Discriminative spatial-temporal feature learning for modeling network intrusion detection systems

Authors: Wanjau, Stephen Kahara[*] | Wambugu, Geoffrey Mariga | Oirere, Aaron Mogeni | Muketha, Geoffrey Muchiri

Affiliations: School of Computing and Information Technology, Murang'a University of Technology, Kenya

Correspondence: [*] Corresponding author. E-mail: steve.kahara@gmail.com.

Abstract: Increasing interest and advancement of internet and communication technologies have made network security rise as a vibrant research domain. Network intrusion detection systems (NIDSs) have developed as indispensable defense mechanisms in cybersecurity that are employed in discovery and prevention of malicious network activities. In the recent years, researchers have proposed deep learning approaches in the development of NIDSs owing to their ability to extract better representations from large corpus of data. In the literature, convolutional neural network architecture is extensively used for spatial feature learning, while the long short term memory networks are employed to learn temporal features. In this paper, a novel hybrid method that learn the discriminative spatial and temporal features from the network flow is proposed for detecting network intrusions. A two dimensional convolution neural network is proposed to intelligently extract the spatial characteristics whereas a bi-directional long short term memory is used to extract temporal features of network traffic data samples consequently, forming a deep hybrid neural network architecture for identification and classification of network intrusion samples. Extensive experimental evaluations were performed on two well-known benchmarks datasets: CIC-IDS 2017 and the NSL-KDD datasets. The proposed network model demonstrated state-of-the-art performance with experimental results showing that the accuracy and precision scores of the intrusion detection model are significantly better than those of other existing models. These results depicts the applicability of the proposed model in the spatial-temporal feature learning in network intrusion detection systems.

Keywords: Network intrusion detection, deep learning, spatial feature learning, temporal feature learning, Convolutional Neural Networks, Bi-directional Long Short Term Memory

DOI: 10.3233/JCS-220031

Journal: Journal of Computer Security, vol. 32, no. 1, pp. 1-30, 2024