Computer Networks 81 (2015) 308–319

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

# DDoS attack protection in the era of cloud computing and Software-Defined Networking

Bing Wang *, Yao Zheng, Wenjing Lou, Y. Thomas Hou

*Virginia Polytechnic Institute and State University, Blacksburg, VA, USA*

ARTICLE INFO

*Article history:*
Received 16 September 2014
Received in revised form 27 January 2015
Accepted 26 February 2015
Available online 6 March 2015

*Keywords:*
DDoS mitigation
Software-Defined Networking
Graphical model

ABSTRACT

Cloud computing has become the real trend of enterprise IT service model that offers cost-effective and scalable processing. Meanwhile, Software-Defined Networking (SDN) is gaining popularity in enterprise networks for flexibility in network management service and reduced operational cost. There seems a trend for the two technologies to go hand-in-hand in providing an enterprise's IT services. However, the new challenges brought by the marriage of cloud computing and SDN, particularly the implications on enterprise network security, have not been well understood. This paper sets to address this important problem.

We start by examining the security impact, in particular, the impact on DDoS attack defense mechanisms, in an enterprise network where both technologies are adopted. We find that SDN technology can actually help enterprises to defend against DDoS attacks if the defense architecture is designed properly. To that end, we propose a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to enable attack detection and a flexible control structure to allow fast and specific attack reaction. To cope with the new architecture, we propose a graphic model based attack detection system that can deal with the dataset shift problem. The simulation results show that our architecture can effectively and efficiently address the security challenges brought by the new network paradigm and our attack detection system can effectively report various attacks using real-world network traffic.



## 1. Introduction

As cloud computing provides on-demand, elastic, and accessible computing services, more and more enterprises begin to embrace this paradigm shift by moving their database and applications into the cloud. At the same time, another epochal concept of the Internet architecture comes to forefront, i.e., Software-Defined Networking (SDN). While cloud computing facilitates the management of computation and storage resources, SDN is proposed to address another laborious issue hindering the evolvement of today's Internet, i.e., the complicated network management. Besides the fact that SDN has been proposed as a candidate of the next generation Internet architecture, companies like Google have already adopted SDN in their internal data centers. Thus, the arrival of the era when cloud computing and SDN go hand-in-hand in providing enterprise IT services is looming on the horizon.

Besides all the widely perceived benefits, the marriage between cloud computing and SDN may also introduce potential risks, especially on network security. Among all the network security problems, we first take a look at Denial-of-Service (DoS) attack. A DoS attack and its distributed version, Distributed Denial-of-Service (DDoS) attack, attempt to make a service unavailable to its intended users by draining the system or network

* Corresponding author.
*E-mail addresses:* bingwang@vt.edu (B. Wang), zhengyao@vt.edu (Y. Zheng), wjlou@vt.edu (W. Lou), thou@vt.edu (Y.T. Hou).

http://dx.doi.org/10.1016/j.comnet.2015.02.026
1389-1286/

resource. Although network security experts have been devoting great efforts for decades to address this issue, DDoS attacks continue to grow in frequency and have more impact recently. Existing DDoS attack defense solutions (to list a few [1–4]) assume a fully controlled network by the network administrators of enterprises. Therefore, the network administrators could place certain hardware pieces in the network to detect or mitigate DDoS attacks. However, in the new network paradigm of cloud computing and SDN, these assumptions no longer stand. Other researchers [5,6] focus on exploiting the benefits of cloud or SDN to defend DDoS attacks. But their target victims still reside in the traditional network environment, which makes their solutions unsuitable for the new network paradigm. To the best of our knowledge, little effort in research community has been made to look into the potential problems or opportunities to defend DDoS attacks in the new enterprise network environment that adopts both cloud computing and SDN.

In this paper, we first analyze the impact of the combination of cloud computing and SDN on DDoS attack defense. We discuss the potential issues under this new paradigm as well as opportunities of defending DDoS attacks. Based on our analysis, we claim that if designed properly, SDN can actually be exploited to address the security challenges brought by cloud computing and the DDoS attack defense can be made more effective and efficient in the era of cloud computing and SDN. We then propose a new DDoS attack mitigation architecture using software-defined networking (abbreviated as DaMask) to demonstrate and substantiate our findings. DaMask contains two modules: an anomaly-based attack detection module DaMask-D, and an attack mitigation module DaMask-M. We build our DaMask-D module based on a graphical probabilistic inference model. Compared with existing graphical model based detection schemes [7–9] which only have model training and testing phases, our DaMask-D features an additional model updating phase to address the *dataset shift* problem in the real world. The dataset shift refers to the fact that the network traffic conditions when we build the model differ from the actual traffic conditions when we use the model. This fact varies from the common assumption used in the existing works where the attack patterns learned from the training data are assumed to be no different from the attack patterns in the future. Our contributions can be summarized as follows:

1. To the best of our knowledge, we are among the first to bring the attention of the impact on DDoS attack defense of the new network paradigm, which is a combination of cloud computing and SDN. Based on our analysis, we find that the marriage of SDN and cloud computing provides a unique opportunity to enhance the DDoS attack defense in an enterprise network environment.
2. To substantiate our claim, we propose DaMask, a highly scalable and flexible DDoS attack mitigation architecture that exploits SDN technique to address the new security challenges brought by cloud computing, including the extended defense perimeter and the dynamic network topological changes.
3. Our DaMask-D module in the DaMask architecture features an additional model update phase, compared to existing graphical-model based network attack detection schemes, which successfully handles the dataset shift problem in the real world and achieves a higher detection rate.
4. At last, we implement our proposed structure and performed a simulation based evaluation using the Amazon EC2 cloud service. The results show that our scheme works well under the new network paradigm and incurs limited computation and communication overhead, which is a crucial requirement of DDoS protection in cloud computing and SDN.

Compared with our preliminary NPSec work [10] which presented the DaMask framework, the journal version completes the DDoS attack defense solution by including an attack detection system in Section 4. The attack detection system which is based on the graphical model detection is not only tailored to accommodate the unique requirement of DDoS attack defending in cloud computing, but also manages to address the data shift problem which decreases the detection performance in most machine learning based solutions. We also add performance evaluation results of the detection module in Section 5.3 including the performance of detecting attacks and the ability of adapting the data shift issue. We organize the remainder of the paper as follows. We analyze the impact of cloud computing and SDN on DDoS attack defense in Section 2. Based on our analysis, we formulate the problem and present our DaMask architecture design in Section 3. The technical details of the DaMask-D module is discussed in Section 4. Section 5 presents the simulation setting and the results. Related work are reviewed and compared with our work in Section 6. We draw concluding remarks in Section 7.

## 2. Analysis

In this section, we briefly review cloud computing and SDN. Then we analyze the impact of the combined technologies on the network protection against DDoS attacks.

### 2.1. Cloud computing

Cloud computing is a computing model which manages a pool of configurable computing resources. Cloud computing can be categorized as *public cloud, private cloud* and *hybrid cloud* in terms of deployment. While public cloud and private cloud are used by public and a single organization, respectively, hybrid cloud is a composition of public and private cloud infrastructures. As a result, hybrid cloud share the properties of both public cloud and private cloud. Hybrid cloud allows companies keeping their critical applications and data in private while outsourcing others to public. Thus, we focus on analyzing the impact of hybrid cloud on DDoS attack defense.