World Journal of Innovation and Modern Technology, Vol. 9, Issue 1 (Dec) 2026
ISSN 2682-5910
DOI: 10.53469/wjimt.2026.09(01).01

Case Design of Mitigating DDoS Attack Based on SDN Architecture

Kang Xie[1], Binghui Tang[2]

School of Computer and Software, Jincheng College, Sichuan University

Abstract: ***SDN is a new network architecture that separates the network into a management plane and a forwarding plane, simplifying network configuration and reducing maintenance costs. DDoS attack is a kind of network attack method which is easy to implement and strong attack. It lacks effective countermeasures in SDN environment. This paper presents a DDoS attack mitigation scheme based on SDN architecture. Firstly, the related concepts and technologies are briefly introduced, then entropy detection and K-Means algorithm are proposed to classify traffic, and finally deal with attack traffic to mitigate the impact of DDoS attacks on SDN environment.***

Keywords: SDN; DDoS attacks; K-Means.

1. INTRODUCTION

Today, the network environment under DDoS attacks is more widespread, and because of its simple launch and difficult to detect accurately, it is often used as a means of attack by the intruder. When a DDoS attack occurs, the flow table area of the OpenFlow exchange will overflow, depleting the controller resources, and eventually causing the network to crash.

Software defined network (SDN) is an independent controller which collects and manages network status information to achieve network centralized management and control. However, if the SDN controller is attacked by DDoS, the communication between the controller and the underlying switch will fail and the whole network will be paralyzed. This article provides a DDoS attack mitigation solution based on the SDN architecture, using generalized entropy to detect anomalous traffic and the K-Means algorithm to cluster traffic, and finally the SDN controller sends instructions to handle the attack traffic. Improved detection rate of attack traffic and SDN defense capabilities. Gvnsgxkbhzkxnkshnxkisndxksn

2. RELATED WORK

2.1 Introduction to DDoS Attacks

A form of denial of service (DoS) cluster attack is DDoS attack. Many scattered hosts form a botnet and attack a specific target with denial of service. Its purpose is to control the user host, making it vulnerable to loss or threatening others.

2.2 Principle and harm of DDoS attack

2.2.1 Characteristics of DDoS attacks at the network layer:

Using certain features of the TCP/IP protocol, a botnet is formed by controlling a large number of low-performance hosts, maliciously sending a large amount of data packets to the server, making the server resource saturation and normal business applications unanswerable.

2.2.2 Characteristics of DDoS attacks at the application layer:

It simulates the format of normal digital packet and the real IP address, avoiding the detection method based on matching features and backtracking to the source port. Disguised as legitimate users, the attacker sends a large number of reasonable requests to the target, such as downloading large files, demanding processing of complex data, etc., draining resources.

When a DDoS attack occurs, the following characteristics often appear:

(1) There are many half-connected TCP requests on the victim host;

(2) forging the source IP, issuing invalid large traffic data, causing network overload, blocking normal network communication;

(3) Take advantage of the flawed transmission protocol on the victim host to quickly issue duplicate service requests, making normal connection requests unable to be processed.

2.3 Known defensive methods

In the SDN network architecture, DDoS attack detection scheme has been quite mature research results. For example:

(1) Determine attack traffic by information entropy

Mei Mengzhe and others proposed a multidimensional conditional entropy detection method, which extracts multidimensional vectors for attack judgment by calculating the conditional entropy values of multiple flow table items [1]. Robinson et al. used a continuous window approach to calculate the information entropy error, which effectively controlled the error rate. However, there are limitations in monitoring DDoS attacks by entropy. The threshold setting is related to the network state. When the network fluctuates, the entropy changes greatly, which will affect the accuracy of detection.

(2) Attack detection using machine learning algorithms

N. Meti et al. compared SVM, Bayesian and neural network methods for detecting DDoS attacks on SDN controllers and demonstrated that machine learning algorithms can discriminate against attack traffic under SDN architecture. Xiao Fu et al. proposed based on KNN algorithm by modular distribution to refine the detection process, improve the detection accuracy, but in the case of high sample size will increase the false alarm rate [2]. The methods in the above literature take advantage of the centralized control function of the SDN controller, But too much data is processed on the controller, which in a large network significantly increases the controller's resource overhead and delays in attack detection, and SDN controllers may be overwhelmed even before attack traffic is detected.

3. DESIGN OF DDOS ATTACK MITIGATION SCHEME IN SDN ENVIRONMENT

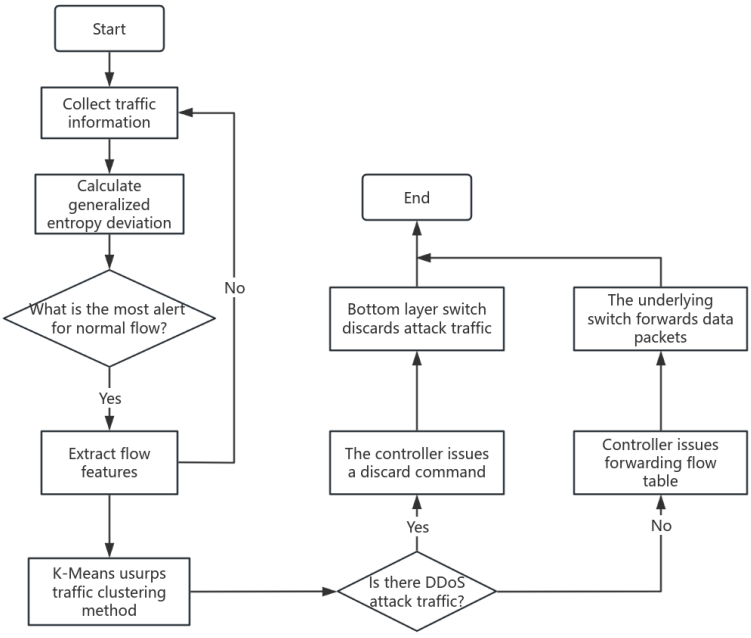

Figure:1

3.1 DDoS Attack Traffic Detection Process

The SDN controller regularly collects traffic information from the underlying switch, calculates the entropy value, extracts the flow characteristics when an exceptional traffic alert occurs, and then calls the K-means algorithm to classify the traffic to determine whether there is attack traffic. Finally, the attack flow is processed to alleviate the DDoS attack in SDN environment.

3.2 Detection based on entropy

Entropy is a general measure of the state of some system of matter and the extent to which it may occur. In information theory, information entropy as a measure of the degree of randomness of the system, the higher the certainty of the information variable, the lower the entropy; The more dispersed the information distribution of the system, the higher the entropy.

When a DDoS attack occurs, the attacker will send a large number of data packets to the victim host, causing the randomness of the network system to decline, which reduces the entropy value. Therefore, the entropity value can be used to detect the presence of a DDOS attack. The calculation formula of information entropy can be expressed as:

$$H = -K \sum_{i=1}^{w} p_i \, log_2 \, p_i \tag{1}$$

Among them, represented as the total sample of the probability space, the sample size in a single window, and the constant of the relevant unit, indicating the probability that a sample will occur.

Compared with the information entropy, the generalized form of the information entropy is more obvious in the case of high probability events, which is conducive to determining the appropriate threshold and improving the accuracy of detection [3].Therefore, we have selected general entropy for flow monitoring in this paper, whose formula is as follows:

$$H_a = \frac{1}{1-a} \log_2 \left(\sum_{i=1}^{w} p_i^a \right) \tag{2}$$

In the SDN environment, the underlying exchange uses flow table to store and forward rules. The source IP, destination IP, the number of digital packets and the IP protocol are extracted from the stream table entries as an information group.

Set each collection of n digital packet, the entropy of the information group is calculated. According to the network state, select the appropriate threshold Y.

Set 5 windows connected to detect, the data packet of a single window is 40, calculate the entropy value of each time, when the entropy value H is less than the threshold Y, it indicates that there may be attack traffic in the network.

Although the entropy value can be used to determine whether there is unusual traffic in the network, there are still events that reduce the randomness of the network under normal circumstances. Therefore, when the system has an abnormal entropy alarm, K-Means algorithm is further used to classify the traffic, and accurately screen the attack traffic.

3.3 Flow feature extraction

The stream feature extraction module is deployed on the SDN controller. Set the time interval to 4 s to collect the flow information of the underlying switching device.

Since DDoS attacks usually contain only one digital packet, the bytes are larger than normal traffic, and the gaps between digital packets arriving are very short. Therefore, four flow characteristics are selected as the input of the attack traffic detection module: packet number, time gap of packet arrival, byte length and packet average size [4].

3.4 Detection of DDoS Attack Traffic Based on K-Means

K-Means algorithm is a kind of clustering algorithm in unsupervised learning, mainly through iterative solution, further cluster all sample points, the end condition: the cluster division of the sample points are convergent to the centroid vector of the cluster, the error and the square of the local minimum. Until the central points of the clusters are stabilized, the cluster of normal traffic and attack traffic are converged.

K-Means algorithm clustering process:

Set the sample set for processing $D = \{x_1, x_2, \cdots, x_N\}$, the maximum number of iterations is N, and the number of cluster trees is K. The number of clusters after clustering $C = \{C_1, C_2, \cdots C_i\}$.

Randomly select K objects from sample set D as initial clustering centers, i.e. centroid vectors: $\mu_i = \{\mu_1, \mu_2, \cdots, \mu_i\}$.

Perform N iterations on all sample points:

(1) Initialize the partitioned cluster C as: $C = \emptyset, j = 1,2, \cdots, k$

(2) Calculate the sample x_i, and the various procardial vectors μ_j, the distance between them: $d_y = x_i - \mu_{j2}^2$

(3) Mark x as d_y, the closest cluster to meet C_x,$C_x = C_x \cup \{x_i\}$

(4) Yes C_j all the data in is recalculated for each cluster center, i.e., the centroid vector is updated: $\mu_j = \frac{1}{|C_J|}\sum_{x \in C_j} x$

(5) In these k clusters, the error sum of squares is required to be sufficiently small, that is, the centroid of each cluster is closest to the sample points of the cluster, and the calculation formula is: $SSE = \sum_{i=1}^{k}\sum_{x \in D} x - \mu_j^2$

(6) When the degree of iteration meets the termination condition or the number of iterations reaches the upper limit , output the cluster division $C = \{C_1, C_2, \cdots, C_i\}$

4. DDOS ATTACK TRAFFIC PROCESSING

After the above flow classification, the attack flow is finally processed to reduce the harm and probability of the network being attacked by DDoS.

In the SDN architecture, the attack traffic can be guided to the safe virtual device or the SDN controller through the OpenFlow switch flow table to issue the discard instruction to the switch, and discard the attack traffic [5].

Attack traffic handling steps:

(1) When the attacker launches a DDoS attack on the server, the packet arrives at the boundary switch S1 in the network. By querying whether there is a flow table item matching the flow label, if there is a flow table item, the packet is directly forwarded.

(2) If the flow table item does not exist, the flow information is uploaded to the SDN controller, and the controller judges whether the flow is DDoS attack traffic by the DDoS attack traffic detection algorithm.

(2) If it is not attack traffic, the flow table containing routing information is issued to make the switch forward the data traffic.

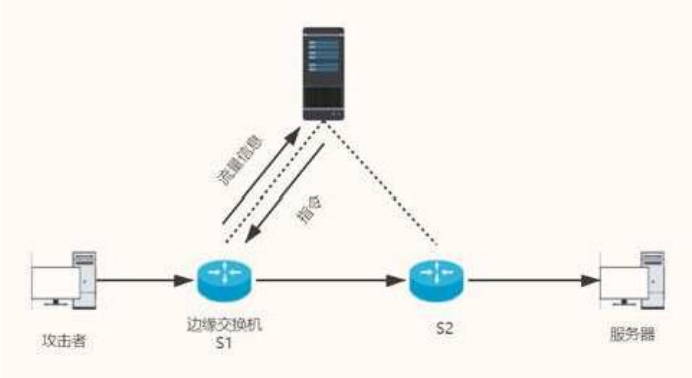

Figure:2

(4) Otherwise, the SDN controller sends a discard instruction to the underlying switch，The switch will drop the attack traffic, and at the same time, the command can be sent to the firewall to block the attack traffic, such as modifying the request timeout parameter or blocking the IP address segment, to avoid the DDoS attack traffic harming the network environment.

5. CONCLUSION

DDoS attack as a low-cost, high-harm network attack means, in the SDN environment, there is no effective countermeasures. Through generalized entropy detection, the abnormal traffic is judged, and the traffic is classified accurately by K-Means algorithm, which can effectively screen attack traffic. Finally, dealing with the attack traffic can directly reduce the harm of DDoS attacks to the SDN environment. However, with the development of the network, DDoS attacks are still evolving rapidly, making the defense scheme against DDoS attacks gradually ineffective. How to prevent the intrusion of DDoS attacks and effectively defend against DDoS attacks still need continuous technical innovation to improve the security of the network environment.

REFERENCES

[1] Mengzhe Mei. Research on DDoS Attack Detection and Defense Based on Multidimensional Conditional Entropy in SDN [D]. Nanchang University of Aeronautics and Astronautics, 2016.
[2] Fu Xiao, Junqing Ma, Xunsong Huang, Wang Ruxuan. A KNN-based DDoS attack detection method in SDN environment [J]. Proceedings of Nanjing University of Posts and Telecommunications (Natural Sciences Edition), 2015, 35 (01): 84-88.
[3] Zhenpeng Liu, Yupeng He, Wensheng Wang, Bin Zhang. DDoS attack detection scheme in SDN environment [J]. Proceedings of Wuhan University (Science and Technology Edition), 2019, 65 (02): 178-184.
[4] Lele Ma. Research on Detection and Defense of DDoS Attacks in SDN Environment [D]. Anhui University, 2019.
[5] Wenwei Wang, Junfei Xiao, Peng Cheng, Yue Zhang. DDoS attack prevention system based on SDN [J]. Computing and modernization, 2021 (02): 117-121 126.