A Review of Differents Techniques Against DDos Attack in Cloud Computing

Toa Bi Irie Guy-Cedric
Research scholar,
Jain University, Bangalore-560043,
India

Dr. Suchithra. R
Head Office of Department of Msc IT,
Jain University, Bangalore-560043,
India

***Abstract*:- The exponential growth of the Internet interconnections has led to a significant growth of cyber attack incidents often with disastrous and grievous consequences. Distributed Denial of Service (DoS) attacks constitutes one of the major threats and among the hardest security problems in today's Internet. Our particular concerns are Distributed Denial of Service (DDoS) attacks, whose impact can be proportionally severe and how we can used some techniques against ddos attack.**

Keywords: DDoS, Cloud computing.

1. INTRODUCTION

Cloud computing is defined as a group of computer interconnected together in network in the same place or different geographical locations to exploit computing power or storage with help of virtualization. A computing cloud is a set of a network enabled services, providing scalable, Quality of Service (QoS) guaranteed, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way [1].

The handling of data network traffic anomalies is still a critical issue that needs to be solved, since anomalies may affect at some point and with some extent parties of a connection.Denial of Service (DoS) and Distributed Denial of Service (DDoS) are definitely a very serious problem in the clouds computing. The main purpose of a DDoS is the interruption of services by attempting to restrict access to a machine or a service rather than undermine the service itself -even. This type of attack is to make a network not able to provide normal service by targeting either the network bandwidth or connectivity. Therefore the methods and resources available to conduct and mask such attacks have dramatically evolved.This problem requires prompt resolution because otherwise organisms, users adopting cloud services would be exposed to increased expenditures while at Greater Risk. In the rest of paper, first we define DDOS attack, second we discuss about some mechanism used to mitigate ddos attack and conclusion.

2. DDOS ATTACKS

2.1. DDOS Definition

A Distributed Denial of Service (DDoS) attack uses multiple computers to launch a coordinated DoS attack against one or more targets. Using client/server technology, the master is able to multiply the power of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplice computers which serve as attack platforms, according to WWW Security FAQ [2]. For that the master uses many tools like IRC, Tribe Flood Network, and program installed on computer victim, and has the time to coordinate and target the victim to launch an attack, called Botnet. Attackers are motivated by personal reason, blackmail, financial gain and terrorism. The objective of master is to overpower the computer resources of the victim while keeping his identity unknown. We can see down table 1 shown a classification of tools and feature in ddos attack.The main goal of ddos attack is to exhausts computer resource of a target.

Attack name	Characteristics				Tools
	Application	Infrastructure	Direct	Reflector	
SYN flooding		✓	✓		LOIC, XOIC
ICMP flooding		✓	✓		TFN, XOIC
UDP flooding		✓	✓	✓	LOIC, XOIC
HTTP (H-DoS) flooding	✓		✓		DDoSIM
XML (X-DoS) flooding	✓		✓		DAVOSET
Ping of Death		✓	✓		Ping
Slowloris	✓		✓		PyLoris, Goloris
Zero-day	✓	✓	✓	✓	Any tool
Smurf		✓		✓	Nemesis, ping

Table1: DDoS attacks, features and tools.

For a good clarification on concept of DDoS attacks it is necessary to make a classification of different types of ddos attack. The classification illustrate by figure 1 [5] is of recent research results and the classification proposed Mirkovic et al. [3], Lee [4].

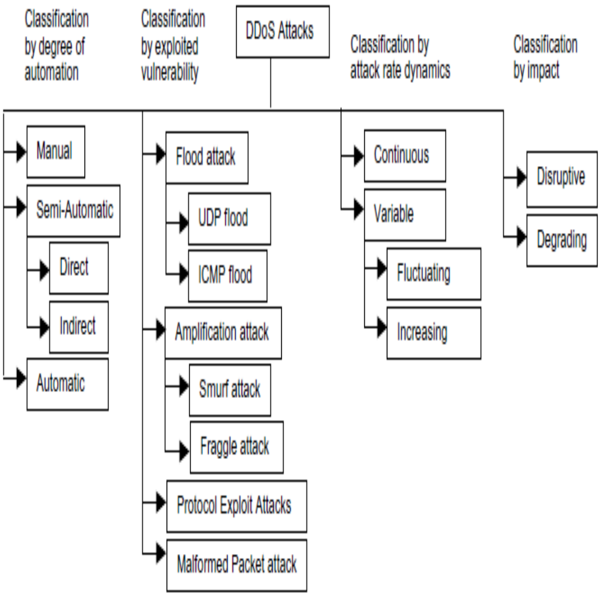

Figure 1: Classification of ddos

3. DEFENSE METHOD AGAINST DDOS ATTACK

3.1 Cloud Trace Back model

CTB Model to defend against DDoS one method is using of Cloud Trace Back (CTB) and Cloud protector. CTB would be utilized in both network structures. The purpose of having CTB in our cloud network is to have ability to trace back the source of these attacks and also make use of a neutral network named cloud protector is to detect and filter such attack CTB and Cloud Protector are located between the each cloud web service to defense against XML-based DDOS attack. This method gave ability to detecting and filtering most of the attack's bases on DDoS. [6].

3.2 Cloud-based Intrusion Detection Service

Intrusion Detection System is a traditional techniques used in virtual machine (VM) for securing networks against DDoS by monitor networks for detecting malicious activity. It is also used in cloud computing and many research have been did to propose some efficiency ids, like A. Abdullah et al.[7] proposed Intrusion detection framework based on Cloud services called Cloud-based Intrusion Detection Services (CBIDS) that not only for commercial solution, but also for open research communities. CBIDS framework consists of three principal components; namely, User Data Collector (UDC), Cloud Service Component (CSC), and Cloud Intrusion Detection Component (CIDC). Communication among UDC and CSC which contains confidential information for forwarding purposes is encrypted. The main purpose of this framework is capable of detecting all possible threats in public and private Clouds and offer opportunity to addition inside an anti-virus.

3.3 Cloud-based Confidence-based filtering

Chen et al. [8] deployed this method base on non-attack period and attack period. Attack period time lots of legitimate packets are captured and analyzed for creating a normal profile according attribute pairs inside the TCP and IP header. Two amounts are computed in CBF which are Confidence and CBF score. Confidence actually is frequency of single and pair attribute in the packet. Included discarding threshold which always compared with a CBF score for using at the attack period time. Because it is not based on attack severity the performance of this method is better than Packet Score. The performance of CBF in depended to the attack situation for example attack type its performance is higher but in attacks such as SQL slammer worms is lower. CBF worked efficiently in large amount of traffic.

3.4 Firewall

A Firewall is the primary and main line of defense for services and applications in a network. The performance of a firewall depends strongly on its hardware capabilities and the availability of resources.

3.5 A game theoretic defense framework against DoS/DDoS cyber attacks

According to Myerson, Roger.B [11], game theory is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers". Game-theoretic techniques have been previously employed in some research area like network security to analyze the interaction between an attacker and a defender during a distributed denial of service (DDoS) attack.

T. Spyridopoulos et al. [12], proposed a modified version of the game-theoretic model proposed by Wu et al. This new model includes many options of point of view of attackers, thus allowing us to do a good analysis and to draw some conclusion for the reaction between attacker and the defender. The aim of this approach is to minimize the cost of damages whatever the techniques choose by the attacker, and for that defender can use different firewall configuration.

Xu et al. [13] proposed a game-theoretic model to defend a web service under DoS attack. They used a single bottleneck link to simulate the attacks. The metrics used for the performance of their system are total throughput of the attackers and their legitimate clients, legitimate client's average amount of time to download a web page, number of concurrent attackers and clients, and packet drop probability of the attackers and the clients.

CONLCUSION

Cloud computing has several features and many benefits for enterprises. In spite of being useful, security is a major challenge in cloud network. Indeed ddos are at the moment a high menace for cloud computing. Many mechanism have been expose and explain for give an general idea about how we can protect the network in cloud computing.

REFERENCES

[1] Lizhe W. and Gregor V. L.,(2008), "Cloud Computing : a Perspective Study," New Generation Computing Volume 28, Number 2, 137-146.

[2] L.D. Stein, J.N. Stewart, The World Wide Web Security FAQ, version 3.1.2, February 4, 2002, Available from <http://www.w3.org/Security/Faq>.

[3] J. Mirkovic, J. Martin, P. Reiher, a taxonomy of DDoS attacks and DDoS defense mechanisms, UCLA CSD Technical Report no.020018.

[4] R.B. Lee, Taxonomies of Distributed Denial of Service networks, attacks, tools and countermeasures, Princeton University, Available from <http://www.ee.princeton.edu/~rblee>.

[5] Christos Douligeris , Aikaterini Mitrokotsa DDoS attacks and defense mechanisms: classification State-of- the-art, sciencedirect, 2003.

[6] Chonka, A. and Y. Xiang, Protecting Cloud Web Services from HX-DoS attacks using Decision Theory. 2012.

[7] Yassin W., Udzir N. I., Muda, Z., Abdullah A.and Abdullah M. T., "A cloud-based intrusion detection service framework", International Conference on Cyber Security, Cyber Warfare and Digital Forensic, IEEE, Malaysia, pp. 213-218, 2012.

[8] Myerson, Roger B. (1991). Game Theory: Analysis of Conflict, Harvard University Press, p. 1. Chapter- preview Links.

[9] G. Karanikas, T. Tryfonas, G. Oikonomou, T. Spyridopoulos; A game theoretic defense framework against DoS/DDoS cyber attacks , sciencedirect 2013.

[10] Transactions on Computers, pages 195–208, 2003.4] Xu and W. Lee. Sustaining availability of web services under distributed denial of service attacks. IEEE