A passive DDoS attack detection approach based on abnormal analysis in SDN environment

Shimin Sun¹, Xinchao Zhang¹, Wentian Huang¹, Aixin Xu¹, Xiaofan Wang¹ and Li Han²*

¹Tianjin Key Laboratory of Autonomous Intelligent Technology and System, School of Computer Science and Technology, Tiangong University, Tianjin, 300387, China
²National Engineering Laboratory for Computer Virus Prevention and Control Technology, School of Computer Science and Engineering, Tianjin University of Technology, Tianjin 300384, China
*Corresponding author’s e-mail: hanli@tjut.edu.cn

Abstract. Most of the detection methods against DDoS attacks are based on periodic detection, which leads to high communication overhead, untimely detection, and slow attack response. This paper proposes a passive abnormality detection approach. First, we record the two flow-table characteristics of the regular switches. Then, based on dynamic threshold method and Grubbs outlier test method, we make a determination of abnormal switches. This method reduces the amount of data duplication and regular traffic collection. Moreover, we use Support Vector Machine (SVM) algorithm to evaluate the performance of the passive anomaly detection method. The experiment results show a better performance than active period DDoS attack detection approaches.

1. Introduction

Software Defined Networking (SDN) face the same threat of Distributed Denial of Service (DDoS) attacks as traditional networks [1]. Resource-consuming attack is a typical kind of DDoS attacks in SDN environment [2]. Many studies focus on the detection methods of DDoS attacks on abnormal traffic identification method. Behal et al. [3] and Naveen et al. [4] proposed the identification methods based on parametric statistics and statistical learning techniques respectively. However, both of them rely on the controller actively requesting flow-table information from the switches periodically [5]. In a flow-table collection period, it may contain hundreds of thousands of flow entries in a large-scale network environment. The efficiency of traffic collection has become a key factor limiting the speed of detection approach response to attacks. Efficient and accurate detection approach of DDoS attacks is a new research topic in the field of SDN security [6]. Traffic full acquisition methods of adaptive frequency and sampling methods have been proposed in recent years. Chowdhury et al. [7] and Ujjan et al. [8] proposed traffic full acquisition methods that maintain a high polling frequency for flows that contribute significantly to the link. Wang et al. [9] extended a copy of the packet number counter of the flow entry to intercept the information of incoming flows in fixed time intervals, and then updated the specific flow counter copy. Houda et al. [10] utilized third-party sampling tools to separate the data collection process from SDN control plane. However, the above traffic full acquisition methods gather a large amount of repetitive traffic and regular traffic. The sampling method may miss important traffic information, resulting in untimely detection and attack response.
In this paper, we devote to detect DDoS attacks by analysing the state variation of OpenFlow switches. Then, we propose a passive abnormality detection approach, which includes the determination mechanism of the abnormal switches and trigger mechanism for traffic detection. The basic idea is that the state of the switch is monitored in real-time without incurring communication overhead. Secondly, the determination of abnormal switches is based on the dynamic threshold method and the Grubbs outlier test method. Subsequently, the DDoS attacks detection is triggered passively by abnormal events. Finally, the performance of the proposed approach is evaluated based on the SVM classification algorithm [11].

2. Methodology and Architecture Model

The architecture model of the proposed approach is shown in Figure 1. The modules are used as controller components to assist the controller to complete flow monitoring, collection, and abnormal identification.

First, based on the forwarding mechanism of flows in the OpenFlow protocol, the flow-table feature counter module monitors the flow-table space utilization rate \( U \) and the flow entry change rate \( R \), and generates a flow-table feature timing distribution diagram. From the perspective of the timing characteristics, the flow-table characteristics of the abnormal switches are obviously different from those of the regular switch. When DDoS attacks are launched, flow-table space utilization rate of abnormal switch is higher, and the flow entry change rate is larger. The distribution of attack traffic in the abnormal switch obviously deviates from regular traffic. In the abnormal determination module, based on two essential features (the flow-table space utilization rate \( U \) and the flow entry change rate \( R \)), an abnormal switch determination strategy is presented. Assume that traffic characteristics at next moment are related to the most recently recorded \( M \) historical data, through the distribution of these \( M \) historical data, the value of switch at the next moment can be evaluated. We regard the traffic that deviates from the predicted value as suspicious traffic and define the switch that forwards the suspicious traffic as an abnormal switch.

2.1. Determination of abnormal switch based on dynamic threshold

We intercept the most recently recorded \( M \) flow-table space utilization rates from the flow-table feature timing distribution diagram. The abnormal determination module dynamically predicts the upper limit of flow-table space utilization rate at the next moment based on the intercepted \( M \) features. We define the prediction upper limit as the threshold \( T_i \). We think that the current flow-table space utilization rate exceeds threshold \( T_i \), which is a necessary condition for a flooding DDoS attack to occur. The calculation method of the dynamic threshold \( T_i \) is given below:

\[
T_i = \lambda \sum_{j=1}^{M} \alpha_j U_j^i, \quad \forall i \in [1, P]; \quad \forall j \in [1, M]
\]

S.t. \[ \sum_{j=1}^{M} \alpha_j = 1 \]

(1)
where \( T_i \) is the upper limit of predicted flow-table space utilization rate for switch \( i \) and is a weighted linear combination of \( M \) historical flow-table space utilization rates. \( U^j_i \) is the \( j \)-th historical flow-table space utilization rate for switch \( i \). \( \alpha_j \) is the weight of the \( j \)-th flow-table space utilization rate, emphasizing the importance of the \( j \)-th historical flow-table space utilization rate in the threshold decision formula. The weight \( \alpha_j \) of the latter moment is greater than the weight of the previous moment. \( \lambda_i \) is the threshold influence factor, which can be dynamically adjusted according to the detection result of the current network scale. The influence factor \( \lambda \) determines the importance of \( M \) historical flow-table space utilization in predicting the feature value at the next moment. The smaller the collection period, the more reliable the prediction and the smaller the influence factor \( \lambda \). The setting of \( \lambda \) also allows bursting of regular traffic, which can be adjusted to reduce the false triggering of alarms due to bursting of regular traffic.

2.2. Determination of abnormal switch based on Grubbs outlier test
We intercept the most recently recorded \( M \) flow entry change rate from the flow-table feature timing distribution diagram. We think that the rate of change of flow entries at the next moment is the same as the historical data and will not be significantly different from the historical data. Therefore, we determine the deviation of changing rate of flow entry according to Grubbs criterion. This paper considers that the current rate of change of flow entries exceeds the Grubbs criterion value, which is a necessary condition for a DDoS attack to occur. The determination method of Grubbs outlier test is given below:

\[
\frac{|X_p - \bar{X}|}{S} > G_{p(M)}
\]

(2)

In the Grubbs formula, the average deviation and standard deviation of historical data are introduced, \( X_p \) is the tested data, \( \bar{X} \) is the average of \( M \) historical data, \( S \) is the standard deviation of \( M \) historical data, and \( G_{p(M)} \) is the value of Grubbs outlier test, where \( p \) is the confidence probability, here 95% confidence probability is selected, and \( M \) is the number of historical data. Compared with the regular flow entry change rate, the flow entry change rate in the DDoS attack is higher and positive. Therefore, the Grubbs outlier test is one-sided, and the one-sided value of Grubbs outlier test formula is as follows:

\[
G_{p(M)} = \frac{(M-1)}{\sqrt{M}} \times \left[ \frac{t^2 \left( \frac{2\alpha \alpha}{M}, M-2 \right)}{M-2 + t^2 \left( \frac{2\alpha \alpha}{M^2}, M-2 \right)} \right]^{1/2}
\]

(3)

where \( t \left( \frac{2\alpha \alpha}{M}, M-2 \right) \) denotes the value of Grubbs outlier test of the t-distribution with degrees of freedom of \( M-2 \) and a significance level of \( \alpha \).

2.3. Passive abnormality detection approach
Based on the above two abnormal determination methods, when an abnormal condition is satisfied, a passive abnormality detection approach will send out an alert and then attack detection will be triggered. Then, the flow data collection module is responsible for the traffic collection of abnormal switches. The feature extraction module extracts eight-element features that can represent the attack traffic. The classification identification module analyses the given eight-element features and determines whether they are regular traffic or DDoS attack traffic.

3. Experimental results and discussion
We set up the experimental environment using Mininet as a network simulator and RYU as a remote...
controller. The environment is deployed in Ubuntu. We built a 4-layer fat-tree network topology (Figure 2). The regular traffic and background traffic are generated using D-ITG [12]. The DDoS attack traffic is generated by Hping3. These traffic samples will be collected as the training input of the classification model. When the passive detection approach starts, flow-table feature counter module records the flow-table space utilization rate $U$ and the rate of change of flow entries $R$ for each switch device. In the generated timing feature diagram, the abnormal determination module intercepts the 100 most recently recorded switch features as the basis of the determination for the initial threshold and the value of Grubbs outlier test.

3. Performance evaluation of abnormal determination module

This experiment verifies the effectiveness of the abnormal determination for the dynamic threshold method and the Grubbs outlier test method. We randomly launch ten different DDoS attacks and set the abnormal determination period as 10 seconds and 3 seconds respectively. The experimental results are shown in Figure 3 and Figure 4.

The results show that the abnormal determination module can respond to the DDoS attacks within the given abnormal determination period in most situations. In theory, since the abnormal determination approach does not incur communication overhead, the abnormal determination period can be smaller, and the response to attack events can be fast in large-scale networks.
3.2. Performance comparison between the proposed approach and active period detection approach

This experiment compares the performance of two detection approaches in terms of both attack response delay and communication overhead. We built the same network environment for both detection approaches and randomly launched 10 DDoS attacks. The triggering mechanism of the traffic collection module is the only difference between the two detection approaches. In the active period detection approach, the controller generates a large amount of communication overhead due to the active collection of traffic. In order not to affect regular network services, the detection period of the active period detection approach cannot be set too small. The setting of period time references to the literature [13] with appropriate time $T=10s$. In the passive abnormality detection approach, the collection and identification of traffic are triggered when the abnormal condition is satisfied. As a result, the attack response delay is the sum of the abnormal determination delay and the traffic detection delay. The abnormal determination period is set as 10s and 3s. After the abnormal event is triggered, the traffic collection period is the same as that of the active period detection approach, both being 10s. The experimental results are shown in Figure 5 and Figure 6.

![Figure 5](image1.png)

**Figure 5. Attack response delay comparison.**

![Figure 6](image2.png)

**Figure 6. Communication overhead comparison.**

Figure 5 shows that since the active period detection approach collects a large amount of regular traffic, it may take multiple periods to identify an attack. Therefore, attack response delay and communication overhead of the active period detection approach are significantly greater than that of the passive abnormality detection approach. Since the passive abnormality detection approach does not incur communication overhead, the abnormal determination period can be smaller. In addition, since only the traffic of abnormal switches is collected, the attack characteristics become more obvious and attacks can be detected within one whole detection period. Figure 5 and Figure 6 show that the proposed approach can respond to DDoS attacks within one whole detection period even if the abnormal determination period is shortened to 3s.

4. Conclusion and future work

In this paper, we propose a passive abnormality detection approach based on the dynamic threshold method and the Grubbs outlier test method to determine anomalous switches. The determination relies on two characteristics (the flow-table space utilization rate $U$ and the flow entry change rate $R$) of switches. Through comparative experiment, this paper verifies the proposed passive abnormality detection approach can respond to attacks more quickly. Furthermore, since only the traffic of abnormal switches is collected, communication overhead is lower. Therefore, the method is more
suitable to be applied in a large-scale networks than other approaches. In future, we will establish abnormality detection approach to respond to new types of attacks.

Acknowledgments
This work was supported by the State Key Laboratory of ASIC & System [grant number 2021KF014]; the National Natural Science Foundation of China [grant numbers 61802281, 61702366, 61972456]; the Natural Science Foundation of Tianjin [grant numbers 19JCYBJC15800, 18JQNZC70300, 18JCTPJPC61900]; the Science and Technology Development Fund of Tianjin Education Commission for Higher Education [grant numbers 2017KJ090, 2018KJ215, 2020KJ012].

References
[1] Xu, Y., Sun, Z. (2020) Research Development of Abnormal Traffic Detection in Software Defined Networking. Journal of Software. 31: 183-207.
[2] Xu, J., Wang, L., Xu, Z. (2020) Survey on Resource Consumption Attacks and Defenses in Software-Defined Networking. Journal of Cyber Security. 5: 72-95.
[3] Behal, S., Kumar, K., Sachdeva, M. (2018) D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. Journal of Network and Computer Applications. 111: 49-63.
[4] Naveen, B., Manu, S. (2019) Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. Automatic Control and Computer Sciences. 53: 419-428.
[5] Wang, M., Lu, Y., Qin, J. (2019) A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback. Computers & Security. 88: 101645.
[6] Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., Zheng, X. (2016) SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications. 68: 65-79.
[7] Chowdhury, S. R., Bari, M. F., Ahmed, R., Boutaba, R. (2014) PayLess: A low cost network monitoring framework for Software Defined Networks. In: IEEE Network Operations and Management Symposium (NOMS). pp. 1-9.
[8] Ujjan, R. M. A., Pervez, Z., Dahal, K., Bashir, A. K., Mumtaz, R., González, J. (2020) Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems. 111: 763-779.
[9] Wang, R., Jia, Z., Ju, L. (2015) An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking. In: IEEE Trustcom/BigDataSE/ISPA. pp. 310-317.
[10] Houda, Z. A. E., Khouchi, L., Hafid, A. S. (2020) Bringing Intelligence to Software Defined Networks: Mitigating DDoS Attacks. IEEE Transactions on Network and Service Management. 17: 2523-2535.
[11] Ye, J., Cheng, X., Zhu, J., Feng, L., Song, L. (2018) A DDoS Attack Detection Method Based on SVM in Software Defined Network. Security and Communication Networks. 2018: 9804061.
[12] Aceto, G., Botti, A., de Donato, W., Pescapè, A. (2013) D-ITG: Distributed Internet Traffic Generator. PIK - Praxis der Informationsverarbeitung und Kommunikation. 36: 49-49.
[13] Xiao, Y., Fan, Z., Nayak, A., Tan, C. (2019) Discovery method for distributed denial-of-service attack behavior in SDNs using a feature-pattern graph model. Frontiers of Information Technology & Electronic Engineering. 20: 1195-1208.