DoS Attack Impact Assessment on Software Defined Networks

Abimbola Sangodoyin[1(✉)], Tshiamo Sigwele[1], Prashant Pillai[2], Yim Fun Hu[1], Irfan Awan[1], and Jules Disso[3]

[1] Faculty of Engineering and Informatics, University of Bradford, Bradford, West Yorkshire BD7 1DP, UK
{a.o.sangodoyin,T.Sigwele,Y.F.Hu,i.awan}@bradford.ac.uk
[2] Faculty of Technology, Design and Environment, Oxford Brookes University, Oxford, UK
ppillai@brookes.ac.uk
[3] Nettitude Limited, Warwickshire CV31 3RZ, UK
jpagnadisso@nettitude.com

Abstract. Software Defined Networking (SDN) is an evolving network paradigm which promises greater interoperability, more innovation, flexible and effective solutions. Although SDN on the surface provides a simple framework for network programmability and monitoring, few has been said about security measures to make it resilient to hitherto security flaws in traditional network and the new threats the architecture is ushering in. One of the security weaknesses the architecture is ushering in due to separation of control and data plane is Denial of Service (DoS) attack. The main goal of this attack is to make network resources unavailable to legitimate users or introduce large delays. In this paper, the effect of DoS attack on SDN is presented using Mininet, OpenDaylight (ODL) controller and network performance testing tools such as iperf and ping. Internet Control Message Protocol (ICMP) flood attack is performed on a Transmission Control Protocol (TCP) server and a User Datagram Protocol (UDP) server which are both connected to OpenFlow switches. The simulation results reveal a drop in network throughput from 233 Mbps to 87.4 Mbps and the introduction of large jitter between 0.003 ms and 0.789 ms during DoS attack.

Keywords: Software Defined Networks · DoS · Network security

1 Introduction

Computer networks have become part of our everyday lives from government to commercial enterprises to individuals [1]. These networks are built from large number of devices such as routers, switches and middle boxes with complex protocols running on them. Network administrators are saddled with the responsibility of configuring these vendor-specific devices and configuration policies are

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
P. Pillai et al. (Eds.): WiSATS 2017, LNICST 231, pp. 11–22, 2018.
https://doi.org/10.1007/978-3-319-76571-6_2

implemented on them. As a result, network management and dynamic response to events and applications are arduous and prone to error.

In addition to the complexity of configuration, operators have little options or mechanisms to respond to difficulties and enforce the required policies in dynamic environments [2]. Similarly, in the face of growing traffic and demand for more data rate from consumers, the service providers need to keep up with the pace through investments in bigger and faster links and edge routers, even though revenues are growing quite slowly [3].

In view of the afore mentioned challenges, the need for a cost effective and programmable network which is robust enough to meet the demand of users is imperative. Thus, the emergence of Software Defined Networks (SDN). SDN has created commendable avenues to overcome age-old problems in networking, while simultaneously enabling the introduction of complex, secure and reliable network policies for next generation networks [4]. As a revolutionary concept, SDN alters existing networks by separating the forwarding functionalities of existing devices, known as data plane from control element, known as control plane [5].

The future of SDN mainly lies in its acceptance and deployment. Technology and its deployment take years before it can be available to end users due to standardisation process and Request for Comments (RFCs). Speculations however remain as to whether same should be expected for SDN or not. According to [1] a proposal for open and programmable network is presented. The need for researchers to run experiment on campus network using an OpenFlow switch is further emphasised in [1]. In line with this, ETHANE, a new network architecture for enterprise was suggested in [6]. For the proposed architecture, in [6], ETHANE switch does not need to learn addresses, support Virtual Local Area Networks (VLANs) or check for source-address spoofing and it has been deployed in a campus environment. The work in [6] was augmented when Google, deployed B4 using OpenFlow switches in their Wide Area Networks (WAN) data centre [7]. Also, with the advent of a Linux foundation collaborative project, OpenDaylight (ODL) [8] platform and VMware NSX virtualisation platform, global acceptance and deployment is envisaged to be no longer far from reach.

In spite of the programmability, flexibility, universal connectivity and decentralised control, which were critical to the success of SDN, these features are at odds with making it more secure. The SDN platform can bring with it several security breaches which include an increased potential for Denial-of-Service (DoS) attacks due to controller centralisation and flow table limitations in network devices [9]. Furthermore, abstraction of flows and underlying hardware resources make it easier for harvesting of intelligence which can be used effortlessly for further exploitation and reprogramming entire network by malicious user [4].

In this paper, the impact of DoS attack on SDN is presented. The simulation has been perfomed using mininet and OpenDaylight controller tools and the simulation result shows that DoS flooding attack on SDN network can degrade network performance by decreasing network throughput and introduce large jitter. This paper is structured as follows: Sect. 2 presents related works on the SDN architecture, vulnerabilities in the SDN architecture and DoS attacks on SDN.

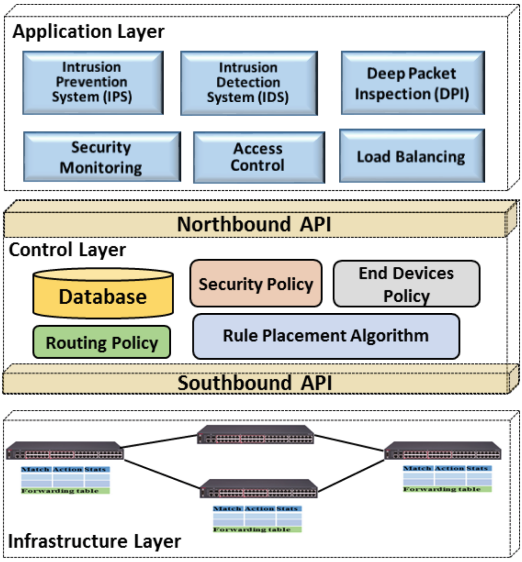

Fig. 1. SDN architecture illustrating the data, control and application layers.

The experimental method and tools are presented in Sect. 3. Then Sect. 4 shows the experimental set-up. The results and analysis are presented in Sect. 5. Finally, the conclusion and future work are presented in Sect. 6.

2 Related Work

2.1 SDN Architecture

SDN architecture encompasses the complete network platform. It is a modular approach that defines chain of command and interoperability within network. Unlike traditional network, the intelligence of data plane devices is removed to a logically centralised control system [10]. Figure 1 presents the SDN architecture showing the data/infrastructure, control and application layer. In an SDN architecture, there are two main elements: the controllers and the forwarding devices. A forwarding device is a hardware or software element specialised in packet forwarding and based on a pipeline of flow tables where each entry of a flow table has: a matching rule, action to be executed on matching packets and counters that keep statistics of matching packets [4]. The controller serves as the brain of the network and it deals with management of network state. Below is a description of various layers:

Infrastructure layer: This layer is also known as data plane. It consists of simple forwarding elements without embedded control or software to take autonomous decisions. It is accessible through the southbound interface and allows packet switching and forwarding.

Control layer: This layer consists of SDN controllers providing a consolidated control functionalities through Application Programming Interfaces (APIs). The crucial value of the controller is to provide abstractions, essential services, and common APIs to developers. Three communication interfaces allows the controller to interact: northbound, southbound and the east/westbound interfaces.

(i) Southbound Interfaces: Southbound interface allows the controller and forwarding elements to interact in the infrastructure layer, thus being the crucial instrument for clearly separating the control and data plane functionality.
(ii) Northbound Interfaces: This interface is the connecting bridge between application layer and control layer. It enables the programmability of the controllers by exposing the data models and other functionalities within the controllers for use by applications at the application layer. The northbound interface is mostly a software ecosystem, hence, a common northbound interface is still an open issue.
(iii) East/Westbound Interfaces: This interface is a special communication interface envisioned for distributed controllers to synchronise state for high availability. Its function include import/export data between controllers and monitoring/notification capabilities to check if a controller is up or notify a takeover on a set of forwarding elements.

Application Layer: The application layer consists of end-user business applications and network services. Example of application that runs here is network virtualisation. Network policy is also defined here.

2.2 Vulnerabilities in SDN Architecture

A number of security analyses has been carried on the vulnerabilities in SDN. Adnan et al. in [5] identified the state of art in SDN security solutions with respect to each layer of SDN architecture. The work focuses on possible security attacks in SDN which could be executed. However, no solution to identified threats is presented. A comprehensive survey of security in SDN is presented in [11,12], the authors identified vulnerabilities introduced by separation of control and data plane. Sandra et al. in [11] presents an overview of SDN security and itemise research work coupled with solution to security issues in SDN. In [12] classification is done using the STRIDE approach and possible SDN security controls is proposed. The concept of offering SDN security as a service is presented in [13].

Kreutz et al. in [2] presents a high level security analysis. Seven main potential threat vectors are presented. Three of the seven identified threat vectors are specific to SDN and relates to the three planes present in SDN architecture. The analysis does not present SDN as a less secure network but triggers the need for innovative ways of responding to the new threats arising from network programmability. The authors state the consequences of these threats in SDN and solutions to the seven threat vectors was proposed.

In [14], a feasibility study on attacking SDN is carried out by fingerprinting to ascertain usage of SDN/OpenFlow switches by the network. The SDN network is then subjected to a specifically crafted flow requests from the data plane to the control plane to exhaust the network resources. Another security vulnerabilities was analysed in ProtoGENI [15]. The authors explored three potential security issues as follows:

(i) **Resource connection:** Once a malicious user obtains access to one experiment node, attacks can easily be launched by utilising the huge ProtoGENI computing resources as a launchpad to harm existing internet users.
(ii) **Wireless Nodes Distribution:** Network sniffing or spoofing can be done here to identify desired node for launching attacks.
(iii) **Virtualization Technology:** In ProtoGENI virtualisation, ProtoGENI resources are shared among as many user as possible. Any bug or compromise from a single device will expose other users in sharing resources to attacks.

The Authors discovered the possibility of using ProtoGENI resources to launch flooding attack to the wider internet. Also, the possibility of compromising confidentiality and availability of other ProtoGENI users is high.

2.3 DoS Attack on SDN

DoS and Distributed DoS (DDoS) attack remains one of the severe network security problems in both traditional network and SDN. Due to separation of control and data plane, an attacker could saturate the controller with malformed packets requiring a flow rule decision. On the other hand, the flow table of the infrastructure device can be overwhelmed with malicious packets. To address bottlenecks of potential saturation attack, AVANT-GUARD [16] introduce connection migration to reduce amount of data-to-control-plane interactions. The method enables the data plane to shield the control plane from saturation attacks. However, the data plane itself is subject to attack. Similarly, a backup strategy which offers resilience against failures in a centralised controlled network is presented in [17]. This approach is an attempt to solve single point of failure bottleneck and it provides seamless transition between primary controller to a back-up controller. However, this solution is limited to centralised implementation and it also raises concern in terms of trust between the east-west interface communications. In addition, Braga et al. [18] proposed lightweight, a new method for detecting DDoS. The proposed method boasts of high rate of true positives and low rate of false alarm using Self Organising Maps (SOM) for flow analysis. The lightweight method consider median values in training the SOM. The drawback of this method is that false negatives are reported when the attack parameter is set to a low value.

The controller has been compared to an operating system capable of managing applications through programmatic interface [19]. Similarly, ETHANE was built to provide network-wide fine-grain policy using a centralised declaration

and enforcing it [6]. While the concept of a centralised controller allow the simplification of policy enforcement and management tasks for network managers, it creates quite a number of bottle necks. In [9], analysis of SDN implementation key challenges has been carried out. The authors opined deployment of SDN technology will contribute to the vision of future communications if outstanding challenges were resolved. In [20] the possibility of DoS attacks and poor rule design that can lead to saturating volumes of controller queries is discussed. Though OpenFlow vulnerabilities in terms of lack of adoption of Transport Layer Security (TLS) for controller-switch communication is highlighted in [20], a number of vulnerabilities proposed was not verified in the work.

3 Experimental Method and Tools

In this experiments, Mininet is used [21]. Mininet is an open source network emulator devoted entirely to OpenFlow architecture and SDN implementation. For the controller, ODL controller is used [22]. ODL integrates open source, open standards and open APIs to deliver SDN platform to make networks more programmable and adaptive. DoS attacks usually engage numerous compromised hosts and a rich topology to launch a successful attack on its victim. While our scenario is much simpler than what is obtainable in real world attacks, we deliberately chose such a low-complexity set-up to expose and analyse the impact of DoS attack on SDN. Common testing tools such as, *ping* and *iperf* are used to generate traffic between host and servers. Figure 2 shows the methodology flowchart with each step explained.

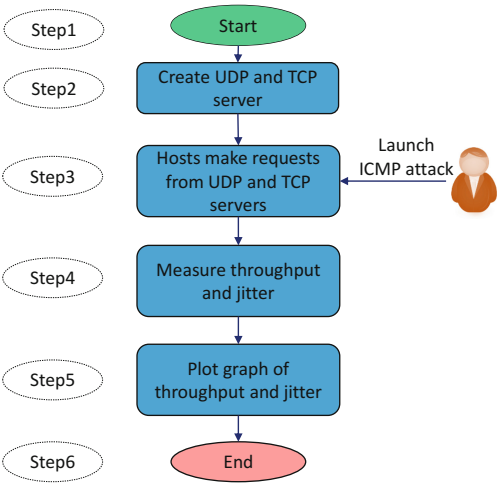

Fig. 2. Methodology flowchart.

Step 1: Start Mininet and ODL controller

```
Sudo mn --custom scenario.py --topo

--controller = remote,ip = x.x.x.x
```

Where x.x.x.x represents the ip address of the remote controller.
Check connectivity using

```
$mininet > net
```

Step 2: Create UDP and TCP server

```
UDP: iperf -s -u -p 5566 -i1
TCP: iperf -s  -p 5566 -i1
```

The TCP server is made to listen on port 5566 with a default window size of 85.3 KB. Similarly, UDP server is made to listen on port 5566 with a default UDP buffer size of 208 KB while receiving 1470 bytes datagrams and the result is monitored every 1 s.

Step 3: Hosts make requests from TCP server and UDP server

```
TCP: -iperf -c x.x.x.x -p5566 -t100
UDP: -iperf -c x.x.x.x -u -t100 -p5566
```

Step 4 and Step 5: Results were extracted using AWK file and results plotted using MATLAB. Then, malicious hosts 5 and 6 launched flooding attack on the servers (similar to step 3). Legitimate traffic is started at the beginning of an experiment, and an attack is launched shortly after for a duration of 100 s.

Step 6: End

```
mininet# ctrl z (end mininet)
Sudo mn -c (clear topology)
```

4 Experimental Set-Up

In this section, a series of experiments are performed to verify the effects of DoS attack in the SDN network. The experimental setup is shown in Fig. 3. To create the scenario in Fig. 3, many software and tools are used as shown in Table 1. There are two servers and four switches in the network. Each switch has a host connected to it. The Transmission Control Protocol (TCP) server is connected to OpenFlow switch1 while User Datagram Protocol (UDP) server is connected to OpenFlow switch3. ICMP flood attack will be launched against both servers by malicious hosts 5 and 6.

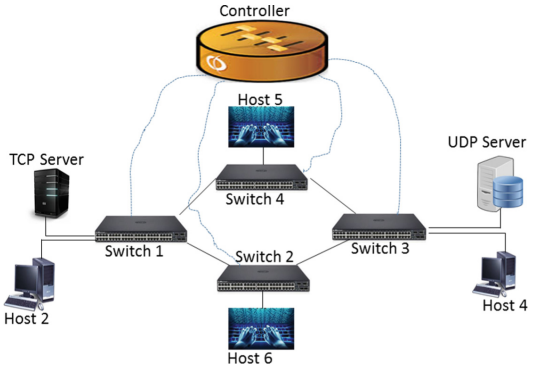

Fig. 3. Experimental setup.

Table 1. Simulation parameters

Simulation	Details
Platform/Enviroment	-Oracle Virtual Box as base environment for simulations
	-Ubuntu OS as base for Mininet v2.2 emulator
	-Ubuntu Server as base for OpenDaylight (Boron) controller
	-Host CPU as intel core i7, 12 G RAM
Attack tool	Hping tool - Hping3 used for flooding attack

5 Results and Analysis

As discussed in the experimental setup, we simulate for two different scenarios; TCP and UDP requests under normal operating condition and under attack. The results for these scenarios are discussed below.

5.1 Effect of DoS Attack on Throughput

Figures 4 and 5 shows a significant drop in throughput due to malicious behaviour (ICMP flood attack) being executed by two attacking nodes. The average throughput for requests made from host 4 to the TCP server is 214 Mbits/s for a total of 2.5 GB of information transferred in 100 s. Similarly, the average throughput of host2 requests from TCP server is 233 Mbits/s for a total of 2.72 GB of information transferred.

Notice that Host 2 shows a better bandwidth utilisation than Host 4 and the reason for this is not far-fetched; they are both connected to OpenFlow switch 1. While the better bandwidth utilisation is seen as an advantage here, it is a major security risk and attractive honeypot to launch attack against the server. The impact of this connection is felt when the server is subjected to ICMP flood attack. During attack, the average throughput dropped to 106 Mbits/s from 214 Mbits/s

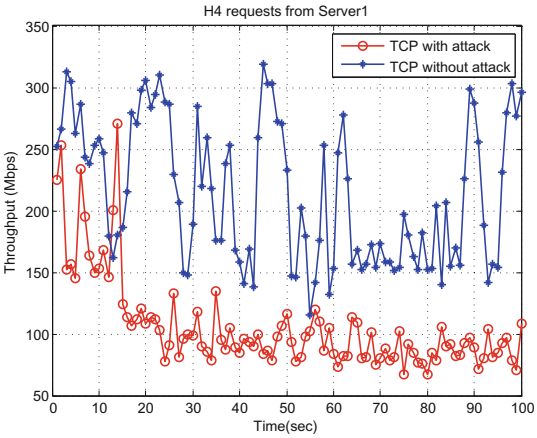

Fig. 4. TCP requests from host 4 to TCP server under ICMP attack.

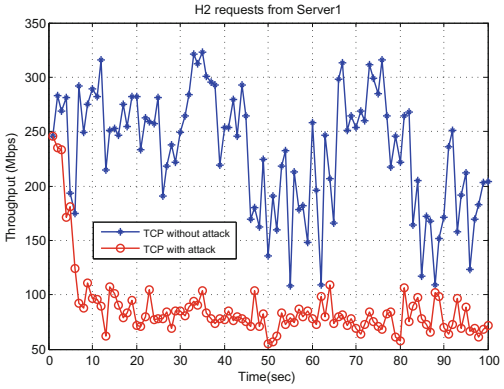

Fig. 5. TCP requests from host 2 to TCP server under ICMP attack.

recorded for H4 requests from server1 without ICMP flood attack. The impact of the attack launched by host 5 and 6 became noticeable after 15 s of transmission and the bandwidth utilisation degraded for the rest of the transmission. The trend is similar for host2 requests from TCP server as degradation started after 8 s of transmission and degraded for the rest of the transmission. The average throughput for h2 requests from TCP server dropped from 233 Mbits/s to 87.4 Mbits/s when the server is under attack. The degradation is more severe for host 2 when under attack even though higher throughput is recorded during normal operation. Hence, the need for better network design, traffic isolation based on priority for mission-critical network and dynamic proactive ways of addressing DoS attacks when the system is under serious attack.

5.2 Effect of DoS Attack on Jitter

Jitter is defined as a variation in the delay of received packets. In Figs. 6 and 7, using UDP buffer size of 208 KB, the jitter varies between 0.003 ms and 0.789 ms. Host 4 Jitter remains within a fair range because it is connected to OpenFlow switch 3 with the UDP server. The spiky delay waveform indicates the presence of congestion in the network. Even though the congestion occurs for a very short period, if the congestion time is more than the scheduled packet transmission time, it will lead to packet drops. Notice that jitter values obtained from host 4 requests to UDP server is better compared to requests from host 2.

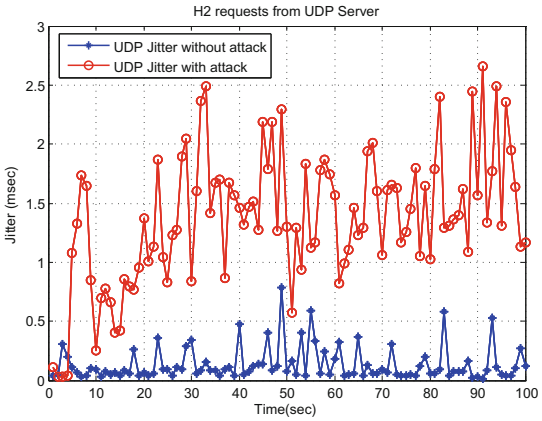

Fig. 6. UDP requests from host 2 to UDP server under ICMP attack.

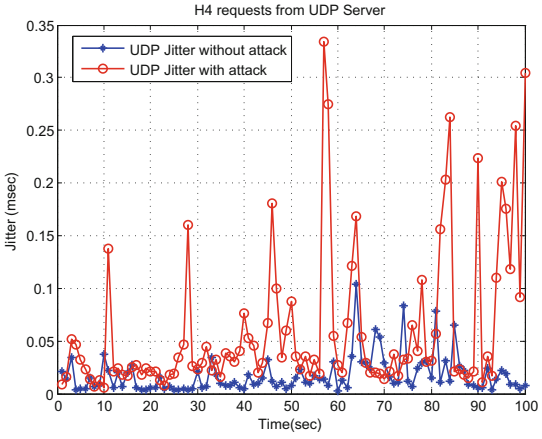

Fig. 7. UDP requests from host 2 to UDP server under ICMP attack.

6 Conclusion and Future Work

In this paper, the impact of DoS attack on SDN has been demonstrated. This study reveals that for a simple network, a DoS attack on the infrastructure plane (UDP and TCP servers) will highly degrade network performance as shown in the performance metrics (throughput and jitter). For a Distributed DoS (DDoS) attack with more active agents, the attack will be more severe. Hence, the need for a robust resilient SDN security architecture. While the evaluation of the impact of DoS attack on SDNs remains a very rigorous endeavour, the work carried out in this paper offers a primer to the objective evaluation of DoS attack on SDNs. The simulation results revealed a drop in network throughput from 233 Mbps to 87.4 Mbps and the introduction of large jitter between 0.003 ms and 0.789 ms during DoS attack. In the future, the mitigation of DoS and DDoS attacks in an exhaustive way at both control and data plane layers will be examined.

References

1. McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L.: OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)
2. Kreutz, D., Ramos, F., Verissimo, P.: Towards secure and dependable software-defined networks. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in software Defined Networking, pp. 55–60. ACM (2013)
3. Das, S., Parulkar, G., McKeown, N.: Rethinking IP core networks. J. Opt. Commun. Netw. **5**(12), 1431–1442 (2013)
4. Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE **103**(1), 14–76 (2015)
5. Akhunzada, A., Ahmed, E., Gani, A., Khan, M.K., Imran, M., Guizani, S.: Securing software defined networks: taxonomy, requirements, and open issues. IEEE Commun. Mag. **53**(4), 36–44 (2015)
6. Casado, M., Freedman, M.J., Pettit, J., Luo, J., McKeown, N., Shenker, S.: Ethane: taking control of the enterprise. ACM SIGCOMM Comput. Commun. Rev. **37**(4), 1–12 (2007)
7. Jain, S., Kumar, A., Mandal, S., Ong, J., et al.: B4: experience with a globally-deployed software defined WAN. ACM SIGCOMM Comput. Commun. Rev. **43**(4), 3–14 (2013)
8. VMware: Software-Defined Data Center (SDDC) (2017). http://www.vmware.com/products/nsx/
9. Sezer, S., Scott-Hayward, S., Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J.: Are we ready for SDN? implementation challenges for software-defined networks. IEEE Commun. Mag. **51**(7), 36–43 (2013)
10. Goransson, P., Black, C., Culver, T.: Software Defined Networks: A Comprehensive Approach. Morgan Kaufmann, Burlington (2016)
11. Scott-Hayward, S., Natarajan, S., Sezer, S.: A survey of security in software defined networks. IEEE Commun. Surv. Tutor. **18**(1), 623–654 (2016)

12. Alsmadi, I., Xu, D.: Security of software defined networks: a survey. Comput. Secur. **53**, 79–108 (2015)
13. Ali, S.T., Sivaraman, V., Radford, A., Jha, S.: A survey of securing networks using software defined networking. IEEE Trans. Reliab. **64**(3), 1086–1097 (2015)
14. Shin, S., Gu, G.: Attacking software-defined networks: a first feasibility study. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 165–166. ACM (2013)
15. Li, D., Hong, X., Bowman, J.: Evaluation of security vulnerabilities by using ProtoGENI as a launchpad. In: Global Telecommunications Conference (GLOBECOM 2011), pp. 1–6. IEEE (2011)
16. Shin, S., Yegneswaran, V., Porras, P., Gu, G.: Avant-guard: scalable and vigilant switch flow management in software-defined networks. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, pp. 413–424. ACM (2013)
17. Fonseca, P., Bennesby, R., Mota, E., Passito, A.: A replication component for resilient openflow-based networking. In: Network Operations and Management Symposium (NOMS), pp. 933–939 (2013)
18. Braga, R., Mota, E., Passito, A.: Lightweight DDoS flooding attack detection using NOX/OpenFlow. In: IEEE 35th Conference on Local Computer Networks (LCN), pp. 408–415 (2010)
19. Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., Shenker, S.: NOX: towards an operating system for networks. ACM SIGCOMM Comput. Commun. Rev. **38**(3), 105–110 (2008)
20. Benton, K., Camp, L.J., Small, C.: OpenFlow vulnerability assessment. In: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, pp. 151–152. ACM (2012)
21. TeamMininet: Mininet (2017) http://www.mininet.org/download/
22. Linux-Foundation-Collaborative-Projects: ODL (2017) https://www.opendaylight.org