DDoS Attack Detection Based on Self-organizing Mapping Network in Software Defined Networking

Chanchan Zhao^{1,2,*} and Feng Liu¹

¹School of Computer and Information Technology, Beijing Jiaotong University, 100044 Beijing, P.R. China

² College of Information Engineering, Inner Mongolia University of Technology, 010051 Hohhot, P.R. China

Abstract. The software defined networking is a new kind of network architecture, the programmability of SDN enables hackers to easily launch DDoS attack on the network through software programming. To solve the problem, a DDoS attack detection scheme based on self-organizing mapping network in the software defined networking was proposed. The first is to give an early warning according to the probability of occurrence of Packet_In event. If the threshold value is exceeded, the characteristics of the flow are calculated and the self-organizing mapping network is used for clustering of eigenvalues to finally detect the DDoS attack flow. The experimental results showed that the DDoS attack detection scheme based on self-organizing mapping network was superior to the comparison scheme in detection rate and false alarm rate.

1 Introduction

The software defined networking(SDN) is a new kind of network architecture that can meet the needs of the future Internet, and its emergence makes it possible to break through the bottlenecks of existing network architecture. The software defined networking separates the control plane and the data plane, shielding the complexity of the underlying network infrastructure, making the management of the whole network more convenient and efficient. At the same time, the centralized management, openness and programmability of SDN make it a good support for the innovation of future new business.

SDN separates the data plane and the control plane, to realize high efficient centralized management of the network. However, this architecture also brings security risks. Because of the existing communication path between the controller and the network device, attackers can send attack packets frequently and the controller are always busy deciding how to forward these packets, but unable to provide services to the legitimate users, which belongs to the control layer DDoS attacks. Similar DDoS attacks can also be launched at the infrastructure level. Flooding of the flow table will deplete the memory resources and make the network unable to provide normal resource access or services, resulting in network collapse. In addition, DDoS attacks may also cause rule modification or fraudulent rules to be insert.

The remainder of this paper is organized as follows. Section 2 reviews some related studies. In Section 3, we propose a attack detection scheme in the software defined networking. The analysis is further validated by extensive simulation experiments introduced in Section 4. Finally, Section 5 concludes this research work.

2 Related work

In the past few years, the size, number and type of DDoS attacks have been increasing year by year. In order to adapt to this situation, the academe and the industry have devoted a lot of research efforts in the detection of DDoS attacks. DDoS attack detection has become a research hotspot in the field of network security.

In SDN, in order to reduce the harm of DDoS attacks, researchers have proposed a series of different solutions. Flow detection and analysis[1] is an effective means of detecting attacks in SDN. Tsinghua University Network Research Center [2] presents a flow analysis method, trigger a "not found" event during each check of the flow table, and then encapsulate the data packet to the controller to send the message, and then check the data packet IP address, however, this method will drain a large number of load to the controller, causing great burden to the controller.

* Corresponding author: cczhao@imut.edu.cn

In order to alleviate the overload of SDN controller, National Technical University of Athens network management and optimization design laboratory (Netmode) [3] adopt In Mon Company's network flow monitoring technology sFlow based on packet sampling to be in charge of the collection of information flow, and reduce the communication between the switch and the control device by lookup the forward flow table. Then analyze the flow variation characteristics of the anomaly module, use the algorithm based on information entropy to detect the anomaly, and generate the rule of flow table to issue to the switch. However, the method of anomaly detection based on information entropy needs to be combined with other technologies to determine the threshold.

In addition to the above detection method based on flow variation characteristics, there is also a method based on the connection migration mechanism. Based on the connection migration mechanism, literature[4] extends the data plane of SDN, designs a security architecture AVANT-GUARD that can defend against DoS attacks, adding the connection migration module and encouraging the trigger module.

In this paper, we argue that a new scheme for DDoS Detection based on SOM to reduce resource consumption, improve detection ratio and false alarm ratio.

3 Attack detection

3.1. SDN flow processing

In the software defined networking, the controller creates rules for each flow. There are two modes in the setting of flow rules: active and passive. In the first model, flow table rule is pre-installed in the flow table, and the flow table rules have been set up before the first packet arrives at the switch; in the second mode, only if the table rules of the corresponding flow in the flow table items do not exist, then the controller can set up rules for such flow table, that is when the first packet arrives at the switch the flow table rules are set up. The software defined networking discussed in this paper takes the second mode by default.

3.2 Packet_In trigger probability

When the flow of the main switch does not have corresponding flow table rules to match with, the Packet_In event is triggered. Based on this, during the time of DDoS attacks, the proportion of Packet_In event data packets triggering is called Packet_In event

triggering probability, is $P(v_a)$, v_a is denoted as the rate of DDoS attack flow.

Let $v_n\mu_d=N$, $v_a\mu_d=A(v_a)$, which represents the number of data packet sent by the normal flow and attack flow in μ_d . The Packet_In proportion of normal flow triggering is:

$$\frac{\varphi}{N} = \frac{\sum_{i=1}^{v_n\mu_d} C(i)}{v_n\mu_d} \quad (1)$$

It can be deduced that the average probability of Packet_In is:

$$\begin{aligned} P(v_a) &= \frac{\sum_{i=1}^{v_n\mu_d} C(i) + \sum_{j=1}^{v_a\mu_d} C_a(j)}{v_n\mu_d + v_a\mu_d} \\ &= \frac{\varphi + \xi(v_a)}{N + A(v_a)} \end{aligned} \quad (2)$$

3.3 Flow feature

The feature vector of flow table is highly abstract to the state information of normal flow and abnormal flow, and the attack flow will show certain regular patterns. We can get the flow table information and analyze the change of network flow distribution characteristics in a certain period of time to detect malicious attacks. Therefore, the selection of flow feature is a necessary part of the DDoS attack detection scheme. In this paper, the following feature parameters are proposed as the basis for detecting DDoS attacks.

(1) Number of source IP address

DDoS attacks generally use IP address fraud and other attacks methods to send a large number of attack packets in a relatively short time to consume the resources of the flow table.

(2) Source IP address Generating Speed

When DDoS attacks occur, an attacker generates a large number of source IP addresses to send data packets to the injured host, and the Source IP address Generating Speed generally starts to change significantly. It can be expressed by the difference between the number of source IP addresses in two adjacent cycles $Src_Num(T_{i+1}) - Src_Num(T_i)$.

(3) Destination port number

In a cycle, the number of ports will fluctuate normally, but DDoS attackers will scan ports and choose different ports to attack. The destination port number will change significantly.

(4) Ports Generating Speed(PGS)

Under normal circumstances, the Ports Generating Speed will be relatively stable within a certain range. When DDoS attack occurs, it will choose port randomly, so the growth rate of ports will also increase. To indicate as:

$$PGS = Port_num / interval \quad (3)$$

Where $Port_num$ is number of ports, $interval$ is the time interval.

(5) Median of Bytes per flow(MBF)

In order to enhance the intensity of malicious attacks, the data packets sent by the DDoS attack are generally very short and contain less bytes. Take the number of bytes per flow as a sample, and each item in the flow table should be sorted in ascending according to the number of bytes, calculated as follows:

$$MBF = \begin{cases} b_{i+1/2} & i \bmod 2 \neq 0 \\ (b_{i/2} + b_{(i+1)/2}) / 2 & otherwise \end{cases} \quad (4)$$

Where b_i stands for item i of the sample set $B = \{b_1, b_2, \dots, b_i, \dots, b_n\}$ composed by the number of bytes in each packet, n is the number of samples, and when $\forall j$ makes $i < j$, $b_i \leq b_j$ still holds.

3.4 Detection scheme

The DDoS detection scheme is described as follows, as shown in Fig. 1.

1)Following the flow procedure specified in 3.1 section, for a packet entering the switch OFS_i which fails to match with flow table and does not know how to operate on, OFS_i will encapsulate such data in Packet_In to send to SC_j . According to the analysis of 3.2, the increase of flow will increase the occurrence probability of Packet_In in the DDoS attack. According to this, when the occurrence probability $P(v_a)$ of Packet_In reach to certain threshold $\frac{\varphi}{N}$, the alarm can be predicted.

2)Carry out the feature extraction according to 3.3 section, the SOM clustering method is used to deal with the data. When an attack is detected, the injured host is located according to the flow table information.

Fig. 1. Flow chart of DDoS attack detection.

The experimental data used in this paper consists of two parts, one part of which is normal flow, which is collected from WIDE project[5] and has typical representativeness. According to literature [6], 50.8% of normal flow adopts TCP protocol, 47.24% adopts UDP protocol, and 1.96% adopts ICMP protocol. The other part of the attack data is released by MIT Lincoln Laboratory. At present, it is still a classic dataset used to study network attacks, and its network environment is close to the real environment, having certain authority.

In this section, the results of the DDoS attack detection scheme in the designed software defined network are analyzed by simulation experiments. The simulation experiment is carried out in the Matlab2010b environment, the parameters used are set according to literature[7].

In this section, two quantitative indicators of Detection Ratio and False Alarm Ratio to judge the detection effect. They are expressed as R_d and R_f respectively, and the formulas are as follows:

$$R_d = \frac{A_a}{A_a + A_n} \quad (5)$$

$$R_f = \frac{N_a}{N_a + N_n} \quad (6)$$

Where A_a is the number of attacks being correctly detected in attack samples, A_n is the number of attacks mistakenly detected as normal in attack samples, N_a is the number of attacks mistakenly detected in normal samples, N_n is the number of attacks correctly detected in normal samples.

As a contrast, this paper carries out a comparative experiment in accordance with the method in literature [7]based on the same data. The result is shown in Fig. 2 and Fig. 3. From the figures, we can see that the detection rate of the proposed scheme is higher than that of the contrast scheme, and the false alarm rate is lower than the corresponding false alarm rate of the comparison scheme.

Fig. 2. Comparison of attack and detection results.

4 Experimental results and analysis

Fig. 3. Comparison of attack and detection results.

5 Conclusions

To solve the issue of the DDoS attack, a DDoS attack detection scheme based on self-organizing mapping network in the software defined networking was proposed. The first is to give an early warning according to the probability of occurrence of Packet_In event. If the threshold value is exceeded, the characteristics of the flow are calculated and the self-organizing mapping network is used for clustering of eigenvalues to finally detect the DDoS attack flow. The experimental results showed that the DDoS attack detection scheme based on self-organizing mapping network was superior to the comparison scheme in detection rate and false alarm rate.

Acknowledgment

This work is supported by the National Key R&D Plan (No. K17B500071), the Natural Science Foundation of Inner Mongolia (No. 2016MS0706, No. 2017MS0702), the Science and Technology R&D Plan of China Railway Corporation (No. 2016J007-B), the Institution of Higher Learning Science Research Project of Inner Mongolia (No. NJZY078) and the Science Research Project of Inner Mongolia University of Technology (No. ZD201522).

References

1. Z.A.Qazi, J.Lee, T.Jin, G.Bellala, M.Arndt, G.Noubir, *Comp. Com.* **43**,4 (2013)
2. G. Yao, J. Bi, P. Xiao, *In IEEE International Conference on Network Protocols.* (2011)
3. K. Giotis, C. Argyropoulos, Androulidakis G, D.Kalogeras, V.Maglaris, *Comput Netw.* **62**,5(2014)
4. S.Shin, V.Yegneswaran, P.Porras, G. Gu, *ACM Sigsac Conference on Computer & Communications Security* . (2013)
5. C. Kenjiro, MAWI working group traffic archive[OL]. 2016[2016-12-8].<http://mawi.wide.ad.jp/mawi/>.
6. D. E.Taylor, J. S.Turner, *Conference of the IEEE Computer and Communications Societies.* (2005)
7. R. Braga, E. Mota, A.Passito, *In Conference on Local Computer Networks.* **8** (2010)