ABSTRACT

Today’s anomaly-based network intrusion detection systems (IDSs) are plagued with detecting new and unknown attacks. The review of the literature builds ideas for researching the problem of detecting these attacks using multi-layered feed forward neural network (MLFFNN) IDSs. The scope of the paper focused on a review of the literature from primarily 2008 to the present found in peer-review and scholarly journals. A key word search was used to compare and contrast the literature to find strengths, weaknesses and gaps. The significance of the research found that further work is needed to improve the performance and convergence rates of MLFFNN IDSs. This literature review contributes to the area of intrusion detection by looking at the effects of architecture, algorithms, and input data on the performance and convergence rates of MLFFNN IDSs.

Keywords: Anomaly Detection, Convergence Rate, Intrusion Detection System, Neural Networks, Performance Rate

INTRODUCTION

The goal of a network intrusion detection system (IDS) is to define normal and abnormal behavior across the computer network (Kabiri & Ghorbani, 2005). Furthermore, they are constantly attacked and must be able to defend against these intrusions. Mafra, Moll, Fraga and Santin (2010) see this as a recurring problem. This research will look into devising a model for detecting these new and unknown attacks using multi-layered neural networks and advanced algorithms. However, these systems have problems that can affect their performance in
detecting intrusions unless they are addressed. These include: poor accuracy, limited real-time performance, reduced scalability, can’t detect new threats and weak response (Kandeeban & Rajesh, 2011a). This research will look into solving some of these problems to improve detection of new and unknown attacks upon network systems.

However, today’s intrusion detection systems are plagued with working in a dynamic attack environment where hackers use new or variants of current threats. Improper detection of attacks can lead to the compromise of sensitive data and possible identity or money theft. A challenge for IDSs is to detect these new threats that adapt to evade current detection methods (Chandola, Banderjee & Kumar, 2009). Current signature-based detection methods cannot keep up with this changing environment (Joo, Hing & Han, 2003). This forces IDSs to adapt to changing environments by using anomaly detection methods. The common model used is an anomaly-based multi-layer feed forward neural network (MLFFNN) IDS. The MLFFNN IDS model takes in traffic data and feeds it through the network to its output without any feedback to the input. These models can adapt to learn about new and unknown intrusions according to Hua and Xiaofeng (2008). However, accurate classification of attacks by anomaly detection is affected by the architecture, input data and the algorithm used (Choudhary & Swarup, 2009). Architecture and algorithms used can affect the performance and convergence rates of anomaly-based IDSs (Choudhary & Swarup, 2009). The performance rate is the measurement of how well the IDS detects intrusions. It consists of the detection rate of how well the device discovers an abnormality and the error rate, which is when the device doesn’t correctly identify the threat. The convergence rate is a measurement of the time it takes to train the IDS. This is measured in seconds and how many times the process has to repeat itself until a certain error threshold is met. Each time the process is repeated is called an epoch. Research is ongoing to optimize MLFFNN IDS performance and convergence rates to handle these dynamic attacks. Contributing to this is the difficulty that an IDS must work correctly in unknown environments and deal with different attacks (Al-Sharafat & Naoum, 2009).

ARCHITECTURE EFFECTS ON MLFF IDS PERFORMANCE AND CONVERGENCE RATES

The MLFFNN architecture is a commonly used model for working with anomaly-based IDSs (Bhaskar, Kamath & Moitra, 2008; Wei, Haoyu, Xu, Yu-xin & Ai-guo, 2010). This makes it a good model to perform further research of its characteristics in looking at improvements to performance and convergence rates in IDSs. The architecture of a MLFFNN is composed of three layers: Input, Hidden and Output. The input layer collects numeric data and passes it to the hidden layer. The hidden layer takes the output from the input layer and determines if the data is an intrusion or normal traffic. The result is sent to the output layer where it is classified according to the specific type of intrusion or as normal traffic. Engen, Vincent and Phalp (2008) found that using just these three layers can provide an adequate model to use. Modeling of a MLFFNN IDS is an important problem according to Bhaskar, Kamath and Moitra (2008). This is because MLFFNN IDS models are complex and hard to design. Wu and Banzhaf (2010) support this and add that the process of automatically constructing these models from the input data can be difficult, especially for solving intrusion detection problems. Ahmad, Abdullah and Alghamdi (2009) used variations of input and hidden layer neurons to determine their model. Others followed a similar path to suit their research needs and to maximize results. The performance of a neural network is sensitive to the number of neurons in the network. Too few neurons can cause poor results and too many will cause over fitting problems according to Ding, Xu, Zhu, Wang and Jin (2011). Also complex and large number of interconnections between neurons can slow down the flow of information in a neural
Impact of the Interoperability of ERPs on Information Systems Disintegration
www.igi-global.com/article/impact-of-the-interoperability-of-erps-on-information-systems-disintegration/186764?camid=4v1a

Design and Development of a Quality Management Information System
www.igi-global.com/chapter/design-development-quality-management-information/36711?camid=4v1a