

ABSTRACT

Improving DDoS Detection using Entropy in SDN

By Dani Prasetiawan

Supervisor: Dr. Maman Abdurrohman, M.T.

Software Designed Network (SDN) is a new technology in the network concept, where divide the data plane (hardware) and the control plane (software), which served as the brain that manages the forwarding of a packet network. This concept can improve flexibility for administrator to design and operate the network.

Over the last decade, Distributed Denial of Service (DDoS) attacks became one of the main network security problems. Although the DDoS mechanism is widely understood, its detection is a very difficult task because of the similarities between legitimate and useless traffic that sent by compromised hosts to their victim. Many methodologies to detect DDoS attack are published today in traditional network, but for SDN are still rare available. The previous DDoS detecting method in SDN utilizes threshold between traffic size subtracted by mean comparing with three of the standard deviation. The shortage of this method is that it will detect sudden increase traffic as DDoS although it just a normal traffic, it will increase false positive.

The objectives of this thesis are utilizing the central control (OpenFlow controller) of SDN for DDoS attack detection and proposing a better solution by improving the previous method by adding second mechanism that will check whether the traffic is a normal traffic or DDoS attack by measure its randomness of packets. After detect as a DDoS attack by the previous method, the new method will check whether the entropy threshold is higher or less than the threshold. If it is higher than will be detected as a DDoS attack. In this research, we prove that the new method can reduce false positive as when there is a temporary sudden increase normal traffic will not detected as a DDoS attack.

Keywords: SDN, Software Defined Network, DDoS Detection, Network Security