

Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing

Qiao Yan and F. Richard Yu

ABSTRACT

Although software-defined networking (SDN) brings numerous benefits by decoupling the control plane from the data plane, there is a contradictory relationship between SDN and distributed denial-of-service (DDoS) attacks. On one hand, the capabilities of SDN make it easy to detect and to react to DDoS attacks. On the other hand, the separation of the control plane from the data plane of SDN introduces new attacks. Consequently, SDN itself may be a target of DDoS attacks. In this paper, we first discuss the new trends and characteristics of DDoS attacks in cloud computing environments. We show that SDN brings us a new chance to defeat DDoS attacks in cloud computing environments, and we summarize good features of SDN in defeating DDoS attacks. Then we review the studies about launching DDoS attacks on SDN and the methods against DDoS attacks in SDN. In addition, we discuss a number of challenges that need to be addressed to mitigate DDoS attacks in SDN with cloud computing. This work can help understand how to make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments and how to prevent SDN itself from becoming a victim of DDoS attacks.

INTRODUCTION

Cloud computing has emerged as a hotspot in both academia and industry due to its essential characteristics, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Currently, security issues have been regarded as the dominant barrier in the development of cloud computing [1]. Security requirements of cloud computing include confidentiality, integrity, availability, accountability, and privacy-preservability. Among these security requirements, availability is crucial since the core function of cloud computing is to provide on-demand service of different levels. If a certain service is no longer available or the quality of service cannot meet the service level agreement (SLA), customers may lose faith in

the cloud system [1]. Denial of service (DoS) attacks and distributed denial of service (DDoS) attacks are the main methods to destroy the availability of cloud computing. In DoS or DDoS attacks, an attacker attempts to make a machine or network resource unavailable to its intended users [2]. DoS attacks are sent by one person or system, while DDoS attacks are sent by two or more persons or systems. An attacker may be a real person or a group of zombies that are controlled by an attacker. An attacker has the capability to send large volume packets to the target with spoofed source IP addresses.

Although some excellent work has been done to defeat DDoS attacks in traditional computing environments, DDoS attacks are becoming more prevalent in cloud computing environments. Moreover, we have started to see new forms of attack based on the new characteristics of cloud computing, such as the emergence of new economic denial of sustainability (EDoS) attacks [1].

Recently, software defined networking (SDN) has attracted much interest as a new paradigm in networking [3]. Although SDN brings numerous benefits by decoupling the control plane from the data plane, there is a *contradictory relationship* between SDN and DDoS attacks. On one hand, the capabilities of SDN (e.g. software-based traffic analysis, logical centralized control, global view of the network, and dynamic updating of forwarding rules) make it easy to detect and to react to DDoS attacks rapidly. On the other hand, the separation of the control plane from the data plane introduces new attacks. Consequently, SDN itself may be a target of DDoS attacks. Indeed, potential DDoS vulnerabilities exist across the SDN platform [4]. For example, an attacker can take advantage of the characteristics of SDN to launch DDoS attacks against the control layer, infrastructure layer, and application layer of SDN.

In this article we first discuss the new trends and characteristics of DDoS attacks in cloud computing environments. We show that SDN brings us a new chance to defeat DDoS attacks in cloud computing environments, and we summarize good features of SDN in defeating DDoS attacks. Then we review the studies about

Qiao Yan is with Shenzhen University.

F. Richard Yu is with Carleton University.