Chapter 2
Detection of Network Attacks With Artificial Immune System

Feyzan Saruhan-Ozdag
Istanbul University-Cerrahpasa, Turkey

Derya Yiltas-Kaplan
https://orcid.org/0000-0001-8370-8941
Istanbul University-Cerrahpasa, Turkey

Tolga Ensari
Istanbul University-Cerrahpasa, Turkey

ABSTRACT

Intrusion detection systems are one of the most important tools used against the threats to network security in ever-evolving network structures. Along with evolving technology, it has become a necessity to design powerful intrusion detection systems and integrate them into network systems. The main purpose of this research is to develop a new method by using different techniques together to increase the attack detection rates. Negative selection algorithm, a type of artificial immune system algorithms, is used and improved at the stage of detector generation. In phase of the preparation of the data, information gain is used as feature selection and principal component analysis is used as dimensionality reduction method. The first method is the random detector generation and the other one is the method developed by combining the information gain, principal component analysis, and genetic algorithm. The methods were tested using the KDD CUP 99 data set. Different performance values are measured, and the results are compared with different machine learning algorithms.

INTRODUCTION

Network security became more important because of increasing usage of internet and network technologies. Diversity of user profiles and increase of users have a big effect on network attacks. Various security policies are developed in the internal structures of institutions to protect the accessibility, integrity, and confidentiality of data against these security threats. These policies are supported by security applications

DOI: 10.4018/978-1-7998-1839-7.ch002

that are important for the network system and can be software or hardware such as firewall and intrusion detection systems (IDS). IDS need a learning process to decide whether the activities occurring on the network are going to be attacked or not. Machine learning is a popular research area that aims to enable machines to make decisions on their own by adopting human learning tactics. There are many studies that apply different machine learning methodologies to detect network attacks in the literature. Nguyen and Choi (2008) used J48 for detection, Koc et al. (2012) used Hidden Naive Bayes Multiclass Classifier, Hosseinpour et al. (2014) benefited from artificial immune system (AIS), Dasgupta and González (2002) used niching technique with genetic algorithm (GA) for generate detector in AIS, and Gupta and Shrivastava (2015) implemented support vector machine (SVM) and bee colony together for anomaly detection. This study is based on AIS algorithms to detect the attacks. AIS has been inspired by the human immune system. This system has been investigated especially for being an effective methodology to detect virus, fraud and fault control (Dasgupta, 1998). Negative selection algorithm (NSA) is effective on categorizing attacks, therefore in this paper the focus will be on this point. NSA uses antigen and anticors' structures which exist within natural immune system. The attacks in a network are assumed as antigen and the self-cells are recognized in the learning process as anticors.

In the literature, the IDS studies are based on two different detection methods: Anomaly detection and the misuse detection. In misuse detection, events on the system are evaluated according to signatures based on the weak points of the system or security policies. Every attack defined on the system has a signature. Behaviors that are not within these signatures are called normal. There should be defined signature for new attacks and it should be introduced to these systems. The main problem with this method is that the new attack type will not be recognized. Whereas anomaly detection determines the behavior on the system as normal or abnormal. In general, the traffic on the network is monitored and an assessment is made according to the thresholds. The system is trained through normal and abnormal situations, then it is expected to make an evaluation for each new data.

There are limited numbers of papers involving IDS and AIS together. A concurrent study was designed with Particle Swarm Optimization (Tabatabaefar et al., 2017). The experimental results were given as the detection and performance measurement rates. There has not been a comparison with any machine learning algorithm. Another IDS study is based solely on regular AIS (Suliman et al., 2018). DoS and Probing attack classes were detected and the results for correctly predicted attacks were calculated. Another study in the literature (Igbe et al., 2017) presents a method to detect DoS/DDoS attacks by using the Dendritic Cell Algorithm involved in AIS algorithms. In this method, the network traffic features were gathered as a vector and then used to retrieve antigen and signals. The signals were processed to be distinguished into dangerous and safe categories. The output signal was determined as anomaly or normal according to the computational values of the antigens.

This paper suggests an approach for IDS using AIS and for detector generation using both classical methods and GA. In order to observe the effect of the system on the decision making ability, feature selection and dimensionality reduction are used together in the pre-process step. KDD CUP 99 data set is used in the experiments. This data set, which is a different version of DARPA 1988 and DARPA 1999, has been prepared in the DARPA 1988 MIT Lincoln laboratory. Sections of this paper are prepared as following: Section 2 demonstrates a short background on IDS. Section 3 contains information about artificial and natural immune systems, GA, feature selection, and dimensionality reduction. Section 4 gives information about the applied approach. Section 5 illustrates experimental results. Finally, Section 6 gives the discussion on the study and Section 7 is about the conclusion and future works.