Received: 20 May 2020 | Revised: 31 August 2020 | Accepted: 29 September 2020

DOI: 10.1002/ett.4150

SURVEY PAPER

WILEY

Network intrusion detection system: A systematic study of machine learning and deep learning approaches

Zeeshan Ahmad[1,2] | **Adnan Shahid Khan**[1] | **Cheah Wai Shiang**[1] | **Johari Abdullah**[1] | **Farhan Ahmad**[3,4]

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Sarawak, Malaysia

[2]Department of Electrical Engineering, College of Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia

[3]Cyber Security Research Group, College of Engineering and Technology, University of Derby, Derby, UK

[4]Institute for Future Transport and Cities, Coventry University, Coventry, UK

Correspondence
Adnan Shahid Khan, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 Kota Samarahan, Malaysia.
Email: skadnan@unimas.my

Abstract

The rapid advances in the internet and communication fields have resulted in a huge increase in the network size and the corresponding data. As a result, many novel attacks are being generated and have posed challenges for network security to accurately detect intrusions. Furthermore, the presence of the intruders with the aim to launch various attacks within the network cannot be ignored. An intrusion detection system (IDS) is one such tool that prevents the network from possible intrusions by inspecting the network traffic, to ensure its confidentiality, integrity, and availability. Despite enormous efforts by the researchers, IDS still faces challenges in improving detection accuracy while reducing false alarm rates and in detecting novel intrusions. Recently, machine learning (ML) and deep learning (DL)-based IDS systems are being deployed as potential solutions to detect intrusions across the network in an efficient manner. This article first clarifies the concept of IDS and then provides the taxonomy based on the notable ML and DL techniques adopted in designing network-based IDS (NIDS) systems. A comprehensive review of the recent NIDS-based articles is provided by discussing the strengths and limitations of the proposed solutions. Then, recent trends and advancements of ML and DL-based NIDS are provided in terms of the proposed methodology, evaluation metrics, and dataset selection. Using the shortcomings of the proposed methods, we highlighted various research challenges and provided the future scope for the research in improving ML and DL-based NIDS.

KEYWORDS

Deep learning, Machine learning, Network anomaly detection, Network intrusion detection system, Network security

1 | INTRODUCTION

With the recent interest and progress in the development of internet and communication technologies over the last decade, network security has emerged as a vital research domain. It employs tools like firewall, antivirus software, and