International Journal of Engineering & Technology, 7 (2.8) (2018) 497-499

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A review on mitigation of the DDoS Attack in cloud in regulated environment

Syed Asia Ayaz Andrabi[1*], Sachi Pandey[2], Akthar Nazir[3]

[1]P.G Student, Computer Science and Engineering, SRM University, Delhi NCR, India
[2,3]Assistant Professor, Department of CSE, SRM University, Delhi NCR, India
**Corresponding Author E-mail:asiasyed744@gmail.com*

Abstract

Distributed Denial of Service (DDoS) attacks are aimed at exhausting various resources of victim hosts, thereby preventing legitimate usage of their computational capabilities. In this paper, a proper and systematic mitigation technique presented to mitigate the DDoS attack in cloud environment. A robust mechanism is presented which consists of software based puzzle generation method to validate the real customer of cloud services provider from non-reals' ones to provide better DDoS attack mitigation solution.

Keywords: *Distributed Denial Of Servic (DDoS), Puzzle Generation*

1. Introduction

DDoS attacks are launched by affecting the victim in following forms: Attacker can find some bug or weakness in the software implementation to disrupt the service. Some attacks deplete all the bandwidth or resources of the victim's system. Attackers scan the network to find the machines having some vulnerability and then these machines are used as agents by the attacker. These are called zombie machines. Spoofed IP's are used by zombie machines. The design of internet gives rise to many conditions causing denial of service attacks. Some of these features will be explained in this section. Security in internet is dependent on hosts. Attackers compromise the security of hosts to launch DDoS attacks and they use spoofed IP addresses making it difficult to trace attack source. Further internet is full hosts. It gives attacker huge amount of options, out of which vulnerable hosts are chosen. Main target of DDoS attack are resources like bandwidth, CPU etc. and the resources are limited in network. If these resources are increased, then impact of the attack can be lowered but still resources will be wasted leading to monetary loss.

A. DDoS Constituents:

Recently, Botnets are being used widely to perform DDoS attacks. This section explains botnet architectures and the tools that have been used to launch DDoS flooding attacks. Many computers are used for launching a DDoS Attack. It makes use of client server technology. In general, DDoS attack comprises of Master, Handler, Agents and victim. The zombies (agents or bots) are the one used by the master to form a botnet. Larger the number of zombies, more disruptive the attack. The Master communicates with agents via handlers. For Example, handlers can be programs installed on a set of compromised devices (e.g., network servers) that attackers communicate with to send commands. Attacker sends command and controls their agent through handlers. Bots are devices that have been compromised by the handlers. The bots carry out the attack on the victim's system. Attacker uses many scanning techniques for finding a vulnerable machine. Random Scan is a simplest strategy which randomly scans whole IPv4 address space as the worm doesn't know where the host is present. It effective only for IPv4 as address space of IPv6 is too vast. Hitlist Scan has a list which contains IP address vulnerable hosts in the Internet. The scanning is done in this list. When it makes another machine a host, part of the initial hit list will be sent to that machine. Route-based Scan reduces the search addresses BGP routing prefixes are used and this prefixes information can reduce the search space drastically. In Divide-and-conquer Scan technique the scanning is done by different hosts on different part of address space hence saving the resources. Apart from these there are other strategies too like Permutation Scan, Local Preference Scan and Topological Scan. Once host is found after scanning, vulnerabilities of that host need to be found to gain its control. More information about these vulnerabilities is available on internet.

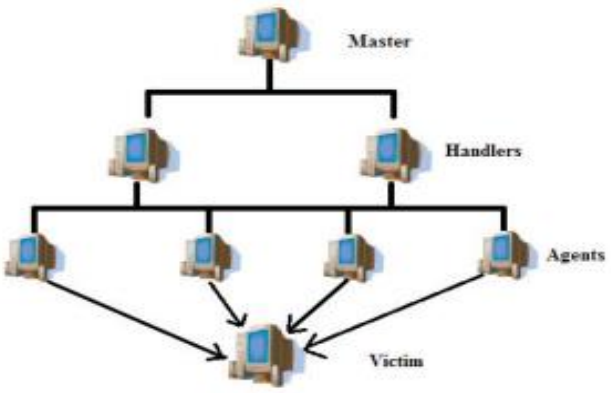

Fig. 1: Constituents of DDoS

B. Classification:

The variety of DDoS attacks are sprouting in the computing world. The major types include Bandwidth based and resource based attacks. Both types consume the entire bandwidth and resources of the network that's been exploited. Through the analysis made, taxonomy. Depending upon the exploited vulnerability it can be further divided into different types:

Bandwidth Depletion Attacks: This type of attack consumes the bandwidth of the victim or target system by flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim network. Tools like Trinoo are usually used to perform these attacks.

Flood Attacks: This attack is launched by an attacker sending huge volume of traffic to the victim with the help of zombies that clogs up the victim's network bandwidth with IP traffic. The victim system undergoes a saturated network bandwidth and slows down rapidly preventing the legitimate traffic to access the network. This is instigated by UDP (User Datagram packets) and ICMP (Internet Control Message Protocol) packets.

Amplification attacks: The attacker sends a large number of packets to a broadcast IP address. In turn causes the systems in the broadcast address range to send a reply to the victim system thereby resulting in a malicious traffic. This type of attack exploits the broadcast address feature found in most of the internetworking devices like routers. This kind of DDoS attack can be launched either the attacker directly or with the help of zombies. The well-known attacks of this kind are Smurf and Fraggle attacks.
Resource Depletion Attacks: The DDoS Resource depletion attack is targeted to exhaust the victim system's resources, so that the legitimate users are not serviced.

Fig. 2: Taxonomy of DDoS Attack

2. Literature survey

In [1] author have described that attacker can easily attack as many computers bas they want. The number of active bots that a botmaster can have is up to thousand levels and it is just because of antivirus and anti-malware software. Recent researches [2], [3], [4], [5], authors have described the essential issue related to the cloud computing and it is DDoS attack.
Subrimanian.T.K , Deepa.B (April 2016) has proposed the various schemes which provides the defense against the DDoS attack,DDoS attack components and intrusion prevention system for DDoS.
Dr.S.Saravana Kumar, R.Senthil Kumar, R.Anuprasad, S.Thiraviam, J.Vignesh (March 2015) has proposed the technique in which the mean value of distance in the exponential smoothening estimation technique. The distance based traffic separation DDoS detection technique uses MMSE (Minimum Mean Square Error) linear predictor to estimate the traffic rates from different distances. If the real value is out of the legal scope, an anomaly situation is detected.
Preeti Daffu, Amanpreet Kaur (April, 2016), author provides the mechanism that is used to beat the DDoS attacks. It involves the prevention before they occur. MTTSF (Mean Time to Security Failure) is calculated and then alternative dynamic plans adopted to mitigate those attacks and then attack packets are filtered out at the end.
Isha Chawla, Pawan Luthra, Daljeet Kaur (March, 2015), the author focus on the various types of DDoS attacks at the different layers of OSI model in cloud and the various mitigation techniques available to overcome with the security issues.
GauravSomani, Manoj Singh Gaur,Dheeraj Sanghi, Mauro Conti, Muttukrishna Rajaran, Rajkumar Buyya (March, 2017),
the paper gives an overview of DDoS attacks against cloud targets is presented, together with solution requirements, and a guideline for efficient solutions, leading to a new multilevel alert-flow. It also gives a vision towards novel "Detection Near Impossible" attacks. The author suggests that traffic filtering alone may not be sufficient to combat DDoS attacks in the cloud environment. It suggests considering sustainability, collaboration, resource management and availability while handling DDoS attack in cloud computing.

3. Problem Identification

Distributed Denial of service attack is a serious threat to the cloud network security. There have been a lot of methodologies and tools devised to prevent DDoS attacks and the reduction of the damages they cause. But there is a problem that most of the methods cannot be achieved simultaneously. It is very difficult to prevent the attack efficiently and to implement the methodologies properly to provide the proper prevention techniques. As per the literature surveys done till now, the existing intrusion techniques that are used to prevent the DDoS attacks are not fully preventing the attacks properly and efficiently. There are certain vulnerabilities remaining in the network due to which the current techniques that are implemented are not working properly in preventing the attack. The techniques that are already implemented in the previous projects needs further improvement and efficiencies so that they can fully prevent the DDoS attack.

4. Proposed Solution

A DDoS attack detection system is presented that uses Multivariate Correlation Analysis (MCA) and Hierarchy Frequency Clustering Algorithm(HFCA) for accurate network traffic characterization by extracting the geometrical correlations between network traffic features. This MCA and HFCA based DDoS attack detection system employs the principle of anomaly-based detection in attack recognition. This makes our solution capable of detecting known and unknown DDoS attacks effectively by learning the patterns of legitimate network traffic only. Furthermore, a triangle-area-based technique is proposed to enhance and to speed up the process of HFCA and MCA.

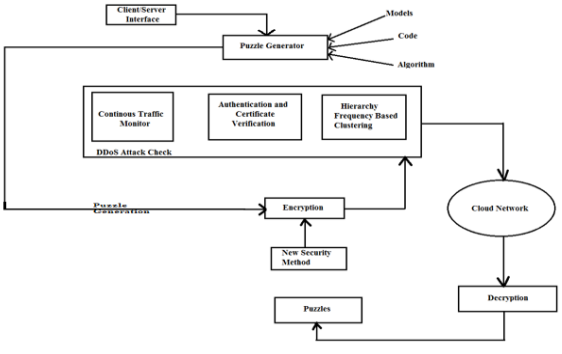

Fig. 3: Block Diagram

We are having a client/server interface from where client and server can enter the system. The puzzle generator will generate a puzzle by using appropriate models, codes and algorithms. This puzzle generator will create a puzzle and this puzzle will be protected by encryption techniques. These encryption techniques are formed by new security methods like RC7 algorithm. After that, this encrypted puzzle will go into DDoS attack check module. In the DDoS check module, first step is clustering of data packets, followed by authentication and verification. Finally, errors will be detected by continuous traffic monitoring by doing this, vulnerability to attacks is reduced and hence DDoS attack can be detected and mitigated. After DDoS check the packets will go into the network and their decryption will take place. Finally, puzzle is obtained safely.

Following are the components of block diagram:

Client/ Server Interface:

It provides the interface to enter the system.

e.g., through password

Puzzle Generator:

By using several algorithms, codes and models the puzzle generator generates the puzzle. The algorithm used will be the RS Algorithm, code will be any text and models will be for sequence number, clustering etc.

DDoS Attack Check:

This module will continuously keep track on the DDoS attacks and will monitor the traffic of data. There are three modules inside this module:

- *Hierarchy Frequency Based Clustering*:

This method of clustering is used to group the data packets that comes from the interface into different clusters. It also determines which cluster contains which data packet, time taken by the data packet to reach the module.

- *Authentication and Certificate Verification:*

It checks the error count and it keeps privilege for at least up to .5 seconds. The authentication and verification is only done by the administrator or by the authenticator.

- *Continuous Traffic Monitor:*

It continuously monitors the traffic and finds the errors in the traffic flow.

New Security Methods:

New security methods for encryption are adopted. Methods like RC7 algorithm are adopted over AES and DES because of less computation time.

5. Conclusion

The paper provides a proper, systematic prevention or mitigation technique to mitigate the DDoS attack in cloud environment. By using this proposed approach helps the service provider in cloud to prevent DDoS attack and provide its genuine customers the requested services. It also filters and validates real customer/ users of cloud from fake ones so that cloud resources and infrastructures cannot be exhaust by the attackers or malwares and hence to prevent/mitigate DDoS attack. This project provides a robust architecture/mechanism/technique, which consists of software based puzzle generation method to validate the real customers of cloud service providers from the non-real ones, and this presented architecture is deployed in cloud environment to provide better DDoS attack mitigation solution and it also strengthen cloud security measures, to help security community to come up with better information and security solution in future for different security problems.

References

[1] IEEE,and Ren PingLiu,Member, IEEE," A System for Denial-of- Service Attack Detection Based on Multivariate Correlation Analysis.", IEEE Transactions On Parallel And Distributed Systems.

[2] Subramaniam.T.K,Deepa.B"Preventing distributed denial of service attacks in cloud environments", Internationl Journal of Information Technology, Control and Automation (IJITCA) Vol. 6, No.2, April 2016

[3] Isha Chawla,Pawan Luthra,Daljeet Kaur,"DDoS Attack In Cloud And Mitigation Techniques"International journal of innovative Science ,Engineering & Technology, July 2015.

[4] Dr.S.SaravanaKumar,R.SenthilKumar,R.Arunprasad,S.Thiravia m,J.Vignesh,″ Detecting and Preventing DDoS Attacks in Cloud", International Journal of Innovative Research in Computer and Communication Engineering , March 2015

[5] Preeti Daffu,Amanpreet Kaur,"Mitigation Of DDoS Attacks In Cloud Computing",978-1-5090-0893-3/16/$31.00 ©2016 IEEE

[6] Gaurav Somani,Manoj Singh Gaur,Dheeraj Sanghi,Mauro Conti,Muttukrishna Rajaran,Rajkumar Buyya,"Combating Ddos Attacks In The Cloud:Requirements,Trends And Future Directions",IEEE 2017

[7] Smita Miraje , Manisha Bharati , "Implementation of Different Software Puzzle Methods against DDOS Attack", International Journal of Innovative Research in Science,Engineering and Technology, Vol. 5, Issue9, September2016.

[8] T. Padmapriya and V.Saminadan, "Handoff Decision for Multi-user Multiclass Traffic in MIMO-LTE-A Networks", 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016) – Elsevier - PROCEDIA OF COMPUTER SCIENCE, vol. 92, pp: 410-417, August 2016.

[9] S.V.Manikanthan and K.srividhya "An Android based secure access control using ARM and cloud computing", Published in: Electronics and Communication Systems (ICECS), 2015 2nd International Conference on 26-27 Feb. 2015,Publisher: IEEE,DOI: 10.1109/ECS.2015.7124833.

[10] S.V.Manikanthan and T.Padmapriya "Recent Trends In M2m Communications In 4g Networks And Evolution Towards 5g", International Journal of Pure and Applied Mathematics, ISSN NO:1314-3395, Vol-115, Issue -8, Sep 2017.