DDOS Defense Strategy in Software Definition Networks

Luo Wenliang
Department of Computer Science
Sichuan Vocational and Technical College
SCVTC
SuiNing, China
E-mail: 183967416@qq.com

Han Wenzhi
Department of Computer Science
Sichuan Vocational and Technical College
SCVTC
SuiNing, China
E-mail: 562212867 @qq.com

***Abstract*—With the advent of the network economy and the network society, the network will enter a ubiquitous and omnipresent situation. Economic, cultural, military and social life will strongly depend on the network, while network security issues have become a common concern of all countries in the world. DDOS attack is undoubtedly one of the greatest threats to network security and the defense against DDOS attack is very important. In this paper, the principle of DDOS attack is summarized from the defensive purpose. Then the attack prevention in software definition network is analyzed, and the source, intermediate network, victim and distributed defense strategies are elaborated.**

Keywords-Software Definition; DDOS; Attack; Defense Strategy

I. INTRODUCTION

There are many kinds of software definition solutions. Some software definitions often conflict with each other, such as simplification, agility, open AP board as extension management, and self-management. Software definition is managed by policy set. After decades of development, the Internet has been widely used in social, political, economic, cultural, military and other fields, and is playing an increasingly important role. Important role [1-4]. But at the same time, computer viruses transmitted through Internet II are exponentially increasing, which also brings great harm to computer users [5-7]. In order to deal with or intercept malicious programs, anti-virus companies have to collect and analyze a large number of suspicious documents through various channels. A large part of the collected suspicious documents are their own viruses or the deformations of existing viruses. In the real sense, only a small part of the new viruses are in fact involved. The manual elimination of the viral documents in a large number of suspicious documents is a heavy workload, and it also gives anti-virus companies and diseases. Toxic analysts cause enormous trouble, so it is necessary to be able to pre-process large amounts of data [8-13]. In this paper, the defense strategies of DDOS attacks are discussed and analyzed, which are based on attack source network, victim network, intermediate network and distributed concept.

A. Overview of DDOS Attack Principle and Defense System

1) Basic overview of DDOS

The danger of DDOS attacks is often beyond people's expectations. Previously, most of the network attacks were carried out by relatively professional personnel who had been trained for a long time. It took time and effort to debug, configure and implement the attack program. Now, even ordinary people who just used computers can launch powerful attacks on top professional websites through the fool DDOS attack tools. What's more, there are a lot of automatic attack codes that can be launched at any time on the Internet. Defense against DDOS attacks is also particularly difficult. Despite a lot of research and development, from reliable computing basis, access control and physical security, multi-level security, password usage, to intrusion detection systems and loss reduction schemes such as firewalls, intrusion detection systems, boundary controllers, virtual private networks, public key heterogeneous systems, and even directly to the present. Real-time detection and response of attacks, real-time tradeoff between system functions and security costs, and intrusion tolerance are studied. But on the network,

978-1-7281-3977-7/19/$31.00 ©2019 IEEE
DOI 10.1109/ICCNEA.2019.00044

especially on the Internet, the security performance of all kinds of software and hardware is different, and users' professional level and security awareness are also different. In addition, there are a large number of attack codes that can be launched and spread automatically at any time. The research and development of DDOS attacks will still be an important challenge. Especially large-scale attack programs.

2) The Principle of Attack

In a certain period of time, a large number of specific data packets (such as service request packets, packets, etc.) are sent directly or through the springboard to the target network, which consumes the network bandwidth or system resources greatly and causes the blocking or even paralysis of the target network. It refers to the denial-of-service attack that the source node of the attack is not one or a few, but a large number of source nodes. It is a large-scale attack based on distributed and collaborative, directly or indirectly attacking the target system or network resources through other controlled computers on the Internet. Different from attacking one target with only one attack mode at a time, multiple attack modes can be run at the same time or multiple targets can be attacked at the same time. Attackers use hundreds of controlled nodes to launch large-scale cooperative attacks on the victim nodes. By consuming resources such as bandwidth, memory and so on, the performance of the attacked end is degraded or even paralyzed and crashed, thus causing other legitimate users to be unable to access normally. Compared with the former, the latter is more destructive and harmful, involving a wider range, and harder to find attackers. Among many network security problems, attacks become one of the most difficult network security problems because of their easy implementation, difficult prevention, and difficult tracing. And its attack effect is very obvious. Servers or network devices cannot provide normal services for legitimate users for a long time, which seriously affects the development of e-commerce, e-government and other network applications.

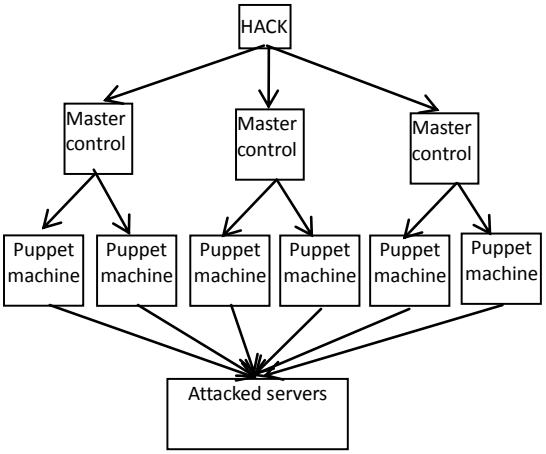

Figure 1. Is the attack principle of DDOS.

3) Flow chart of defense system

Figure2 shows that the whole defense system needs to maintain two databases, IAD (IP Address Database) and Attack IP Address Database (AIAD). IAD is the IP address of the normal package that visits the website frequently, i.e. Frequent IP Address. AIAD is the IP address of the attack packet when an attack occurs. The operation steps of the system are as follows:(1) Detecting whether an attack occurs: The system is based on the ability to respond in time when an attack occurs. Therefore, it is necessary to adopt effective detection algorithm for detection. When an attack is detected, enter 2).(2) Otherwise, learn IAD and update IAD. Determine whether the source address is in IAD: If the source address is in IAD, it indicates that the source address is the legitimate address that is frequently accessed, and the data packet is regarded as normal traffic, it can be passed through. Otherwise, the feature rules of attack packets are extracted. And update AIAD. Enter 3).(3) Determine whether the address is in AIAD: If the source address is in AIAD, it means that the source address is the DDOS attack source address, regard the packet as the attack package, and consider it carefully. Otherwise, for normal flow, through.

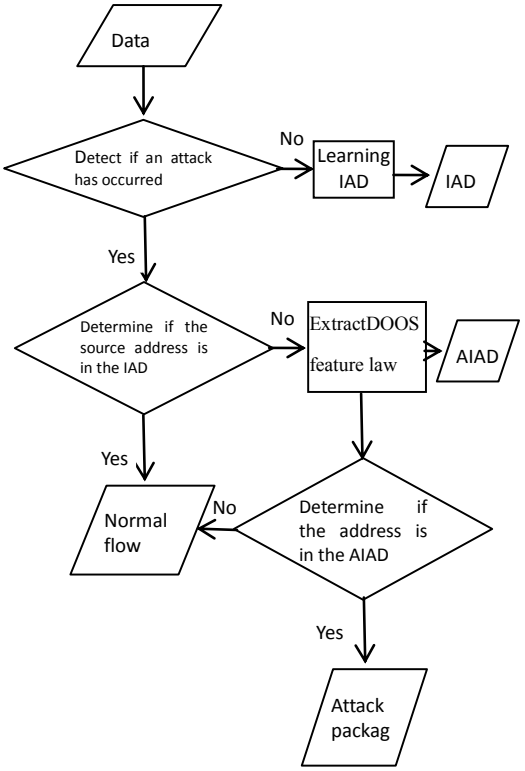

Figure 2. Flow chart of defense system

II. Software Definition Network Attack Prevention

A. Suspicious Document Software Detection

Some software is mostly non-profit and free to serve the vast number of netizens. It scans the uploaded suspicious files online through the latest version of virus detection engine provided by various manufacturers, and can display the test results, thus providing you with suspicious suggestions. At the same time, these websites provide suspicious documents and analysis reports for anti-virus vendors, update their software through anti-virus vendors, and benefit more and more users. The general process of online detection software is to open the home page, select the file you want to upload, select the file and click the "Send Document" button. Then it will upload your files to the server of the website and analyze them. Later, it will observe the scanning results. In the scanning results, it will show the number of virus scanned, as well as the name, version, and virus library date and virus name of the anti-virus software. If shown as, it means that the file is basically secure.

B. Antivirus Cloud Technology

Anti-virus cloud is a computer "cloud" by transferring virus analysis. The anti-virus system uses multiple anti-virus engines to virtualize and parallelize detection functions, which can significantly increase overall protection. Anti-virus cloud mainly uses cloud computing model to transfer the main function end of virus protection to cloud server. On the server side, the anti-virus engine running in the virtual machine sandbox is combined to protect the virus, and the network flow sensor is established to detect the executable files before entering the client. In addition, the anti-virus cloud has faster processing speed and analysis results than traditional anti-virus software, including what researchers call "retrospective detection". It is not a simple task to analyze executable files through network services. Suspicious executable files must be acquired and isolated so that they can be sent to the upper analysis services. Analysis services must be effective and malware must be blocked.

C. Key Points in Software Virus Detection

Detection rate and false alarm are two very important indicators in anti-virus software evaluation, and in the process of co-use of multi-anti-virus software, the improvement of detection rate is also the most mentioned problem. However, detection rate and false alarm is always a pair of contradictions. Without the innovation of algorithm, the pursuit of high detection rate will increase while false alarm will also increase, and the detection rate after reducing false alarm will also be affected. Detection rate and false alarm are two very important indicators in anti-virus software evaluation, and in the process of co-use of multi-anti-virus software, the improvement of detection rate is also the most mentioned problem. However, detection rate and false alarm is always a pair of contradictions. Without the innovation of algorithm, the pursuit of high detection rate will increase while false alarm will also increase, and the detection rate after reducing false alarm will also be affected. Proportion of virus files. The false alarm rate refers to the percentage of the false alarm event information in the

total event information in a certain period of time, that is, the proportion of the number of times that the anti-virus software recognizes the normal event as an attack event and alarms the behavior. Misinformation is the most worrying thing of anti-virus software, and it is inevitable that any anti-virus software may have false alarm and killing, which is inevitable, just like any software has vulnerabilities, but in the case of assurance, it can minimize false alarm.

III. Defense Strategy of DDOS Attack

A. Source Policy

In this strategy, defense nodes are deployed on the Internet's entry router. These nodes constantly observe the data packets passing through the router, and find that there may be an attack, then filter and limit the flow of the exit packets. In the D-WARD strategy, the source router sends the bidirectional packets to the defense nodes, which flow into the source network and out of the source network. The node carries out real-time traffic statistical analysis on these data packets, and compares the statistical value with the normal traffic model that was set up beforehand, and classifies the data packets by comparing. Packets that are inconsistent with the traffic model will be filtered out, while other packets will be limited by traffic. The analysis of bidirectional packet is very important. It is difficult to judge intrusion only by outgoing packet, because the outgoing packet of DDOS attacker is much more than the incoming packet. For example, in TCPSYN attack, because of the forgery of a large number of IP addresses, the real attacking packet sender can only receive very few ACK reply packets. In this way, the attack packet is intercepted as early as possible, which prevents it from entering the core of the Internet and mixes it with legitimate traffic, thus reducing the congestion of the victim network.

B. Intermediate Network Strategy

The consumption of network resources by DDOS attacks is not only reflected in the attacked network, but also in the intermediate network from the proxy host to the target host. In the defense strategy of intermediate network, defense nodes are usually located on the core router, which detects anomalies through the anomaly detection mechanism on the router, and restricts the flow of data. Because there are a large number of data packets flowing through the core router, once the attack is successfully detected, it can be quickly suppressed; when the attack reaches the victim end, its harm has been minimized.

C. Victim End Strategy

Due to historical reasons, most of the DDOS defense systems are designed based on the application of the attacked side, which is easy to understand, because the attacked directly suffered from DDOS attacks and suffered losses, there is an urgent need for DDOS defense system. In the victim-side strategy, defense nodes are deployed on the boundary router of the victim-side network, responsible for attack detection and corresponding traffic restrictions. Because of the proximity to the victim, it is very easy to detect abnormalities.

D. IP Filtering Strategy

Early DDOS attack flow types were often very limited. However, recent research indicates that current DDOS attack packets often use randomly generated spoofed source addresses, source ports, and even payloads. This makes effective filtering of attack packets increasingly difficult, requiring more advanced traffic modeling techniques. Therefore, using hash technology to establish an efficient IP search technology to solve, use $S_i = \{S_1^i, S_2^i, S_3^i, ...S_n^i\}$ to indicate the set of all legal IP addresses that appear on the network on day i, where $|S_i| = n_i$. $F^k = \{f_1, f_2, f_3, ..., f_m\}$ is used to represent a set of constant IP addresses from day 1 to k, where $|F^k| = m$. Use $A = \{a_1, a_2, a_3, ...a_x\}$ to indicate the IP address that appears in the DDOS attack. Because a network is frequently accessed, it is a relatively fixed set of IP addresses. As we analyzed earlier, DDOS attacks use randomly forged IP addresses. The following is the relationship obtained by observing the k-day flow:

$$|S_1 \cup S_2 \cup ... \cup S_k| < \sum_{i=1}^{k} n_i << |A|$$

E. Distributed Strategy

It can be seen from the discussion of the above three strategies that a single-point strategy cannot effectively prevent DDOS attacks. Effective strategies should include three sensitive locations, victim, intermediate network and source, which lead to the concept of distributed strategy. In the distributed strategy, defense nodes with different functions are deployed in at least two locations in three locations, and each node completes attack detection and response through cooperative mode of work. Distributed defense system combines attacker-side defense, source-side defense and intermediate network defense. The defense of the attacked side is responsible for detecting the attack, transmitting information to other participants, and other participants are responsible for curbing the attack flow. The ultimate goal is to establish a response at the node as close as possible to the source so as to effectively contain the attack flow and avoid indirect damage to the legitimate flow. Distributed strategy. Because of the separate deployment of detection and response points, the detection accuracy and response speed are improved. Especially, the strategy combining the victim, the intermediate network and the source is very effective for DDOS attack defense. This strategy can filter and control attack data packets from the source to the victim layer, and provide a good quality of service for legitimate data packets.

IV. Conclusion

At present, DDOS attacks have become the main threat to the stable operation of the Internet. This attack can be easily implemented. Any ordinary user can download DDOS attack software from the Internet and successfully implement DDOS attack. Moreover, attackers usually use counterfeit source IP addresses, which makes it difficult for attackers to be tracked. DDOS attacks are easy to launch and difficult to track, and DDOS guided attacks occur widely.

References

[1] Zhang J, Yang Z, Wang J, et al. SDN Communication Quality Assurance Strategy with DDoS Defense and Routing Optimization[J]. Telecommunications Science, 2015.

[2] Li C, Yan W, Yuan X, et al. Detection and defense of DDoS attack–based on deep learning in OpenFlow‐based SDN[J]. International Journal of Communication Systems, 2018(2):e3497.

[3] Zheng J, Namin A S. The Impact of Address Changes and Host Diversity on the Effectiveness of Moving Target Defense Strategy[C]// Computer Software & Applications Conference. 2016.

[4] Sadr M A M, Ahmadian-Attari M, Amiri R, et al. Worst-Case Jamming Attack and Optimum Defense Strategy in Cooperative Relay Networks[J]. IEEE Control Systems Letters, 2018, 3(1):1-1.

[5] Cui Y, Yan L, Li S, et al. SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks[J]. Journal of Network & Computer Applications, 2016, 68:65-79.

[6] Jakaria A H M, Rashidi B, Rahman M A, et al. Dynamic DDoS Defense Resource Allocation using Network Function Virtualization[C]// ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security'17). 2017.

[7] Jiang Y, Zhang X, Quan Z, et al. An Entropy-Based DDoS Defense Mechanism in Software Defined Networks[J]. 2016.

[8] Zhang J, Yang Z, Wang J, et al. SDN Communication Quality Assurance Strategy with DDoS Defense and Routing Optimization[J]. Telecommunications Science, 2015.

[9] Gulisano V, Callau-Zori M, Fu Z, et al. STONE: A streaming DDoS defense framework ☆[J]. Expert Systems with Applications, 2015, 42(24):9620-9633.

[10] Jog M, Natu M, Shelke S. Distributed capabilities-based DDoS defense[C]// International Conference on Pervasive Computing. 2015.

[11] Gong D, Tran M, Shinde S, et al. Practical Verifiable In-network Filtering for DDoS defense[J]. 2019.

[12] Widagdo G B, Lim C. Analysis of Hybrid DDoS Defense to Mitigate DDoS Impact[J]. Advanced Science Letters, 2017, 23(4):3633-3639.

[13] Kalkan K, Altay L, Gür G, et al. JESS: Joint Entropy-Based DDoS Defense Scheme in SDN[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(10):1-1.