UMass Dartmouth
COLLEGE OF ENGINEERING

Computer and
Information Science
Department

MASTER'S PROJECT (SPRING 2016)

TOPIC: ***Defending Against Denial-of-Service Attacks in Software Defined Networks***

PRESENTOR: Yashwanth Nandanam

ADVISOR: Dr. Haiping Xu

DATE & TIME: Thursday, March 31, 2016, 2:00 PM

LOCATION: Dion 303

COMMITTEE MEMBERS: Dr. Firas Khatib and Dr. Paul Gracia

ABSTRACT

Software-defined networking (SDN) offers a new centralized control plane paradigm that manages the network elements dynamically. SDN technology abstracts the control and data plane of network devices by enabling network devices to be programmable and allowing dynamic configuration changes on the control plane. As major benefits of using SDN, the SDN paradigm can significantly improve network efficiency and lower the cost to establish a network system. Despite the many advantages of using SDN, common network intrusions, such as Denial of Service (DoS) attack and Distributed DoS (DDoS) attack, are still major concerns in this new network paradigm. In this project, we demonstrate how to identify and mitigate two major DoS and DDoS attacks in SDN, namely TCP SYN attack and Botnet based attack. We simulated the major attacks utilizing the network virtualization technologies and open source SDN components, including POX, an open source development platform for Python-based SDN control applications. We developed control applications in Python running on top of SDN POX controller to mitigate the major attacks. The simulated environment contains major SDN components such as SDN POX controller and Open Virtual Switches (OVS) as well as network entities such as routers, servers, normal clients, and attackers. To detect network flows due to attacks, we set up a malicious flow threshold for each type of the attacks. The attack mitigation applications running on the controller detect malicious network flows that are above the threshold, and treat flows that are below the threshold as normal network requests. Our experimental results show that the attack mitigation applications can effectively detect and block major DoS and DDoS attacks in SDN; while at the same time, it allows regular network flows coming from the normal clients.