


Chapter 15

Fuzzy Rule-Based Layered Classifier and Entropy-Based Feature Selection for Intrusion Detection System

Devaraju Sellappan

 <https://orcid.org/0000-0003-3116-4772>

Sri Krishna Arts and Science College, India

Ramakrishnan Srinivasan

 <https://orcid.org/0000-0002-8224-4812>

Dr. Mahalingam College of Engineering and Technology, India

ABSTRACT

Intrusion detection systems must detect the vulnerability consistently in a network and also perform efficiently with the huge amount of traffic. Intrusion detection systems must be capable of detecting emerging and proactive threats in the networks. Various classifiers are used to classify the threats as normal or intrusive by supervising the system activity. In this chapter, layered fuzzy rule-based classifier is proposed to detect the various intrusions, and fuzzy entropy-based feature selection is proposed to identify the relevant features. Layered fuzzy rule-based classifier is proposed to improve the performance of the intrusion detection system. KDD dataset contains various attacks; these attacks are grouped into four classes, namely Denial-of-Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R). Real-time dataset is also considered in this research. Experimental result shows that the proposed method provides good detection rate, minimizes the false positive rate, and less computational time.

DOI: 10.4018/978-1-7998-5728-0.ch015

INTRODUCTION

Recent scenario, most of the people have connected with internet for their specific purpose and other related purpose. So, the Intrusion Detection System (IDS) is important for any individual or organization to safeguard their information from unauthorised users. Organizations are using hardware and software devices to secure their information, eventually most of the intruders were not detected. Today the information is more important for any organization, so need to protect the information from unauthorised users because many unauthorised users are using different techniques to detect the information and exploit the systems are more vulnerabilities. Whenever the informations are transmit from one host to another host, which does not provide the protection from unauthorised users. In these aspects, Security is essential to protect the information.

Intrusion Detection Systems (IDS) are usually classified into two groups: Signature based and Anomaly based intrusion detection system. The signature based intrusion detection system detects the intrusion by comparing with its existing signatures in the log files. The anomaly based intrusion detection system which is observed from network when it behavior deviates from the normal attacks. Intrusion Detection System is classified as Network based intrusion detection system and Host based intrusion detection system. The network based intrusion detection system is a system which detect the misbehavior whenever the system can able to communicate with each other over the network. The host based intrusion detection system is a system which monitor and analyze the computer system if there is any misbehavior. (Devaraju & Ramakrishnan, 2013).

Fuzzy Rule-based technique is used to process the large volume of raw data easily. The various techniques are Association Rule, Clustering, Decision Trees, Neural Networks and Data Mining. The various authors have tried to improve the performance and reduce the false positive rate of intrusion detection system. Even though there are some misbehavior happening in intrusion detection system and could not be improve the performance and reduce the false positive rate due to the dataset contains large volume of data. The data contains many features and the authors were used all the features for processing but some features are not important.

In this paper, try to create a new set of fuzzy rulesets based on the protocol features which will help us to improve the performance, reduce the false positive rate and less processing time. There are three types of protocol feature are considered such as tcp, udp and icmp. Mainly attacks are depending on the any one of the protocol feature so need to category the data based on the protocol features to reduce the feature as well. The uniquenesses of the proposed paper are as follows:

- i) Fuzzy entropy-based feature selection is proposed to select the most relevant features from KDD dataset.
- ii) Fuzzy rule-based classifier is proposed to generate the new sets of fuzzy rules using selected features to classify the attacks by using KDD dataset and Real-time dataset.
- iii) Layered classifier is proposed to get better the performance and less computational time.

The organization of the paper is as follows: Background of the related work, discusses fuzzy entropy-based feature selection and layered fuzzy rule-based classifier; describes experimental work of the proposed methods; and provides a conclusion.

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/fuzzy-rule-based-layered-classifier-and-entropy-based-feature-selection-for-intrusion-detection-system/261735

Related Content

Security in Digital Marketing: Challenges and Opportunities

Albérico Travassos Rosário (2023). *Confronting Security and Privacy Challenges in Digital Marketing* (pp. 206-233).

www.irma-international.org/chapter/security-in-digital-marketing/326398

Honeypot Baselineing for Zero Day Attack Detection

Saurabh Chamotra, Rakesh Kumar Sehgal and Ram Swaroop Misra (2017). *International Journal of Information Security and Privacy* (pp. 63-74).

www.irma-international.org/article/honeypot-baselineing-for-zero-day-attack-detection/181549

Towards the Development of a Holistic Framework of Project Complexity: A Literature Based Review

Saleem Gul (2019). *International Journal of Risk and Contingency Management* (pp. 1-17).

www.irma-international.org/article/towards-the-development-of-a-holistic-framework-of-project-complexity/227019

End-to-End Security Comparisons Between IEEE 802.16e and 3G Technologies

Sasan Adibi and Gordon B. Agnew (2008). *Handbook of Research on Wireless Security* (pp. 364-378).

www.irma-international.org/chapter/end-end-security-comparisons-between/22058

Trust and Reliability Management in Large-Scale Cloud Computing Environments

Punit Gupta (2021). *Large-Scale Data Streaming, Processing, and Blockchain Security* (pp. 66-89).

www.irma-international.org/chapter/trust-and-reliability-management-in-large-scale-cloud-computing-environments/259465