Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

A new hybrid teaching learning based Optimization -Extreme learning Machine model based Intrusion-Detection system

Mustafa Qahatan Alsudani [a,*], Salah H. Abbdal Reflish [a], Kohbalan Moorthy [b], Myasar Mundher Adnan [c,d]

[a] Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-sadiq University, Najaf, Iraq
[b] Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Kuantan, Malaysia
[c] Islamic University, Najaf, Iraq
[d] Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, 81310 Johor Bahru, Malaysia

ARTICLE INFO

Article history:
Available online 13 July 2021

Keywords:
Fast Learning Network
Intrusion detection system
Optimization

ABSTRACT

Currently, effective Intrusion-detection systems (IDS) still represent one of the important security tools. However, hybrid models based on the IDS achieve better results compared with intrusion detection based on a single algorithm. But even so, the hybrid models based on traditional algorithms still face different limitations. This work is focused on providing two main goals; firstly, analysis based on the main methods and limitations of the most-recent hybrid model-based on intrusion detection, secondly, to propose a novel hybrid IDS model called TLBO-ELM based on the Firefly algorithm and Fast Learning Network.

Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.

1. Introduction

Technology has over the many years impacted the current days based on several applications like marketing, shopping, and messaging [1,2]. Moreover, most of these technologies connect to internet which makes them facing the attacks and virus risk. There are several tools the researchers have been developed during last decades for provides safe environment for users. Furthermore, Intrusion Detection System (IDS) is one of the powerful software [3] that is used to monitor computer network for the detection of normal or abnormal behaviors [4–6]. An IDS monitors a network for signs of invasion which could manifest in abnormal system behaviors or violation of network security policies. Moreover, there are several limitations of the conventional IDS [7–9], such as high rate false alarms, lack of continuous adaptation to changing malicious behaviors, and highly uneven data distribution. Furthermore, the incorporation of machine learning (ML) [10] can enhance the performance of IDS [11,12] as the ML algorithms can ensure optimum performance. This work provides several contributions based on ML models: firstly, analysis of the most recent models of ML-based IDS, secondly, proposed a new hybrid model which includes Extreme Learning machine (ELM) and Teaching Learning based Optimization (TLBO) algorithms which can fill the gaps in the current ML models based on IDS.

2. Overview of intrusion detection system

Technological advancements in the present world have made connectivity easier than ever [13]. A large amount of information (personal, military, government, and commercial) are hosted on network infrastructures worldwide. The security of network infrastructures is attracting great research interest due to the huge number of intellectual properties which can be easily acquired through the internet. The society has become over-reliant on technology as people depend on computer systems for their daily information and entertainment [2,13–15].

Moreover, IDS represents one of powerful security tool which monitoring the system activities for any abnormal system behaviors or violation of network security policies. Moreover, IDS perform several functions [16] such as Monitors and analyzes the activity of the system users and Checks the critical system and data file integrity. In general IDS techniques divided into anomalies or signatures of attack are used by the detection system for the detection of attacks, and these techniques determine the effectiveness of an IDS [6,12,17–20]. Furthermore, works proposed hybrid models based on IDS such as optimize for machine learning algorithms achieved better results in compared with models based on single

* Corresponding author.
E-mail addresses: dfjj77128@gmail.com, salah.muslim@uobasrah.edu.iq (M. Qahatan Alsudani).

https://doi.org/10.1016/j.matpr.2021.07.015
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Nanoelectronics, Nanophotonics, Nanomaterials, Nanobioscience & Nanotechnology.