Advances in Economics, Business and Management Research, volume 31

4th International Conference on Management Science and Management Innovation (MSMI 2017)

A Research Review on SDN—Based DDOS Attack Detection

Weidong ZHU
Information Center
Beijing Jiaotong University
Beijing, China
e-mail: wdzhu@bjtu.edu.cn

Xiujuan YI
School of Computer and Information Technology
Beijing Jiaotong University
Beijing, China
e-mail: 16120443@bjtu.edu.cn

***Abstract*—Software definition network (SDN) is a new network architecture, which can realize centralized control of the network by separating the control plane and the data plane. With the introduction of the control plane as a manager of the network, a single point of failure is introduced too. When the network device cannot get access to the SDN controller, the entire network will breakdown. The controller is vulnerable to distributed denial of service (DDOS) attacks, resulting in resource exhaustion, so that the switch cannot get the services of controller. In this paper, different DDOS attack methods are classified according to the different levels of attack and detection positions, and the methods are analyzed and compared. Finally, the problems of DDOS attack detection in SDN are discussed and the potentials for further research are presented.**

Keywords-component; software definition network (SDN); distributed denial of service (DDOS); OpenFlow; entropy; machine learning

I. INTRODUCTION

A. *Software Defined Network (SDN)*

Software Defined Network (SDN) is a network innovation architecture proposed by the clean slate research group at Stanford University. Its core technology, OpenFlow, separates the network device control plane from the data plane, thus realizing the flexible control of the network flow, and providing a good platform for the core network and application innovation. As shown in Figure 1, SDN's typical architecture is divided into three layers, the top layer is the application layer, including various services and applications; intermediate control layer is mainly responsible for dealing with data plane scheduling, maintenance of network topology and state information; The underlying infrastructure layer is responsible for data processing, forwarding and status collection based on flow table. The northbound interface between application layer and the control layer is the core of the open network. The generation of control layer realizes the separation of control plane and forwarding surface, which is the basis of centralized control. The SDN switch of the infrastructure layer is connected to the controller of the control layer through a trusted channel. The controller controls the switch to forward data by distributing the flow table down. Flow table is composed of multiple flow items [1]. Take the current mature OpenFlow protocol as an example, OpenFlow1.0 prescribes the flow table entries have three parts: Header Fields, Counters and Actions. The packet header field contains 12 tuples, mainly to match the data packets, as shown in Table 1. The most important feature of SDN are data forwarding and control separation, but also has a network virtualization and open interfaces and other features.

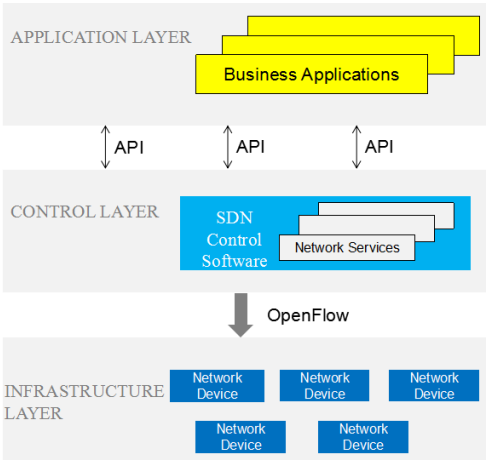

Figure 1. SDN network architecture

TABLE I. HEADER FIELD OF PACKET

Ingress Port	Ether Source	Ether Des	Ether Type	VLAN ID	VLAN Priority	IP Src	IP Dst	IP Proto	IP TOS bits	Src Port	Dst Port

Since the SDN separates the control plane and the forwarding plane, the transitions are achieved. Therefore, in the SDN, the switches do not process the incoming packets. They only look for matches in the forwarding table. If there is no match, the packet is sent to the controller for processing. The controller is a SDN operating system, processing the packet, and decide whether the packet is forwarded or discarded in the switch. By applying this procedure, SDN separates the forwarding and processing planes. If the connection between the switch and the controller is lost, the network will lose its processing plane. This means that the packet is no longer processed in the controller, and the controller gets lost, and then the SDN architecture will be lost as well. One of the possibilities that can make the controller unreachable is distributed denial of service (DDoS) attack.

B. Distributed Denial of Service (DDOS)

Distributed Denial of Service (DDOS) attack uses a sufficient number of puppet machines to generate a huge number of attack packets, launches a DOS attack on one or more targets, and exhausts the victim's resources. As a result that the host will lose the ability to provide normal network services. According to the DDOS attack principle shown in Figure 2 [2], the attacker first infiltrates the unprotected host (including the host computer and puppet machine), and then implants attack procedures. When an attack is launched, the attacker sends an attack command to the host computer. Then the attack command is issued by the host computer to the puppet machine. The attack program on the puppet machine starts from the dormant state and sends special data packets to the victim. These packet groups cannot be handled properly by the victim, thus wasting a lot of system resources of the victims. This is a serious threat to the network security. DDOS attacks are one of the most serious threats to today's network security and form a challenge to network availability. The use of bounce attacks and IP source address forgery makes attacks more difficult to detect. In the case of the current network situation, every corner of the world is likely to be attacked by DDOS, but as long as it is possible to detect such attacks and respond as much as possible, the loss can be minimized. Therefore, the research of DDOS attack detection method has been paid special attention to [3].

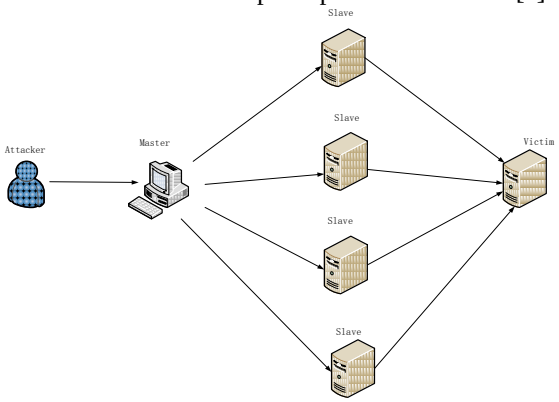

Figure 2. DDOS attack principle

In SDN's DDoS attacks [4], a large number of packets are sent to the host or group of hosts in the network. If the source addresses of the incoming packets are spoofed, which is usually the case [5], the switch will not find a match and has to forward the packet to the controller. The collection of legitimate and DDoS spoofed packets can bind the resources of the controller into continuous processing up to the point where they are completely exhausted. This will make the controller unreachable for the newly arrived legitimate packets and may bring the controller down causing the loss of the SDN architecture. Even if there is a backup controller, it has to face the same challenge.

This paper is organized as follows: In the second section, the DDOS attack in SDN is introduced in terms of three layers. Section 3 describes the current DDOS attack detection methods in SDN in different categories. Finally, section 4 includes a summary and prospects of further research directions.

II. DDOS ATTACKS IN DIFFERENT LAYERS

As is shown in Figure 1, SDN is divided into three main functional layers vertically, including the infrastructure layer, control layer and application layer. So the potential DDOS malicious attacks can also be launched in the three-layer SDN architecture. According to the possible target, we can divide DDOS attacks on SDN into three categories [6]: application layer DDOS attack, control layer DDOS attack and infrastructure layer DDOS attack.

Application layer DDOS attack: for the SDN application layer DDOS attacks, it can attack applications on top of the application, and the northbound API. Since the isolation of applications or resources of SDN cannot be solved well [7], DDOS attacks on one application may affect other applications.

Control Layer DDoS Attack: Because the SDN controller centrally controls the entire network, the controller is a particularly attractive target for DDOS attacks in the SDN architecture. The following methods can trigger a control plane DDOS attack: attack controller, northbound API, southbound API, westbound API or eastbound API [6]. For example, many conflicting flow rules from different applications can lead to DDOS attacks on the control layer. In SDN operations, the OpenFlow switch checks incoming packets (packet header fields, such as source port, destination port, source IP address, destination IP address, etc.) based on the flow entry [8], and a specified operation can be executed if a match is found. Otherwise, the packet will be sent to the controller using the Packet-In control message. When a large number of forged IP address packets are sent together, no match will be found in the flow table and packets will be sent to the controller. With this processing delay, a malicious attacker can modify a flow entry to cause a legitimate packet to be discarded, cloning a flow table entry that can cause the flow table to overflow. This is called a DDOS attack on the controller. Under this attack, the controller becomes inaccessible and cannot process the new legal packet. When the data plane sees new network packets and do not know how to process, the data plane usually requires the control plane to get traffic rules. In the case of no flow matching in the flow table, there are two options for handling new streams: transfer a complete packet or part of the packet header to the controller to resolve the query. With the increase in network traffic, sending a complete packet to the controller will take up a higher bandwidth [6] [9].

Infrastructure DDOS attacks: There are two methods to launch data plane DDOS attacks. One is attacking SDN switches of the infrastructure, and the other is attacking the southbound API. For example, if the header information is sent to the controller, the packet itself must be stored in the node memory until the flow entry is returned. In this case, it is easy for an attacker to perform DDOS attacks on nodes by setting some new and unknown streams. As the memory element of the node can be a bottleneck due to high cost, an attacker could potentially overload the switch memory (e.g., targeting to exhaust Ternary Content Addressable Memory

(TCAM). [6][9]. The generated fake request can produce many useless traffic rules that need to be maintained by the data plane, making it difficult for the data plane to store the flow rules of the normal network flow.

III. DDOS Detection Method in Sdn Environment

A. DDOS Detection Based on Entropy

Entropy can be used to determine the randomness. The main reason for using entropy for DDOS detection is that it can determine the randomness of incoming traffic. The higher the entropy is, the higher the randomness of the flow; on the contrary, the lower the entropy, the higher the determinacy of the flow [10]. Under normal circumstances, network packets have a greater randomness, so entropy is closer to the maximum possible. And when a DDOS attack occurs, a large number of illegal packets are sent to the attacked host. If the traffic is classified according to the appropriate traffic characteristics, it is found that the entropy has a sharp drop compared to the normal case. So the entropy can be used to detect DDOS attacks as an indicator.

Assuming that there are n packets in a window, pi is the probability of occurrence of each element in the window. Accordingly the entropy can be defined as:

$$H = -\sum_{i=1}^{n} p_i \log p_i \quad (1)$$

In [11], a DDOS attack detection algorithm based on entropy is proposed. The algorithm uses the characteristics of centralized control of the controller to efficiently process the information of the packet. By calculating the entropy, the DDOS attack is detected and an alarm is issued. The detection algorithm in this paper is deployed in the controller, collecting packet information of each window forwarded to the controller. The entropy of the packet in each window is calculated according to its probability distribution, and the attack is judged according to the threshold. This algorithm takes the number of Packet_In packets received by the controller as the standard for dividing the window. In order to calculate the entropy, it is necessary to classify the packets in the window according to the characteristics of the traffic, such as the source IP address, source port, destination IP address, destination port, or combination of packets. Because the SDN switch only forwards the packet to the controller when it needs to establish a new flow, and the DDOS attacker often disguises the source IP address, the algorithm computes the entropy according to the destination IP address. In general, the algorithm has the following characteristics: the change of current controller is small, parameters can be customized and system resource consumption is small. Generally, it is a lightweight DDOS attack detection algorithm. [1] Improved a DDOS attack detection method based on information entropy. The authors selected the source IP address and TTL value of the flow table to calculate entropy. The sliding window is combined with the non-parametric CUSUM algorithm to amplify the abnormal entropy to detect the DDOS attack. The method has a lower false alarm rate and higher sensitivity, less resources, faster detection speed, and very suitable for SDN environment.

Babenko [12] proposed the use of entropy calculation for DDOS detection, The proposed method records the eigenvalues of a property X in the network information stream as N, X = {ni, i = 1, 2, ..., N} it indicates that the eigenvalue appears in the measurement data ni times, $s = \sum_{i=1}^{N} n_i$ indicating the total number of eigenvalues that occur, so that the information entropy of property X in this information flow can be calculated:

$$H(X) = -\sum_{i=1}^{N} (\frac{n_i}{S}) \ln(\frac{n_i}{S}) \quad (2)$$

And then the entropy is compared with a threshold set in advance, and if it is lower than the threshold value, it is judged as an abnormality. But the shortcoming of the method proposed by Babenko is that it uses a fixed threshold to determine whether an attack occurs and that a large number of experiments are required to calculate the threshold. But the network situation is constantly changing, and a host of dropped calls or a switch downtime will have a great impact on the distribution of internal network traffic. In the literature [10], the DDoS detection method based on entropy calculation is an improvement of Babenko's method. The weighted average entropy method is used to dynamically generate thresholds. The improved method has the following two advantages on the basis of detecting DDoS attack correctly:

- Simplify the configuration process. This method does not need to use a lot of experiments to determine the fixed entropy, the thresholds are dynamically generated through the weighted average entropy method.
- Dynamically adapt to the current network status. The method averages the normal entropy of the previous calculation according to the increasing weight. It can maintain the accuracy of detection, and deal with the increased visiting flow at the same time, so as to adapt to changes in the network, and reduce the false alarm rate.

B. DDOS Detection Based on Machine Learning

With the informatization of traditional industries [10], we produce massive digital information every day. By analyzing these data, we can draw out the valuable data. Due to the huge amount of data, human processing alone is unrealistic, so we introduce machine learning.

Because the traffic characteristics in the normal state and under attack are different, the attack detection problem can be regarded as a classification problem, that is, classifying the given feature data to determine whether the current network state is normal or abnormal. The specific process is: First, select the appropriate network flow characteristics as a set of sample sequences, and add a mark for each sample sequence, that is, normal or abnormal, and then, according to the characteristics of the sample sequence to build the

classification test model, and finally, the model is used to determine the markings of the unlabeled feature samples. In [13], the flow table eigenvalues for the destination address are constructed by obtaining the flow table entries installed in the OpenFlow switch. The support vector machine is used to classify the training samples and realize the detection of DDoS attacks. The DDoS attack detection method is implemented by the prototype system and integrated into the SDN network environment, which verifies its correctness and validity. But the importance of port growth is ignored when selecting traffic characteristics. DDoS attacks will randomly generate the port number, the port number will increase dramatically. In [14], a modular DDOS attack detection method based on KNN algorithm is proposed in SDN environment. The method selects five key traffic characteristics of SDN network, and uses the optimized KNN algorithm to detect traffic anomaly of the selected traffic characteristics. Attack detection method includes three modules, flow table collection module, flow feature extraction module and classifier module. The flow table collection module periodically sends a flow table request to the OpenFlow switch. The flow table information returned by the switch is sent through the encrypted channel to the flow table collection node. The flow feature extraction module is responsible for receiving the flow table collected by the flow table collection module and extracting the five characteristics of the DDOS-related five tuples. Each five-tuple is identified by the switch ID that collects itself, and then monitors which switches have discovered DDOS attacks. The KNN classifier module is responsible for classifying the collected five tuples to distinguish whether the traffic is DDOS attack traffic or normal traffic during that time. Finally, the KNN classifier module is experimentally verified based on the NOX controller and the Net FPGA switch. Experiments show that this method has a better detection rate and a lower false alarm rate than SVM. However, the importance of the flow rate is ignored when the feature data is selected. When the attack occurs, the number of flow entry requests will also increase within a fixed time.

In [15], a DDoS attack detection method based on BP neural network in SDN environment is proposed. This method obtains the flow table entry of OpenFlow switch, analyzes the DDoS attack characteristics in SDN environment, and extracts six important features such as the success rate of flow table matching and the flow rate of the flow table. By analyzing the changes of six related eigenvalues, the BP neural network algorithm is used to classify the training samples to realize the detection of DDoS attacks. BPNN attack detection method includes five modules, flow table collection module, feature extraction module, data training module, attack detection module and attack processing module, The flow table collection module and the feature extraction module are the same as the corresponding modules proposed in [14]. The data training module uses the BPNN algorithm to train the collected eigenvalue information. The attack detection module judges whether the current network is attacked by comparing the network packets and the training results. The flow table collection module is the same as the corresponding module proposed by the feature extraction module and the literature [14]. The data training module uses the BPNN algorithm to train the collected eigenvalue information. The attack detection module judges whether the current network is attacked by comparing the network packets and the training results. The attack processing module will inform the controller to process the attack if the attack is detected. The advantage of this approach is that the key attributes of the traffic under the SDN architecture are extracted and analyzed more comprehensively, and the load of the entire network is reduced by setting the threshold. The effectiveness of the method is verified by the deployment in a software-defined network environment.

IV. SUMMARY AND OUTLOOK

The emergence of SDN (Software Defined Network) and related technologies, which has brought new opportunities for traditional network. Meanwhile, the problems of security have gradually become a bottleneck to limit its development. Especially for the current popular DDoS attacks, which have been studied for a long time, the relevant technologies are also basically mature. However, SDN is a new architecture, and there are few themes of DDoS in papers. The existing solutions are applied to the SDN, which means that SDN is regarded as a normal production network. Ignoring the role of controller, the DDoS attacks are not solved fundamentally. This paper based on the characteristics of SDN and the latest research on DDoS attack detection methods introduces the layers of DDoS attacks, and the classification of DDoS attacks is analyzed and summarized.

With the development of network attack technology, DDoS shows the characteristics of diversity, complexity and so on. It becomes more and more difficult to detect. With the rapid development of social network, mobile internet, internet of things, cloud computing and other fields, big data is increasingly becoming the current focus, and the massive data processing puts forward higher requirements for the internet. It means that we need to configure the internet frequently and call the internet resources on the basis of demands. SDN, a new example in network management, is an inevitable trend of development. Therefore, it is necessary to strengthen the detection of DDoS attack in SDN, which can limit the development of DDoS attack.

REFERENCES

[1] Yuan-Zhong Shu,Meng-Zhe Mei, “Wen-Qiang Huang et al. Research on DDoS Attack Detection Based on Conditional Entropy in SDN Environment”. Wireless Internet Technology, 2016(5):75-76.

[2] Shuo Li, Yu-Jie Du, Qing-Wei Liu.”A Summary of Defense Mechanism of DDoS Attack.” Microcomputer information, 2006, 22(2X):28-30.

[3] Fen Yan, Jia-Jia, Jin-Feng Zhao et al.”Summary of DDoS Attack Detection”. Computer Application Research, 2008, 25(4):966-969.

[4] Mousavi S M, Sthilaire M. Early detection of DDoS attacks against SDN controllers[C]// International Conference on Computing, NETWORKING and Communications. IEEE, 2015:77-81.

[5] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred,”Statistical approaches to DDoS attack detection and response”,

Proc. of DARPA Information Survivability Conf. and Exposition, Vol.1, pp.303-314.

[6] Yan Q, Yu F R, Gong Q, et al. “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges” IEEE Communications Surveys & Tutorials, 2016, 18(1):602-622.

[7] D. Kreutz, F. Ramos, and P. Verissimo, “Towards secure and dependable software-defined networks,”in Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw., 2013, pp. 55–60.

[8] Kokila R T, Selvi S T, Govindarajan K. DDoS detection and analysis in SDN-based environment using support vector machine classifier[C]// Sixth International Conference on Advanced Computing. IEEE, 2015.

[9] S. Sezer et al.”Are we ready for SDN? Implementation challenges for software-defined networks”.IEEE Commun. Mag., vol. 51, no. 7, pp. 36–43, Jul. 2013.

[10] He Li. “Research on DDoS Traffic Identification and Control Technology Based on SDN.” Nanjing University of Posts and Telecommunications, 2016.

[11] Zi-Zheng Han.”A Method of DDoS Attack Based on Entropy Detection in SDN.” Information Technology, 2017(1):63-66.

[12] Babenko T V. Research of Network Traffic Entropy as A DDoS-Attack Indicator[J]. Scientific Bulletin of National Mining University, 2013, pp. 254-256.

[13] He-Fei Li, Xin-Li Huang, Zheng-Qi Zheng. “A DDoS Attack Detection Method and Its Application Based on Software Defined Network.” Computer Engineering, 2016, 42(2):118-123.

[14] Fu Xiao, Jun-Qing Ma, Xun-Song Huang et al.” Detection of DDoS Attack Based on KNN in SDN Environment. “Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition). 2015, 35(1):84-88.

[15] Xiao-Rui Wang, Lei Zhuang, Ying Hu,et al. “Detection of DDOS Attack Based on BP Neural Network in SDN Environment.”Computer Application Research.