A SURVEY ON TECHNIQUES TO DIFFERENTIATE DDOS ATTACKS FROM FLASH CROWDS

Ms C.Malathi

Deptt. Of CSE, Sree Vidyanikethan Engg.College, Tirupati.

ABSTRACT

Flash crowds and DDOS attacks have very similar properties in terms of internet traffic. DDOS attacks are malicious requests that does not need to be handled by a server and flash crowd consist of legitimate requests, the server has responsibility to handle as many requests as possible during a flash event. So the attack flows are generated by the same pre built programs (attack tools), whereas the flash crowds come from the randomly distributed users all over the Internet. So in this paper, we aim to differentiate DDOS attack flows from flash crowds based on the following methods: Flow Correlation Coefficient, Packet Arrival Patterns, Information Distance and Probability Metrics.

I

Keywords: DDOS, Flash Crowds, Flow Correlation Coefficient, Packet Arrival Patterns, Information Distance, Probability Metrics.

I INTRODUCTION

A DOS attack is one in which the goal of the attacker is to gain unauthorized privileged access, but it can be just as malicious. The DoS concept is easily applied to the networked world. The DoS is disruption and inconvenience. A denial of service, or DoS, is a category of attack in the security engineering. Routers and servers can handle a finite amount of traffic at any given time based on factors such as hardware performance, memory and bandwidth. If this limit or rate is increased, new requests will be rejected. As a result, genuine traffic will be ignored and the object's users will be denied access. A DDOS can be thought of as an improved form of a traditional DOS attack. Instead of one intruder flooding a target with traffic, numerous machines are used in a "master-slave", multi-tiered configuration. The coordinated attack was designed to disable several of the Internet's root name servers. The attack was sophisticated and complex, known as a distributed denial of service (DDOS) prevents genuine traffic from reaching major sites for several hours. A cracker breaks into a large number of Internet-connected computers (often using automated software known as an auto router) and installs the DDOS software package (of which there are several changes). The DDOS software allows the intruder to remotely control the compromised computer, thereby making it a "slave". From a "master" device, the attacker can inform the slaves of a target and direct the attack. Thousands of machines can be controlled by a single point of contact. Start time, stop time, target address and attack type all can be communicated to slave

computers from the master machine via the Internet. When used for one purpose, a single machine can produce several megabytes of traffic. Several hundreds of machines can generate gigabytes of traffic. Yahoo, eBay, Buy.com, and CNN were but a few major sites who were inaccessible to their customers for certain period of time. A flash event (FE) is a large surge in traffic to a particular Web site causing a dramatic increase in server load and putting severe strain on the network links leading to the server, which results in substantial increase in packet loss and congestion. Flash Events represent legitimate traffic to a website. This means the website wants to service these requests as well as possible, while DOS attacks are unwanted and should not be serviced, instead they should be ignored or controlled.

II. DISCRIMINATING DDOS ATTACKS FROM FLASH CROWDS USING FLOW CORRELATION COEFFICIENT

Distributed Denial of Service (DDOS) attack is threat to the Internet and botnets are usually the engines. Sophisticated botmasters attempt to disable detectors by reducing the traffic patterns of flash crowds. In this, the size and organization of current botnets and the current attack flows are usually more similar to each other compared to the flows of flash crowds. So we present a flow similarity-based approach to discriminate DDOS attacks from flash crowds, which remains a burning problem to date. Distributed Denial of Service (DDOS) attacks pose a critical threat to the Internet. Individual attacks are becoming stronger and more sophisticated. Motivated by huge financial rewards, such as renting out their botnets for attacks or collecting sensitive information for malicious purposes, hackers are encouraged to organize botnets to commit these crimes. To sustain their botnets, botmasters take advantage of various antiforensic techniques to disguise their traces, such as code obfuscation, memory encryption, fresh code pushing for resurrection, peer-to-peer implementation technology or flash crowd mimicking. Flash crowds are unexpected, but genuine, sudden surges of access to a server, such as breaking news. One powerful strategy for intruders is to simulate the traffic patterns of flash crowds to fly under the radar. This is referred to as a flash crowd attack. The current most popular defence mechanism against flash crowd attack is the use of graphical puzzles to differentiate between bots and humans. This method involves human responses and can be annoying to users. The behavior-based discriminating methods work well at the application layer. Bots are caught by honeypots and analyzed thoroughly via inverse engineering techniques. Botnet infiltrations are further implemented to collect first-hand information about their activities and implemented a peer-to-peer-based botnet . The following facts concerning the current botnets.

1. The attack tools are prebuilt programs they are usually the same for one botnet. A botmaster issues a command to all bots in his botnet to start one attack session.

2. The attack flows that are at the victim end are an aggregation of many original attack flows, the aggregated attack flows share a similar standard deviation as an original attack flow, and the flow standard deviation is usually smaller than that of genuine flash crowd flows. The reason for phenomenon is that the number of live bots of a current botnet is far less than the number of concurrent legitimate users of a flash crowd. However, we observed that the number of concurrent users of the flash crowds of World Cup 98 is at the hundreds of

thousands level. Therefore, in order to launch a flash crowd attack, a botmaster has to force his live bots to generate many more attack packets, e.g., web page requests, than that of a legitimate user. As a result, the aggregated attack flow possesses a small standard deviation compared with that of a flash crowd, which results in the phenomenon we see in Fig. 1. Based on observation, we found that the similarity among the current DDOS attack flows is higher than that of a flash crowd. Therefore, we propose a flash crowd attack detection method using the flow correlation coefficient. We aim to protect potential victims (e.g., web servers, mail servers) from flash crowd attacks within a community network. A community or ISP network often operates with the same Internet service provider domain or the virtual network of different entities in which are all cooperating at one another. The community network benefits the defence of DDOS attacks in a wider range and in a cooperative way. So the established model for DDOS attacks detection in a community network where the potential victim is situated.

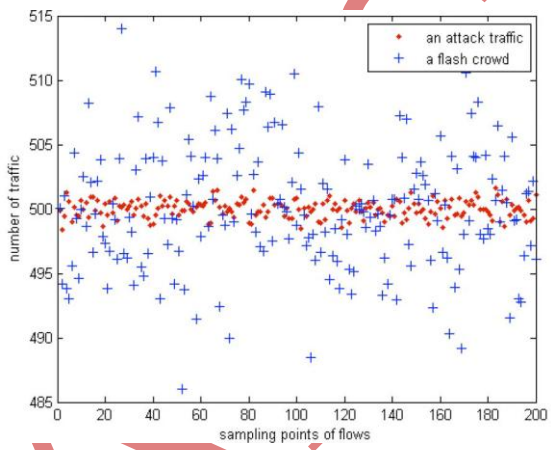

Fig1: The difference between an aggregated attack traffic and a flash crowd traffic under the current botnet size and organization.

III. DISCRIMINATING DDOS ATTACK TRAFFIC FROM FLASH CROWD THROUGH PACKET ARRIVAL PATTERNS

Current DDOS attacks are carried out by attack tools, worms and botnets using different packet-transmission strategies and various types of attack packets to beat defense systems. Those problems lead to defense systems requiring various detection methods in order to identify attacks. DDOS attacks can mix their traffics during flash crowds. By doing so, the complex defense system cannot detect the attack traffic in time. So in this paper, a behavior based detection that can discriminate DDOS attack traffic from traffic generated by real users is proposed. By using Pearson's correlation coefficient, comparable detection methods can extract the repeatable features of the packet arrivals. We consider the situation where a server is overwhelmed by flash crowd flows and/or DDOS attacks as illustrated in Fig.2 A server connects to the Internet and provides a service to

public Internet users. Legitimate users do not harm the server or the service. 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. DDOS attack is, 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. This accelerates the DOS condition to the server. The behavior of the bot can be detected by the victim's server by observing the predictable arrival rate.

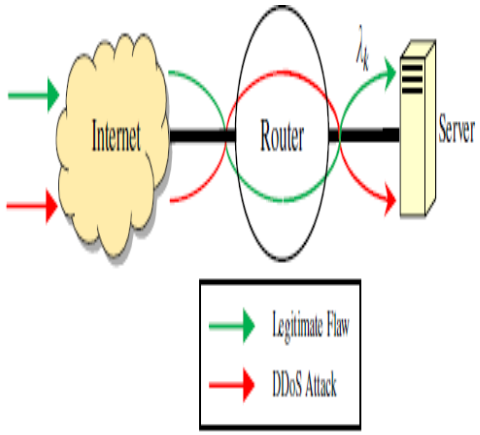

Fig2: Accumulative arrival rate

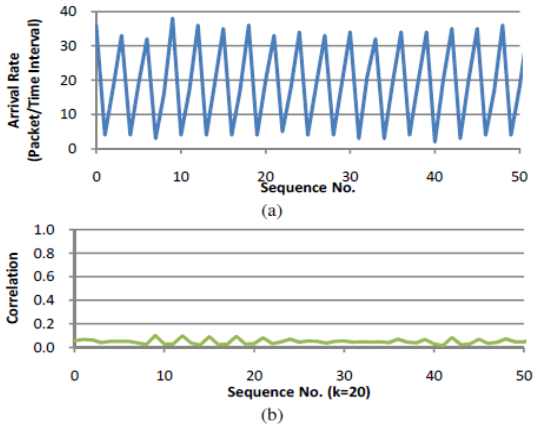

Fig 3. Experiment on sample dataset 1 (CID55) with method 1, (a) packet arrival plot, and (b) correlation from different *k*=20.

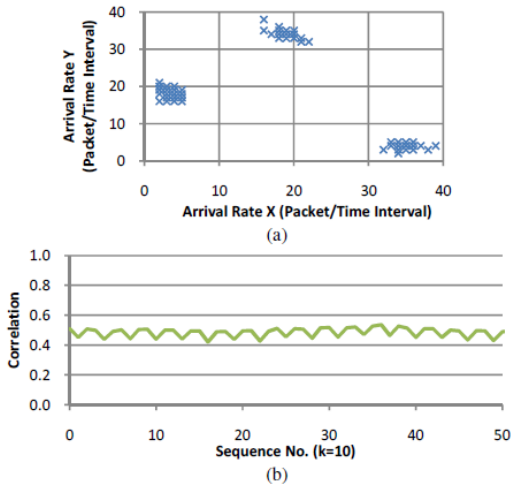

Fig4. Experiment on generated dataset 1 (CID55) with method 2, (a)packet arrival plot, and (b) correlation with *k*=10.

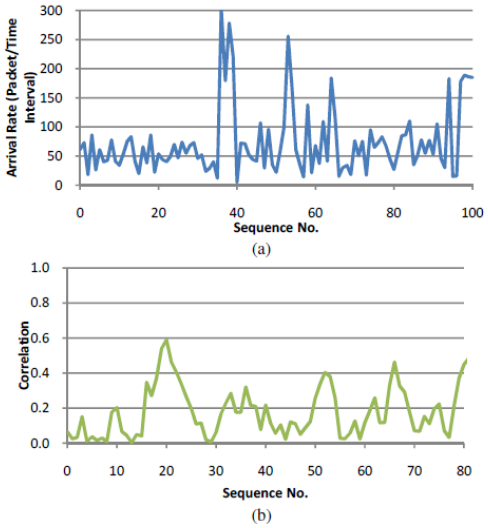

Fig5. Experiment on sample dataset 2 (M17060) with method 1, (a) packet arrival plot, and (b) correlation from different *k*=20.

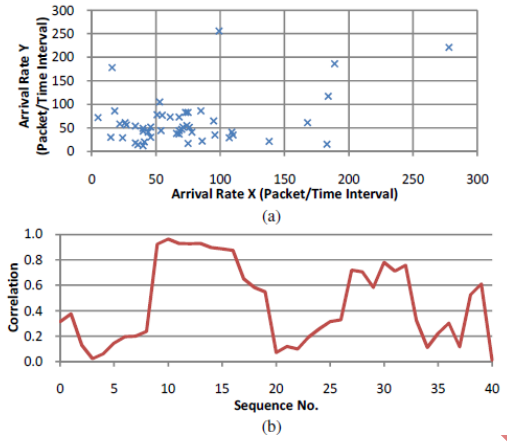

Fig 6. Experiment on sample dataset 2 (M17060) with method 2, (a) packet arrival plot, and (b) correlation with *k*=10.

IV. DISCRIMINATING DDOS FLOWS FROM FLASH CROWDS USING INFORMATION DISTANCE

Discriminating DDOS flooding attacks from flash Crowds pose a challenge for the network security community. Due to the vulnerability of the original design of the Internet, attackers can easily mimic the patterns of legitimate network traffic to fly under the radar. So in this, DDOS attack flows from flash crowds and motivated by the following fact: the attack flows are generated by the same prebuilt program (attack tools), however, flash crowds come from randomly distributed users all over the Internet. Therefore, the flow similarity among DDOS attack flows is much stronger than that among flash crowds. We employ abstract distance metrics, the Jeffrey distance, the Sibson distance, and the Hellinger distance to measure the similarity among flows to achieve our goal. We compared the three metrics and found that the Sibson distance is the most suitable. We Then the algorithm to the real datasets and the results indicate that the proposed algorithm can differentiate them with an accuracy around 65%.

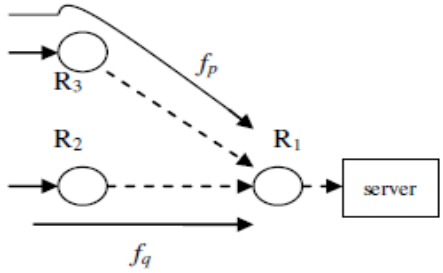

Fig 7. Similarity Measure with the Hellinger Distance

The proposed strategy can differentiate DDOS attack flows and flash crowds more than 65% (13 out of 20) of the time.

The Sibson distance is best metric among the three metrics for discriminating DDOS attack flows from flash crowds.

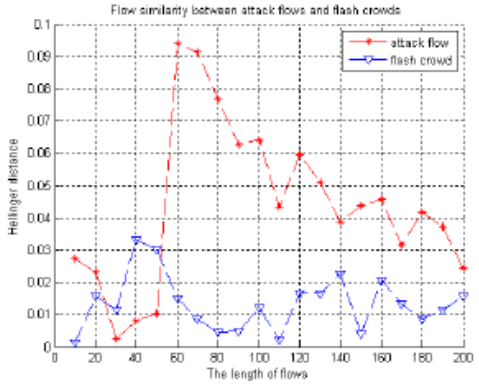

Fig8. Similarity measure with the Hellinger distance

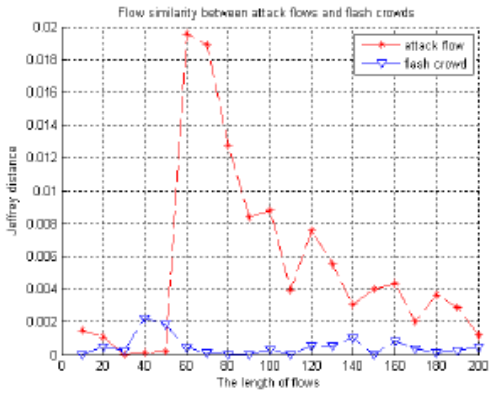

Fig 9. Similarity measure with the Jeffrey distance

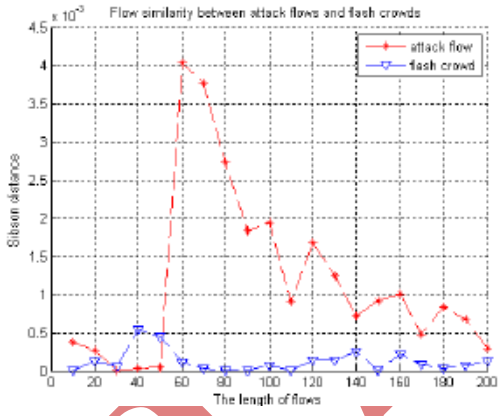

Fig10. Similarity measure with the Sibson distance

V. DISTINGUISHING DDOS ATTACKS FROM FLASH CROWDS USING PROBABILITY METRICS

Both Flash crowds and DDOS (Distributed Denial -of-Service) attacks have very similar properties in terms of internet traffic, however Flash crowds are legitimate flows and DDOS attacks are illegitimate flows, and DDOS attacks have been a serious threat to internet security and stability. In this paper we propose a set of novel methods using probability metrics to distinguish DDOS attacks from Flash crowds effectively, and our simulations show that the proposed methods work well. In particular, these methods can not only distinguish DDOS attacks from Flash crowds clearly, but also can distinguish the anomaly flow being DDOS attacks flow or being Flash crowd flow from Normal network flow effectively. Furthermore, we show our proposed hybrid probability metrics can greatly reduce both false positive and false negative rates in detection.

VI. CONCLUSION

In this paper we surveyed on four different techniques to differentiate DDOS attack from flash crowd. Among the techniques "Discriminating DDOS Attacks from Flash Crowd Using Flow Correlation Coefficient" shows better results.

REFERENCES

[1] Shui Yu, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 6, JUNE 2012.

[2] Theerasak Thapngam, Shui Yu, Wanlei Zhou and Gleb Beliakov "Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns" The First International Workshop on Security in Computers, Networking and Communications pno 969-974.

[3] Shui Yu, Theerasak Thapngam, Jianwen Liu, Su Wei and Wanlei Zhou "Discriminating DDoS Flows from Flash Crowds Using Information Distance" International Conference on Network and System Security pno 351-356.2009.

[4] Ke Li, Wanlei Zhou, Ping Li, Jing Hai and Jianwen Liu "Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics" Third International Conference on Network and System Security pno: 9-17 .2009.