusion Detection And Its Applications

E.Kesavulu Reddy (Member IAENG)
Assistant Professor, Computer Science, S.V.University College of CM & CS, Tirupati, Andhra Pradesh, India

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 detect 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 intrusion detection system is rule-based analysis using Denning's profile model. Soft computing is a general term for describing a set of optimization and processing techniques are Fuzzy Logic (FL), Artificial Neural Networks (ANNs), Probabilistic reasoning (PR), and Genetic Algorithm (GAs). The idea behind the application of soft computing techniques are ANNs in implementing IDSs is to include an intelligent agent in the system i.e Capable of disclosing the latent patterns in abnormal and normal connection audit records and generalize the patterns to new connection records of the same class. In the previous studies neural networks are implementing with the capability of detecting normal or 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 a difficult endeavor, the increasing prevalence of distributed network-based systems and insecure networks such as the Internet has greatly increased the need for intrusion detection.

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**
  Detect vulnerabilities on internal networks and firewalls There are two primary models to analyzing events to detect attacks:

Anomaly detection typically involves that vary from established patterns for users, or groups of users. Anomaly detection typically involves the creation of knowledge bases that contain the profiles of the monitored activities The second approach to intrusion detection is misuse detection. This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system [9][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. 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.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

Expert systems are the most common form of rule-based intrusion detection approaches [5] [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], [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 concentrate 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 NETWORK INTRUSION DETECTION SYSTEMS

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. 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.

B. Advantages of Neural Network-based Misuse Detection Systems

The first advantage in the utilization of a neural networking the detection of instances of misuse 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 distorted. Similarly, the network would possess the ability to conduct an analysis with data in a non-linear fashion. Both of these characteristics is important in a networked environment where the information which is received is subject to the random failings of the system. Further, because some attacks may be conducted against the network in a coordinated assault by multiple attackers, the ability to process data from a number of sources in a non-linear fashion is especially important. The inherent speed of neural networks is another benefit of this approach. Because the protection of computing resources requires the timely identification of attacks, the processing speed of the neural network could enable intrusion responses to be conducted before irreparable damage occurs to the system. Because the output of a neural network is expressed in the form of a probably the neural network provides a predictive capability to the detection of instances of misuse. Neural network-based misuse detection system would identify the probability that a particular are event, or series of events, was indicative of an attack against the system. As the neural network gains experience it will improve its 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 if this 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

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

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. While this would be a very valuable ability, since attackers often emulate the "successes" of others, 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

C. Disadvantages Of Neural Network-Based Misuse Detection Systems

There appear to be 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 that are used are 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 individual attacks sequences, and this quantity of sensitive information is difficult to obtain.

D. 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 misuse detection :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.

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 However, ANNs are the most commonly used soft computing technique in IDSs. An ANN is information, n processing system that is. inspired by the way 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 activation 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 connection record that 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. The most commonly reported application of n al networks in Ss is to train the neural net on a sequence of information uni each of which may be an audit record or a sequence of commands.

V. 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

VI. FUTURE WORK

Practical IDSs should include several attack types. In order to avoid unreasonable complexity in the neural network, an initial classification of the connection records to normal and general categories of attacks can be the first step. The records in each category of intrusions can then be further classified to the attack types.

VII. ACKNOWLEDGMENT

I am most thankful to Sri.Y.Konda Reddy, Founder & Chairman, Rayalaseema Educational Institutions, Tirupati, Andhra Pradesh, India sponsor financial assistance to support my research work to attending the World Congress on Engineering.

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.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

[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 Detections pp 1-10

[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, Pp .476-481.

AUTHOR BIOGRAPHY

I am Dr.E.Kesavulu Reddy working as Assistant Professor Dept. of. Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati (AP)-India. I received Master of Computer Applications and Doctorate in Computer Science from S.V.University, Tirupati, and Andhra Pradesh India. Also I received Master of Philosophy in Computer Science from M.K. University, Madurai, and Tamilnadu, India. I am one paper presented in WCECS2010, U.S.A and two papers published in WCE 2011 & 2012, London, U.K. I published various papers in International and National Journals, also attending in International and National conferences. My research interest in the field of Computer Science in the area of Elliptic Curve Cryptography-Network Security, Data Mining, and Software Engineering.