Hindawi
Security and Communication Networks
Volume 2022, Article ID 9663052, 23 pages
https://doi.org/10.1155/2022/9663052

WILEY | Hindawi

Review Article

A Systematic Review on Hybrid Intrusion Detection System

Elijah M. Maseno,[1,2] **Zenghui Wang**,[2] **and Hongyan Xing**[3]

[1]*School of Information Technology for Defence Systems, Defence Forces Technical College, Nairobi 19120-00501, Kenya*
[2]*College of Science, Engineering and Technology, University of South Africa, Pretoria 1709, South Africa*
[3]*Collaborative Innovation Center for Meteorological Disaster Prediction and Evaluation, Nanjing University of Information Science and Technology, Nanjing 210044, China*

Correspondence should be addressed to Zenghui Wang; wangzengh@gmail.com

Received 23 December 2021; Revised 5 March 2022; Accepted 29 March 2022; Published 10 May 2022

Academic Editor: Leandros Maglaras

As computer networks keep growing at a high rate, achieving confidentiality, integrity, and availability of the information system is essential. Intrusion detection systems (IDSs) have been widely used to monitor and secure networks. The two major limitations facing existing intrusion detection systems are high rates of false-positive alerts and low detection rates on zero-day attacks. To overcome these problems, we need intrusion detection techniques that can learn and effectively detect intrusions. Hybrid methods based on machine learning techniques have been proposed by different researchers. These methods take advantage of the single detection methods and leverage their weakness. Therefore, this paper reviews 111 related studies in the period between 2012 and 2022 focusing on hybrid detection systems. The review points out the existing gaps in the development of hybrid intrusion detection systems and the need for further research in this area.

1. Introduction

The Internet has thrived, hence an increase in information sharing, making network security a problem of concern. Attackers around the globe have their eyes on computer systems with the motive of deploying attacks. The security of an electronic device is breached when a successful attack occurs. Intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource" [1]. The *Integrity* aspect of a given infrastructure serves to ensure information remains unaltered by unauthorized users. *Availability* incorporates all aspects of the infrastructure that makes information readily available to users in the system. *Confidentiality* implies that the information in a given system is protected from unauthorized access and viewing by external parties. Therefore, a computer network is considered to be fully secured when the core objectives of these three attributes are sufficiently met. To help achieve these objectives, intrusion detection systems have been developed with the primary intent of monitoring incoming traffic in computer networks for any potential malicious intrusions.

An intrusion detection system (IDS) scans information system resources and reports any malicious activities in the system. More advanced IDSs have the capability of acting against the attacks. The action taken by this advanced IDS is to block the malicious users or activities from accessing the computer resources. We have two major categories of intrusion detection systems, which include misuse based and anomaly based. Misuse-based IDSs are developed to flag known attacks using patterns of the known attacks [2]. Misuse detection systems use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. The positive side of misuse IDS is the ability to detect known attacks with great precision. The major challenge facing this type of IDS is their inability to flag new forms of attacks [3]. Misuse intrusion detection systems stand out because of their ability to flag many or all known attack patterns. The main problem facing misuse-based systems is the inability to flag emerging attacks or zero-day