Chapter 14

Intrusion Detection Using Deep Belief Network and Extreme Learning Machine

Zahangir Alom
University of Dayton, USA

Venkata Ramesh Bontupalli
University of Dayton, USA

Tarek M. Taha
University of Dayton, USA

ABSTRACT

Security threats for computer networks have increased dramatically over the last decade, becoming bolder and more brazen. There is a strong need for effective Intrusion Detection Systems (IDS) that are designed to interpret intrusion attempts in incoming network traffic intelligently. In this paper, the authors explored the capabilities of Deep Belief Networks (DBN) – one of the most influential deep learning approach – in performing intrusion detection after training with the NSL-KDD dataset. Additionally, they examined the impact of using Extreme Learning Machine (ELM) and Regularized ELM on the same dataset to evaluate the performance against DBN and Support Vector Machine (SVM) approaches. The trained system identifies any type of unknown attack in the dataset examined. In addition to detecting attacks, the proposed system also classifies them into five groups. The implementation with DBN and SVM give a testing accuracy of about 97.5% and 88.33% respectively with 40% of training data selected from the NSL-KDD dataset. On the other hand, the experimental results show around 98.20% and 98.26% testing accuracy respectively for ELM and RELM after reducing the data dimensions from 41 to 9 essential features with 40% training data. ELM and RELM perform better in terms of testing accuracy upon comparison with DBN and SVM.

DOI: 10.4018/978-1-5225-1759-7.ch014

1. INTRODUCTION

Cyber Security is a perennial problem for most organizations including banks, retail stores, and critical infrastructures (such as power grids). Cyber-attacks can be disastrous and pernicious, leading to the exposure of sensitive personal and business information, disrupting critical operations, and causing significant economic damage. One of the key forms of defense against cyber-attacks is network intrusion detection. Other types of attacks include internal threats and Advanced Persistent Threats (APT). These are typically carefully constructed, and are dangerous due to internal users' privileges to access network resources. With this in mind, and the increasing sophistication of attacks, new approaches to protect network resources are always under investigation. Intrusion detection systems are typically used to detect and thwart inside and outside threats.

The current research on intrusion detection and prevention is being done through hardware and software implementations. Software implementations, such as SNORT and BRO, are complex programs to detect malwares entering over the network. Although these approaches have high accuracies, they can also have high false positive rates. As a result, human evaluation is needed to distinguish between actual intrusions and false positives. Several hardware approaches have been proposed to accelerate intrusion detection algorithms and software. These have typically used FPGAs and ASICs. An alternative memristor based approach for intrusion detection (Bontupalli, 2014) used a brute force string matching architectures to classify packet data. This system is programmable and has high throughput along with very low power consumption.

Neural networks have good learning and inherent detection capacity which could be leveraged if they are trained well for intrusion detection. Neural network approaches toward intrusion detection potentially provide high detection accuracy and low false positive rates. Multi-layer perceptron models have been under extensive research for intrusion detection. Conventional recurrent neural network (RNN) training algorithms, such as the back propagation through time (BPTT) and real-time recurrent learning (RTRL), can be used for faster convergence speeds. In this paper, intrusion detection using deep learning approaches, in particular deep belief networks (DBN) are examined. Additionally, we examine the potential of other deep learning and advanced machine learning approaches such as SVM, ELM, and RELM for intrusion detection. The main contributions of this work are:

1. Proposed a comprehensive intrusion detection system for cyber security using deep learning (DBN);
2. Examine intrusion detection using ELM and RELM techniques;
3. Performance evaluation of intrusion detection with ELM, RELM, DBN, and SVM for finding the state of the art testing accuracies.

The proposed model improves the classification rate for known and unknown attacks with minimum false alarm rates. The rest of the paper is organized according to the following ways: Section 2 examines related work while Section 3 provides background on intrusion detection systems. Sections 4, 5, and 6 provide background on Restricted Boltzmann Machines (RBM), DBN, and ELM respectively. A discussion on the dataset used for training and testing is given in Section 7 and experimental results are described in Section 8. Finally, conclusion and future directions are discussed in Section 9.