Chapter 2
Detecting Cyber Threats With a Graph-Based NIDPS

Brendan Ooi Tze Wen
Taylor's University, Malaysia

Tan Zheng Shen
Taylor's University, Malaysia

Najihah Syahriza
Taylor's University, Malaysia

Yap Zhe Hin
Taylor's University, Malaysia

Nicholas Chan Wei Xian
Taylor's University, Malaysia

Siva Raja Sindiramutty
Taylor's University, Malaysia

Nicki Gan Wei
Taylor's University, Malaysia

Teah Yi Fan Nicole
Taylor's University, Malaysia

ABSTRACT

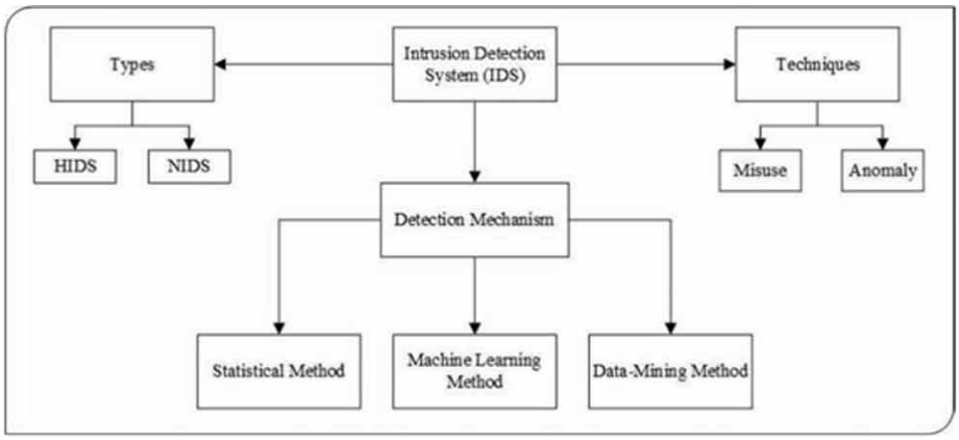
This chapter explores the topic of a novel network-based intrusion detection system (NIDPS) that utilises the concept of graph theory to detect and prevent incoming threats. With technology progressing at a rapid rate, the number of cyber threats will also increase accordingly. Thus, the demand for better network security through NIDPS is needed to protect data contained in networks. The primary objective of this chapter is to explore the concept of a novel graph based NIDPS through four different aspects: data collection, analysis engine, preventive action, and reporting. Besides analysing existing NIDS technologies in the market, various research papers and journals were explored. The authors' solution covers the basic structure of an intrusion detection system, from collecting and processing data to generating alerts and reports. Data collection explores various methods like packet-based, flow-based, and log-based collections in terms of scale and viability.

DOI: 10.4018/978-1-6684-7625-3.ch002

INTRODUCTION

According to Kumar, Gupta, and Arora (2021) and Sulaiman et. al. (2021), an intrusion detection system abbreviated as IDS, is software that can detect unauthorised traffic or entry into a host or network by detecting unusual behaviours or by examining multiple data streams within the host or network processes. The demand for sophisticated IDSs is necessary in the 21st century due to rapid advancements in the field of Internet of Things (IoT) with more devices than ever being connected to the Internet. Such advancements have also encouraged the wide-spread use of cloud technologies, which may be storing confidential or sensitive user data (Sulaiman et al., 2021). The move to cloud technologies have caused these services to be prone to cyber-attacks from malicious users resulting in data breaches, Distributed Denial of Services (DDoS), compromised communication between senders and receivers among other issues (Kumar, Gupta and Arora, 2021; Ponnusamy, Humayun, et al., 2022). Before the discovery and deployment of the IDS, other steps have been taken to overcome the vulnerabilities such as the implementation of more secure internet protocols. HyperText Transfer Protocol Secure (HTTPS) and Secure Socket Layer (SSL) were among the protocols introduced as well as Firewalls and various cryptography techniques to further secure these spaces. Figure 1.0 provides an overview of the types, detection mechanisms and techniques used in various types of IDS.

Figure 1. Overview of IDS
Source: Aljanabi, Ismail, and Ali (2021)



Definition and Importance of IDS and NIDS

Among the common detection mechanisms that are employed on Intrusion Detection Systems are rule-based detection and statistical-based detection (Adnan et. al, 2021). Rule-based detection also known as knowledge-based detection is where an administrator or a super-user would define set parameters also known as rules for normal use. When a user who may be a regular user or intruder performs an action or activity that is not within the defined parameters, an alert will be sounded, and countermeasures will take place. Such systems could also be trained using datasets that contain information on normal activities or actions, an intrusion into the system will then be detected when an action outside of the training