Different Types Of Distributed Denial Of Service Attack Detection And Prevention Techniques

P. Subhashini, K. Sai Nithin, Ms. E. Hemalatha, Dr. Akalpita Das

Abstract : Distributed Denial of Service (DDoS) attack is a Denial of Service (DoS) attack that is made in large scale over a potential service in distributed environment. Adversaries targeting such attack makes a sustainable effort to exploit software vulnerabilities in computers through which attack is made on a target server. Such computers that unwittingly cooperate attacker are known as zombies where attacker keeps malicious piece of software known as agent. As countermeasures are being developed from time to time, the attackers are enhancing their tools to launch DDoS attacks. In this context, it is essential to have counter measures that defend existing and future DDoS variants. However, it needs thorough understanding pertaining to scope and detection methods for handling such massive attacks. This paper provides insights on different terms associated with DDoS attacks, different attack types and counter-measures existing. It also covers the attacks and countermeasures in cloud computing. Provided comprehension of the DDoS attacks and their scope, it is possible to device new countermeasures for well-known and future DDoS attacks.

Keywords : DoS, Distributed Denial of Service (DDoS) attack, Security, Cloud Computing

1. INTRODUCTION

Denial of Service (DoS) is the attack in which an attacker sends fake requests to a server which will become busy and cannot serve genuine requests. When this attack is made in large scale in a distributed environment, it is known as DDoS attack [1]. DDoS attacks caused huge losses to organizations. It is reported that these attacks are occurring frequently. It is the problem that needs sustainable effort. The existing solutions may not be sufficient in future as the attackers invent new model operandi for launching such attacks. Therefore, it is essential to have knowledge on various attacks and counter measures in cloud computing or in distributed computing in general. This paper provides review of many kinds of DDoS attacks, their counter measures. It also covers DDoS attacks that target servers in cloud computing environment including attack scenario, methods for detection, prevention and mitigation besides the procedure followed to handle DDoS attacks.In the literature found in [1]- [20] there are many approaches found in detecting DDoS attacks and preventing them. Preventing flooding attacks is studied in [1], [7] and [10]. The usage of different botnets for launching attacks is explored in [2], [3], [13]. From the literature it is understood that there is need for further research on the DDoS attack detection and prevention mechanisms. However, it is essential to understand them first. Towards this end, in this paper, we have reviewed literature that includes DDoS attacks in distributed environments and also cloud environments. The remainder of the paper is structured as follows. Section 2 focuses on DDoS attack models. Section 3 provides handshake method to detect attacks. Section 4 focuses on DDoS attacks and counter measures in cloud computing. Section 5 concludes the paper and provides directions for future work.

- *P. Subhashini is associate professor in computer science and engineering in MLRIT, Hyderabad, India. E-mail: subhashinivalluru@gmail.com*
- *K. Sai Nithin, Is currently pursuing Master's at MLR Institute of Technology, Hyderabad India. E-mail : sainithin.karra@gmail.com*
- *Ms. E. Hemalatha is associate professor in computer science and engineering in JNTUH, Hyderabad, India. Email: hemamorarjee@jntuh.ac.in*
- *Dr. Akalpita Das is associate professor in computer science and engineering in GIMT, Guwaati, India. E-mail: akalpita_cse@gimt-guwahati.ac.in*

2. DDOS ATTACK MODELS

As presented in Figure 1, there are different DDoS attack models. They are broadly classified into agent-handler models and IRC based models. The former is of two types again based on communication system. They are known as client-handler communication and agent-handler communication. The IRC based DDoS attack networks may use either public channel or secret or private channel.

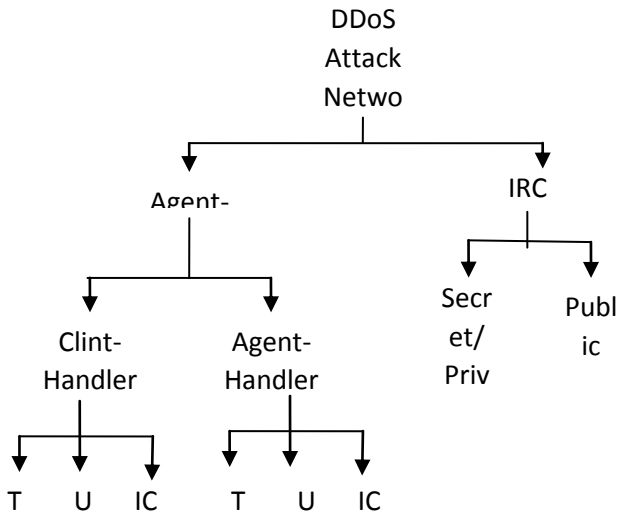

Figure 1: *Different types of DDoS attack networks*

As presented in Figure 1, there are different protocols associated with the agent – handler based attack models. These protocols are exploited by the attackers to launch DDoS attackers.

2.1 Agent-Handler Model

The agent handler based model contains different things in the attack network. They include agents, handlers and clients. Client is the platform with which attacker communicates. The handlers are nothing but the software packages through which attacker communicates to agents. Agent is the malicious code used to launch attacks. Attacker make attacks in such a way that the presence of attackers is hidden and it cannot be traced. They use different communication protocols such as TCP, ICMP or UDP.

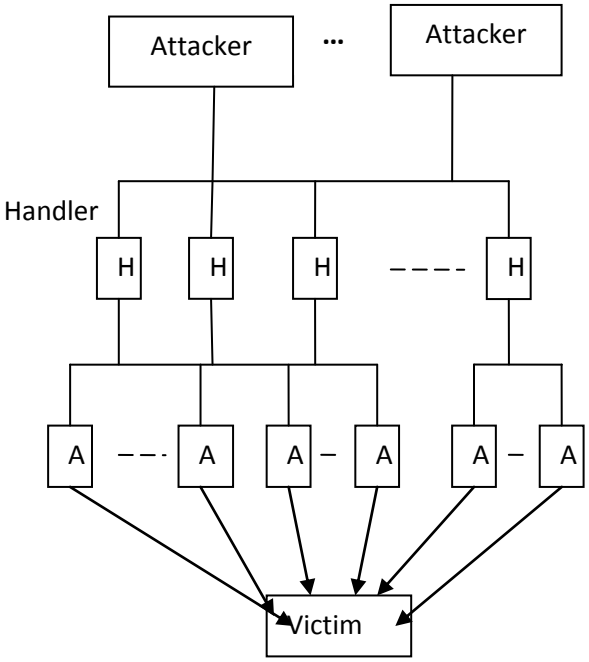

Figure 2: *Agent-Handler model*

In descriptions of DDoS tools, the terms handler and agents are sometimes replaced with master and daemons respectively. Also, the systems that have been violated to run the agent software are referred to as the secondary victims, while the target of the DDoS attack is called the (primary) victim.

2.2 IRC-Based DDoS Attack Model

Internet Relay Chat (IRC) is a multi-user, on-line chatting system. It allows computer users to create two-party or multi-party interconnections and type messages in real time to each other [6]. IRC network architectures consist of IRC servers that are located throughout the Internet with channels to communicate with each other across the Internet. IRC chat networks allow their users to create public, private and secret channels. Public channels are channels where multiple users can chat and share messages and files. Public channels allow users of the channel to see all the IRC names and messages of users in the channel [7]. Private and secret channels are set up by users to communicate with only other designated users. Both private and secret channels protect the names and messages of users that are logged on from users who do not have access to the channel [8].

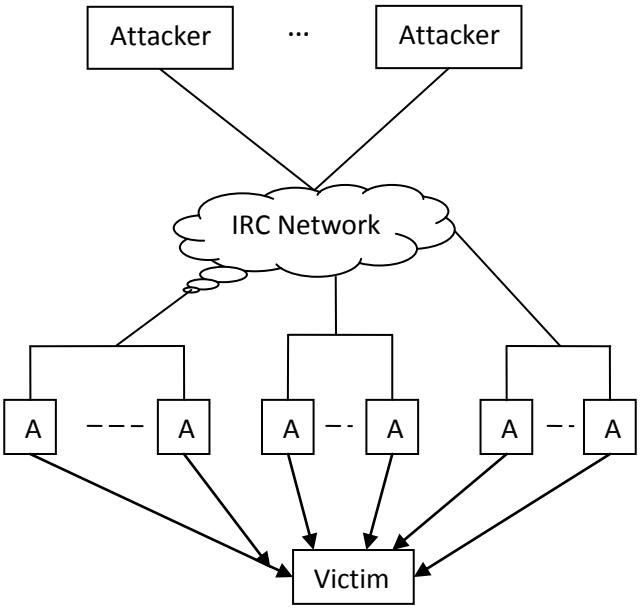

Figure 3: *IRC-Based DDoS attack model*

An IRC-Based DDoS attack network is similar to the Agent-Handler DDoS attack model except that instead of using a handler program installed on a network server, an IRC communication channel is used to connect the client to the agents. By making use of an IRC channel, attackers using this type of DDoS attack architecture have additional benefits. For example, attackers can use “legitimate” IRC ports for sending commands to the agents [9]. This makes tracking the DDoS command packets much more difficult. Additionally, IRC servers tend to have large volumes of traffic making it easier for the attacker to hide his presence from a network administrator. A third advantage is that the attacker no longer needs to maintain a list of agents, since he can simply log on to the IRC server and see a list of all available agents [9].

3. HANDSHAKE PROCESS TO DETECT ATTACKS

There is possibility of using 3 way handshake in order to identify presence or absence of DDoS attacks. In the three way hand shake between normal user and victim or server, there is genuine process that will be carried out. The acknowledgement is given back from genuine users.

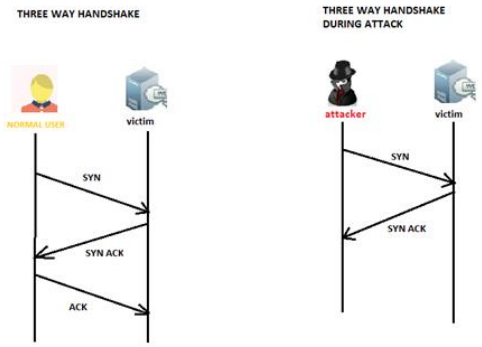

Figure 4: *Handshake process to detect DDoS attack*

As can be seen in Figure 4, the three way handshake provides the ability to know the presence or absence of attacker. In case of an attaker sending requests to victim, the SYN ACK is given by victim server to attaker. However, attacker does not send the ACK back to the victim server. This is the proof to know the presence of an attacker.

4. DDOS ATTACKS IN CLOUD COMPUTING

In the contemporary era, organizations attach much importance to the data. Traditionally data is maintained in secondary storage media. With the emergence of cloud, there is shift in the paradigm. Enterprises, due to exponential growth of data, are outsourcing data to public cloud. Outsourcing large volumes of data to cloud has many advantages including cost effectiveness and elasticity. In fact, cloud storage helps in economy of scale, data redundancy techniques, the concept of tiers in data management for reducing cost, and Service Level Agreements (SLAs) for safeguarding interests of cloud consumers. It also provides service without time and geographical restrictions besides supporting business continuity, elasticity, flexible pay options, increased mobility and cost effectiveness. Figure 5 shows cloud based environment with physical and virtual machines.

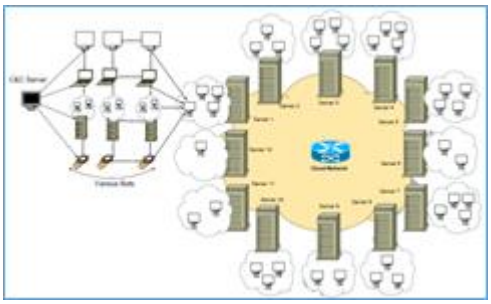

Figure 5:*DDoS attack scenario in cloud environment*

As explored in [8], there are different cloud platforms. However, there is specific DDoS attack scenario illustrated in Figure 5. There is need for protection from such attacks. Various bots are used to launch DDoS attacks. When multiple machines are compromised and used as zombies, they can use the agent injected by the attacker and launch attacks in a massive scale. There are many reasons for the success of attacks in cloud.

4.1 Auto Scaling

Due to virtualization technology cloud computing became affordable. There are concepts of using VMs on top of physical machines to have scaling. Auto-scaling is another important feature of cloud. It is explored in [16] where auto scaling provision of cloud is illustrated. It is possible to scale it dynamically as and when needed at runtime. Thus auto-scaling is an important feature of cloud that may be exploited by attackers.

4.2 Pay-as-you-go accounting

Another important feature used by attackers from cloud is that the provision for sharing resources in pay per use fashion. Thus they cloud gain resources for attack from the cloud. Resources can be added on the fly based on the need. Thus due to affordable pricing of cloud, attaackers may exploit its reosurces to launch DDoS attacks.

4.3 Multi-Tenancy

Multi-tenancy is the technique that helps in executing more than one VM of different VM owners in a physical server. This will help in increasing the hardware utilization and improves returns on investment to the cloud server providers. This feature also can be exploited by the attackers.

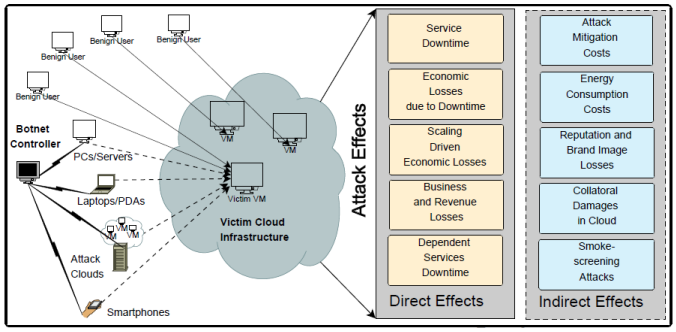

Figure 6*:DDoS attack in cloud, its effects*

As presented in Figure 6, there are direct and indirect effects of DDoS attacks. The direct attacks include service downtime, economic losses to the victim organization due to service downtime, scaling driven economic losses, business and revenue losses and dependent services downtime. There are indirect effects of DDoS attacks in cloud computing. They include smoke screening attacks, collateral damages in cloud, reputation and brand image losses, energy consumption costs and attack mitigation costs.

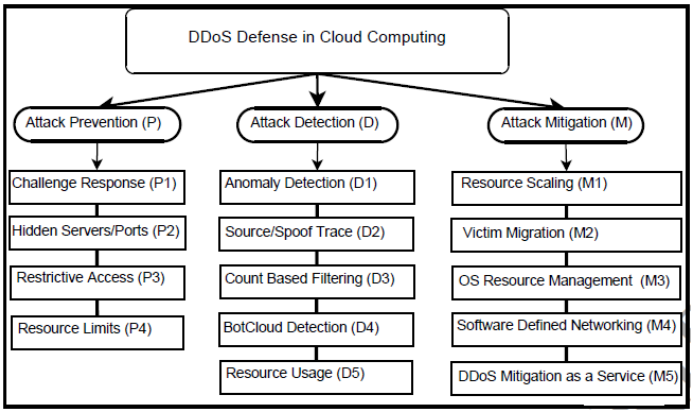

Figure 7: *DDoSdefense mechanisms in cloud computing*

As presented in Figure 7, there are many attack prevention approaches such as a challenge response system, hidden servers, restrictive access and resource limits. Attack detection methods include anomaly detection, source/spoof trace, count based filtering, BotCloud detection and resource usage. Attack mitigation methods on the other hand include resource scaling, victim migration, OS resource management, software defined networking (SDN) and DDoS Mitigation as a Service.

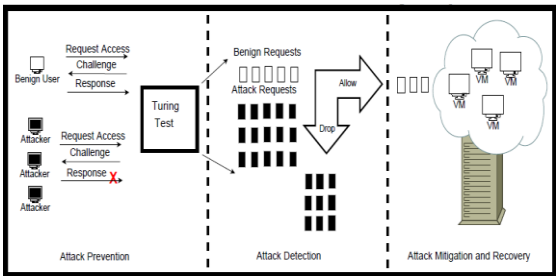

Figure 8: *Protection against DDoSattack at different levels*

As shown in Figure 8, challenge response system is followed to prevent attacks. When a challenge is thrown by the system, there will be no response from the attacker. Such requests will not be processed. Some attacks overcome this. In such cases attack detection is carried out followed by attack mitigation and recovery.

4. SUMMARY OF FINDINGS

This section provides summary of important findings of the review that has been carried out. It throws light into different techniques, merits and demerits.

Table 1: *Shows the summary of findings*

Reference	Technique	Advantages	Limitations	Utility
[1]	Dynamic Path Identifier (D-PID)	Effectively prevent DDoS flooding attacks.	Still there is scope for enhancing this approach with highly dynamic configurations.	Helps in understanding DDoS attacks especially flooding attacks.
[5]	Survey of DDoS attacks.	Provides methodologies for detecting DDoS attacks	Solutions are theoretical in nature and to be improved with empirical study.	Helps in ascertaining different methods to detect DDoS attacks.
[6]	Bandwidth DDoS attack detection strategies.	Prevents BW-DDoS attacks	Theoretical foundation and not empirical details.	Comprehension on BW-DDoS
[7]	Defense mechanisms against DDoS flooding attacks.	Prevents flooding kind of DDoS attacks	Theoretical foundation without practical work.	Helped in understanding data mining design principles for big data mining.
[8]	Provides techniques for preventing DDoS attacks in P2P networks.	Prevents DDoS attacks in P2P networks.	The solutions are theoretic in nature.	Good comprehension on DDoS in P2P networks.
[9]	DDoS as scalability problem	Both push and pull attacks are prevented.	Solution depends on infrastructurescalability	Provides good comprehension on the scalability issues.
[10]	FireCol	Prevents DDoS intrusions	Low overhead solution	Gives knowledge on collaborative protection network.
[11]	New information metrics	Measure the presence of traffic anomalies	Limited to low-rate DDoS attacks	Comprehends low-rate DDoS attacks.
[13]	SpotIt	Network layer DoS defense is provided	DoS resistant network architecture is still desired	Network layer DoS prevention
[18]	Bloom filter forwarding	DoS attacks on bloom filter forwarding are prevented.	Theoretical foundation is provided.	Helps in comprehending bloom filter forwarding
[20]	Keeping path identifiers secret	Improves performance to prevent DDoS attacks	Forgeable PID can cause issues.	PIDs and their probability to forgery are understood.

As presented in Table 1, there are different mechanisms to deal with DDoS attacks. Such attacks in different kinds of wide area networks, prevention measures, their merits and demerits are summarized.

5. CONCLUSIONS AND FUTURE WORK

DDoS attacks caused huge losses to organizations. It is reported that these attacks are occurring frequently. It is the problem that needs sustainable effort. The existing solutions may not be sufficient in future as the attackers invent new model operandi for launching such attacks. Therefore, it is essential to have knowledge on various attacks and counter measures in cloud computing or in distributed computing in general. This paper provides review of many kinds of DDoS attacks, their counter measures. It also covers DDoS attacks that target servers in cloud computing environment including attack scenario, methods for detection, prevention and mitigation besides the procedure followed to handle DDoS attacks. From the review, it is understood that, providing counter measures to DDoS attack is not a onetime solution. It is therefore an open problem to improve the state of the art from time to time for business continuity and growth. It is also important to detect DDoS spoofed and non-spoofed attacks. Another important aspect of the research is to effectively discriminate between DDoS attacks and flash crowds. Our future work is aligned on these lines towards an effective framework for detecting and preventing DDoS attacks.

REFERENCES

[1] Luo, H., Chen, Z., Li, J., & Vasilakos, A. V. (2017). Preventing Distributed Denial-of-Service Flooding Attacks With Dynamic Path Identifiers. IEEE Transactions on Information Forensics and Security, 12(8), 1801–1815.

[2] Hossein Rouhani Zeidanloo, Mohammad Jorjor Zadeh shooshtari, Payam Vahdani Amoli,M.
Safari and Mazdak Zamani. (2010). A Taxonomy of Botnet Detection Techniques. IEEE, p1-5.

[3] Jerome Fran¸cois, Shaonan Wang, Radu State, and Thomas Engel. (2011). BotTrack: Tracking Botnets using NetFlow and PageRank. IEEE, p1-15.

[4] Kumar V. P., Sundaram, A. P., Kumar M. B., and Iyengar N. Ch. S. N (2011). Analysis ofDDoS Attacks in Distributed Peer to Peer Networks. Journal of Global Research in ComputerScience, 2(7), p10-16.

[5]Monowar H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya and J. K. Kalita. (2012). DetectingDistributed Denial of Service Attacks: Methods, Tools and Future Directions. The ComputerJournal, p1-20.

[6] Opeyemi.A.Osanaiye. (2015). hort Paper: IP Spoofing Detection for Preventing DDoS Attack in Cloud Computing . International Conference on Intelligence in Next Generation Networks, p139-141.

[7] Carlin, A., Hammoudeh, M., &Aldabbas, O. (2015). Defence for Distributed Denial of Service Attacks in Cloud Computing. Procedia Computer Science, 73, 490–497.

[8] Choi, J., Choi, C., Ko, B., & Kim, P. (2014). A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft Computing, 18(9), 1697–1703.

[9] MohdNazri Ismail, AbdulazizAborujilah, Shahrulniza Musa and AAmirShahzad. (2012). New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment . International Journal of Computer Science and Security . 6 (4), p1-12.

[10] J. Francois, I. Aib, and R. Boutaba, “Firecol: a Collaborative Protection Network for the Detection of Flooding ddos Attacks,” IEEE/ACM Trans. on Netw., vol. 20, no. 6, Dec. 2012, pp. 1828-1841.

[11] Y. Xiang, K. Li, W. Zhou, “Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics,” IEEE Trans. on Inf. Foren. and Sec., vol. 6, no. 2, pp. 426 - 437, May 2011.

[12] T. Koponen, S. Shenker, H. Balakrishnan, N. Feamster, I. Ganichev, A. Ghodsi, P. B. Godfrey, N. McKwoen, G. Parulkar, B. Raghavan, J. Rexford, S. Arianfar, D. Kuptsov, “Architecting for innovation,” ACM Comput. Commun. Rev., vol. 41, no. 3, July 2011,

[13] X. Liu, X. Yang, and Y. Lu, “To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets,” In Proc. SIGCOM- M’08, Aug. 2008, Seattle, WA, USA.

[14] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, “Pathlet routing,” in Proc. SIGCOMM’09, Aug. 2009, Barcelona, Spain, pp. 111 - 122.

[15] H. Luo, Z. Chen, J. Cui, H. Zhang, M. Zukerman, C. Qiao, “CoLoR: an information-centric internet architecture for innovations,” IEEE Network, vol. 28, no. 3, pp. 4 - 10, May 2014.

[16] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, kc claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, “Named data networking,” ACM Comput. Commun. Rev., vol. 44, no. 3, pp. 66 - 73, Jul. 2014.

[17] D. Raychaudhuri, K. Nagaraja, A. Venkataramani, “MobilityFirst: a ro- bust and trustworthy mobility-centric architecture for the future Internet,” Mobile Comput. and Comm. Rev., vol. 16, no. 3, pp. 2 - 13, Jul. 2012.

[18] M. Antikainen, T. Aura, M. Sarela, “Denial-of-service attacks in bloom- filter-based forwarding,” IEEE/ACM Trans. on Netw., vol. 22, no. 5, pp. 1463 - 1476, Oct. 2014.

[19] H. Luo, Z. Chen, J. Cui, H. Zhang, “An Approach for Efficient, Accurate, and Timely Estimation of Traffic Matrices,” In Proc. IEEE Global Internet Symposium (GI’14), May 2014, Toronto, Canada, pp. 67-72.

[20] H. Luo, J. Cui, Z. Chen, M. Jin, H. Zhang, “Efficient integration of software defined networking and information-centric networking with CoLoR,” in Proc. IEEE GLOBECOM’14, Dec. 2014, Austin, TX, USA, pp. 1962-1967.