World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:16, No:07, 2022

Real-Time Network Anomaly Detection Systems Based on Machine-Learning Algorithms

Authors : Zahra Ramezanpanah, Joachim Carvallo, Aurelien Rodriguez

Abstract : This paper aims to detect anomalies in streaming data using machine learning algorithms. In this regard, we designed two separate pipelines and evaluated the effectiveness of each separately. The first pipeline, based on supervised machine learning methods, consists of two phases. In the first phase, we trained several supervised models using the UNSW-NB15 data-set. We measured the efficiency of each using different performance metrics and selected the best model for the second phase. At the beginning of the second phase, we first, using Argus Server, sniffed a local area network. Several types of attacks were simulated and then sent the sniffed data to a running algorithm at short intervals. This algorithm can display the results of each packet of received data in real-time using the trained model. The second pipeline presented in this paper is based on unsupervised algorithms, in which a Temporal Graph Network (TGN) is used to monitor a local network. The TGN is trained to predict the probability of future states of the network based on its past behavior. Our contribution in this section is introducing an indicator to identify anomalies from these predicted probabilities.

Keywords : temporal graph network, anomaly detection, cyber security, IDS
Conference Title : ICISP 2022 : International Conference on Imaging and Signal Processing
Conference Location : Paris, France
Conference Dates : July 19-20, 2022