IJRECE VOL. 4 ISSUE 3 JULY.-SEPT. 2016 ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)
DOI: 10.13140/RG.2.1.5009.8168

The Study of Distributed Denial of Services Fact, Figures and Issues

Gurleen Kaur[1],Saumya Rajvanshi[2], Gurjot Singh Sodhi[3]
[1]*M.Tech (Student), Shaheed Udham Singh College of Engineering and Technology, Tangori, Mohali*
[2]*Assistant Professor, Shaheed Udham Singh College of Engineering and Technology, Tangori, Mohali*

Abstract- Scalability and vibrant formation of service clouds can be susceptible to Distributed Denial of Service attacks. The attack on network facilities causes a presentation decrease in the cloud applications or can shut them down. Moreover, due to the extraordinary distribution of the facility components, finding the original attacking service becomes a distant additional complex task. This paper supporters a DDoS attack detection approach for service clouds and develops efficient algorithms to resolution the creating facility for the attack. The detection approach is composed of four levels such that every level notices indications of DDoS attacks from its native data. A low-rate DDoS attack allows legitimate network traffic to permit and chomps little bandwidth. So, recognition of this type of attacks is very difficult in high speed networks. In this paper, several information metrics, namely, Hartley entropy, Shannon entropy, and generalized entropy are evaluated to detect low-rate DDoS attacks. We describe individualities of system traffic and unsuitable metric facilitates building an functioning model to sense low-rate DDoS attacks.

Keywords- Applications, Distributed Denial of Service attacks, facility components and detection approach.

1. INTRODUCTION

DDoS attacks use a set of compromised hosts to make Internet services unavailable. Attackers are continually improving their ability to launch future [1] DDoS attacks by infecting unsuspecting hosts. These attacks normally chompa massive quantity of resources from a server that makes the server inaccessible to genuine users; they also chomp network bandwidth by cooperating network traffic.

DDoS attacks are cooperative distributed large scale attacks and can supper by both strengthened and wireless nets. Hence, both industry and academia are interested in defending their systems from DDoS attacks, safeguarding uninterrupted admittance by legitimate users.

It is challenging to distinguish malicious traffic from legitimate traffic [2] since they are similar based on traffic behavior alone. There are two types of traffic that can usually cooperation a host or a system with DDoS attacks. They are:
(a) high-rate DDoS attack traffic, which is excellent and alike to a flash troop and
(b) little amount DDoS attack traffic, which is similar to legitimate traffic.[3] Since both have characteristics of legitimate traffic, it is crucial to detect a DDoS attack and responsibility within a small time intermission.

Most current work aims to sense DDoS attacks launched by botnets. A botnet is a large network of compromised hosts that is bots or slave machines controlled by one entity .The master can send malformed packets through a synchronized host to the target host. However, detection of botnets is hard and an effective solution needs to monitor all machines that[4] can possibly become active bots in a botnet.

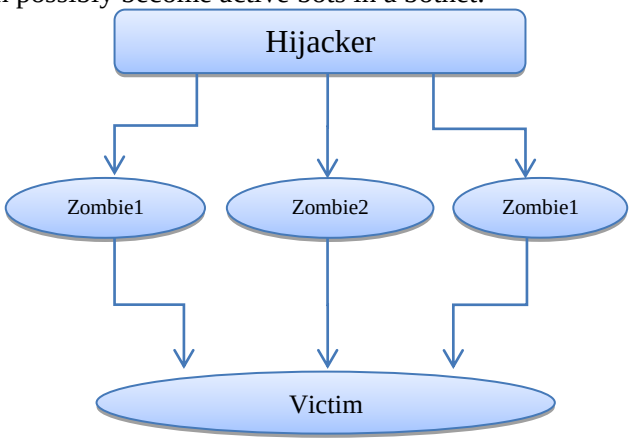

Fig. 1 Direct Attack

A successful attack prevents the victim from providing desired QoS to its legitimate clients. The most commonly researched type of service denial is the flooding-based attacks intended to overwhelm a limited, critical set of targets. Such flooding attacks attempt to perform continued resource exhaustion at a well-provisioned target.

II. ISSUES OF DISTRIBUTED DENIAL OF SERVICES

The major economic driver behind running a web service on a cloud is charging the customers according to their actual usage. Hence, cloud computing allows

DOI: 10.13140/RG.2.1.5009.8168

customers to scale up their services to serve a large number of requests. This feature of "pay-as-you-use" has transformed the problem of DDoS attacks in the cloud into a financial one. In the event of a DDoS attack, the impact of flooding requests detected at a particular service may have passed several intermediate [5] services before reaching this service.

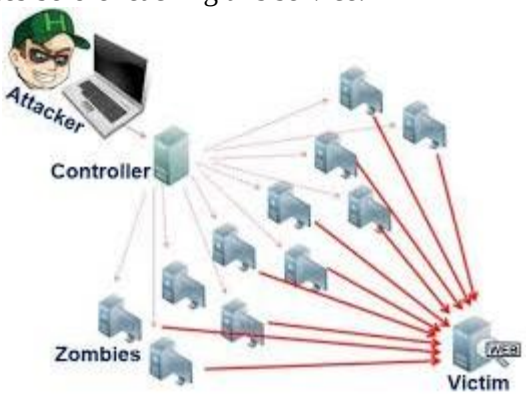

Fig. 2 BBC Distributed Denial of Services Attack

Thus, the owners of intermediate services that have received, processed, and passed illegitimate requests from the original attacking service will be charged for processing those undesired requests. This problem of finding the service originating the attack (i.e. the attack entry point) is an accountability issue.

III. DETECTION OF DDOS ATTACK

To detect DDoS attacks early and identify the attack originating service to isolate it and protect other services in the service. The solution is distributed across service, tenant, application, and cloud levels. At the service level, attack detection and mitigation includes authenticating and syntactically validating received requests before getting processed at the web service[6]. Moreover, the service can detect DDoS attacks by watching the number of messages received from other services. The tenant level corroborates the detection information across its services to find if it is facing a DDoS attack. At the application level, the performance degradation of the service chain can be used to detect DDoS attacks. Determines the real services that have been used by attackers by corroborating and verifying the information received from other levels.

The supports of this paper are as:

(i) A provision cloud DDoS attack recognition method based on a distributed architecture that uses message flow as a metric for detection and

(ii) A distance algorithm that measures the deviation between the flow rates of requests at different time intervals to monitor symptoms of DDoS attacks. By using flow

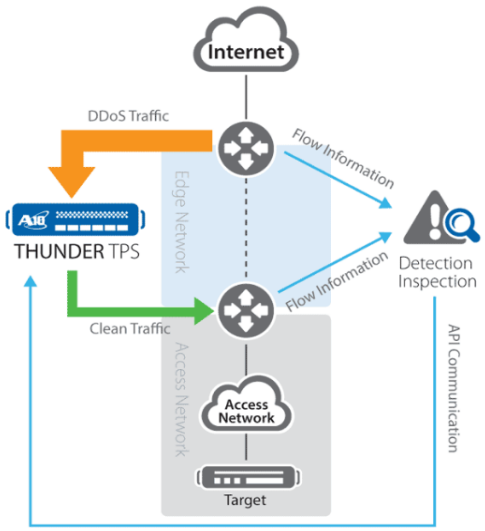

Fig. 3 DDoS Protection via Asymmetric Mode

distance variation rather than fingerprints of specific attacks; monitoring is independent of attack features.

IV. RELATED WORK

Theerasak Thapngam et al., 2011[7] In this paper, they proposed a behaviour based detection that can distinguish DDoS attack traffic from traffic produced by real users. By using Pearson's correlation coefficient, those comparable detection methods can citation the repeatable sorts of the packet arrivals. The widespread simulations were tested for the accuracy of detection. They then achieved experiments with numerous datasets and our results affirm that the projected technique can distinguish traffic of an attack foundation from sincere traffic with a quick response.

Jae-Hyun Jun et al., 2011 [8] This paper describes as, the DDoS attack, which is consuming all of the computing or communication resources essential for the service, is recognized very problematic to protect. The threat posed by network attacks on large network, such as the internet, difficulties effective discovery method. Therefore, an intrusion detection system on large network is need to effectual real-time detection. In these broadside, implemented the entropy-based detection mechanism against DDoS attacks in order to agreement the transmission of normal traffic and prevent the flood of abnormal traffic.

Young-Tae Han et al., 2012 [9] This paper, presented effect of the TTL Expiry DDoS attack with the attack scenario in the tested consisted with commercialized network equipment's.

V.K Soundar Rajam et al., 2013 [10] This paper proposed trace back mechanism with an actual optimization algorithm termed ACOPID in autonomous

DOI: 10.13140/RG.2.1.5009.8168

system with DPM inflicts two major advantages. They had predicted the complete attack path and efficiently tracing the DDoS attack source. Our contribution is on host IP trace back with DPM based on autonomous system to trace back the DDoS attack source with the design information with summary false positive rate.

Ahmad Sanmorino et al., 2013 [11] In this study, they discussed how to handle DDoS attacks in the form of discovery method based on the design of flow entries and handling mechanism using layered firewall. Tests carried out using three scenarios that is simulations on normal network environment, unsecured network, and secure network. Then, analysed the simulations result that has been done. The method used successfully filtering incoming packet, by released packets from the assailant when DDoS attack happen, while still is able to receive packets from legitimate hosts.

Table no: 1 Sample DDoS attacks

Attack Type	Exploitation Method	Mitigation
Oversized Payload	Querying a service using an overly expanded request message	XML size checking before parsing
Coercive Parsing (Deep-Nested XML, XDoS)	Sending a SOAP message with an unlimited amount of opening tags in the SOAP Body	Strong input validation given a specified schema
Flooding Attack(XML ping of death)	Sending numerous requests to the service to make it unavailable for legitimate requests.	Throttling mechanisms for resource Allocation

V. FACTS AND FIGURES

Distributed denial of service operations remains one of the most popular forms of attack, according to a report from Kaspersky Labs. The occurrences are relatively humble to arrange, and extremely problematic to defend against, making them one of the most favoured tools for an attacker, be they a nation-state like China or an activist group like Anonymous [5, 6].

DDoS attacks are used to interrupt a processor network's aptitude to purpose by flooding it with information, thus rejecting service to authentic users. DDoS attacks are also extremely under-reported, rendering to Kaspersky's research.

Kaspersky intelligences the following information on DDoS attacks after the second neighbourhood of this year:

- Figures: The longest DDoS attack persisted 60 days, 1 hour, 21 proceedings and 9 seconds. The uppermost number of DDoS attacks in contradiction of a single site was 218.
- Attacks by Country: 89% of DDoS traffic was produced in 23 republics. The US and Indonesia made up a combined 10% of attack traffic.

Table no: 2 Fact and Figures

Serial no.	Facts	Figures
1.	Extremely difficult to defend against	(Longer) persisted 60 days, 1 hour, 21 minutes and 9 seconds
2.	most favoured tools for an attacker	(highest) DDoS attacks against a single site was 218

Table no: 3 Best ways to stop DDoS attack

Sr no.	Best ways
1	Deployment Methods and Detection
2.	Performance Metrics
3.	Assure Scalability

VI. CONCLUSION

DDoS attacks can cause plain disturbance to the constancy of the Internet. In this paper, we have presented a novel IP Address Interaction Feature algorithm, which is based on the source addresses interaction of normal flow and the source addresses half interaction, sudden traffic variation, addresses many-to-one dissymmetry, dispersed source IP addresses and concentrated target addresses of DDoS attack flow. Using the IAI feature and SVM, we also proposed a simple but effective DDoS detection method. This method uses the IAI time series to describe the state characteristics of network flows, and then a detection of DDoS attack flows is indeed a classification problem of IAI time series. Using the training samples obtained from the normal flows and attack flows to train classifier, and then use them to classify the current network flows and detect DDoS attacks.

VII. REFERENCES

[1] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal Kumar Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." Contemporary Computing (IC3), 2014 Seventh International Conference on. IEEE, 2014.

[2] Anantvalee, Tiranuch, and Jie Wu. "A survey on intrusion detection in mobile ad hoc networks." Wireless Network Security. Springer US, 2007. 159-180.

[3] Chhabra, Meghna, and B. B. Gupta. "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-Hoc Network (MANET)." Research Journal of Applied Sciences, Engineering and Technology 7.10 (2014): 2033-2039.

DOI: 10.13140/RG.2.1.5009.8168

[4] Alqahtani, Sarra, and Rose Gamble. "DDoS Attacks in Service Clouds."System Sciences (HICSS), 2015

[5] Jae-Hyun Jun, Hyunju Oh, and Sung Kim. "Real time detection and classification of DDoS attacks using Enhanced SVM with string kernels." Recent Trends in Information Technology (ICRTIT), 2015 International journals on. IEEE, 2015.

[6] Watteyne, Thomas, and Kristofer SJ Pister. "Wireless Sensor Networks: Technology Overview." The Internet of Things: Connecting Objects to the Web (2013): 53-95.

[7] Thapngam, Theerasak, et al. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns." Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. IEEE, 2011.

[8] Jun, Jae-Hyun, Hyunju Oh, and Sung-Ho Kim. "DDoS flooding attack detection through a step-by-step investigation." Networked Embedded Systems 48th Hawaii International Conference on. IEEE, 2015.
for Enterprise Applications (NESEA), 2011 IEEE 2nd International Conference on. IEEE, 2011.

[9] Han, Young-Tae, et al. "Vulnerability of small networks for the TTL expiry DDoS attack." Computing, Communications and Applications Conference (ComComAp), 2012. IEEE, 2012.

[10] Soundar Rajam, V. K., et al. "Autonomous system based traceback mechanism for DDoS attack." Advanced Computing (ICoAC), 2013 Fifth International Conference on. IEEE, 2013.

[11] Sanmorino, Ahmad, and SetiadiYazid. "Ddos attack detection method and mitigation using pattern of the flow." Information and Communication Technology (ICoICT), 2013 International Conference of. IEEE, 2013.