ABSTRACT

Software Defined Network or SDN, is a new approach in network programming for designing, building, and managing computer networks by separating the control plane from the data plane to centralize the network to concentrate all settings at the control plane. SDN can dynamically monitor, modify, and manage network behavior through open interface software.

Network development has frequently encountered issues related to network security and network attacks. In contrast with conventional networks, SDN has various advantages, one of which is that SDN can implement centralized control functions on the controller, which makes the controller the heart of SDN. The centralized nature of SDN makes it a target for attacks, one of which is a Distributed Denial of Service (DDoS) attack.

Several approaches to detect attacks in SDN have been proposed, but few consider the security of the controller. Therefore, a security system is needed to overcome the problem of attacks that occur on SDN controllers. To address the problem, a DDoS attack detection system is built using a Machine Learning algorithm, namely Random Forest, whose algorithm performance is optimized by using Hyperparameter Tuning to achieve high accuracy in the detection process. The InSDN dataset, consisting of a total of 56 classes, was used in this research. This method proved to be effective in detecting DDoS attacks, with an accuracy value of 99.99%. The findings demonstrate that Hyperparameter Tuning Random Forest is an effective method for detecting DDoS attacks on SDN.

Keywords: Software Defined Network, Distributed Denial of Service, Machine Learning, Random Forest, Hyperparameter Tuning.