Chapter 10
Association Rule-Mining-Based Intrusion Detection System With Entropy-Based Feature Selection: Intrusion Detection System

Devaraju Sellappan
https://orcid.org/0000-0003-3116-4772
Sri Krishna Arts and Science College, Coimbatore, India

Ramakrishnan Srinivasan
https://orcid.org/0000-0002-8224-4812
Dr. Mahalingam College of Engineering and Technology, Pollachi, India

ABSTRACT

Intrusion detection system (IDSs) are important to industries and organizations to solve the problems of networks, and various classifiers are used to classify the activity as malicious or normal. Today, the security has become a decisive part of any industrial and organizational information system. This chapter demonstrates an association rule-mining algorithm for detecting various network intrusions. The KDD dataset is used for experimentation. There are three input features classified as basic features, content features, and traffic features. There are several attacks are present in the dataset which are classified into Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). The proposed method gives significant improvement in the detection rates compared with other methods. Association rule mining algorithm is proposed to evaluate the KDD dataset and dynamic data to improve the efficiency, reduce the false positive rate (FPR) and provides less time for processing.

DOI: 10.4018/978-1-7998-5348-0.ch010

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Today many people have connected with internet for their business purpose and other related purpose. So, the intrusion detection system (IDSs) is important for any industry to protect their information from intruders. Industries are using software and hardware devices to secure the information, even though many intruders were not identified. Today the information is most important role in our life. So, need to protect the data from intruders because many malicious users are using various techniques to exploit the systems vulnerabilities. While the information is sent from one system to another, there is no protection from intruders. In these aspects, need to protect the information more securely.

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

Data mining technique is used to process the large volume of raw data easily. The various techniques are Association Rule, Clustering, Decision Trees and Neural Networks. 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 IDS 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 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 any one of the protocol features so need to category the data based on the protocol features to reduce the feature as well. The purpose of the systems is i) to generate association rules to improve the detection rate and ii) to refine the association rules correctly to reduce the false alarm. The association rule-based systems are developed using Java Development Kit (JDK) for better performance applied to KDD dataset and dynamic data using Association Rule-Mining Algorithm.

The paper is organized as follows: In Section 2, discusses the related work, Section 3, discusses KDD Dataset Description, Section 4, discussing Entropy based Feature Selection, Section 5, describes the Methodology. Section 6 gives the results and discussion and Section 7 deals with conclusion of the research work.

RELATED WORK

There are various techniques have been proposed. They are statistical methods, neural network, data mining etc. In this section, the various techniques used for intrusion detection systems are discussed.

C-Means Clustering was applied for intrusion detection which uses minimum testing dataset and reducing the features by using reduction algorithm to improve the detection time (Minjie & Anqing, 2012). A novel twin support vector machine and SVM were used to overcome the normal traffic patterns and classification accuracy (Nie & He, 2010; Srinivas, Andrew & Ajith, 2004; Sumaiya & Aswani, 2017).

22 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/association-rule-mining-based-intrusion-detection-system-with-entropy-based-feature-selection/261978

Related Content

The Covert Strengthening of Islamic Extremists under Ronald Reagan and George W. Bush
Jason Cooley (2014). *International Journal of Cyber Warfare and Terrorism (pp. 17-28).*
www.irma-international.org/article/the-covert-strengthening-of-islamic-extremists-under-ronald-reagan-and-george-w-bush/127384

Blind Image Source Device Identification: Practicality and Challenges
Udaya Sameer Venkataand Ruchira Naskar (2020). *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications (pp. 558-575).*
www.irma-international.org/chapter/blind-image-source-device-identification/251449

A Lone Wolf vs. an Affiliated Terrorist: Knowledge Inference on Who Poses More Danger to the Tourist
Donald Douglas Atsa'amand Ruth Wario (2022). *International Journal of Cyber Warfare and Terrorism (pp. 1-9).*
www.irma-international.org/article/a-lone-wolf-vs-an-affiliated-terrorist/304045

Cyber Attacks and Preliminary Steps in Cyber Security in National Protection
Faruk Aydinand O. Tolga Pusatli (2015). *Cybersecurity Policies and Strategies for Cyberwarfare Prevention (pp. 269-285).*
www.irma-international.org/chapter/cyber-attacks-and-preliminary-steps-in-cyber-security-in-national-protection/133934

Advanced Network Data Analytics for Large-Scale DDoS Attack Detection
Konstantinos F. Xylogiannopoulos, Panagiotis Karampelasand Reda Alhajj (2017). *International Journal of Cyber Warfare and Terrorism (pp. 44-54).*
www.irma-international.org/article/advanced-network-data-analytics-for-large-scale-ddos-attack-detection/185603