Chapter 27
A Hybrid NIDS Model Using Artificial Neural Network and D-S Evidence

Chunlin Lu
Chinese Academy of Sciences, China

Mingjie Ma
Chinese Academy of Sciences, China

Yue Li
Chinese Academy of Sciences, China

Na Li
Institute of China Mobile Communication Company Limited, China

ABSTRACT

Artificial Neural Networks (ANNs), especially back-propagation (BP) neural network, can improve the performance of intrusion detection systems. However, for the current network intrusion detection methods, the detection precision, especially for low-frequent attacks, detection stability and training time are still needed to be enhanced. In this paper, a new model which based on optimized BP neural network and Dempster-Shafer theory to solve the above problems and help NIDS to achieve higher detection rate, less false positive rate and stronger stability. The general process of the authors' model is as follows: firstly dividing the main extracted feature into several different feature subsets. Then, based on different feature subsets, different ANN models are trained to build the detection engine. Finally, the D-S evidence theory is employed to integration these results, and obtain the final result. The effectiveness of this method is verified by experimental simulation utilizing KDD Cup1999 dataset.

1. INTRODUCTION

Network intrusion detection has played a central role to discover the process of abnormal behavior characteristics and provide early warning, to achieve the purpose of monitoring network behavior and network intrusion defense. With the development of network technology, network attacks become more and more complex and hidden. Detection precision and stability are two crucial indicators to evaluate the IDSs (de Sá Silva, L. et al.2008). The traditional method, such as rule-based expert systems and statistical

DOI: 10.4018/978-1-7998-0414-7.ch027

approaches (Manikopoulos, C & Papavassiliou. S 2002) are difficult to deal with those problems such as huge network traffic volumes in high speed network environment, especially a large number of video traffic data, imbalanced network data distribution, and the difficulty to provide continuous adaptation.

In addition of that, artificial intelligence and machine learning have shown limitations in achieving high detection accuracy and fast processing times when confronted with these requirements. More and more researches explore new methods (such as artificial neural network) to solve the problems. Among the researchers who use neural network to work on IDS, BPNN is the first choice due to its ability of accurate prediction and better persistence over the other ANN techniques. However, BP neural network itself has some drawbacks such as easy to fall into local minimum, slow convergence, weaker detection stability, network instability, high training time etc (Shah, B., & Trivedi, B. H. 2012; Patel, A., Taghavi, M., Bakhtiyari, K., & Júnior, J. C. 2013). In order to solve the above problems, in this paper, we propose a novel anomaly detection model based on optimized BP neural network and D-S theory to enhance the detection precision for low-frequent attacks, detection stability and reduce the training time. To illustrate the applicability and capability of the new approach, the results of experiments on KDD Cup1999 dataset demonstrated better performance in terms of detection precision, detection stability and training time.

The rest of this paper is organized as follows. We discuss the related work on IDS in Section 2. In Section 3, we elaborate the framework of our model, and explain its principles and working procedures. To evaluate the model, Section 4 illustrates the results and discussions of experiments. Finally, Section 5 draws the conclusions.

2. RELATED WORK

As mentioned above, more and more researches use artificial neural network to improve the performance of IDS. According to the number of the ANN techniques used, ANN based IDS can be categorized as: Simple ANN Based IDS and Hybrid ANN Based IDS.

Simple ANN applied to IDS mainly includes: Back Propagation neural network (BPNN). Back Propagation neural network (BPNN) (Wei, Z., Hao-yu, W., Xu, Z., Yu-xin, Z., & Ai-guo, W. 2010) is used to detect intrusion behavior, due to its ability of accurate prediction and better persistence. Authors of this paper illustrate BPNN is good in detection of the known and unknown attack. But, to train the BPNN, number of the epochs required was very high which lead to very high training time. If network is over trained then it can decrease the performance, and to overcome, one has to define the early stopping condition. Some researchers have compared the effectiveness of the simple ANN based IDS with other methods such as support vector machines and neural network (SVM)(Mukkamala, S., Janoski, G., & Sung, A. 2002), intrusion IDS using self-organizing maps(SOM) (Pachghare, V. K., Kulkarni, P., & Nikam, D. M. 2009), simulated annealing neural network(SANN) (Gao, M., & Tian, J. 2009) . Simple ANN based IDS had been shown to have lower detection performance and long training time, especially in dealing with a large amount of data at a high speed.

Hybrid ANN Based IDS is hybrid ANN which combines more than one ANN techniques. The motivation for using the hybrid ANN is to overcome the limitations of individual ANN. Horeis T et.al (Horeis, T. 2003) used a combination of SOM and radial basis function (RBF) networks. The system offers generally better results than IDS based on RBF networks alone. (Mafra, P. M., Moll, V., da Silva Fraga, J., & Santin, A. O. 2010) propose two layers approach, called Octopus-IIDS, based on KNN and