International Journal of Web-Based Learning and Teaching Technologies
Volume 17 • Issue 2

Enhanced SCADA IDS Security by Using MSOM Hybrid Unsupervised Algorithm

Sangeetha K., Kebri Dehar University, Kebri Dehar, Ethiopia
Shitharth S., Kebri Dehar University, Kebri Dehar, Ethiopia
Gouse Baig Mohammed, Vardhaman College of Engineering, India

ABSTRACT

Self-organizing maps (SOM) are unsupervised neural networks that cluster high dimensional data and transform complex inputs into easily understandable inputs. To find the closest distance and weight factor, it maps high dimensional input space to low dimensional input space. The closest node to data point is denoted as a neuron. It classifies the input data based on these neurons. The reduction of dimensionality and grid clustering using neurons makes to observe similarities between the data. In the proposed mutated self-organizing maps (MSOM) approach, the authors have two intentions. One is to eliminate the learning rate and to decrease the neighborhood size, and the next one is to find out the outliers in the network. The first one is by calculating the median distance (MD) between each node with its neighbor nodes. Then those median values are compared with one another. If any of the MD values significantly varies from the rest, they are declared as anomaly nodes. In the second phase, they find out the quantization error (QE) in each instance from the cluster center.

KEYWORDS

Internet Security, Intrusion Detection System (IDS), Mutated Self-Organizing Maps (MSOM), Quantization Error (QE), Self-Organizing Maps (SOM), Supervisory Control and Data Acquisition (SCADA)

1.INTRODUCTION

Supervisory control and data acquisition system are such an integral part of the latest automation industries. This receives data from various sources like sensors, RTU (Remote Terminal Units) and smart meters. The major tasks performed by SCADA (Rakas et al., 2020; Tamy et al., n.d.) is to monitor the connected data fetching sources. SCADA systems are mainly used to control and monitoring purposes in various industrial applications. It can be used for a small office building to monitor environmental conditions also used to monitor complex conditions in a nuclear power plant SCADA (Ferrag et al., 2020; Khan et al., 2019; Waagsnes & Ulltveit-Moe, n.d.) . To protect control systems, systems are evaluated before being deployed in production. So the operators have a good understanding of what types of vulnerability those systems may be introducing into their environment. One of the challenges of control systems is that many of them have been developed in an environment that works very well in operations, but they don't have all of the cybersecurity safeguards built into them (Shitharth et al., 2021; Suaboot et al., 2020). Sensor nodes which sense physical phenomenon that

DOI: 10.4018/IJWLTT.20220301.oa2

occur around them. These sensor nodes are majorly used for medical purposes, agriculture, industrial purposes, and so on. SCADA system uses wired or wireless sensor networks to transport the data from the master station. SCADA systems mainly use wireless sensor networks due to their frequent changing topology nature and the possibility of reconfiguration of networks. Using the wireless sensor networks this information or data is transmitted through a router, firewall, and switches. The first layer of protection is a router. The router should be configured with a VPN tunnel on the router side. Firewalls in control systems are used to protect unauthorized access (Priyanga et al., 2019; Teixeira et al., 2018). Data should be encrypted, to increase the level of information security, while accessing information through the internet. Various security threats (Gao et al., n.d.; Gao et al., 2020; Shitharth & Winston, 2016) are evolving every day like unauthorized access to the control software, virus infection and one more major threat is intruders sending malicious packets to host devices. By sending these packets anyone can control the SCADA devices.

2. RELATED WORK

SCADA network system has a high level of flexibility and adaptability, yet it consumes notable resources (Gao et al., 2020). Feature sets of these techniques are easily accessible by the attacker. SCADA systems are vulnerable to LOWSPAN or IP based networks. Lowspan architecture for SCADA systems is used for various applications (Shitharth & Winston, 2016). When SCADA systems used in industrial environments, it requires high receptivity, high acceptance, stability, and measurements. Yang, et al (n.d.) suggested a deep learning model for detecting the intrusions from the SCADA system based on the hand-crafted features. The main intention of this paper was to develop a retaining scheme for handling new threats by characterizing the salient temporal patterns. Ghosh, et al (2019) conducted a detailed survey on various issues and challenges related to the SCADA security. Here, the different types of threats could affect the normal operations of SCADA systems have been investigated, which includes masquerade, virus and norms, eavesdrop, Denial of Service (DoS), and Trojan horse. Qassim, et al (2017) intended to analyze various security vulnerabilities in the SCADA systems for ensuring the increased security of data transmission. Here, various testbed approaches have been validated based on the parameters of scalability, reliability, accuracy, safety, and repeatability. Almalawi, et al (2015) developed a data drivel clustering approach for detecting the normal and precarious stages of SCADA systems by using the proximity based detection rules. The main purpose of this work was to minimize the false positives by estimating the Euclidean distance for relabeling the critical states. In addition to that, the rank based precision measure was also computed for analyzing the efficiency of this IDS framework. Mo, et al (2013) presented a comprehensive survey for identifying the integrity attacks of SCADA networks. The aim of this review was to provide the possible countermeasures for detecting the harmful intrusions against the SCADA networks.Gumaei, et al (2020) implemented a cyberattacks detection framework for enhancing the security of SCADA based on the optimal selection of features. Here, the Correlation based Feature Selection (CFS) model was utilized to enhance the detection accuracy of network by eliminating the irrelevant features. In addition to that, the KNN algorithm was deployed to accurately predict the intrusions based on the optimal set of features. Kalech, et al (2019) suggested a temporal pattern recognition approach incorporated with the Hidden Markov Models (HMM) for ensuring the security and reliable communication in SCADA networks. Here, the feature extraction was mainly peformed to analyze the normal behavior of temporal patterns. Also, it utilized the HMM for categorizing the types of intrusions according to the generated patterns of the given dataset. Lai, et al (2019) employed a CNN model for predicting the anomalies with increased accuracy and reduced misclassification results. Here, the correlation between the features have been analyzed with reduced cost of error for identifying the anomalies. Also, the different types of classification techniques such as HMM, SVM ensemble, DT and CNN models have been validated and compared based on the accuracy. From the analysis, it was observed that the CNN model outperforms the other techniques with high performance