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 attached 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.

0163-6804/15/$25.00 © 2015 IEEE

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 attached in SDN with cloud computing.

To the best of our knowledge, the contradictory relationship between SDN and DDoS attacks has not been well addressed in previous work. Essentially, it is the unique dynamics associated with SDN and DDoS attacks that present unique challenges beyond the existing works. We believe that the initial steps we have taken here 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.

The rest of the article is organized as follows. We present the new trends of DDoS in cloud computing environments. Some good features of SDN in defeating DDoS attacks are discussed. We review the work about launching DDoS attacks on SDN. Some open research issues are presented. Finally, we conclude this study.

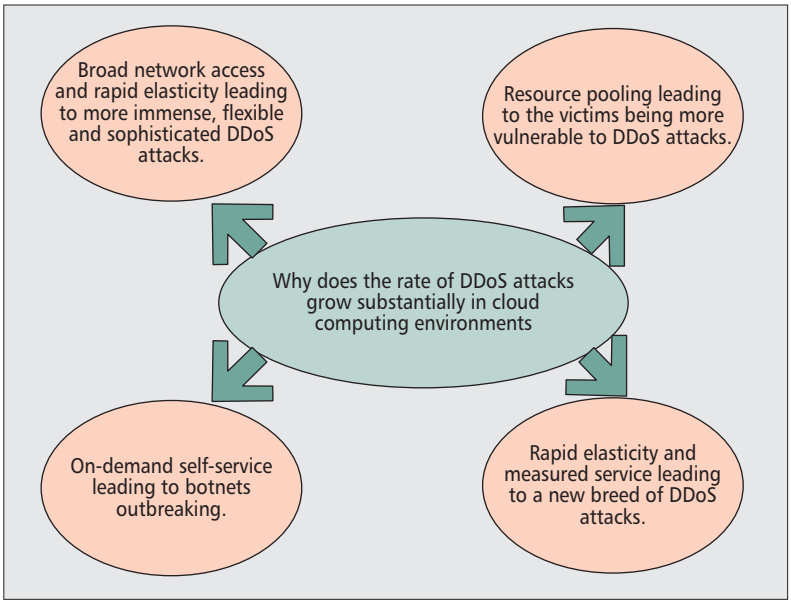


Figure 1. The reasons that the rate Of DDoS attacks in cloud computing environments grows substantially.

DDoS Attacks in Cloud Computing Environments are Growing

In this section we explain the reasons why the rate of DDoS attacks in cloud computing environments has grown substantially based on the essential characteristics of cloud computing, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service, as shown in Fig. 1.

On-Demand Self-Service Leading to Botnets Outbreak

One major reason why the rate of DDoS attacks in cloud computing has grown substantially is the emergence and development of botnets. Botnets are networks that are formed by bots or machines compromised by malware. Large-scale botnets (e.g. Srizbi, Kraken/Bobax, and Rustock) have gained notoriety for performing DDoS attacks.

It remains fairly complex to infect a sufficient number of machines in a short time frame in traditional networks. But the on-demand self-service capabilities of the cloud could be used by hackers to instantly create a powerful botnet. With cloud computing, malware-as-a-service is being used for launching DDoS attacks. Because of competition among suppliers, the price of malware-as-a-service has been falling rapidly. Cheap prices make it easier to use botnets to launch large-scale DDoS attacks in cloud computing environments than in traditional networks.

Broad Network Access and Rapid Elasticity Leading to More Immense, Flexible, and Sophisticated DDoS Attacks

With cloud computing's capabilities of broad network access and rapid elasticity, attackers can not only launch immense DDoS attacks, but also produce more flexible and more sophisticated DDoS attacks by using heterogeneous thin or thick client platforms, which are discussed in the following.

More Immense DDoS Attacks in Cloud Computing: The size and frequency of DDoS attacks have grown dramatically as attackers take advantage of botnets and other high-speed Internet access technologies to overwhelm their victim's network infrastructure. In March 2013, Spamhaus, an organization that maintained lists of spammers, came under a massive DNS reflection DDoS attack. The greatest attack traffic was reportedly as high as 300Gbps.

More Flexible DDoS Attacks in Cloud Computing: Because of cloud computing's capabilities of broad network access, mobile devices such as smartphones and tablets are expected to become a significant launching platform for DDoS attacks. The rising bandwidth and processing power and the lack of security of mobile devices make them an ideal platform for hackers to compromise for DDoS attack campaigns.

More Sophisticated DDoS Attacks in Cloud Computing: DDoS attacks are becoming larger and more frequent, and they are becoming more sophisticated as they pinpoint specific applications (e.g. DNS, HTTP or VoIP) or a weak point in the victim's system design. Although sophisticated DDoS attacks require more understanding of the attacked system, they usually use less traffic and are harder to detect.

Resource Pooling Leading to the Victims More Vulnerable to DDoS Attacks

In cloud computing, virtualization technology and multi-tenant infrastructure on one hand make attackers launch DDoS attacks more easily, and on the other hand cause the victims to be more vulnerable to DDoS attacks.

• Virtualization technology makes attackers launch DDoS attacks more easily: Virtualization technology can be used by attackers to preset for DDoS attacks before launching attacks. Virtual

With rapid elasticity and measured service, adopters of the cloud service model are charged based on a pay-per-use basis of the cloud's server and network resources. With this model, a conventional DDoS attack on server and network resources is transformed in a cloud environment to a new breed of attack.

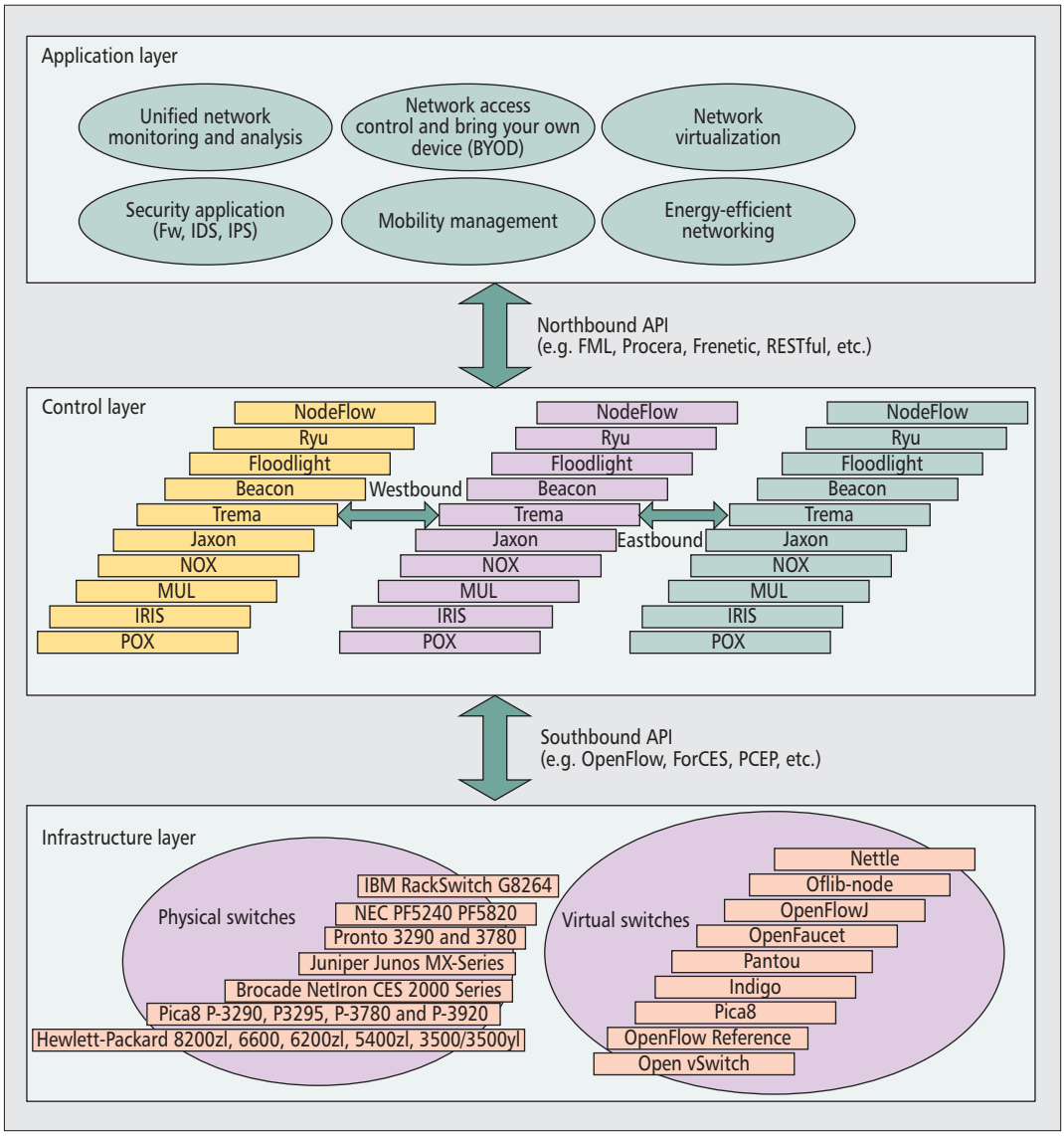


Figure 2. High-level overview of the SDN architecture.

machines can be built using little memory or disk space to launch more attacks with less costs.

• Virtualization technology and multi-tenant infrastructure cause the victims to be more vulnerable to DDoS attacks: Researchers have shown that on a DoS attack, the performance of a web server hosted in a virtual machines can degrade by up to 23 percent, while that of a non-virtualized server hosted on the same hardware degrades by only eight percent [5]. Since the cloud computing environment is inherently a multi-tenant infrastructure, an attack against a single customer is actually an attack against all customers in that given cloud.

Rapid Elasticity and Measured Service Leading to a New Breed of DDoS Attacks

With rapid elasticity and measured service, adopters of the cloud service model are charged on a pay-per-use basis of the cloud's server and network resources. With this model, a conventional DDoS attack on server and network resources is transformed in a cloud environment into a new breed of attack that targets the cloud adopter's economic resources, e.g. economic denial of sustainability (EDoS) attacks [1].

The goal of an EDoS attack is to deprive the victims (i.e. regular cloud customers) of their long-term economic viability. An EDoS attack succeeds when it causes financial burden on the victim. For example, attackers who act as legal cloud service clients continuously send requests to a website hosting in cloud servers to consume bandwidth, which bills to the cloud customer owning the website. It seems to the web server that this traffic does not reach the level of service denial, and it is difficult to distinguish EDoS attack traffic from other legitimate traffic [1].

Is SDN a Silver Bullet for Defeating DDoS Attacks?

Enterprises have enthusiastically embraced cloud computing, which offers an effective way to reduce capital expenditure (CapEx) and operational expenditure (OpEx) [1]. However, security

and privacy issues become a critical concern. As mentioned before, DDoS attacks are becoming the biggest threat to the availability of cloud computing. Traditional DDoS attacks mitigating mechanisms are meeting with various difficulties. SDN, as a new paradigm for enabling innovation in networking research and development, provides us with a new way of thinking to solve the problem. In this section we first introduce SDN and OpenFlow. Then we discuss the good features of SDN in defeating DDoS attacks.

What is Software-Defined Networking

SDN is currently attracting significant attention from both academia and industry. The Open Networking Foundation (ONF) is a nonprofit consortium dedicated to the development, standardization, and commercialization of SDN. ONF has provided the most explicit and well received definition of SDN as follows: "In the SDN architecture, the control and data planes are decoupled, network intelligence and state are logically centralized, and the underlying network infrastructure is abstracted from the applications" [6].

ONF presents a high-level architecture for SDN that is vertically split into three main functional layers: the infrastructure layer, the control layer, and the data layer (see Fig. 2).

- Infrastructure layer: Also known as the data plane, it consists mainly of forwarding elements (FEs), including physical switches and virtual switches. These switches are accessible via an open interface to switch and forward packets.
- Control layer: Also known as the control plane, it consists of a set of software-based SDN controllers providing a consolidated control functionality through open APIs to supervise the network forwarding behavior through an open interface.
- Application layer: It mainly consists of the end-user business applications. Examples of such business applications include network virtualization, mobility management, security applications, and so on.

SDN is often linked to the OpenFlow protocol. OpenFlow is an open protocol, which is proposed to standardize the communication between the switches and the controller in an SDN architecture.

SDN is closely related network function virtualization (NFV). Although both SDN and NFV aim at increasing the agility and flexibility of networks and decreasing complexity and cost, they use different methods. In SDN, control planes are separated from data planes, while in NFV, network devices are replaced by software. SDN and NFV are not dependent on one another, but one can be benefit from the other.

Good Features of SDN in Defeating DDoS Attacks

SDN has many good features, and these good features offer many benefits for defeating DDoS attacks, as shown in Fig. 3.

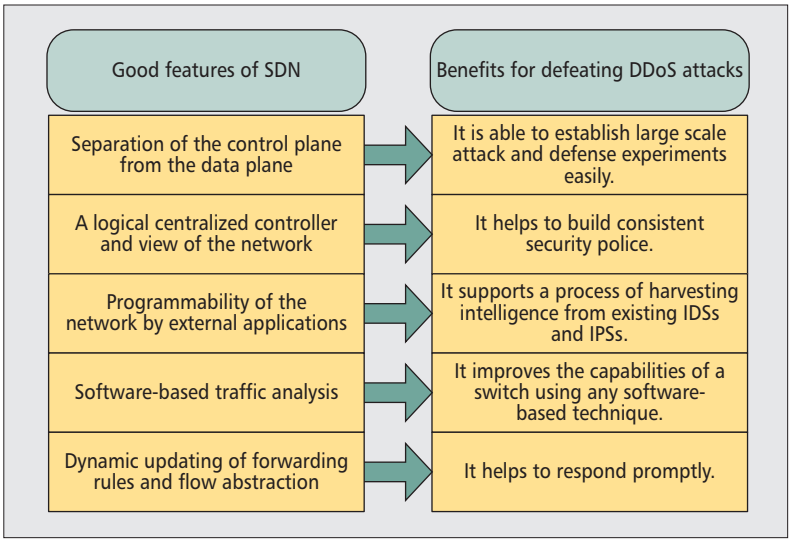


Figure 3. Good features of SDN in defeating DDoS attacks.

• Separation of the control plane from the data plane: DDoS attacks are not a new problem. Since Yahoo, Amazon, and other well-known web sites were subjected to DDoS attacks in 2000, researchers have presented many methods to mitigate DDoS attacks. But in traditional networks, researchers cannot experiment with their ideas on a large scale in a real network setting, hence the performance of the presented algorithms cannot be well tested and verified. SDN decouples the data plane from the control plane, and thus makes it possible to easily establish large scale attack and defense experiments. The high configurability of SDN offers clear separation among virtual networks, permitting experimentation in a real environment [3]. Progressive deployment of new ideas can be performed through a seamless transition from an experimental phase to an operational phase [3]. This feature of SDN offers great convenience in putting forward new thoughts and methods for DDoS attack mitigation.

• A centralized controller and view of the network: The controller has network-wide knowledge of the system and global views to build consistent security policies and to monitor or analyze traffic patterns for potential security threats. Centralized control of SDN makes it possible to dynamically quarantine compromised hosts and authenticate legitimate hosts based on the information obtained through requesting end hosts and remote authentication dial in user service (RADIUS) servers for users' authentication information and system scanning during registration [3]. In a multi-tenant model such as cloud computing, distinguishing tenants' activities and provisioned resources plays an important role in anomaly detection. TaheriMonfared *et al.* [7] proposed a method to build the per-tenant view by use of an OpenFlow controller. The controller provides a unified view of the network, and is aware of the tenant logic. The monitoring node communicates with the controller to build a per-tenant view of the network and generates monitoring information for each tenant.

• Programmability of the network by external applications: The programmability of SDN supports a process of harvesting intelligence from existing intrusion detection systems (IDSs) and

SDN holds great promise in terms of mitigating DDoS attacks in cloud computing environments. However, the security of SDN itself remains to be addressed. Many security issues may happen in SDN, such as unauthorized access, data leakage, malicious applications, configuration issues.

intrusion prevention systems (IPSs) [4]. More intelligent algorithms can be flexibly used based on different DDoS attacks. Within the infrastructure-as-a-service (IaaS) clouds, to prevent vulnerable virtual machines from being compromised in the cloud, Chun-Jen Chung *et al.* [8] proposed a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE. The proposed framework leverages OpenFlow network programming APIs to build a monitor and control plane over distributed programmable virtual switches in order to significantly improve attack detection and mitigate attack consequences.

- Software-based traffic analysis: Software-based traffic analysis greatly enables innovation, as it can be performed using all kinds of intelligent algorithms, databases, and any other software tools. Motivated by the flexibility of the SDN architecture and the observation that most mobile malware requires Internet connections, Jin and Wang designed a system that detects mobile malware through real-time traffic analysis using the SDN architecture [9].
- Dynamic updating of forwarding rules and flow abstraction: Dynamic updating of forwarding rules assist in the prompt response to DDoS attacks. Based on the traffic analysis, new or updated security policy can be propagated across the network in the form of flow rules to block the attack traffic without delay. Yu *et al.* [10] proposed a memory-efficient system for distributed and collaborative per-flow monitoring, called DCM. DCM uses Bloom filters to represent monitoring rules using a small size of memory. It utilizes SDN's ability to dynamically update forwarding rules to install a customized and dynamic monitoring tool into the switch data plane [10].

Are DDoS Attacks a Nightmare for SDN?

SDN holds great promise in terms of mitigating DDoS attacks in cloud computing environments. However, the security of SDN itself remains to be addressed. Many security issues may happen in SDN, such as unauthorized access, data leakage, malicious applications, configuration issues, etc. [4]. This article focuses on DDoS attacks. In this section, we first discuss how SDN itself may be a target of DDoS attacks. Then we provide an overview of available solutions to this problem.

Possible DDoS Attacks on SDN

SDN itself may be a target of DDoS attacks. Since SDN is vertically split into three main functional layers — infrastructure layer, control layer, and application layer — potential malicious DDoS attacks can be launched on these three layers of SDN's architecture. Based on the possible targets, we can classify the DDoS attacks on SDN into three categories: application layer DDoS attacks, control layer DDoS attacks, and infrastructure layer DDoS attacks, as shown in Fig. 4.

Application Layer DDoS Attacks: There are two methods to launch application layer DDoS attacks: attack applications, or attack the northbound API. Since isolation of applications or resources in SDN is not well solved, DDoS attacks on one application can affect other applications.

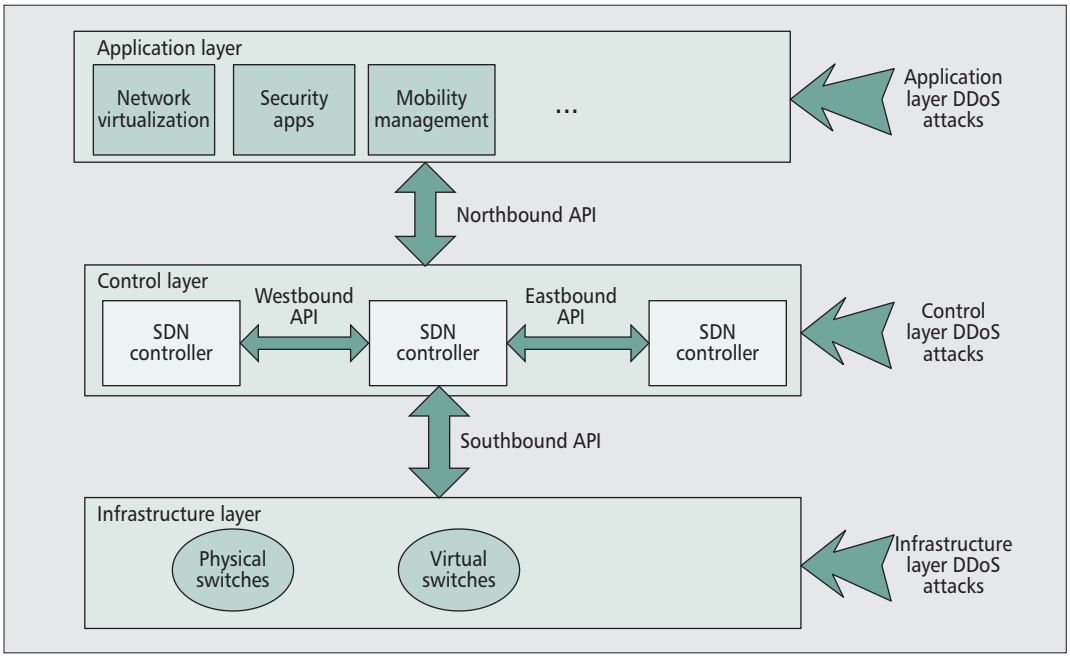
Control Layer DDoS Attacks: The controllers could potentially be seen as a risk of single point of failure for the network, so they are a particularly attractive target for DDoS attacks in the SDN architecture. The following methods can launch control layer DDoS attacks: attacking the controller, the northbound API, the southbound API, the westbound API, or the eastbound API. For example, many conflicting flow rules from different applications may cause DDoS attacks on the control plane. Within the operation of SDN, the data plane will typically ask the control plane to obtain flow rules when the data plane sees new network packets that it does not know how to handle [6]. There are two options for the handling of a new flow when no flow match exists in the flow table: either the complete packet or a portion of the packet header is transmitted to the controller to resolve the query. With a large volume of network traffic, sending the complete packet to the controller would occupy high bandwidth.

Infrastructure Layer DDoS Attacks: There are two methods to launch infrastructure layer DDoS attacks: attack switches or attack the southbound API. For example, if only header information is transmitted to the controller, the packet itself must be stored in node memory until the flow table entry is returned. In this case, it would be easy for an attacker to execute a DoS attack on the node by setting up a number of new and unknown flows. As the memory element of the node can be a bottleneck due to high cost, an attacker could potentially overload the switch memory (e.g. targeting to exhaust TCAMs). The generated fake flow requests can produce many useless flow rules that need to be held by the data plane, thus making it difficult for the data plane to store flow rules for normal network flows [6].

To demonstrate the feasibility of DDoS attacks, a new SDN network scanning prototype tool (named SDN scanner) is proposed in [11] to remotely fingerprint networks that deploy SDN. This method can be easily operated by modifying existing network scanning tools (e.g. ICMP scanning and TCP SYN scanning). The attack can be conducted to an SDN network by a remote attacker, and it can significantly degrade the performance of an SDN network without requiring high performance or high capacity devices.

Porras *et al.* [12] show that OpenFlow applications may contradict or override one another, incorporate vulnerabilities, or possibly be written by adversaries. In the worst case, an adversary can use the deterministic OpenFlow application to control the state of all OpenFlow switches in the network [12]. A rule conflict is said to arise when the candidate OpenFlow rule enables or disables a network flow that is otherwise inversely prohibited (or allowed) by existing rules [12]. Hackers may use rule conflict to launch DDoS attacks.

Because DDoS attacks use forged source IP addresses or faked traffic, simple authentication mechanisms could mitigate forged or faked traffic flows. But if an attacker assumes the control



SDN itself may be a target of DDoS attacks. Since SDN is vertically split into three main functional layers, including infrastructure layer, control layer and application layer, potential malicious DDoS attacks can be launched on these three layers of SDN's architecture.

Figure 4. Potential DDoS attacks can be launched on these three layers of SDN's architecture.

of an application server that stores the details of many users, it can easily use the same authenticated ports and source MAC addresses to inject authorized, but forged, flows into the network [13].

Although OpenFlow provides optional support for encrypted transport layer security (TLS) communication and a certificate exchange between the switches and the controller(s), using TLS/SSL does not per se guarantee secure communications. The security of those communications is as strong as its weakest link, which could be a self-signed certificate, a compromised certificate authority, or vulnerable applications and libraries [13]. Moreover, the TLS/SSL model is not enough to establish and assure trust between controllers and switches. After an attacker gains access to the control plane, it may be capable of aggregating enough power force (in terms of the number of switches under its control) to launch DDoS attacks.

Available Solutions

We summarize possible DDoS attacks on SDN and available solutions in Table 1.

FortNox is a new security policy enforcement kernel as an extension to the open source NOX OpenFlow controller, which mediates all OpenFlow rule insertion requests [12]. FortNOX implements role-based authentication to determine the security authorization of each OpenFlow application (rule producer), and enforces the principle of least privilege to ensure the integrity of the mediation process.

For security, OpenFlow provides optional support for encrypted transport layer security (TLS) communication and a certificate exchange between the switches and the controller(s) [14], and the use of oligarchic trust models with multiple trust-anchor certification authorities (e.g. one per sub-domain or per controller instance) is a possibility [13]. Moreover, securing communications with threshold cryptography across controller replicas (where the switch will need at least n shares to get a valid controller message) may be helpful. Additionally, the use of dynamic, automated, and assured device association mechanisms may be considered, in order to guarantee trust between the control plane and data plane devices [13].

The use of IDSs with support for runtime root-cause analysis could help identify abnormal flows [13]. This could be coupled with mechanisms for dynamic control of switch behavior (e.g. rate bounds for control plane requests).

AVANT-GUARD is a new framework to advance the security and resilience of OpenFlow networks with greater involvement from the data plane [15]. It addresses two security challenges for SDN-enabled networks. The first goal is to secure the interface between the control plane and the data plane, and shield it from saturation attacks by a connection migration technique on the data plane. The second goal is to improve responsiveness so that security applications can efficiently access network statistics to respond to threats by creating actuating triggers when a predefined trigger condition is detected.

Open Problems

There are many open research problems that are still not well investigated and need to be addressed by future research efforts. In this section we discuss some of the most important open research issues to mitigate DDoS attacks in cloud computing environments by use of SDN.

How to Defeat Application Layer DDoS Attacks Using SDN

According to new research by Gartner, there will be noticeable growth in the incidence of application layer DDoS attacks. Access to payload information is crucial for application DDoS

Possible DDoS attacks	Attack implementation methods	Available solutions
Application layer DDoS attacks	By attacking application	FortNOX [12]
	By attacking northbound API	
Control layer DDoS attacks	By attacking controller	Transport Layer Security (TLS) [14] FortNOX [12] AVANT-GUARD [15]
	By attacking northbound API	
	By attacking southbound API	
	By attacking westbound API	
	By attacking eastbound API	
Infrastructure layer DDoS attacks	By attacking switch	Transport Layer Security (TLS) [14] AVANT-GUARD [15]
	By attacking southbound API	

Table 1. Possible DDoS attacks on SDN and available solutions.

attack mitigation. Moreover, this information needs to be obtained at considerably reduced latencies and with reasonable cost.

Current SDN architectures only provide the visibility and control on L2-L4. Thus, defeating application layer DDoS attacks may not benefit from the current OpenFlow implementation. Major efforts need to be spent in this area in order to to extend traffic intelligence to Layer 4 to Layer 7 with good trade-offs between performance and security.

How to Defeat Mobile DDoS Attacks Using SDN

With the number of smart devices increasing, popular apps will be installed and millions of their instances can be running at the same time. Both the mobile devices and the apps can be used to initiate DDoS attacks. Based on the current trend of usage of mobile devices and cloud computing, we believe the battlefield of DDoS attacks and defense will shift from the traditional network to the mobile cloud computing environment. Because mobile networks use super proxies, the simple filter method based source IP addresses may not be used since it will also block legitimate traffic. Although some efforts have been made to extend SDN capability to mobile devices for many network problems (e.g. QoS, virtualization, and fault diagnosis), more research needs be done to defeat mobile DDoS attacks using SDN.

How to Implement Multiple Locations Defensive Methods

Many multiple locations defensive methods have been presented in traditional networks. Multiple locations defense is comprised of multiple defense nodes deployed at various locations such as the source, the destination, or the networks [2]. For instance, detection can be done at the victim side and the response can be initiated and distributed to other nodes by the victim. So we believe with widely deployment of SDN in carrier networks, there are many research opportunities to implement multiple locations defensive methods using SDN to defeat DDoS attacks.

How to Cooperate Among the Key Defensive Points

Since attackers cooperate to perform successful attacks, defenders must also form alliances and collaborate with each other to defeat DDoS attacks [2]. A cooperation defense mechanism is the best way to combat DDoS attacks, and many methods have been proposed in traditional networks. Cooperation among the key defensive points can be greatly beneficial to attack prevention, detection, and response. The feature of global view and dynamic updating of forwarding rules of SDN will greatly reduce the cost of cooperation. However, this topic has not been well researched in SDN.

How to Build a DDoS Attacks Tolerant System Using SDN

Since it is very difficult to accurately detect DDoS attacks and prevent them in a timely manner, a DDoS attacks tolerant system may be more realistic. A DDoS attacks tolerant system is a system designed with a fault-tolerant design approach, and it can operate correctly despite attacks. For instance, the system may provide service that meets the requirements of a service-level agreement (SLA) even under an attack by triggering automatic mechanisms to regain and recover the compromised services and resources. A DDoS attacks tolerant system often has some essential properties such as redundancy, diversity, and independence. These properties are easier to implement in SDN networks than in traditional networks. Although some efforts on building a DDoS attacks tolerant system have been made, how to use SDN characteristics to realize attack tolerant systems is a new direction that needs to be addressed by future research efforts.

Conclusions

In this article we first discussed the reasons why DDoS attacks are becoming more prevalent in cloud computing environments. Since SDN could be a good tool to defeat DDoS attacks in cloud computing environments, we presented some good features of SDN in defeating DDoS attacks. After that we discussed how SDN may be a victim of DDoS attacks. We reviewed the studies about how to launch DDoS attacks on SDN and how to deal with this problem. We also discussed some significant open problems.

In summary, SDN creates a very fascinating dilemma: a promising tool to defeat DDoS attacks, versus a vulnerable target of DDoS attacks. 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 are an urgent problem that needs to be addressed. This article attempted to briefly explore the current technologies related to SDN and DDoS attacks,

and we discussed future research that may be beneficial in these issues.

References

[1] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 2, 2013, pp. 843–59.

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 4, 2013, pp. 2046–69.

[3] W. Xia *et al.*, "A Survey on Software-Defined Networking," *IEEE Commun. Surveys & Tutorials*, 2014, to be published.

[4] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN Security: A Survey," *Proc. IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, pp. 1–7.

[5] R. Shea and J. Liu, "Performance of Virtual Machines under Networked Denial of Service Attacks: Experiments and Analysis," *IEEE Systems J.*, vol. 7, no. 2, 2013, pp. 335–45.

[6] S. Sezer *et al.*, "Are We Ready for SDN? Implementation Challenges for Software-Defined Networks," *IEEE Commun. Mag.*, vol. 51, no. 7, 2013.

[7] A. TaheriMonfared and C. Rong, "Multi-Tenant Network Monitoring Based on Software Defined Networking," *Proc. OTM Conf. Move to Meaningful Internet Systems*, 2013.

[8] C.-J. Chung *et al.*, "Nice: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems," *IEEE Trans. Dependable and Secure Computing*, vol. 10, no. 4, July 2013, pp. 198–211.

[9] R. Jin and B. Wang, "Malware Detection for Mobile Devices Using Software-Defined Networking," *Proc. IEEE 2nd GENI on Research and Educational Experiment Wksp. (GREE)*, 2013, pp. 81–88.

[10] Y. Yu, Q. Chen, and X. Li, "Distributed Collaborative Monitoring in Software Defined Networks," arXiv preprint arXiv:1403.8008, 2014.17

[11] S. Shin and G. Gu, "Attacking Software-Defined Networks: A First Feasibility Study," *Proc. 2nd ACM SIGCOMM Wksp. Hot Topics Software Defined Networking*, 2013, pp. 165–66.

[12] P. Porras *et al.*, "A Security Enforcement Kernel for OpenFlow Networks," *Proc. 1st Wksp. Hot Topics in Software Defined Networks*, 2012, pp. 121–126.

[13] D. Kreutz, F. Ramos, and P. Verissimo, "Towards Secure and Dependable Software-Defined Networks," *Proc. 2nd ACM SIGCOMM Wksp. Hot Topics in Software Defined Networking*, 2013, pp. 55–60.

[14] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3, Third Quarter 2014, pp. 1617–34.

[15] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AvantGuard: Scalable and Vigilant Switch Flow Management in Software-Defined Networks," *Proc. ACM SIGSAC Conf. Computer & Commun. Security*, 2013, pp. 413–24.

Biographies

QIAO YAN (yanq@szu.edu.cn) is a professor at the College of Computer Science and Software Engineering at Shenzhen University, Shenzhen, China. She received her Ph.D. degree in information and communication engineering from Xidian University, Xi'an, China, in 2003. From 2013 to 2014 she worked at Carleton University, Ottawa, Canada, as a visiting scholar. Her research interests are in network security, cloud computing, and software-defined networking. Her current focus is research and development of security of software defined networking.

F. RICHARD YU (richard.yu@carleton.ca) is an associate professor at Carleton University, Canada. He received the IEEE Outstanding Leadership Award in 2013, Carleton Research Achievement Award in 2012, the Ontario Early Researcher Award (formerly Premier's Research Excellence Award) in 2011, the Excellent Contribution Award at IEEE/IFIP TrustCom 2010, the Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and the Best Paper Awards at IEEE ICC 2014, Globecom 2012, IEEE/IFIP TrustCom 2009, and the Int'l Conference on Networking 2005. His research interests include cross-layer design, security, green IT, and QoS provisioning in wireless networks. He serves on the editorial boards of several journals, including *IEEE Transactions on Vehicular Technology* and *IEEE Communications Surveys and Tutorials*. He has served on the Technical Program Committee (TPC) of numerous conferences, such as the TPC co-chair of IEEE INFOCOM-MCV'15, Globecom'14, WiVEC'14, INFOCOM-MCC'14, Globecom'13, GreenCom'13, CCNC'13, INFOCOM-CCSES'12, ICC-GCN'12, VTC'12S, Globecom'11, INFOCOM-GCN'11, INFOCOM-CWCN'10, IEEE IWCMC'09, VTC'08F, and WiN-ITS'07, and as the publication chair of ICST QShine'10, and the co-chair of ICUMT-CWCN'09.

SDN brings a very fascinating dilemma: a promising tool to defeat DDoS attacks, versus a vulnerable target of DDoS attacks. How to make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments and how to prevent SDN itself becoming a victim of DDoS attacks are an urgent problem that needs to be addressed.