ABSTRACT

This research aims to investigate DDoS attacks in SDN using Shannon entropy and PPDIOO methodology and their consequences. This is intended to determine whether SDN (Software-Defined Network) is vulnerable to DDoS (Distributed Denial of Service) attacks and whether Shannon entropy is effective in identifying such attacks. This research has broader implications for the dynamics of security and performance in layered networks facing DDoS attacks, and several scenarios conducted on SDN networks show a correlation between DDoS and entropy values across various anomalous data paths. The PPDIOO framework ensures that the model follows a logical sequence of identifying objectives, planning and designing attack scenarios followed by implementing them ensuring consistency in data collection. The parameters can be further divided into four sections and will summarize the entire attack framework. This study sheds light on how DDoS attacks can easily compromise SDN infrastructure while at the same time highlighting how Shannon entropy can be accurately used to identify these types of attacks. This study provides practical suggestions for designing more robust security mechanisms to protect SDN against DDoS attacks in the future.

Keywords: SDN, DDoS, Shannon Entropy, POX Controller, PPDIOO.