Distributed Collaborative DDoS detection method based on traffic classification features

Xiong Zeyu, Wang Yongjun, Wang XiaoFeng
School of Computer Science
National University of Defense Technology
ChangSha410073 P.R. China

***Abstract*—This paper classifies the DDoS attack prevention technology from the view of defense stage and defensive position. DDoS attacks have relatively low proportion of normal flow in the boundary network at the attack traffic, and the characteristics of the network are not very obviously. For these characteristics, design and implement collaborative detection of DDoS attacks method are proposed. Simulation results show that the distributed collaborative DDoS detection method has good timeliness, accuracy and scalability than the single-point detection and route-based distributed detection scheme.**

Keywords-Traffic classification;distributed collaborative; DDoS

I. INTRODUCTION

Internet security elements including many aspects: confidentiality, integrity and availability. For different security elements have different forms of attack. Such as network packet interception and eavesdropping threat to the confidentiality of the data, malicious tampering of messages will threaten the integrity of the data. DoS and DDoS attacks are the main forms of attack for availability [1]. DDoS attacks are distributed, an attacker initiated this attack by manipulating distributed Internet puppet host of different locations at the same time. When the stream of attacks from different puppet host converged, the stream at victim host will become very large, and will soon become system halted or network congestion.

DDoS attacks have become one of the major Internet security threats, but DDoS attack prevention have no breakthrough in the forecast and counterattack. The general view in the industry today, DDoS attacks is difficult to avoid in basic architecture of the Internet, the research hotspot focous on distributed prevention policy research. Yu et al [3] have suggested aroute-based distributed detection scheme. Debra L Cook et al[4] have researched a single-point detection scheme,but not able to predict the DDoS attacks accurately.

This paper focus on the design and implementation of distributed collaborative DDoS detection method designed and implemented a collaborative DDoS attacks detection method. For the abnormal obvious hidden DDoS attacks that causing network traffic anomaly is not obvious. The system is suitable for the hosts that are close to the source of the attack, such as border routers, this can detect the DDoS attack before the attack traffic arrived or serious harm caused to the victim host. It will improve rapid response capability in the network suffered DDoS attacks, and reduce the DDoS harm to the network. We simulate and analyze the timeliness, accuracy and scalability of distributed collaborative DDoS detection method, and compare with the based routing distributed detection method and single-point detection method, it will show the advantage of our method.

II. PROBLEMS OF DISTRIBUTED DDOS DETECTION

Distributed denial of service attack by means of the client/server technology, combine multiple computers together as an attack platform to launch a DoS attack on one or more target, thereby exponentially increase the power of denial-of-service attacks. Usually, the attacker uses a steal account to install DDoS master program on a computer, the master program build a large number of communication with agent programs, the agent program has been installed on many computers on the Internet. The agents received the instruction and start the attack. By the use of client/server technology, the master control program can activate hundreds of agent programs in few seconds.

Hackers usually do not go directly to control puppet machines, but to transmit the attack traffic on puppet machines, it is one of the reasons that DDoS attacks are difficult to trace. From the view of the attacker, who certainly do not want to be exposed, while more puppet machine the attacker used, the victims will get more evidence to analyze. After the occupation of a machine, the senior attacker would consider how to build back door and clean out the log. If the attacker deleted the entire log, the administrator will know that is was once the invasion, people cannot see the exception if the attacker pick the relevant log to delete, so the attacker can control puppet machine for a long time.

There are variety types of DDoS attacks, divided into the following four categories in accordance with the different angles [2]: IP Spoofing Attack, Ping of Death attacks, Teardrop attacks and Smurf attacks. DDoS attacks developed rapidly since the late 1990s, and significantly increased its defense difficult than other dorms of attack. The distributed nature of DDoS attacks is significantly, the attack preparation time is getting shorter, the automation and imperceptibility are getting better, attack power and attack range are increasing.

Published by Atlantis Press, Paris, France.

III. DISTRIBUTED COLLABORATIVE DDOS DETECTION METHOD

The design of distributed collaborative DDoS detection method including four modules: information gathering, local detection, information fusion and global decision.

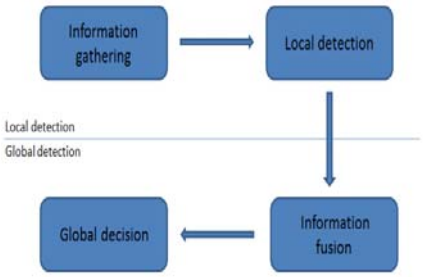

Figure 1. Steps of Distributed Collaborative DDoS detection

Detection of DDoS attacks focused on the number of message which has a specific IP address as the destination IP address. However, in the actual situation, the IP address space is huge, it is impossible to record the number of each destination IP address one by one. Therefore, we use the popular Sketch data structure [5] records the number of packets at different destination IP addresses. Whenever a packet arrives, detection nodes extracted destination IP address from the packet as the Key value, and then update the Sketch data structure. Information collection on detection node divided with a fixed sampling interval, each sampling interval generates a Sketch data structure called summary matrix. The data collection of system is basically completed by Libpcap. Libpcap (Packet Capture library) is developed by the Lawrence Berkeley National Laboratory, University of Berkeley Research Institute. Through direct access to the data link layer, by use of BPF (Berkeley Packet Filter) mechanism in Linux, it works for application layer to capture the underlying packet.

The task of local detection is to extract useful information for DDoS detection from summary matrix. Detection nodes save the current and the previous sampling interval summary matrix. At the end of the sampling interval, for each entry in summary matrix, detection node calculates the degree of change, a positive value indicates an increase, and a negative value indicates a decrease. If the ratio of the change is greater than the threshold value α , we consider the entry as suspicious entry. Mapped to the destination IP address of the entry may have been under DDoS attack. The threshold affects the result of collaborative DDoS detection. If the setting is too large, it may lead to underreporting rate. Extreme cases may regard the entry which ratio is positive as suspect entry. According to parameter settings, each entry corresponding to 216-220 IP addresses, therefore it consume a lot of resources to find the IP address from Sketch reverse. Reverse Sketch [6] directly solve the above problem.

Each detection node makes initial integration for shared information received. For each entry, it calculates the number of all the received shared information on a sampling interval value and the current sampling interval value, so that the plurality of messages combined into one, it effectively reduce the number of messages. In this process, if the detection node receives a certain number of shared information from other detection nodes, and in all of these information, the ratio of information which report an suspect entry is less than the threshold value b, we consider that the suspicious do not have universality, does not comply with the characteristics of a DDoS attacks, such suspicious entry in the fusion process is discarded.

After the initial integration of information, the information will forward to the destination node. Such information includes the suspicious entry address, the value of entry in the current and previous sampling interval, and the number of partial information after fusion. The final destination of this information is destination detection node, which becomes the final decision node. Compared with the sampling interval before, if an entry value in the current sampling interval have a change greater than a certain threshold value, and the number of detection node which reports this abnormality entry also reaches a certain percentage, it is determined that the destination address associated with the entry may have been under attach. After analysis of the information in the received partial information and after fusion, the decision node will obtain a set of entry. These entries is considered to be associated with the destination IP address, and the work to find the destination IP address will accomplish by Reverse Sketch. Reverse Sketch is able to fund the IP address associated with a known entry rapidly. Each IP address is mapped to H entries in Sketch structure by different hash function. In H entries which an IP address corresponding to, if the ratio of attack entry number is greater than a certain percentage, we consider that the destination address is under DDoS attacks.

IV. RESULT OF SIMULATION EXPERIMENT

In simulation experiment of collaborative DDoS detection, we have deployed a large network consisting of 65 nodes, the DDoS attack is launched by 15 edge nodes, and the destination is the 67th node in Area 7, in order to run out of the server's resources to achieve the purpose of denial of service soon.

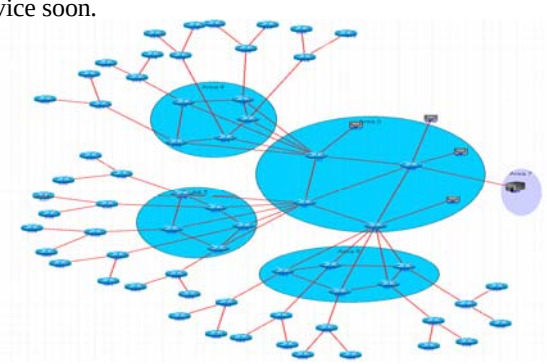

Figure 2. Network topology in experimental deployment

On the timely analysis on three different detection scheme: route-based distribution detection, distributed collaborative detection and single-point detection, we use the time difference Δt between attack detected and began as an indicator, and analyze the timeliness of different methods, and detect the attack degree of target node when the alarm generate. Comprehensive evaluation of the attack degree is calculated by CPU usage, memory usage, and bandwidth usage.

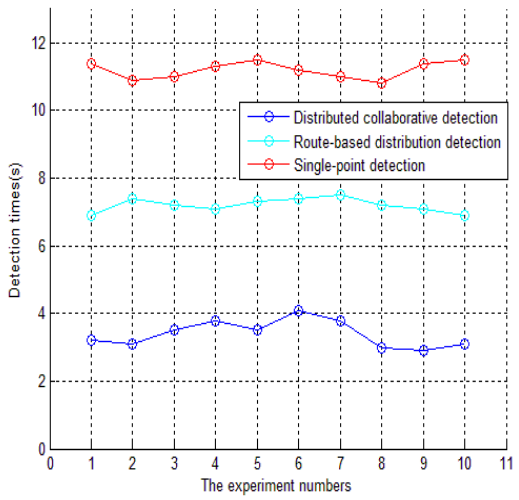

Figure 3. Timeliness contrast of three detection scheme

Among them, the detection time of distributed collaborative detectionis3.4s, the route-based distribution detection scheme is 7.2s, and the single-point detection scheme is 11.2s.

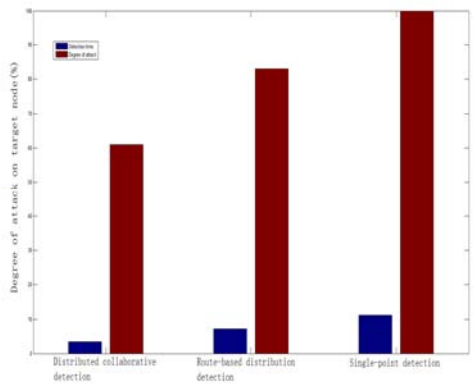

Figure 4. Degree of attackon target node when program generates the attack alarm

When the program generates the attack alarm, the degree of target under distributed collaborative detection scheme is 61%, the route-based distribution detection scheme is 83%, and the single-point detection scheme is 100%.

Analysis on the experimental data, from the indicator of timeliness, compared to route-based distribution detection scheme and single-point detection scheme, our detection scheme have more timely, when our detection scheme make an attack alarm, the attack degree of target node is the lowest.

In the accuracy of the analysis of three different detection schemes, we use two indicators: detection rate and false positive rate, which are mentioned above. For different three detection scheme, we carried out 10 experiments, each set of experimental batches attack node send 10 attack streams, through statistic, we get the total number of attack, the number of alarm, and the number of false alarm in each scheme. Finally, we calculated the average detection rate and false positive rate of three different detection schemes.

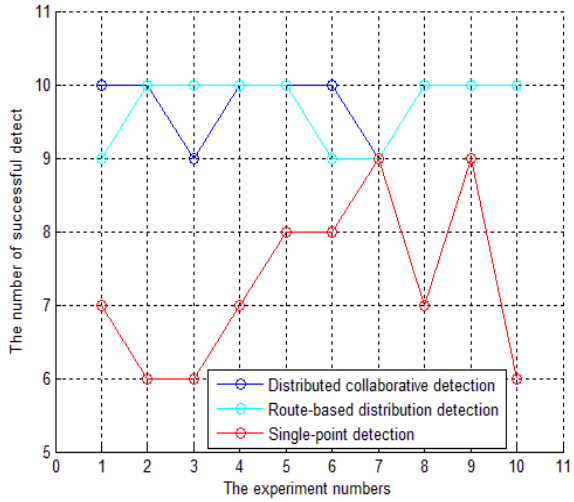

Figure 5. The fluctuations of number that three detection scheme successfully detect the attack

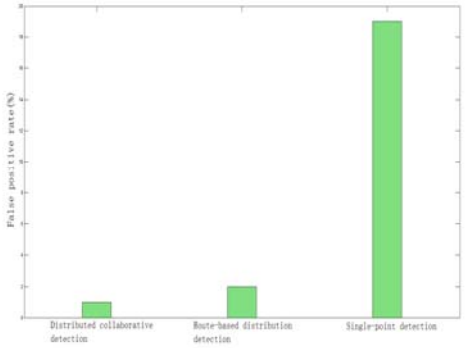

Figure 6. The average false positive rate of the three detection scheme

Distributed collaborative detection scheme get the false positive rate of 1%, the route-based distribution detection schemeis2%, and the single-point detection scheme is 19%.

After the analysis of the experimental results, we found that distributed collaborative DDoS detection scheme and route-based distribution detection scheme have a higher detection rate and low false positive rate, but single-point detection scheme has a lower detection rate and a higher false positive rate.

V. CONCLUSIONS

In this paper, we propose a distributed collaborative DDoS detection method. We use Libpcap packet to capture the network traffic packets, and use Sketch structure to store traffic information. On this basis, we design the local detection module to filter the suspicious information preliminary, by monitoring the transmission of information sharing so as to achieve the effect of distributed collaborative detection, and finally we design the global decision-making module for final decision-making. In the future, we will further analyze the relationship between the distribution of the nodes and detection results, in order to improve the performance of the detection scheme.

ACKNOWLEDGMENT

The work was partially supported by the the National Natural Science Foundation of China (No.61202333) and the Research Fund for the Doctoral Program of Higher Education of China (No.20104307110003).

REFERENCES

[1] Li Jun, “Comprehensive Analytical of DDoS attack. Network security technology and application” , pp. 8-10, September 2007.9(Chinese).

[2] Li Yanheng, “Research on DDoS Detection Technology”. National University of Defense Technology. 2006. (Chinese)

[3] Yu Chen, Kai Hwang, Wei-Shinn Ku, “Collaborative Detection of DDoS Attacks over Multiple Network Domains,” IEEE Trans. Parallel Distrib. Syst. Vol.18, 2007, pp. 1649-1662 .

[4] Debra L Cook, William G Morein, Angelos D Keromysis, etc, “Websos Protecting web servers from ddos attacks, ” Proceeding of the 11th IEEE Internationaleon Conference on Networks(ICON), USA, Columbia University, 2003.

[5] Krishnamurthy B, Sen S, Zhang Y, Chen Y, “Sketch—Based change detection: Methods, evaluation, and applications,” Proc, of the ACM SIGCOMM Internet Measurement Conf. New York: ACM Press, 2003, pp.234-247.

[6] Schweller R, Li ZC, Chen Y, GaoY,Gupta A, “Reverse Hashing for High-speed Network Monitoring: Algorithms, Evaluation, and Applications.” Proc.Of the 25th IEEE Int’l Conf. on Computer Communications. New York: IEEE, 2006. pp.1397-1408.