Implementing an Intrusion Detection System for Software Defined Networks using Artificial Intelligence

S.B. Ihalagedara[1], M. Koswaththa[1], S. Senewirathna[1], M.B. Dissanayaka[1]*, A. Udunuwara[2]

[1]*Department of Electrical and Electronic Engineering, University of Peradeniya, Peradeniya, 20400, Sri Lanka*
[2]*Sri Lanka Telecom PLC, Colombo 01, 503, Sri Lanka*
**maheshid@eng.pdn.ac.lk*

This study presents an artificial intelligence (AI) based innovative approach for an Intrusion Detection System (IDS) within a Software-Defined Networking (SDN) environment. The research involves testing and identifying the most effective algorithm of machine learning and deep learning, specifically XGBoost, Logistic Regression, LightGBM, and Artificial Neural Network (ANN), for intrusion detection. The methodology consists of creating a virtual SDN using Mininet, a virtual network emulator package, with five hosts and three switches to emulate real-world network scenarios. The OpenDaylight SDN controller is integrated into this network, facilitating seamless communication and control. Rest API and Wireshark tool are used to control the SDN controller and monitor the traffic of the network. Learning models are integrated into the SDN controller to monitor and analyze network traffic effectively and detect the attack types of DoS, DDoS, BOTNET, BFA, Probe, U2R, and Web-attack with a minimum false positive rate. We have used a publicly available SDN intrusion detection dataset to train these learning models. Hyperparameter tuning is carried out to determine the optimal conditions of each learning model and comprehensive performance comparison is carried out using accuracy, precision, recall, and F1-score. At model training, the highest accuracy of 99.9% was achieved through XGBoost algorithm while ANN with ten layers followed closely with an accuracy of 99.26%. These findings were further validated through the emulated SDN network. Our finding showed that the proposed models can successfully prevent a DDoS attack through the integration of the SDN controller and the machine learning model. These observations demonstrate the significant potential of machine learning and deep learning techniques for effectively coping with cyberattacks and improving cybersecurity strategies. In conclusion, this study presents a promising approach to enhance cybersecurity in SDN networks through AI approaches.

Keywords: machine learning, deep learning, cybersecurity, intrusion detection systems, software defined network