소프트웨어 정의 네트워크를 위한 샘플링 기반 서비스거부공격 탐지 시스템 개선

뉘엔신응억* 최진태* 김경백*
*전남대학교 전자컴퓨터공학부
e-mail : sinhngoc.nguyen@gmail.com, jefron1100@gmail.com, kyungbaekkim@jnu.ac.kr

Enhancement of Sampling Based DDoS Detecting System for SDN

Sinhngoc Nguyen*, Jintae Choi*, Kyungbaek Kim*
*Dept. of Electronics and Computer Engineering, Chonnam National University

Abstract

Nowadays, Distributed Denial of Service (DDoS) attacks have gained increasing popularity and have been a major factor in a number of massive cyber-attacks. It could easily exhaust the computing and communicating resources of a victim within a short period of time. Therefore, we have to find the method to detect and prevent the DDoS attack. Recently, there have been some researches that provide the methods to resolve above problem, but it still gets some limitations such as low performance of detecting and preventing, scope of method, most of them just use on cloud server instead of network, and the reliability in the network. In this paper, we propose solutions for (1) handling multiple DDoS attacks from multiple IP address and (2) handling the suspicious attacks in the network. For the first solution, we assume that there are multiple attacks from many sources at a times, it should be handled to avoid the conflict when we setup the preventing rule to switches. In the other, there are many attacks traffic with the low volume and same destination address. Although the traffic at each node is not much, the traffic at the destination is much more. So it is hard to detect that suspicious traffic with the sampling based method at each node, our method reroute the traffic to another server and make the analysis to check it deeply.

Keyword: SDN, DDoS, Sampling Based Method, Intrusion Detection and Prevention System (IDPS)

1. Introduction

DDoS attack is one of the main challenges of Internet Security today. DDoS can make the victim to be flooded by sending large amount of traffic. It drains out of the computing and communicating resource of victim in a short of period time. Most of attackers exploit the error of services or protocol such as NTP, SSDP, and DNS to deploy an attack. There are several attacks that use NTP protocol to increase the traffic up to 400Gbps from many sources [1] [2].

Within the growing of network devices, the connection becomes more complicated. Since the network consist of heterogeneous devices, it require an enormous number of services and protocol in communication such as network time, identity and services discovery to help those devices synchronize and cooperate smoothly. These services and protocols may be vulnerable to attack. Although the devices make a low volume of request, many devices will generate a big volume request at the same destination. All of them reach to the security in the network.

This paper is primarily concern with how to handle multiple attacks from many IP addresses and how to resolve the suspicious traffics in the network. For the first problem, we use a table to mark the flows which setup to switch. It can handle multiple attack events coming and avoid the conflict rule in the switches. For the other, we reroute the suspicious traffic to another server to make the analysis deeply.

2. Related Work

Recently, there had been many researches that use SDN to create the defense mechanism for DDoS attack. Some of them have been published such as [3] [4] [5]. In [3], they optimize an artificial neural network (ANN)-based classifier to detect anomalies in flow traffic. The result look at high degree of accuracy, but it still loses important information in process of sampling. So they propose a sampling method to improve the performance of flow-based anomaly detection in sampled traffic. The detection rate improve by about 5% by using that method. In [4] present an adaptive, feature aware sampling technique that reduces the loss of information bounded with the sampling process, thus minimizing the decrease of anomaly detection efficiency. In [5], the author provides an architecture named FlowTrApp, which base on SDN to detect and mitigate DDoS attack on DataCenter. FlowTrApp bases on the application that use L7 constraint to detect and mitigate the DDoS attack for web application.

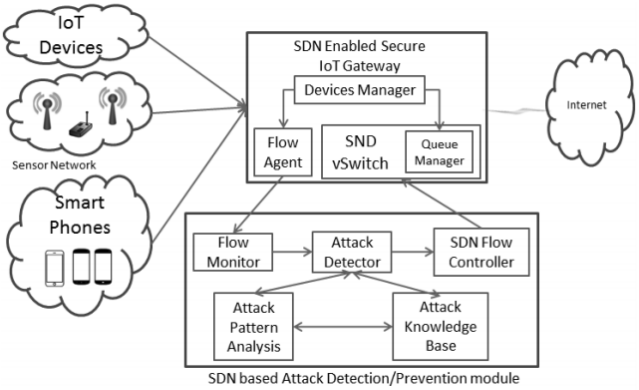

Figure 1. Sampling Based Method in IDS

In general, to detect the DDoS in the network, we had to use Intrusion Detection System (IDS) such as Snort to analyze the traffic and find out the abnormal ones. There are two important methods that is almost use in IDS, these are sampling based method and full scan based method.

In the sampling based method, the traffic going through gateway must be sampled before forwarding to the IDS system [7]. The architecture of the sampling based method for detection system is depicted in Figure 1. The system have two big modules, first one is SDN Enable Secure IoT Gateway and SDN Based Attack Detection/Prevention module [6]. Each gateway in the network is attached with a sampling agent whose job is to collect traffic samples and send to the Flow Monitor. The Flow Monitor processes the collected traffic samples and converts the data into a readable format for the Attack Detector. Then the Attack Detector analyzed the data to recognize ongoing attack based on the predefined detection rules. If an attack is detected, an event will be created to store information of the attack into database. The preventing application will periodically check the database and get the information of the new attack. Based on that information, the preventing application will inform the SDN Flow Controller to install defending rules on the gateway to block the attacking traffics. These defending rules are temporary and they will be kept in flow table of the gateway for 20 seconds before being removed.

In the full scan based method, all traffic going through the gateway must be forward to the IDS system to be analyzed. If an attack is detected, the IDS system informs the controller to deploy defending rules in each gateway to block the malicious traffic. The advantage of the full scan based method is that it has high accuracy and is able to detect the abnormal traffic which is not significantly larger than the normal traffic. The full scan based method is also easy to implement and does not require much additional component to select and sample the traffic. However, this method has a downside that it causes significant overhead to the IDS system at high traffic. Therefore, the full scan based method should only be applied when the total traffic is not too high and the amount of abnormal traffic is a small potion of it.

The advantage of the sampling based method is that it sign ificantly reduces the overhead for IDS system. However, a bi g disadvantage of this method is that the accuracy of the IDS system is depended on the sampling rate. At a slow sampling rate, it is likely that the IDS system will miss the suspicious t raffics; furthermore, the sampling based method

Algorithm 1: Block traffic algorithm.
Input:
Income_packet is the traffic from attacker
snort_database is the connection to snort database in MySQL

```
1:  if ruleMatching(income_packet)
2:          importDatabase(income_packet)
3:  data = getNewEventData(snort_database)
4:  topo = getTopoInfor()
5:  if (isExistFlow(data))
6:          warning "Exist Flows for this event"
7:  else
8:          flow = genNewFlows(data)
9:          switch = getSwitch(topo)
10:         setupFlow(flow, switch)
```

timestamp	ruleid	switchid	src_ip	dst_ip
1489680564.83	14910	openflow:141009632299655	10.0.0.6	10.0.0.4
1489680564.89	14911	openflow:141009632186767	10.0.0.6	10.0.0.4
1489680564.95	14912	openflow:110937293283142	10.0.0.6	10.0.0.4
1489680565.02	14913	openflow:141009632186836	10.0.0.6	10.0.0.4
1489680565.09	14914	openflow:110937293271337	10.0.0.6	10.0.0.4
1489680565.15	14915	openflow:963354559053	10.0.0.6	10.0.0.4
1489680573.75	14916	openflow:141009632299655	10.0.0.8	10.0.0.4
1489680573.8	14917	openflow:141009632186767	10.0.0.8	10.0.0.4
1489680573.87	14918	openflow:110937293283142	10.0.0.8	10.0.0.4
1489680573.93	14919	openflow:141009632186836	10.0.0.8	10.0.0.4

Figure 2. Existing Table of Flow

also needs a sampling module to sample the traffic, hence it requires more complicated implementation. Therefore, the sampling based method is usually applied at the gateway closer to the victim because the attacking traffic through the gateway is significantly larger than normal traffic of IoT devices.

In this paper, we propose solution to handling the multiple attacks from many sources and resolve the suspicious attack in the network. For handling multiple attacks, we build an application that is integrated to IDS to analyze the attack events, and generate the preventing rule to block the attack traffic. In IDS, we use sFlow to sampling the traffic and send these samples to analyzer machine. In here, we use the Snort rule to detect the attack traffic and store these events into MySQL by using Barnyard. The application gathers information of events from database and network topology from the controller, and generates the preventing rules. We use a table to store the existing rule in the switches. After check the existing, these rules will be set to switches through OpenDayLight Beryllium API. In addition, with the suspicious packet, it is hard to detect by the sampling based method. We propose the rerouting solution to handle the suspicious traffic on the network. It will be reroute to another server, and make a full scan to check deeply. In the rest of paper, we discuss the solution in section 3. In section 4, we show the evaluation for the system, and we make the conclusion in section 5.

3. Solution for handling the DDoS attack

3.1 Handling multiple attack

In the reality, an attack may start from many source, it means that many devices make an attack to victim. In our

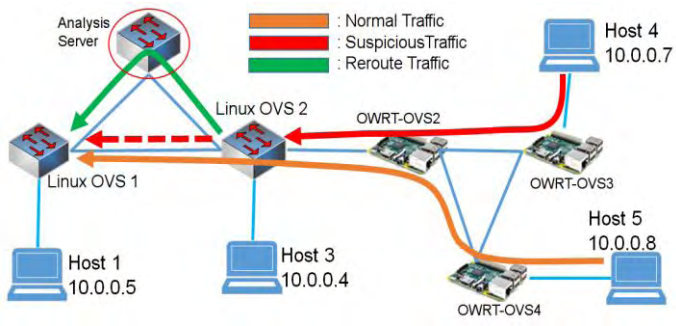

Figure 3. Handle Suspicious Traffic

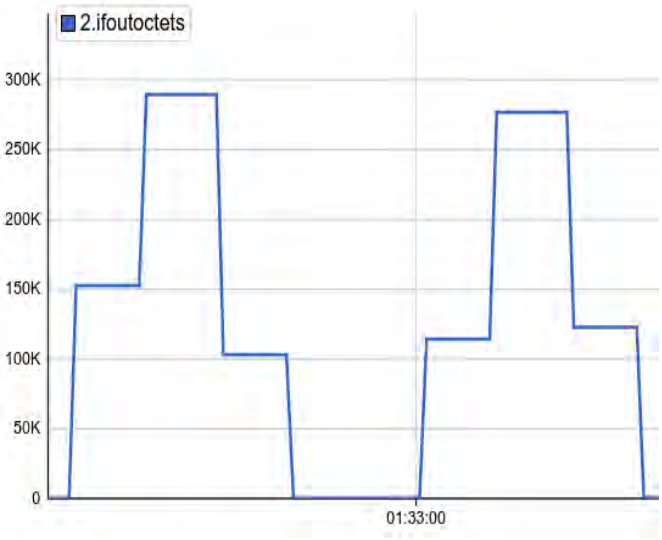

Figure 4. Result of Prevention

system, the Snort may detect many attack events in a short of period time. It requires the preventing application must handle all the events in the database.

Our application provides a buffered list to store a large of data reading from database and an existing rule table to check the existing flow before setting to switch. This table which shows in Table 1 will be updated when we setup a new rule to switch or delete a rule from switch. The table includes timestamp to mark the setup time, ruleid is the ID of setup rule, switchid is the id of switch, src_ip and dest_ip are the source IP and destination IP collected from Event Database. For each event in the list, we check the existing rule in the table by isExistRule function.

Algorithm 1 shows the flow of detecting and preventing of attack traffic in our system. It includes several functions such as ruleMatching, importDatabase, getNewEventData, so on.

By this way, we can handle multiple attack events and remove the redundant rule before setup to switch. It helps reducing the conflict of rule in the switch as well as improving the performance of preventing.

3.2 Handling Suspicious Attacks

In many cases of attacks, attacker can fake the traffic that similar to the normal case, it is hard to detect the attack with sampling based method. In this case, we reroute the traffic to Analysis Server showed as Figure 2, and do the analysis with

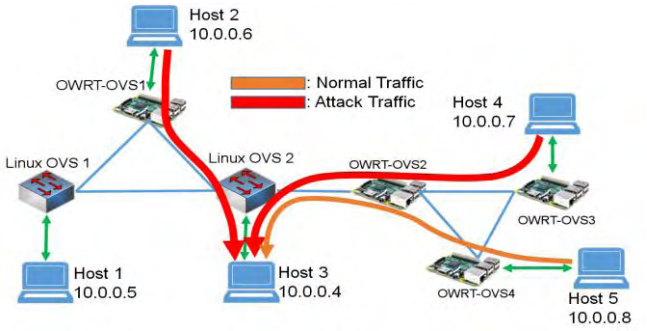

Figure 5. Scenario for Multiple Attacks

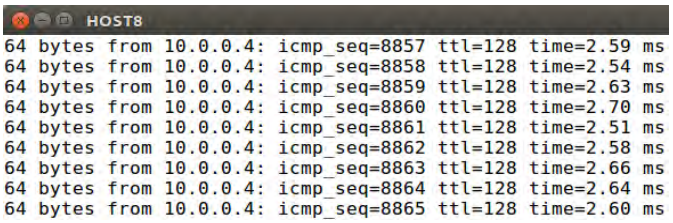

Figure 6. Normal Traffic

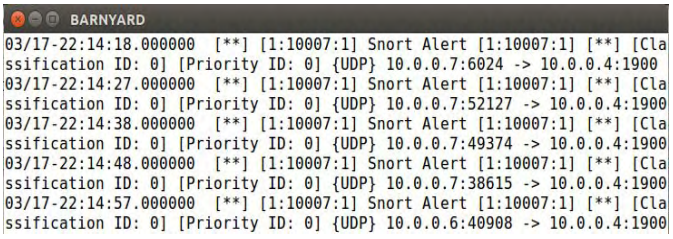

Figure 7. Detection Result

that traffic to check one more times. In this figure, there is a normal traffic from Host 5 and another abnormal traffic from Host 4. Both of them go through node Linux OVS 2, the abnormal traffic will be detected and rerouted to Analysis Server. Then we can use full scan based method to analyze the suspicious packet to find out the attack traffic deeply.

In case of full scan based method, we can take a look at detail to all the packets forwarded to Analysis Server. If the system detects an attack, it informs the controller to deploy preventing rules into each node in the network to block the malicious traffic. The advantage of the full scan based method is that it has high accuracy and is able to detect the abnormal traffic which is not significantly larger than the normal traffic. The full scan based method is also easy to implement and does not require much additional component to select and sample the traffic. However, this method has a disadvantage that it causes significant overhead to the IDS system at high traffic. But in case of suspicious, that is a good method to analyze the suspicious traffic. Because it is just the traffic coming from the nodes which detect the suspicious packet, it is too small enough to use full scan based method

4. Evaluation

4.1 Attack Scenario

To examine the viable of multiple attack handling, we build a Tedbed with SDN to test the detecting ability of the system. The scenario in the Figure 4 show the multiple

attacks from many sources. In that, Host 2 and Host 4 make an attack to Host 3. Instead, Host 5 just made a normal request Host 3. In this scenario, we expect that our solution can detect the attacks from Host 2 and Host 4, generate the preventing rule for that hosts, and allow the normal traffic from Host 5

4.2 Setup Tedbed

We build the tedbed based on SDN, it include SDN controller, two OpenvSwitch linux machines and four OpenvSwitch OpenWRT boards , five hosts (Host 1, Host 2, Host 3, Host 4, Host 5) showed as Figure 4. We use OpenDayLight Beryllium for controller, Snort as the Intrusion Detection System, and the sFlow-toolkits as the traffic sample collector. In each SDN-enabled gateway, there is one sFlow agent to help collecting traffic sample and send to sFlow-toolkits

4.3 Detection Result

The result of detection showed in Figure 6 with the detailed information of attack traffic such as UDP protocol, source IP, source port, destination IP address 10.0.0.4, and destination port 1900. In the result, we can see two attack sources. These are 10.0.0.6 and 10.0.07 IP address. According to scenario, Host 5 with IP 10.0.0.8 is the normal request. In the result of detection, Snort does not detect Host 5 as the attack traffic, and in the Figure 5 Host 5 still make the ping request. It allows for the normal traffic to send and receiving the data in the network.

4.4 Prevention Result

The result of prevention showed in the Figure 3 with vertical is ifoutoctets of traffic, and horizontal is detecti on time. When having the attack, the line will be incre ased, the top of attack volume upto 300K. After detecti ng the attack, our system generates the preventing rule and setup to the switch. It drops the attack traffic, so t he line go down, we can see it equal 0 at the place be tween two peak

5. Conclusion

In this paper, we propose solution to handling multiple attacks from many sources, and resolving suspicious attack. In addition, we build the tedbed based on SDN to evaluate our method for handling multiple attacks. The result shows at good for detecting and preventing ability of our system.

In the future work, we will implement the tedbed for resolving suspicious attack, and take a look at full scan based method to analyze the suspicious traffic in deeply.

Acknowledgement

This work was supported by the National Research Foundation of Korea Grant funded by the korean Government(NRF-2014R1A1A1007734). This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2016-R2718-16-0011) supervised by the IITP(Institute for Information & communications Technology Promotion).

References

[1] Rudman L, Irwin B Characterization and analysis of NTP amplification based DDoS attacks, InInformation Security for South Africa (ISSA), 2015 2015 Aug 12 (pp. 1-5). IEEE.

[2] Czyz J, Kallitsis M, Gharaibeh M, Papadopoulos C, Bailey M, Karir M. Taming the 800 pound gorilla: The rise and decline of ntp ddos attacks, InProceedings of the 2014 Conference on Internet Measurement Conference 2014 Nov 5 (pp. 435-448). ACM.

[3] Jadidi, Zahra, et al. "Performance of flow-based anomaly detection in sampled traffic." Journal of Networks 10.9 (2015): 512-521.

[4] Karel Bartos , Martin Rehak, IFS: Intelligent flow sampling for network security-an adaptive approach, Networks, v.25 n.5, p.263-282, September 2015

[5] Buragohain, Chaitanya, and Nabajyoti Medhi. "FlowTrApp: An SDN based architecture for DDoS attack detection and mitigation in data centers." Signal Processing and Integrated Networks (SPIN), 2016 3rd International Conference on. IEEE, 2016.

[6] 뉘엔 신 녹, 이윤기, 이왕광, 신기원, 김경백(Kyungbaek Kim). 서비스 거부 공격 탐지 및 방어를 위한 SDN 기반 IoT 게이트웨이 설계 (Design of SDN based IoT Gateway for Detecting and Preventing DoS attack). In Proceedings of 2016 년도 한국스마트미디어학회(KISM) 추계학술대회, October 28-29, 2016, 호남대학교, 광주.

[7] 이윤기, 김승욱, 부 둑 티엡, 김경백(Kyungbaek Kim) SDN 을 위한 샘플링 기반 네트워크 플러딩 공격 탐지/방어 시스템 (Sampling based Network Flooding Attack Detection/Prevention System for SDN). 한국스마트미디어학회(KISM) 스마트미디어저널 (Smart Media Journal), 4 권 4 호, pp. 24-32, December 31, 2015.