ABSTRACT

Nowadays, Software Defined Networking (SDN) almost exclusively applied to network infrastructures. Because SDN separates the control plane and data plane, the network administrator can manage everything from a single console. However, the control plane of the SDN technology is vulnerable against various attacks such as distributed denial of service (DDoS), denial of service (DoS), brute force attack, and others.

An example of technology that can prevent this DDoS attack is an intrusion detection system (IDS). The anomaly-based IDS works by detecting any anomalous traffic in the network flow and comparing it with the normal ones. The convolutional neural network (CNN) is one of the algorithms that can be used in anomaly-based IDS. This method works by training any dataset of captured packets on the network flow and converting it to an image. This process, which is still challenging, has to be done in a short time to avoid any vulnerabilities on the network.

In this research, there are two methods for converting data to images. First, convert the data to an colors image, and second, convert the data to a grayscale image. After the conversion method is done, the next step is to train the dataset with the CNN method. To help with this process, this method will use TensorFlow as the back-end, where the Graphical Processing Unit is used to process the training method.

Based on the simulation, the grayscale images have better accuracy at 99.4% compared with the red-blue image at 99.3%. An increase in the number of dataset gives a negative trend to the accuracy metric. When the dataset is increased to 7,000, the accuracy metric drops as low at 98.7%. Reducing the dataset's feature has little effect on the dataset, with only red-blue image accuracy increasing by 0.1%. While CNN has the same accuracy as random forest (RF) at 99.4%, this method has more flexibility by adding a filter to the image to increase the accuracy.

Keywords: cybersecurity, IDS, SDN, CNN, deep-learning.