ABSTRACT

During the development of computer networks today. A software is designed to build network infrastructure, namely Software Defined network (SDN). Software Defined Network (SDN) is the basic concept of SDN is to perform an explicit separation between control and forwarding planes, and then abstracting the system and isolating the existing complexity in components or sub-systems by defining a standard interface. In conventional networks, network administrators are required to handle tens, hundreds or even thousands of network devices within an organization. This problem is often found in the industrial world. This is where Software Defined Network (SDN) provides a promising architecture for future networks and can provide benefits with programmability of controllers to manage all traffic on the network. Despite the advantages that SDN has, there are challenges to the security of the SDN network. Namely its vulnerability to Distributed Denial of Service (DDoS) attacks. Distributed Denial of Service (DDoS) is one of the attacks that can attack components in the SDN architecture. In this study, a DDoS attack detection and mitigation system was built to detect and mitigate DDoS attacks on the SDN architecture using the SOM algorithm. SOM is applied to machine learning models to classify normal traffic and DDoS attack traffic based on features taken from the dataset, namely speed of flow entries and speed of source IP. From the test results that have been carried out the system is able to detect and mitigate DDoS attacks. By measuring the accuracy of getting the best results of 76.33333% using a learning rate of 0.50 and a test size of 0.30.

Keywords: Software Defined Network (SDN), Self-organizing Map (SOM), Machine Learning, Distributed Denial Of Service (DDoS)