ABSTRACT

Networks in various sectors of life, ranging from education, health, to business, are very closely connected, which makes the function of one sector often depends on the network infrastructure in other sectors. LAN (Local Area Network) is often found in various places such as homes, offices, and campuses. Although commonly used, managing networks at the enterprise level is not easy because it requires complex tools. To solve this problem, Software Defined Network (SDN) technology was developed, allowing administrators to control network traffic remotely or via the cloud. However, SDN is also vulnerable to cyberattacks such as DDoS (Distributed Denial of Service). DDoS is an attack that sends fake traffic packets continuously to overwhelm and bring down the system. According to a Cloudflare report, by 2023, DDoS attacks increased significantly by 65% compared to the previous quarter, showing an increase in the frequency and complexity of attacks. To counter this threat, the authors developed a DDoS detection system on SDN networks using machine learing, specifically the Naïve Bayes algorithm, which is designed to classify attacks effectively and efficiently. The Naïve Bayes algorithm model that the author built, classifies based on packet entry, packet entry and the ratio between packet entry and packet entry. In its application, this model is applied to the RYU Controller, a controller used in SDN and run with the python programming language. This research also calculates the accuracy value using 30% of the data as test data and 70% of the data as training data. The results of the accuracy measurement test is with an average of 95%, which means it is very high when compared with research with other machine learing algorithms.

Keyword : Software Defined Network (SDN), Distributed Denial of Service (DDoS), Naïve Bayes, Machine Learning, RYU Controller