ABSTRACT

SDN Separates the Control Plane and data plane so that SDN is Centralized. In The SDN Network, the Controller is the heart of the network, when controller gets a Distributed Denial Services (DDoS) Attack, will disrupt network availability on switch and controller. In Addition, with limited Resources, the training process on Machine Learning must be reduced. Thus, increasing accuracy and reducing Machine Learning time in DDoS detection on SDN becomes important.

To improve accuracy and reduce training time on DDoS attacks in SDN networks, we propose DDoS detection using a Machine Learning with Ensemble K-Means++ and Random Forest algorithms. In the experimental stage, we used InSDN as a Dataset. This research consists of two stages, the first stage is feature selection and then instance reduction using K-means++ and classification using Random Forest. The second stage is the detection test model method on the SDN network using the mininet emulator as a network environment in the process of capturing normal and attacks data then using data from IoTID20.

The Research using Ensemble K-means++ and Random Forest methods can reduce training time and increase the accuracy of the test model classification in detecting DDoS on SDN networks using normal and attack data from new generated test data on SDN and from IoTID20. The algorithms get an average training time of 2.4 seconds and can detect normal and attack traffic using new generated attacks and normal data by 81.1% and getting 64.3% accuracy using the normal and Mirai attack from (IoTID20).

Keyword : DDoS Attack, SDN, Machine Learning, Security