ABSTRACT

The rapid development of data communications has resulted in a long on-going research and development for Intrusion Detection System (IDS). Along with the increasing rates of Distributed Denial of Service (DDoS) attacks, a scalable approach is expected more than ever. One of many approaches for improving IDS is by using Machine Learning (ML) method. This undergraduate thesis proposes to build an IDS model using Convolutional Neural Network (CNN) algorithm which is the specialized type of ML model since this algorithm has already been achieved a rapid breakthrough among other ML models on several field of study.

This undergraduate thesis is conducted by experimentations that will emphasize more on the approach of how to utilize CNN to build and evaluate a highly accurate classifier to classify between benign and malicious network traffic. In order to incorporate CNN on an IDS, the experiment will be started by converting CSE-CIC-IDS2018 sample into a pixelate image as an input to the IDS model. The best model will be chosen by comparing performance metrics of each model on different parameter combinations and the final model will be evaluated with k-fold Cross-validation technique to make sure the finest performance is obtained.

The optimal model is determined based on the value of convolution filter, dropout, dense layer, and batch size of the ML model. The results of the experiments show that the model achieved its optimal performance with the value of 16 for convolution filter, 0.3 for dropout, 128 for dense layer, and 2048 for batch size. Furthermore, with k-fold as evaluation tool, the model chosen has shown a consistent and stable high-performance metrics, especially with nearly perfect classification for all type of traffic with more than 99% of accuracies and losses results lower than 0.2%. Based on the final result obtained, the author concluded that the model implemented on this undergraduate thesis is not only successful, but also is better compared to other traditional ML-based IDS in terms of performance metrics.

Keywords: Intrusion Detection System, Machine Learning, Convolutional Neural Network