Expert System for Intrusion Detection and Its Applications

Dr.E.Kesavulu Reddy,
Assistant Professor
Department of Computer Science
College of Commerce management & Computer Science
S.V.University, Tirupati, Andhra Pradesh-INDIA-517503
Email: ekreddysvu2008@gmail.com

Abstract: 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. This paper presents a succinct review of the application of various Artificial Intelligence technique sand their advances in the design, development and application of Intrusion Detection Systems (IDS) for protecting computer and communication networks from intruders.

Key Words: Intrusion Detection, Misuse Detection, Neural Networks, Artificial Intelligence, Experts Systems.

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 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

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 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. Intrusion detection systems placed in typical locations shown in the figure below

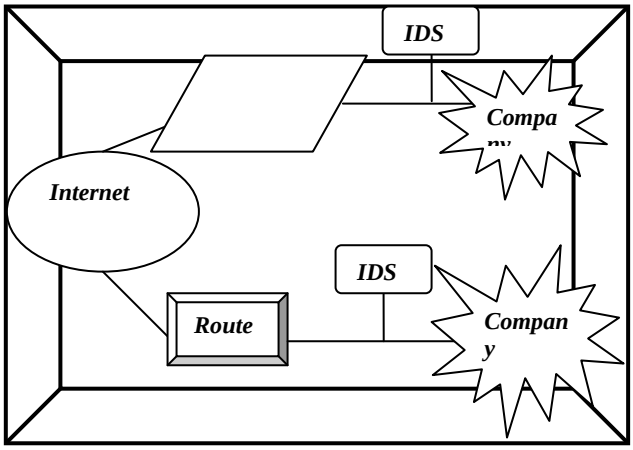

Fig.1.1.Intrusion Detection systems placed in typical locations.

2.3. 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 [6] and [14].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],[6],[12] and [14].

Rule-based systems also lack flexibility in the rule-to audit record representation. Slight variations in an attack sequence can affect 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 system [10] and [11].

intrusion detection device. A number of non-expert system-based approaches to intrusion detection have been developed in the past several years. [2], [4], [5], [7], [15], and [15]. 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, [6] [7], [11]. 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 [9]. Neural networks were specifically proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior. Two types of architecture of Neural Networks can be distinguished.

- Supervised training algorithms: where in the earning 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

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. A typical ANN framework is shown in figure 2. ANN is a close emulation of the biological nervous system. In this model, a neuron multiplies the inputs by weights, calculates the sum, and applies a threshold. The result of this computation would then be transmitted to subsequent neurons. Basically, the ANN has been generalized to:

$$y_i = f\left(\sum_k W_{ik} X_k + \mu_i\right)$$

Where xk are inputs to the neuron *i*, *wik* are weights attached to the inputs, μ*i* is a threshold, offset or bias, *f* (•) is a transfer function and *yi* is the output of the neuron. The transfer function *f* (•) can be any of: linear, non-

linear, piece-wise linear, sigmoidal, tangent hyperbolic and polynomial functions. Some of the versions of ANN, depending on which algorithm is used at the summation stage, include: Probabilistic Neural Networks, Generalized Regression Neural Networks and Multi-Layer Perceptron Neural Networks. The most commonly used learning algorithm of ANN is the Feed-Forward Back-propagation algorithm [3][16].

Figure: 1.2.Artificial Neural Networks Framework

V. ARTIFICIAL INTELLIGENCE

Computational Intelligence (CI), an offshoot of AI, covers all branches of science and engineering that are concerned with the understanding and solving of problems for which effective computational algorithms do not yet exist. Thus, it overlaps with some areas of Artificial Intelligence and a good part of Pattern Recognition, Image Analysis and Operations Research. CI relies on heuristic algorithms such as in Fuzzy Systems, Neural Networks, Support Vector Machines and Evolutionary Computation. In addition, CI also embraces techniques that use Swarm Intelligence, Fractals and Chaos Theory, Artificial Immune Systems, Wavelets, etc. [3].

AI naturally transformed into Computational Intelligence (CI) with the introduction of the concept of Machine Learning. A major focus of machine learning research is to automatically learn to recognize complex attributes and to make intelligent decisions based on the correlations among the data variables. The machine learning concept can be categorized into three common algorithms viz. supervised, unsupervised and hybrid learning. The hybrid learning combines the supervised and unsupervised techniques to generate an appropriate function and to meet a specific need of solving a problem.

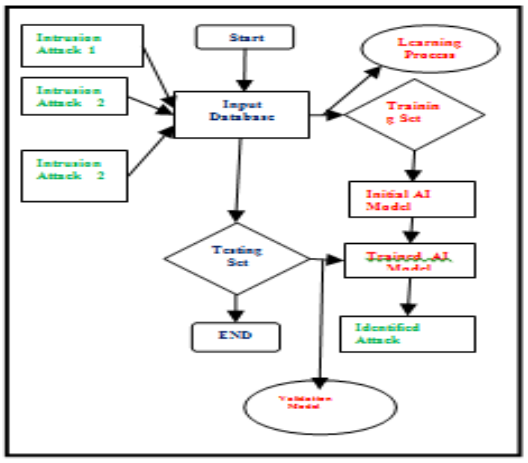

Figure 1.4.A AI Model framework for Computational Intelligence

VI. EXPERT SYSTEM FOR NETWORK INTRUSION DETECTION

Definition of Expert System Abraham (2005), stated that the basic components of an expert system are The knowledge base stores all relevant information, data, rules, cases, and relationships used by the expert system. A frame-based representation is ideally suited for object-oriented programming techniques. Expert systems making use of frames to store knowledge are also called frame-based expert systems. The most important characteristic of any expert system is that the knowledge is separated from control logic.

A. .Knowledge Base

The highly specialized knowledge of the problem area is located in the knowledge base. This module contains the problem facts, rules, concepts, and relationships. The first step to build the knowledge base is to gather the knowledge from human experts, which should be stored in the knowledge base.

B. .Working Memory

The working memory contains the facts about a problem that are collected during one consultation of the expert system. When a new problem has to be solved, the user enters information about the problem into the working memory.

C. Inference Engine

In logic, a rule of inference, inference rule, or transformation rule is the act of drawing a conclusion based on the form of premises interpreted as a function which takes premises, analyzes their syntax, and returns a conclusion (or conclusions).

VII. EXPERT SYSTEM FOR NETWORK INTRUSION DETECTION

The information including Knowledge Base, Rule sets, and other configurations related to run the Expert System

to detect Network Intrusion. The knowledge base contains specific feature of different network intrusion behaviour, which taken from database record about knowledge base and stored as variables of the web application, meanwhile the rule set is the rules that must be passed by real-time data packets. The rule sets are also taken from Database record about rule sets and stored to structure the application. The expert system for Network Intrusion detection as shown in the figure 1.5.

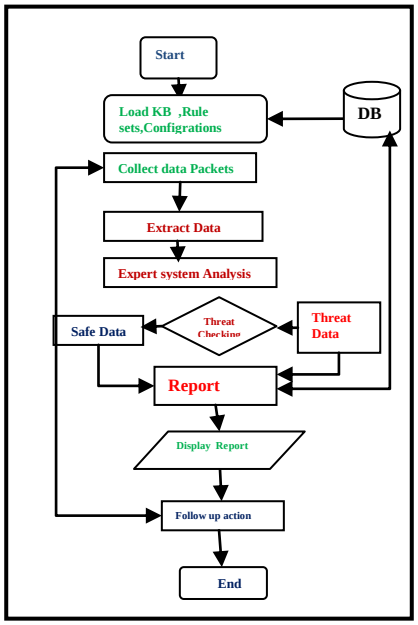

Figure 1.5. Expert System for NIDS

8. 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. In this paper explains the different intrusion detection systems with Artificial Intelligence and Expert systems.

AUTHOR INFORMATION

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. My research interest in the field of Computer Science in the area of Elliptic Curve Cryptography-Network Security, Data Mining, Neural Networks.

ACKNOWLEDGEMENT

I must be highly thankful to Sri Venkateswara University for providing facilities and supporting partially finance assistance for International research events.

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] J.B. Petrus, F. Thuijsman, and A.J. Weijters, “Artificial Neural Networks: An Introduction to ANN Theory and Practice”, Springer,1995, pp. 37-57.

[4] 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.

[5] 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.

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

[7] 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.

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

[9] 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.

[10] 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.

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

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

[13] 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.

[14] Sebring, M., Shell house, E., Hanna, M. & Whitehurst, R. (1988) Expert Systems in Intrusion Detection: Stanford-Chen, S. (1995, May 7). Using Thumbprints to Trace Intruders. UC

[15] Davis..Symeonidis, A. L., and Mitkas, P. A., 2005. Agent Intelligence through Data Mining. Multi-agent Systems, Artificial Societies, and Simulated Organizations International Book Series, Springer Business Media. Series 14: 200. USA:

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

[17] Y. Wang, "Fuzzy Clustering Analysis by using Genetic Algorithm", Innovative Computing, Information and Control Express Letters 2 (4), 2008, pp. 331-337.