## *ABSTRACT*

*Technology is growing along with the development of computer networks. In designing a good network infrastructure, it takes a network architecture that is dynamic, and easy to adapt and manage for hardware and software adjustments. To achieve this, we need a concept known as Software Defined Network (SDN). On an SDN network, it is very possible for administrators to provide network provisioning quickly without the need to manually configure the network because it is centralized in one controller. However, SDN also has several shortcomings, namely being single of failure and vulnerable to attacks, one of the attacks that is vulnerable to SDN is vulnerable to DDoS attacks. To prevent DDoS attacks from happening, one of the things that must be done is to detect DDoS attacks that appear. To detect DDoS there are several ways or methods that can be applied such as using machine learning or statistical methods. In this study, a research was conducted using statistical methods to detect DDoS attacks that appeared. One of the statistical DDoS attack detection methods to be studied is to detect attacks using entropy. To detect attacks using entropy, a threshold value, windows size, and count are needed as parameters to detect the emergence of DDoS attacks. In this study, a threshold value of 0.87 was used, a windows size of 26, and a count of 5, and the highest accuracy was 72.857142857142857% from 30 experiments using entropy as a method to detect attacks.*

*keyword− **SDN, Entropy, DDoS, windows size. Threshold***