ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.2 , No.6, Pages : 190-193 (2013)
*Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India*

# A SECURE COMMUNICATION IN ARTIFICAL NEURAL NETWORKS

**Amarkanth Reddy K**[1]
[1]Department of CSE, Visvesvaraya College of Engineering & Technology, Hyderabad, AP, India

## ABSTRACT

The aim of the present paper is a neural network approach to intrusion detection. 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. We present an approach to the process of misuse detection and secured communication over networks

***Keywords:*** *Intrusion Detection, Neural Networks, Rule-based Analysis, Training Strategies.*

## INTRODUCTION

The rapid development and expansion of World Wide Web and local network systems have changed the computing world in the last decade. However, this outstanding achievement has an Achilles' heel: 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 computer systems have urged different organizations to increasingly implement various systems to monitor data flow in their networks by Kemmerer and Vigna [12] Intrusion detection: a brief history and overview.

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 intrusions 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 frequency of events in a connection or as a user's violation of the legitimate profile developed for his/her normal behaviour.

In view of the above Thuraisingham [1] Building Secure survivable semantic webs.

Carpenter and Grossberg [2] A Massively Parallel Architecture for a Self-Organizing Neural pattern Recognition Machine. Chung et.al [3] Simulating Concurrent Intrusions for Testing Intrusion Detection Systems. Fox et.al [4] A neural network approach towards intrusion detection. Lichodzijewski et.al [5] Host-based intrusion detection using self-organizing maps. Debar et.al [6] A neural network component for an intrusion detection system. Daivid Poole et.al [7] Computational Intelligence. Kristopher Kendall [8] A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems. Srinivas Mukkamala [9] Intrusion detection using neural networks and support vector machine. Cunningham and Lippmann [10] Improving intrusion detection performance using keyword selection and neural networks. Sinclair et.al [11] An application of machine learning to network intrusion detection.

Because of the increasing dependence which companies and government agencies have on their computer networks the importance of protecting these systems from attack is critical. A single intrusion of a computer network can result in the loss or unauthorized utilization or modification of large amounts of data and cause users to question the reliability of all of the information on the network. There are numerous methods of responding to a network intrusion, but they all require the accurate and timely identification of the attack. This paper presents an analysis of the applicability of neural networks in the identification of instances of external attacks against a network. The results of tests conducted on a neural network, which was designed as a proof of concept, are also presented. Finally, the areas of future research that are being conducted in this area are discussed.

Different neural network structures are analyzed to find the optimal neural network with regards to the number of hidden layers. An early stopping validation method is also applied in the training phase to increase the generalization capability of the neural network. The results show that the designed system is capable of classifying records with about 91% accuracy

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.2 , No.6, Pages : 190-193 (2013)
*Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India*

with two hidden layers of neurons in the neural network and 87% accuracy with one hidden layer.

**INTRUSION DETECTION SYSTEMS**

The timely and accurate detection of computer and network system intrusions has always been an elusive goal for system administrators and information security researchers. The individual creativity of attackers, the wide range of computer hardware and operating systems, and the ever changing nature of the overall threat to target systems have contributed to the difficulty in effectively identifying intrusions. 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.

There are two general categories of attacks which intrusion detection technologies attempt to identify - anomaly detection and misuse detection. Anomaly detection identifies activities 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 general 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. While anomaly detection typically 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.

**Rule Based Analysis**

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. The early intrusion detection research efforts realized the inefficiency of any approach that required a manual review of a system audit trail. While the information necessary to identify attacks was believed to be

present within the voluminous audit data, an effective review of the material required the use of an automated system. 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 .An expert system consists of a set of rules that encode the knowledge of a human "expert". These rules are used by the system to make conclusions about the security-related data from the intrusion detection system. Expert systems permit the incorporation of an extensive amount of human experience into a computer application that then utilizes that knowledge to identify activities that match the defined characteristics of misuse and attack.

**NEURAL NETWORKS**

An ANN is an information 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. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all of the neurons in the next layer. The learning process is essentially an optimization process in which the parameters of the best set of connection coefficients (weighs) for solving a problem are found and includes the following basic steps:

- Present the neural network with a number of inputs (vectors each representing a pattern)
- Check how closely the actual output generated for a specific input matches the desired output
- Change the neural network parameters (weights) to better approximate the outputs

An artificial neural network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The result of the transformation is determined by the

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.2 , No.6, Pages : 190-193 (2013)
*Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India*

characteristics of the elements and the weights associated with the interconnections among them. By modifying the connections between the nodes the network is able to adapt to the desired outputs. Unlike expert systems, which can provide the user with a definitive answer if the characteristics which are reviewed exactly match those which have been coded in the rule base, a neural network conducts an analysis of the information and provides a probability estimate that the data matches the characteristics which it has been trained to recognize. While the probability of a match determined by a neural network can be 100%, the accuracy of its decisions relies totally on the experience the system gains in analyzing examples of the stated problem.

**Application of Neural Networks in Misuse Detection**

The first advantage in the utilization of a neural network in 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 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.

While there is an increasing need for a system capable of accurately identifying instances of misuse on a network there is currently no applied alternative to rule-based intrusion detection systems. This method has been demonstrated to be relatively effective if the exact characteristics of the attack are known. However, network intrusions are constantly changing because of individual approaches taken by the attackers and regular changes in the software and hardware of the targeted systems. Because of the infinite variety of attacks and attackers even a dedicated effort to constantly update the rule base of an expert system can never hope to accurately identify the variety of intrusions. The constantly changing nature of network attacks requires a flexible defensive system that is capable of analyzing the enormous amount of network traffic in a manner which is less structured than rule-based systems. A neural network-based misuse detection system could potentially address many of the problems that are found in rule-based systems

**Early Stopping Validation Method**

The over-fitting problem in neural network takes much training time. The reasonable solution was to define a validation data set and monitor the classification error on this data set while the neural network was being trained. The neural network was trained this time by applying early stopping validation method. Figure shows the error of the training process versus progress of training epochs for one training session. The error on the training set (darker curve) was decreasing after epoch number 45; however, the training process was stopped because the error on the validation set was constant for ten epochs.

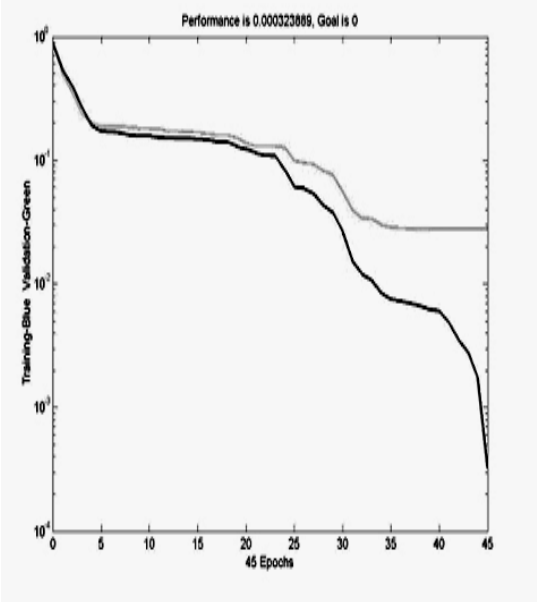


**Fig 1** : The training process error when the early stopping validation method

Here the darker curve shows the error on the training set and the brighter curve presents the error on validation set. As a result of more than 99% correct classification on this dataset using the neural network structure is reported. Here training time was decreased because the number of training epochs was restricted by early stopping. The training-validation time in this

ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.2 , No.6, Pages : 190-193 (2013)
*Special Issue of ICETEM 2013 - Held on 29-30 November, 2013 in Sree Visvesvaraya Institute of Technology and Science, Mahabubnagar – 204, AP, India*

implementation was less than 5 hours which is an improvement over 25 hours training time in over-fitting problem

## CONCLUSION

An approach for a neural network based intrusion detection system, intended to classify the normal and attack patterns and the type of the attack, has been presented in this paper. We applied the early stopping validation method which increased the generalization capability of the neural network and at the same time decreased the training time. Research and development of intrusion detection systems for secure communication system over networks has been ongoing since the early 1980'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. It should be mentioned that the long training time of the neural network was mostly due to the huge number of training vectors of computation facilities. However, when the neural network parameters were determined by training, classification of a single record was done in a negligible time. Therefore, the neural network based IDS can operate as an *online* classifier for the attack types that it has been trained for. From the practical point of view, the experimental results imply that there is more to do in the field of artificial neural network based intrusion detection. 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. Research community should develop and implement technology for secured communication over networks.

## REFERENCES

[1] B Thuraisingham (2002): Building Secure survivable semantic webs, Proceedings I4ih IEEE International Conference on Tools with Artificial Intelligence

[2] G A Carpenter and S Grossberg (1987): A Massively Parallel Architecture for a Self-Organizing Neural pattern Recognition Machine. Computer Vision, *Graphics and Image Processing*, 37, pp. 54-115.

[3] M Chung, N Puketza, R A Olsson and B Mukherjee (1995): Simulating Concurrent Intrusions for Testing Intrusion Detection Systems: Parallelizing. *In NISSC*. pp. 173-183.

[4] K Fox, R Henning, J Reed and R Simonian (1990): A neural network approach towards intrusion detection, Proceedings of 13th National Computer Security Conference, *Baltimore, MD*, pp. 125-134, 1990.

[5] P Lichodzijewski, A N Zincir Heywood and M I Heywood (2002): Host-based intrusion detection using self-organizing maps, *Proceedings of the 2002 IEEE World Congress on Computational Intelligence, Honolulu, HI*, pp. 1714-1719, 2002.

[6] H Debar, M Becker and D Siboni (1992): A neural network component for an intrusion detection system, *Proceedings of 1992 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California*, pp. 240 – 250.

[7] Daivid Poole, Alan Makworth, and Randi Goebel (1998): Computational Intelligence, *New York: Oxford University Press.*

[8] Kristopher Kendall (1999): A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, *Master's Thesis, MIT*.

[9] Srinivas Mukkamala (2002): Intrusion detection using neural networks and support vector machine, *Proceedings of the 2002 IEEE International Honolulu, HI*.

[10] R Cunningham and R Lippmann (1999): Improving intrusion detection performance using keyword selection and neural networks, *Proceedings of the International Symposium on Recent Advances in Intrusion Detection, Purdue, IN*.

[11] C. Sinclair, L. Pierce, and S. Matzner, "An application of machine learning to network intrusion detection.

[12] R. A. Kemmerer and G. Vigna (2002): Intrusion detection: a brief history and overview," *Computer*, vol. 35, no. 4, pp. 27–30, 2002.