SDN을 위한 네트워크 플러딩 공격 탐지 및 방어 시스템의 KOREN상의 평가

부 둑 티엡, 김경백
전남대학교 전자컴퓨터공학부
e-mail : ductiep91@gmail.com, kyungbaekkim@jnu.ac.kr

Evaluation of Network Flooding Attack Detection/Prevention System for SDN in KOREN Network

TIEP VU DUC, KYUNGBAEK KIM
Department of Electronics and Computer Engineering,
Chonnam National University

요 약

Nowadays security has been one of the hot issues of SDN researches. Because of flexible management of flows with SDN controller, network security functions can be deployed with SDN. Some SDN based DoS attack detection systems have been proposed in the past few years. Especially, a sampling based network flooding attack detection and prevention system was proposed to defend the SDN based network from DoS attacks. They were evaluated through network emulators or local testbeds, however it is not clear whether the proposed system is viable to large scale SDN. In this paper, we evaluate the sampling based network flooding attack detection and prevention system for SDN over KOREN (Korea Advanced Research Network), to understand the impact of large scale network and DoS attack on the flooding attack detection and prevention system. Through the real implementation based evaluation, we demonstrate that the proposed system successfully defends against network flooding attacks.

1. Introduction

Recently, Software Defined Networking (SDN) has been developed rapidly by enormous efforts from researchers around the world. The goal of SDN is to simplify the network administration via a centralized control. However, the centralized control is also a single point of failure, where attacker can exploit to conduct cyber attack such as Denial of Service (DoS) attack that results in significant loss of service [1]. Accordingly, security of SDN system is one of the top concerns nowadays.

New researches are conducted for evaluating SDN based security system as well as the suitability of SDN for security systems such as [2,3,4,5,6]. In [2], a SDN-based IPS Development Framework was provided to support network engineer to easily design and implement their own IPS system. In [3,4,5], the OpenFlow controller were used to analyze traffic and detect the DoS attack. Accordingly, the Openflow must process a huge a mount of packets and that results in low performance. In [6], a better method to detect and mitigate the SYN Flooding attack was proposed by utilizing sFlow to collect cumulative traffics from each of its agent instead of forwarding all packets to OpenFlow controller.

Recently, an sampling based network flooding detection and prevention system for SDN was proposed with the main focus on automatic detection and prevention of DoS attack [7,8]. In the proposed system, sFlow is used to collect traffic samples from each switch. Then snort is used to analyze the traffic samples instead of the controller, hence it reduces the overhead of the centralized controller. If snort detects an attack, an controller application will take action to defend the detected attack.

These previous systems were evaluated by using network emulator or a local testbed, which have only a small number of hops and links. In a large scale SDN network such as the Korea Advanced Research Network (KOREN), the huge number of hops and links can have significant impact to the performance of the SDN-based security system. to understand about this issue, in this paper we evaluate the sampling based network flooding detection and prevention system for

SDN over KOREN.

The rest of the paper is organized as follows: in section 2, we present the sampling based network flooding detection and prevention system for SDN. Section 3 describes the performance evaluation of the system in local testbed while the evaluation on KOREN are presented in section 4. Finally, we conclude this paper in section 5.

2. Sampling based Network Flooding Detection and Prevention System

The overall structure of the sampling based network flooding detection and prevention system is depicted in Figure 1. The system has five main blocks: Sampling Collector, Attack Detector, Event Database, Attack Defender and SDN Controller. In each switch, an sampling agent is running to collecting traffic samples and send to the Collector. The Collector processes the collected traffic samples and convert the data into a readable format for the Attack Detector. Then the Attack Detector analyzed the data to determine whether or not a switch is being attacked based on the pre-defined detection rules. If an attack is detected, an event will created in the Event Database to store information of the attack. The Attack Defender will periodically check the Event Database and get the information of the new attack. Based on the information, the Attack Defender will inform the SDN controller to install defending rules on the switches to block the attacking traffics.

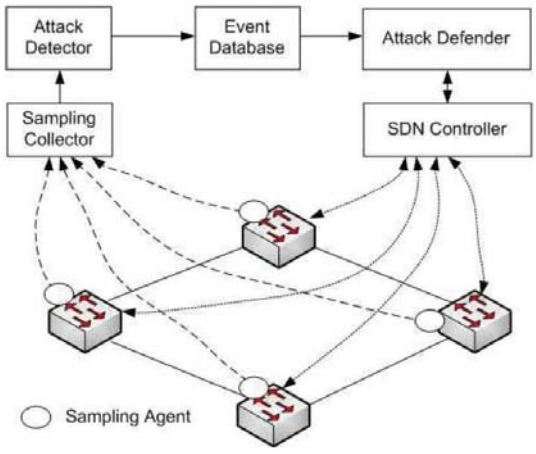

Figure 1. The sampling based network flooding detection and prevention system [8]

3. Evaluation on Local testbed

In this section, we evaluate the sampling based network flooding detection and prevention system using our local testbed in Chonnam National University (JNU). The testbed has six computers: a SDN Controller PC, two OVS switches and three hosts as shown in Figure 2. In the controller computer, we install all five components of the proposed system. The sFow-toolkit [11] is utilized as the traffic sample collector and there is one sFlow agent in each switch to help collect traffic sample. The Snort [10] is used as the Attack Detector, and a mysql database is designed to store Attack Event detected by Snort. The OpenDaylight [9] is used as the SDN controller. We implemented the Attack Defender as an OpenDaylight application, which periodically check the Event Database to obtain new attack information and install defending rules into switches. Each defending rule will last ten seconds. After that, the Attack Defender will delete them.

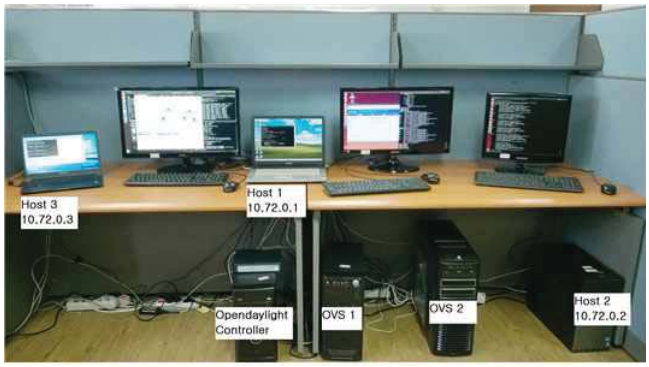

Figure 2. The JNU local testbed

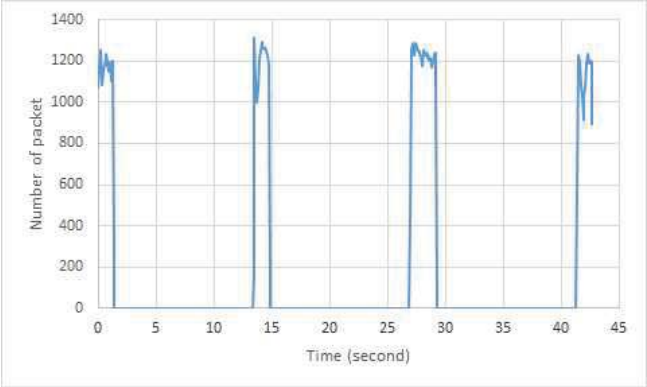

Figure 3. Traffic load graph when one host is attacking another host in JNU local testbed

In the experiment, we use hping3 running on one host to flood TCP SYN packets to a server running on another host while our system is activated. The attacking traffic are captured in order to measure its packet rate. The result is shown in Figure 3. It can be seen that the attack was successfully detected and the attack traffic was blocked totally during ten seconds of

the defence. We can also observe that the system reacts very quickly to the attack. It is around 2 seconds after the attack begins, the system detects and installs defending rules to block the flooding traffic.

The evaluation in the local testbed shows the efficiency of the proposed system in small scale SDN network. In order to understand the impact of large scale SDN networks to performance of the proposed system, we will evaluate of the system in KOREN testbed.

4. Evaluation on KOREN

The KOREN tesdbed consists of two local testbeds located at Chonnam Nation University (JNU) and Jeju National University (JEJU). The two testbeds are connected through the KOREN network. The JNU testbed is the same as local testbed used in the last section. In the JEJU testbed, we have one OVS switch and two virtual hosts. The topology of KOREN testbed is depicted in Figure 4 with four possible attack scenarios.

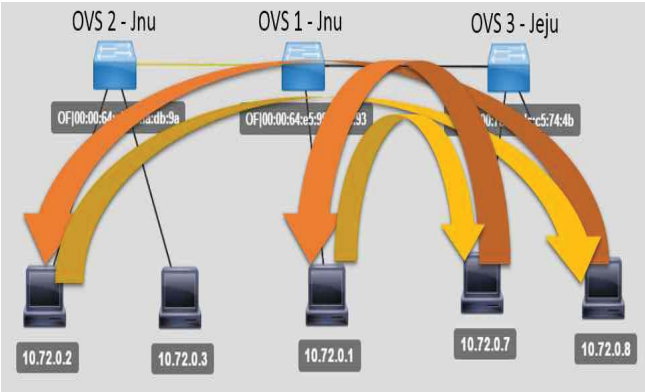

Figure 4. The topology of KOREN testbed with some possible attack scenarios

In the experiments, we conducts two attack scenarios: attack from JNU site to JEJU site and vice versa. In the first experiment, a host from JNU site will flood TCP SYN packets to a server running in a JEJU host while in the second experiment, we do the opposite way, in which a host from JEJU site will flood TCP SYN packets to a server running a JNU host. In each experiment, we also capture the attack traffics and measure its packet rates. The results of the first and the second experiments are depicted in Figure 5 and Figure 6 respectively.

Figure 5 illustrates the packet rate of the attacking traffic to the JEJU host. It can be seen that the system has detected the TCP SYN flooding attack, and the defending rules are installed in the switches. During the

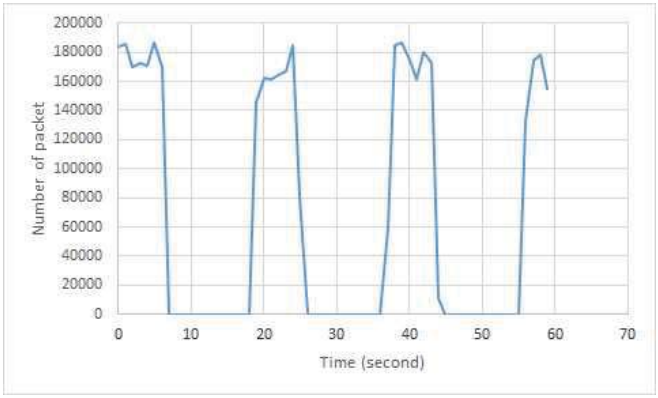

Figure 5. Traffic load graph when JNU is attacking JEJU

10 seconds of the defence, the packet rate of attacking traffic drops to zero, that means the attack was totally blocked. However, it takes around 8 seconds for the system to act against the flooding attack, which is 4 times larger the local testbed response time.

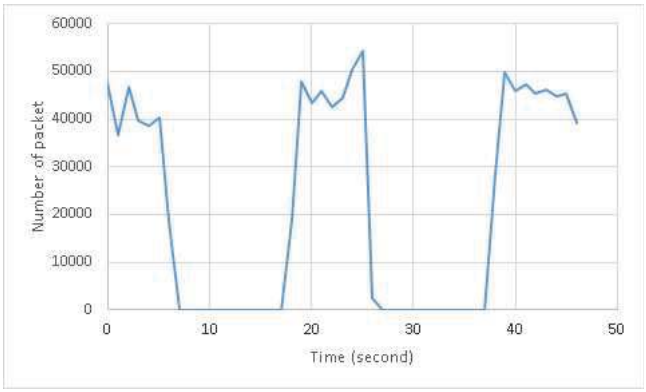

Figure 6. Traffic load graph when JEJU is attacking JNU

The attack from JEJU site is also detected and defended successfully as shown in Figure 6. Similar to the first experiment, the system responses to the flooding attack after around 8 seconds.

In short, the sampling based network flooding detection and prevention system is feasible in large scale SDN network. However, due to the large number of hops and links, the response time of the system to the attack will be much slower than in local testbed.

5. Conclusion

Recently, security of SDN network has become a hot issue. By using local testbed, we demonstrate the efficiency of the sampling based network flooding detection and prevention system. The system is also viable in large scale network such as KOREN. However, the slow response time is an issue of the

proposed system in large scale SDN network. In future, we are going to seek an efficient approach to mitigate the issue.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the korean Government(NRF-2014R1A1A1007734).

References

[1] S. Scott-Hayward, G. O'Callaghan, S. Sezer, "SDN security: a survey," in Proc. IEEE SDN4룬, 2013.

[2] Zhengyang Xiong. "An SDN-based IPS Development Framework in Cloud Networking Environment", 『2014 mster thesis』. 2014.

[3] R. Braga, E. Mota, A. Passito, "Lightweight DDoS Flooding Attack Detection using NOX/OpenFlow", Proceeding of the 35th Anual IEEE Conference on Local Computer Networks, pp. 408-415, 2010.

[4] N.N Dao, Junho Park, Minho Park, Sungrae Cho, "A Feasible Method to combat against DDoS Attack in SDN Network", in Proceedings of ICON 2015, 2015.

[5] Martin Andreoni Lopez, Otto Carlos M. B. Duarte, "Provinding Elasticity to Intrusion Dection Systems in Virtualized Software Defined Networks", ICC 2015, 2015.

[6] M. Nugraha, I. Paramita, A. Musa, D. Choi, B. Cho, "Ultilizing OpenFlow and sFlow to Detect and Mitigates SYN Flooding Attack", Journal of Korea Multimedia Society, Vol. 17, No. 8, pp. 988-994, 2014.

[7] 이윤기, 김승욱, 김경백, "SDN환경에서 네트워크 플러딩 공격 탐지 및 방어 시스템 구현", In Proceedings of 2015년도 한국스마트미디어학회(KISM) 추계학술대회, October 23-24, 2015, 조선대학교, 광주.

[8] 이운기, 김승우그, 부 둑 티엡, 김경백, "SDN을 위한 생플링 기반 네트워크 플러딩 공격 탐지/방어 시스템", KISM Smart Media Journal, 4권 4호, pp. 24-32, Dec 31, 2015.

[9] "https://www.opendaylight.org", Accessed: 2016-03-01.

[10] "https://www.snort.org/", Accessed: 2016-03-01.

[11] "http://www.inmon.com/technology/sflowTools.php", Accessed: 2016-03-01.