DDoS attack detection based on entropy in SDN environment.

Abstract:

Distributed Denial of Service (DDoS) attacks are a major threat to network availability and can cause significant damage to network infrastructures. In this project, we propose an entropy-based approach for detecting DDoS attacks in Software Defined Networks (SDN). The proposed approach leverages the programmability and centralization of SDN to calculate entropy on a per-IP basis, and identify abnormal traffic patterns that indicate an ongoing DDoS attack. The proposed technique utilizes the IP inthe network to calculate entropy.

This statistical approach is effective in detecting volume-based DDoS attacks such as UDP floods. The approach is implemented using Python and evaluated through emulation using Mininet. Our experiments demonstrate that the proposed approach effectively detects DDoS attacks. The proposed approach is implemented in a POX controller and uses the SDN control plane. The proposed approach has the potential to be used as an effective tool for network administrators to secure their SDN environments against DDoS attacks.