A Novel Distributed Denial of Service (DDoS) Attacks Discriminating Detection in Flash Crowds

[1]B. Saritha, [2]C. Rajasekar

[1]M.Tech from Siddhartha Educational Academy Group of Institutions, JNTU Anantapur, A.P.
[2]Assistant Professor, Siddhartha Educational Academy Group of Institutions, JNTU Anantapur, A.P

Abstract: *A Distributed denial of service (DDoS) attack is a most popular and crucial attack in the internet. Its motive is to make a network resource unavailable to the legitimate users. Botnets are commonly the engines behind the attack. In our deep study of the size and organization of current botnets, found that the current attack flows are usually more similar to each other compared to the flows of flash crowds In this paper we are concentrating flash crowd and DDoS there are two steps involved, first it is necessary to differentiate normal traffic and flash crowd by using Flash Crowd Detection Algorithm. Second we have to differentiate flash crowd and DDoS by using Flow Correlation Coefficient (FCC). By using this FCC value, algorithm proposed called Adaptive discrimination algorithm is used to detect the DDoS from the flash crowd event. And a sequential detection and packing algorithm used to detect the attacked packets and filter it out .By using above mentioned algorithms we can improve the accuracy in filtering the attacked packets and also the time consummation is reduced.*

Keywords: *Flow Correlation, botnets, DDos.*

1. INTRODUCTION

A network is a group of or two or more computer systems linked together. There are many types of computer networks are available. Communication between the systems are carried out by message passing, while passing message some types of attacks may occur to collapse the actual message. The attacks are classified as two types they are Active and Passive. An "active attack" tries to change system resource. A "passive attack" tries to learn or make use of information from the system but does not affect system resources (E.g., see: wiretapping). we are concentrating on Active attacks .Our focus is DDoS (Distributed Denial of Service Attack) it is one type of active attack.

DDoS stands for Distributed Denial of Service attack. It is a form of attack where a lot of zombie computers (infected computers that are under the control of the attacker) are used to either directly or indirectly to flood the targeted server(s) – victim, with a huge amount of information and choke it in order to prevent legitimate users from accessing them (mostly web servers that host websites). In most cases, the owners of the zombie computers may not know that they are being utilized by attackers. In some cases, there is only a periodic flooding of web servers with huge traffic in order to degrade the service, instead of taking it down completely.

In recent days DDoS is one of the main threats in the internet. there are many solutions have been proposed but still there is a problem in the internet world for that we are proposing an efficient algorithm to detect the attack and also filtering the attacked packets .In general computing environment, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to the legitimate (actual) users.

Types of DDoS attacks are

☐ Consumption of computational resources

☐ Disruption of configuration information

☐ Disruption of physical network components

Current DDoS attack remains a high security threat to IT security on the Internet. The attacks are carried out by attack tools, worms, and botnet with the help of attack variants of packet transmission

such as TCP/SYN, UDP and HTTP request floods [5]. These are the sources of DDoS attack. They are powerful and can crush any server and host. Now the main challenges for DDoS attack detection are flash-crowd attack.

Flash-crowd attack [6] is the phenomenon of a high dense of illegitimate packets from attack sources. The attack traffic is viewed the same as legitimate users' traffics (called flash crowd). Attack sources pretend to be real users and pump a large volume of request packets that flood the target victim. In this case, the defense/detection system could be beaten and the server has difficulty surviving the attack which causes it to crush or degrade the servers' performance.

Statistical-based defense systems [7] against DDoS attacks based on header information from IP packets such as IP address, time-to-live (TTL), protocol type (port number), etc. The detection can discriminate "normal" traffic from "abnormal" traffic which is more likely to be an attack. However, some botnets, e.g. Mydoomcan bypass detection approaches through the victim. This is because the approaches consider the Transport layer and/or Network layer. Therefore, the botnets which generate similar legitimate HTTP packets can avoid detection. Even though the attacking HTTP traffic is aggregated, they still look like flash crowd.

Heuristic-based defense systems [8] against DDoS attack based on the threshold value. Each approach may need to calculate its own threshold value to critic the current observing traffic. The drawback of heuristic detection approaches is their inability to consider legitimate traffic mixed with attacking traffic. Hence, packets from legitimate users may be blocked or eliminated during attack incidents occur.

In this paper we propose solution to detect the traffic pattern of the packet by perceiving packet arrivals. Proposed technique is an effective method to discriminate packets among DDoS attack sources and actual users. . The packets from the attack sources must be eliminated, but the user packets must get through the server. The contributions of the paper are listed as follows

• **Fast detection**: The system must be able to detect the DDoS attacks in time.

• **Reliability**: The system must not cause false positive and false negative in results.

• **Accuracy:** The system must be able to respond as soon as the flash-crowd traffic arrives at the server.

• **Flexibility:** The system must be able to detect all form of attack packets such as malformed IP, TCP, UDP, ICMP, etc.

In the above diagram the users are sending data packets to the server within the time period as mentioned in the fig-1, acknowledgement is received by the user. for eg. Number of packets sent by the user is 50 per second means,if number of packets has increased means traffic will also increase either it would be a flash crowd or DDoS.

Flash crowd is also one type of attack, it is a large surge of traffic on a particular web site causing dramatic increase in server load and putting severe strain in network on the network link leading to the server which results in considerable increase in packet loss and congestion.
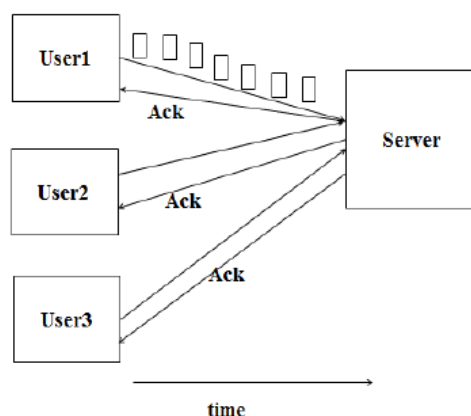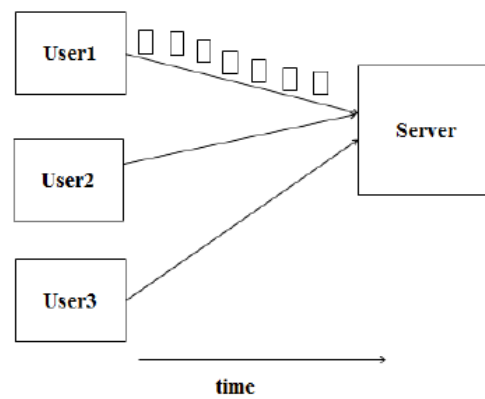

Fig-1. *(normal traffic)*

Fig-2. *(DDoS attack)*

In the above diagram users are sending packets to the server. if the acknowledgement is not received means there is a DDoSattack.
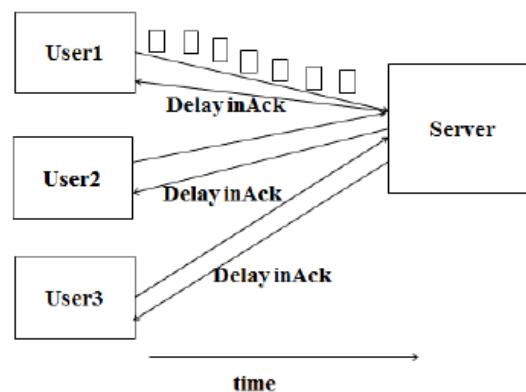

Fig-3. *(flash Crowd attack)*

In the above diagram users are sending high volume of packets to the server. Congestion will occur acknowledgement will come but some delay will arise then it is a flash crowd event.

2. RELATED WORKS

As the damage by DDoS attack increases, a great number of detection methods have been presented. Many of these methods are based on identifying anomalies in network traffic.

Ke Li, Wanlei Zhou [1] proposed novel approaches using probability metrics to discriminate DDoS and flash crowd attacks .These methods identify the flash crowd attacks efficiently from the DDoS attacks and also minimizes the false positives and false negatives while identifying the attacks. Probability metric approach failed to maintain the same accuracy to discriminate the flash crowd attack for huge attack traffic.

Shui Yu, TheerasakThapngam [2] proposed three metrics for information distance measures, the Jeffrey distance, the Hellinger distance, and the Sibson distance used to discriminate the flash crowd and DDoS attacks. The flow similarities are used to calculate the information distance and they proved that Sibson distance metric is more accurate in discriminating flash crowd attack. But the accuracy of discriminating the attacks is limited to 65%, which results the poor accuracy. TheerasakThapngam and GlebBeliakov [3] proposed discriminating method based on the packet arrival patterns. Pearson's correlation coefficient is used to define the packet patterns. Here patterns are defined by using the repeated properties observed from the traffic flow and also calculates the packet delay. Defining the packet pattern and discriminating the flash crowd attacks using pattern or packet delays are difficult for large flows.

Jie Wang, Raphael C.W.Phan, John [4] simulated both DDoS traffic and Flash Crowds traffic by designing a special test bed-based simulation method with Spirent Test Center hardware platform. This method detects only port based flash crowd attacks but they failed to detect for application and other flash crowd attacks.

3. PROPOSED WORKS

Consider the situation where a server is overwhelmed by flash crowd flows and/or DDoS attacks as illustrated in Fig.4. A server connects to the Internet and provides a service to public Internet users. Legitimate users do not harm the server or the service. However, the busy server could suffer a flash crowd (FC) event which is observed as a sudden high demand in service requests from Internet users. A flash crowd could overwhelm a server and create a DoS condition which results in either a delay of response or a complete crash.
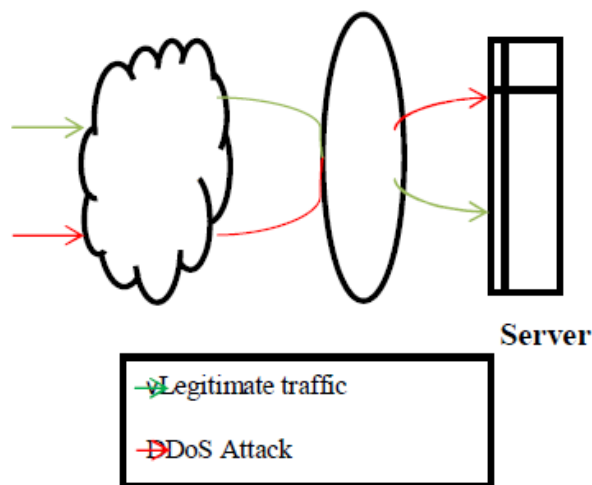

Fig-4

DDoS attack is, however, more harmful than a flash crowd. Zombie machines (or bots) are compromised and controlled by attackers. The (botnet) attacks could be synchronized to overwhelm the victim in a specific period of time. The situation could be worse when a flash crowd merges with a DDoS attack as shown in Fig. 1. This accelerates the DoS condition to the server.

4. ADAPTIVE DISCRIMINATING DETECTION

By using Discriminating Algorithm we can differentiate the DDoS from flash crowds. Flow Correlation Coefficient value is calculated for similar two suspicious flows to differentiate DDoS attacks from Flash crowds. In this paper the Adaptive Discriminating Algorithm is used, in that previous FCC (Flow correlation Coefficient) value is given as a feedback value to the input. By using this method the hackers cannot judge the feedback value and they cannot trace the detection strategy. We can detect the attack and also filter it out by using the sequential packing and detection.

5. SEQUENTIAL DETECTION WITH PACKING

We assign a sequential ID for all packets which are participating in the transfer, the given a set of suspect IDs, we first randomly assign (i.e., distribute their requests) them to the available testing servers in set A, where each server will receive requests from approximately the same number of clients, For each test round, we identify the IDs on the negative servers as legitimate clients, and "pack" them into a number of non-testing machines. Since they need no more tests, only normal services will be provided for the fourth coming rounds. As more testing servers will speed up the tests, given at most server machines in total, as long as all identified legitimate clients can be handled by the non-testing capacity servers. If any server containing only one active ID is found under attack, the only ID is surely an attacker. Then its ID is added into the black-list and all its requests are dropped. Iterate the algorithm until all IDs are identified, malicious, or legitimate. Via the "packing" strategy, legitimate clients can exempt from the influence of potential attacks as soon as they are identified.

6. RESULTS AND DISCUSSION

In this paper, our main motive is to discriminate flash crowd attacks from genuin e flash crowds . Found that DDoS attack flows own higher similarity compared with that of flash crowd flows under the current conditions of botnet size and organization. We used the flow correlation coefficient as a metric to measure the similarity among suspicious flows to differentiate DDoS attacks from genuine

flash crowds. We theoretically provided the feasibility of the proposed detection method.

Future work is to investigate the possibility of organizing a super botnet, which has a sufficiently large number of live bots to be at the proposed method.

REFERENCES

[1] Ke Li, Wanlei Zhou, Ping Li, and Jianwen Liu , Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics, IEEE Third International Conference on Network and System Security 2009,pages 9-17.

[2] Shui Yu, TheerasakThapngam, Jianwen Liu, Su Wei and WanleiZhou, Discriminating DDoS Flows from Flash Crowds Using Information Distance, IEEE Third International Conference on Network and System Security,2009, pages 351-355

[3] TheerasakThapngam, Shui Yu, Wanlei Zhou and GlebBeliakov,DiscriminatingDDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns, The First IEEE International Workshop on Security in Computers, Networking and Communications,2011,pages 952-958

[4] Jie Wang, Raphael C.W. Phan, John N. Whitley and David J. Parish ,DDoS Attacks Traffic and Flash Crowds Traffic Simulation with a Hardware Test Center Platform, IEEE

[5] Y. Xie and S.Z. Yu, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors Networking," IEEE/ACM Transactions on Networking, vol. 17, no. 1, pp. 54 - 65, February 2009.

[6] G. Oikonomou and J. Mirkovic, "Modeling Human Behavior for Defense against Flash-Crowd Attacks," in Proceedings of IEEE International Conference on Communications 2009 (ICC '09), pp. 1 - 6, 11 August 2009.

[7] L. Feinstein, D. Schnackenberg R. alupari and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," in Proceedings of the DARPA Information Survivability Conference and Exposition, vol1, IEEE CS Press, 22-24 April 2003, pp. 303–314.

[8] S. Yu, T. Thapngam, J. Liu, S. Wei and W. Zhou, "Discriminating DDoS Flows from Flash Crowds Using Information Distance," in Proceedings of the 3rd IEEE International Conference on Network and System Security,18-21 October 2009.