available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks

*Morteza Amini**, *Rasool Jalili*, *Hamid Reza Shahriari*

Department of Computer Engineering, Sharif University of Technology, Azadi Avenue, Tehran, Iran

ARTICLE INFO

Article history:
Received 25 April 2005
Revised 4 April 2006
Accepted 18 May 2006

Keywords:
Network security
Intrusion detection systems
Misuse detection
Anomaly detection
Unsupervised neural network
Self-organizing map
Adaptive resonance theory

ABSTRACT

With the growing rate of network attacks, intelligent methods for detecting new attacks have attracted increasing interest. The RT-UNNID system, introduced in this paper, is one such system, capable of intelligent real-time intrusion detection using unsupervised neural networks. Unsupervised neural nets can improve their analysis of new data over time without retraining. In previous work, we evaluated Adaptive Resonance Theory (ART) and Self-Organizing Map (SOM) neural networks using offline data. In this paper, we present a real-time solution using unsupervised neural nets to detect known and new attacks in network traffic. We evaluated our approach using 27 types of attack, and observed 97% precision using ART nets, and 95% precision using SOM nets.

1. Introduction

The increasing reliance on networked computers, and the growing expertise in subverting such systems, makes intelligent and adaptive threat detection vital.

Computer security revolves around confidentiality, integrity, and availability. Integrity refers to the trustworthiness of data or resources, and is usually phrased in terms of preventing improper or unauthorized change. Integrity mechanisms fall into two classes: prevention or detection (Bishop, 2003).

Prevention mechanisms try to maintain the integrity of data by blocking unauthorized attempts to change data. On the other hand, detection mechanisms do not try to prevent violations of integrity, but simply report that data integrity can no longer be assumed (Bishop, 2003). Intrusion Detection Systems (IDSs) attempt to detect intrusion and attacks through analyzing events in computer systems or networks. IDSs can be classified as being based on anomaly detection or misuse detection depending on how they analyse data (Cannady, 1998; Coolen and Luijf, 2002).

Misuse detection systems detect known attacks using attack patterns and signatures known a priori, while anomaly detection systems detect attacks by observing deviations from normal behaviour of the system, network, or users (Amini and Jalili, 2004).

Some early research on IDSs explored neural nets for intrusion detection. These can be used only after training on normal or attack behaviours, or combination of the two. Both supervised and unsupervised neural nets have been

* *Corresponding author*. Tel.: +98 21 66164019; fax: +98 21 66164020.
E-mail addresses: m_amini@ce.sharif.edu (M. Amini), jalili@sharif.edu (R. Jalili), shahriari@ce.sharif.edu (H.R. Shahriari).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.05.003

used. Most supervised neural net architectures require retraining to improve analysis on varying input data, but unsupervised nets, which offer greater adaptability, can improve their analysis capability dynamically (Cannady, 1998).

In this paper, we introduce RT-UNNID (Real-Time Unsupervised Neural-Net-based Intrusion Detector). This can detect network-based attacks using unsupervised neural nets in real-time, and has facilities for training, testing, and tuning of unsupervised nets for intrusion detection purpose. Using the system, we evaluated two types of unsupervised Adaptive Resonance Theory nets (ART-1 and ART-2) and a traditional unsupervised Self-Organizing Map (SOM) net. We present a practical solution for using unsupervised neural nets for real-time intrusion detection, compare the performance of such neural nets in real-time intrusion detection, and introduce ART nets as a better solution for dynamic IDSs.

The remainder of the paper is organised as follows: Section 2 discusses related work on intrusion detection using neural networks. Section 3 describes a practical way toward using unsupervised neural networks in intrusion detection. Section 4 introduces the RT-UNNID system and describes its main components. Section 5 focuses on data feature selection and preprocessing in this system. Section 6 discusses the unsupervised neural-net-based engine and how ART and SOM neural nets may be used. Section 7 presents experimental results, and Section 8 draws conclusions and describes future work.

2. Related work

Neural-net-based IDSs can be classified into the following four categories.

2.1. *MLFF neural-net-based IDSs*

The first category includes the systems built on Multi-Layer Feed-Forward (MLFF) neural nets, such as the Multi-Layer Perceptron (MLP) and Back Propagation (BP). MLFF neural nets have been used in most early research in neural-net-based IDSs. Works including Ryan et al. (1998) and Tan (1995) used MLFF neural nets for anomaly detection based on user behaviours. MLFF nets that trained on known attack patterns or signatures were used for misuse detection in Cannady (1998) and Ghosh and Schwartzbard (1999), while Bonifacio (1998) and Lippmann and Cunningham (2000) focused on incorporating MLFF nets with techniques such as keyword selection and expert systems. Other researchers have compared the effectiveness of MLFF neural nets to other methods such as Support Vector Machine (SVM) and Multivariate Adaptive Regression Splines (MARS) (Mukkamala et al., 2002, 2004); MLFF neural nets have been shown to have lower detection performance than SVM and MARS.

2.2. *Recurrent and adaptive neural-net-based IDSs*

This category includes systems built on recurrent and adaptive neural nets such as ELMAN and CMAC. By getting feedback from its output or its protected system, the neural net preserves the correlation of current system inputs with previous system inputs and states (Cannady, 2000; Debar et al., 1992; Debar and Dorizzi, 1992). Debar et al. used a simplified ELMAN recurrent net (GENT) and multi-layer recurrent net with back-propagation to predict the next acceptable command (Debar et al., 1992; Debar and Dorizzi, 1992). Cannady has applied the CMAC (Cerebellar Model Articulation Controller) net – a form of adaptive neural nets – to learn new attacks autonomously by modified reinforcement learning (Cannady, 2000).

2.3. *Unsupervised neural-net-based IDSs*

The third category uses unsupervised learning neural nets to classify and visualize system input data to separate normal behaviours from abnormal or intrusive ones. Most of the systems in this category use Self-Organizing Maps (SOMs), while a few use other types of unsupervised neural nets. Fox (Kevin et al., 1990) was the first to apply an SOM to learn the characteristics of normal system activity and identify statistical variations from the normal trends. In Rhodes et al. (2000), multiple SOMs are used for intrusion detection, where a collection of specialized maps are used to process network traffic for each protocol such as TCP, UDP, and ICMP. Each neural net is trained to recognise the normal activity of a single protocol. Girardin in Girardin (1999) used SOM for visualizing the network activity that provides new ways for network administrators to explore, track, and analyse intruders. This approach is different from both anomaly and misuse detection and considers human factors to support the exploration of network traffic and judgment about anomaly packets. Höglund et al. (2000) trained SOM on a collection of normal data from UNIX audit data and used it for detecting anomalous user activity. Li used statistical methods for anomaly detection; active users are compared to historical profiles, and are classified as normal if their behaviour closely matches their historical profiles (Li, 1997). Using ART-2 net for clustering users by command profiles in this system greatly improved the prediction rate.

Some recent research has explored using multiple neural nets in a hierarchical structure to improve classification accuracy. In Lichodzijewski et al. (2002b), hierarchical SOMs are applied to examine session data by users on a UNIX system in order to find behavioural anomalies. In Zhang et al. (2001), a Hierarchical Intrusion Detection (HIDE) system is introduced which can detect network-based attacks as anomalies using statistical preprocessing and neural net classification. Five different types of neural net classifiers – Perceptron, Back Propagation (BP), Perceptron–Back propagation-Hybrid (PBH), Fuzzy ARTMAP, and Radial-based Function – were evaluated. In Lichodzijewski et al. (2002a), a two-level hierarchical SOM was applied to detect intrusions. The system has emphasis on the representation of time and incremental development of a hierarchy. The SOM in this system is able to detect attack patterns over a sequence of connections. The NSOM system described in Labib and Vemuri (2002) uses a structured SOM to classify real-time Ethernet network data, and can classify DoS attacks graphically as opposed to normal traffic by demonstrating that the clustering of neurons is very different between them.