Abstract

Ashraf F Tamam

Performance Analysis and Evaluation of Software Defined Networking Controllers against Denial of Service Attacks

The Software defined networking (SDN) utilization within networking architecture represents a way of looking at how networks are configured, controlled, and operated. Managed services such as routing, load balancing, and security can be automated and centralized dynamically in SDN controllers. Controllers act as the centralized repository of policy and control instructions for the network that packets are transmitted through it. Any transmitted packets flooded from an attacker that intends to access the controller will result to Denial of Service (DoS) attack. Thus, this paper is devoted to simulate and examine the impact of DoS attack on the bandwidth of two different linked hosts (Server/client) by SDN controllers as POX, RYU, and Opendaylight (ODL) controllers. The network performance is tested and emulated by using different testing tools of simulation in Mininet such as Hping3, iperf, jperf, wireshark and miniedit. Also, the performances of the controllers against DoS attack proposed by different protocols using user datagram protocol (UDP) and transmission control protocol (TCP) which will be assess via OpenFlow switch.