International Journal of Synthetic Emotions
Volume 8 • Issue 1 • January-June 2017

Network Traffic Intrusion Detection System Using Fuzzy Logic and Neural Network

Mrudul Dixit, Department of Electronics and Telecommunication, MKSSS's Cummins College of Engineering for Women, Pune, India

Rajashwini Ukarande, Department of Electronics and Telecommunication, MKSSS's Cummins College of Engineering for Women, Pune, India

ABSTRACT

Intrusion Detection System (IDS) are actively used to identify any unusual activities in a network. To improve the effectiveness of IDS, security experts have embedded their extensive knowledge with the use of fuzzy logic, neuro-fuzzy, neural network and other such AI techniques. This article presents an intrusion detection system in network based on fuzzy logic and neural network. The proposed system is evaluated using the KDD Cup 99 dataset. The fuzzy system detects the intrusion behavior of the network using the defined set of rules. Whereas neural network trains the network based on the input and uses the trained system to predict the output. The evaluation depicts the effectiveness of the selected method in terms of selection of attributes which gives high True Positive Rate and True Negative Rate, with good precision in attack detection.

KEYWORDS

Artificial Neural Network, Backpropagation Algorithm, Denial of Service, Fuzzy Logic, Intrusion Detection System (IDS), KDD Cup 99 Dataset, Probe

INTRODUCTION

The latter half of last century has seen tremendous growth of security systems, which will ensure data privacy in current network. As given in et al. (Landwehr et al., 1994) all network systems suffer from security vulnerabilities which are technically difficult and economically costly to be solved by the manufacturers. Here, the Intrusion Detection Systems (IDS) plays a vital role, which detects anomalies and attacks in the network. The research in the intrusion detection field is mostly on anomaly-based especially in academic research; it is considered as the most powerful method because of its theoretical potential for addressing the novel attacks. Anomaly detectors identify the possible attack attempts by building profiles which represent normal usage and then compare it with current behavior data to find out a likely mismatch et al. (Srinivasu et al., 2009) Many IDS are designed using various techniques out of which the authors will compare fuzzy based system with that of neural network. Researchers focused on fuzzy rule learning and neural network training for effective intrusion detection using data mining techniques. Considering these points, the authors have developed a fuzzy rule based system in detecting the attacks and will compare the performance with the neural network system.

DOI: 10.4018/IJSE.2017010101

The fuzzy system makes use of effective rules to identify the design strategy, obtained by mining the data effectively. The fuzzy rules generated from the proposed strategy can be able to provide better classification rate in detecting the intrusion behavior. While neural network trains the training dataset such that it can detect the attack in a testing dataset efficiently. In this article authors have compared both the methods based on some performance parameters and found the most efficient method for this type of application.

LITERATURE REVIEW

Intrusion Detection System

An IDS is designed to monitor the network traffic and examine traffic data for protocol anomalies, that represent potential attacks and suspicious activities; and alerts the network administrator (Cisco, 2014). It works like a defence system which prevents hostile activities compromising of system securities (Kazienko & Dorosz, 2003). In anomaly based systems, the network administrator states the baseline or normal threshold of the network. The IDS monitors the network traffic and compares it against stored patterns of normal behaviour, so that any pattern violating its behaviour will be defined as system attack. The assumptions of IDS are that the intruder's behaviour has to be unusual from that of the normal users. The main components of an Intrusion Detection System are:

1. Information Source: data used by the IDS;
2. Analysis engine: process of intrusion detection;
3. Response: action taken for detection of intrusion.

Fuzzy Inference

In 1964 Lotfi A. Zadeh, from University of California, Berkeley introduced a paper on fuzzy sets which created the idea of grade of membership, emphasizing on imprecise and vague outputs. In 1965, he came up with fuzzy multistage decision-making, fuzzy similarity relations, fuzzy restrictions and linguistic variables. Mamdani developed the first fuzzy logic controller in 1974. It was an attempt to control a steam engine and boiler by synthesizing a set of linguistic control rules obtained from experienced human operators (Kay, 2004). A fuzzy rule is a simple If-Then rule which provides an easy means to express and capture the human mind to summarize data and focus on decision-relevant information. Fuzzy inference deriving logical conclusions from existing fuzzy rule base (Naik, 2012 & Tikk, 2002). It is the mapping of fuzzy input onto a fuzzy output space with the help of fuzzy rules. The rule base is the key component of a fuzzy inference system.

Artificial Neural Network

In 1943 Neuro-physiologist Warren McCulloch and mathematician Walter Pitts wrote a paper on how neurons might work and modelled a simple neural network using electrical circuits et al. (Dilag et al., 2000). It is similar to training a system by taking into consideration the idea of human neural scheme. Typically, the neural network has efficient results in several applications (Radhwan *et al*., 2015; Ghosh *et al*.; 2015; de Vries *et al*.; 2015; Hore *et al*., 2016a; 2016b; Chatterjee *et al*., 2016; Li *et al*.; 2017; Acharjya & Anitha, 2017; Guesgen, & Marsland, 2016; Arora *et al*., 2016). Here, Levenberg Marquardt algorithm is used which is the fastest Backpropagation algorithm. In the training period, the training data is given as input to the input layer. The net input layer acts as an output to the hidden layer and the data propagates to the output layer. Here, all hidden nodes are multiplied with their respective weights and summed up. Similarly, the output layer nodes get input from the net hidden layer nodes which get multiplied with their respective weights and are summed up. These outputs are then compared with the target output values giving the error value. This forward traversing of the node values is known as the forward pass. This error value is used to update the weights of the output and hidden nodes which