International Journal of Information Technology and Knowledge Management
January-June 2008, Volume 1, No. 1, pp. 79-84

INTRUSION DETECTION USING NEURAL NETWORK TECHNIQUES

Aarti Singh & Girish Sharma

Abstract

Security of an information system is its very important property, especially today, when computers are interconnected via internet. Because no system can be absolutely secure, the timely and accurate detection of intrusions is necessary. For this purpose, Intrusion Detection Systems (IDS) were designed. There are two basic models of IDS: misuse IDS and anomaly IDS. Misuse systems detect intrusions by looking for activity that corresponds to the known signatures of intrusions or vulnerabilities. Anomaly systems detect intrusions by searching for an abnormal system activity. Most IDS commercial tools are misuse systems with rule-based expert system structure. However, these techniques are less successful when attack characteristics vary from built-in signatures. Artificial neural networks offer the potential to resolve these problems. As far as anomaly systems are concerned, it is very difficult to build them, because it is difficult to define the normal and abnormal behavior of a system. But for building anomaly system, neural networks can be used, because they can learn to discriminate the normal and abnormal behavior of a system from examples. Therefore, they offer a promising technique for building anomaly systems. This paper presents an overview of the applicability of neural networks in building intrusion systems and discusses advantages and drawbacks of neural network technology.

Keywords: Intrusion Detection System (IDS), misuse IDS, anomaly IDS, Kohonen´s self-organizing maps, Back propagation neural networks

1. Introduction

Today, when computers are connected via Internet and information systems gather and store important data, security of an information system has become very crucial. A secure information system should provide data confidentiality, data and communication integrity and assurance against denial-of-service attack (Mukherjee 1994). Data confidentiality protects against an unauthorized disclosure. Data integrity is concerned with the accuracy, faithfulness and non-corruptibility of data. Denial of service is a threat that takes place whenever the quality of system services falls below a predefined threshold or if the system services are completely inaccessible. The conventional approach to create a secure information system is to build a protective shield around it. For this purpose various methods of identification, authentication and mandatory access techniques are used. But there are a number of limitations to this prevention based approach. Firstly it is probably impossible to build a completely secure system, further

it could be impractical: the prevention based security philosophy necessarily constraints user's activity and productivity.

Intrusion Detection Systems (IDS) can be classified into two main categories: misuse and anomaly intrusion detection systems. Misuse refers to the known attacks that make use of the known system vulnerabilities. Misuse systems define attack signatures, i.e. patterns of activities that are known to be vulnerable. The misuse systems monitor the system activities in order to find out the defined signatures, the presence of which indicates an attack. Misuse systems have several draw backs, firstly it is difficult to create an exhaustive attack database and so some attacks might go unrecognized. Further it wouldn't be able to identify attack sequences containing small variations in the known attack signatures and would miss those attack events entirely. This would be very severe draw back since this is a very common technique of intrusion (to create new attack sequences by making small variations in the existing sequences). Anomaly systems are based on a different principle. They create a model of acceptable (normal) system activities and try to identify variations from this normal behavior (model).

Technical implementation of misuse systems is usually easier in comparison with the technical implementation of anomaly systems. It is based on expert knowledge of the usual attacks. From this knowledge, a database of attack signatures is built up. Anomaly systems are more difficult to realize because it is very difficult to explicitly define the normal behavior of a system. Since Neural networks, can learn things through examples thus using NN it can be possible to create a baseline of normal system behavior.

1.2 Neural Networks

Artificial neural networks (ANN) are a computing technology which came into existence in the beginning of 1940s. It got place in domain of Artificial Intelligence. ANN is an information processing paradigm which is inspired by the way biological nervous systems , such as the brain, process information. ANN is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. An artificial neuron is a device with many inputs and one output. The neuron has two modes of operation; the training mode (supervised & unsupervised) and the using mode. The best architecture to use depends on the type of problem to be represented by the network. There are various types of network architecture: Feed forward, feedback, fully interconnected net, competitive net, etc.

Following two types of neural networks are broadly used in the context of Intrusion detection systems: (i) Multilayered feed forward neural networks (ii) Kohonen´s self-organizing maps.

Multilayered feed forward neural networks (Fig. 1) are in essence 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. Kohonen's self-organizing maps (SOMs) are a promising technique for cluster analysis (Kohonen 1982). They are adapted for unsupervised learning. General SOM architecture is shown below in Fig. 2.

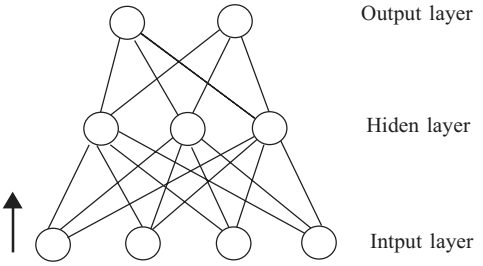

Figure 1: A Multilayered Feed Forward Neural Network with Three Layers

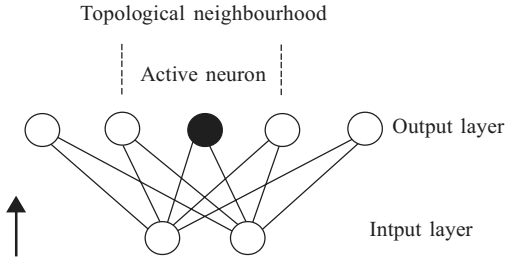

Figure 2: Kohonen's Self-organizing Maps (SOMs)

Misuse intrusion detection systems are based on expert knowledge of the usual attacks. From this knowledge, a database of attack signatures is created. The misuse IDSs spends a lot of time performing comparison of system activity with a database of attack signatures. While some signatures are simple to define and the algorithm for the database checking is straightforward, some others are very difficult to define and test. A typical example can be port scan. Port scan can be considered as an attempt to intrude a system, usually via internet. An intruder tries to find out a vulnerable server residing on some port. Although the intruder does not do any direct damage, one typically treats a port scan as an attack due to its possible malicious implications. Therefore the misuse IDS should look for such events. Here major problem is to define a signature of this event. Misuse IDS analyses incoming packets, but the intruder can perform some modifications in the identifiable items so as to overcome revealing of intrusion.* A straightforward port scan is relatively easy to detect because of the same source address, source port address and because every destination port is eventually tried. However the intruder can change the source address and source port in packets and send packets over a long time period. for example, by probing a single port after every few hours.*

Neural Networks can be useful in these situations. James Canady in his research paper 'Artificial neural networks for misuse detection' [9] has illustrated this. Fig. 3 given below indicates the principal of neural solution. Some important attributes of the incoming packets, denoted by $p1, p2, ..., pn$, are extracted by Feature extraction block shown in the figure. Output of the feature extraction block which is denoted by $q1, q2, ..., qn$ is then fed as input to the SOM neural network. The SOM neural network then classifies each input qi into one of the clusters, represented by it. Numbers assigned

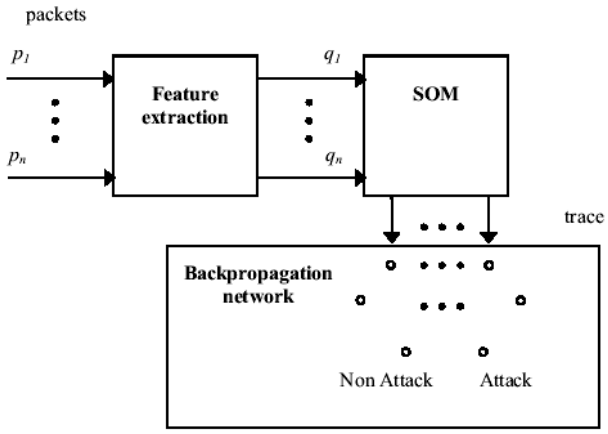

Fig. 3: Neural Network Component of Misuse Intrusion Detection System

to SOM nodes have to be chosen in such a way, that the topology of SOM lattice was preserved. It means that numbers assigned to the nodes of SOM lattice, which are near neighbors, do not differ a lot. The SOM block of the system must be trained beforehand by unsupervised learning and back propagation network by supervised learning. Using the same technique a SYN flood attack can be detected.

2. ANOMALY IDS WITH NEURAL NETWORKS

Anomaly detection systems do not know what the specific intrusion look like. They have the model of normal behavior of the system and they look for the deviations from the normal behavior for potential intrusions.

The main difficulty in developing an anomaly based system lies in defining normal behavior of the system. We can only define normal behavior only to a limited extent as behavior being a dynamic attribute; can change at any instant due to so many genuine reasons. But still we can identify abnormal behavior for e.g. In an organization the employees log into the systems during office hours i.e. from 9 am to 5or 6 pm. If one day, most of the users are logged into the system at 12 in night, then this event is certainly very abnormal and could be a sign of an unauthorized activity. By identifying such anomalies, anomaly IDS could identify potential intrusions.

As already explained it is very difficult to define normal activity of a system. In this situation neural networks can be quite useful as we can exploit there ability to learn from examples and also their capability of abstraction. The learning ability means that it is not necessary to define normal behavior of the system explicitly. Generalization allows the anomaly system to recognize when an attack sequence has been changed slightly. The neural networks are able to recognize a variant of an attack that might be missed by a misuse system.

In their paper they presented a system called NNID (Neural Network Intrusion Detector). NNID is a back propagation neural network trained to identify users based on what commands they use during the day. This system is implemented in the UNIX environment. UNIX maintains a log for each user which contains commands along with the resources used by each user. NNID creates a vector called 'user profile' using this log information, which in turn serves as 'print' of a user. This system was tested for 100 commands and 10 users. The system was 96% accurate in detecting unusual activity, with 7% false alarm rate.

CONCLUSION

Intrusion detection systems came into existence in 1980s and are in the process of research and development since then. Misuse based IDS can never be 100% reliable due to their dependency on signature databases. Thus entire scope of development and improvement lies in anomaly based IDS. While designing an anomaly detection system we can exploit the neural network's ability to learn and its ability to generalize. Neural network can learn to discriminate between normal and abnormal system behavior from examples. No explicit definition of the abnormal system behavior is necessary and thus major obstacle in building anomaly system could be overcome. Neural network approach seems promising for future developments in the area of IDSs.

REFERENCES

[1] Herve Debar, "An Introduction to Intrusion-Detection Systems," *IBM Research*, Zurich Research Laboratory.

[2] Magnus Almgren, Herv_e Debar, and Marc Dacier, (2000), "A Light-weight Tool for Detecting Web Server Attacks," In Gene Tsudik and Avi Rubin, Editors, Proceedings of NDSS 2000 (Network and Distributed System Security Symposium), 157-170, San Diego, CA, The Internet Society.

[3] Stefan Axelsson, (2000), "Intrusion Detection Systems: A Survey and Taxonomy," Department of Computer Engineering Chalmers University of Technology, Goteborg, Sweden.

[4] "Towards a Taxonomy of Intrusion_Detection Systems." by Herve Debar, Marc Dacier and Andreas Wespi, IBM Research Division, Zurich Research Laboratory.

[5] Huseyin Cavusoglu, Birendra Mishra, (2005), Anderson Graduate, Srinivasan Raghunathan "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research*, **16**(1), 28-46.

[6] Robert J. Shimonski, (2002), **"**What You Need to Know About Intrusion Detection Systems**"** Published.

[7] 'Intrusion Detection-Overview of the Technology', (2002), Jamie French, Whitehats.ca, Published, Nov 13, 2002C.

[8] Kaufman C., R. Perlman and M. Speciner, (2002), "Network Security: Private Communication in a Public World," Second Edition., Upper Saddle River, NJ: Prentice Hall PTR.

[9] James Canady, "Artificial Neural Network for Misuse Detection."

[10] Jake Ryan, Meng-Jang Lin, and Risto Miikkulainen, "Intrusion Detection with Neural Networks."

[11] A. Vesely and D. Brechlerova, (2003), "Neural Networks in Intrusion Detection Systems," Presented at International Conference Agrarian Perspectives XII (CUA Prague, September 18-19, 2003).

[12] Jean-Philippe Planquart, GSEC Certification-version 1.2d "Application of Neural Network to Intrusion Detection."

[13] Mehdi Moradi and Mohammd Zulkernine "A Neural Network Based System for Intrusion Detection and Classification of Attacks."

[14] Zheng Zhang Jun Li, C. N. Manikopoulos, Jay Jougenson, and Jose Ucles, (2001), "HIDE: A Hierarchical Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification," Proceedings of the 2001 IEEE Workshop on 'Information Assurance and Security.

[15] Richard P. Lippman, and Robert K.Cunningham, "Improving Intrusion Detection Performance Using Keyword Selection and Neural Networks."

[16] Alan Bivens, Chandrika Palagiri, Rasheda Smith, Boleslaw Szymanski, and Mark Embrechts, 'Network-based Intrusion Detection Using Neural Networks," Published in Proceedings of "Intelligent Engineering Systems Through Artificial Neural Networks ANNIE-2002."

[17] Martin Botha and Rossouw von Solms, "Utilizing Neural Networks for Effective Intrusion Detection."

Aarti Singh
Lect. MCA Deptt. JMIT Radaur, Haryana, INDIA
E-mail: singh2208@gmail.com

Girish Sharma
Asstt. Prof., BPIBS, I. P. University, Delhi, INDIA
E-mail: gkps123@gmail.com