I. J. Computer Network and Information Security, 2017, 3, 36-44
Published Online March 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.03.05

Distributed Defense: An Edge over Centralized Defense against DDos Attacks

Karanbir Singh
Research Scholar, Dept of R.I.C, I. K. Gujral Punjab Technical University, Jalandhar, Punjab, INDIA
E-mail: karan_nehra@yahoo.co.in

Kanwalvir Singh Dhindsa
Professor, Dept. of CSE, Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib, Punjab, INDIA.
E-mail: kdhindsa@gmail.com

Bharat Bhushan
Associate Prof., Dept of Computer Application, Guru Nanak Khalsa College, Yamunanagar, INDIA
E-mail: bharat_dhiman@sify.com

Abstract—Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a target/victim system or network resource/service. It can be launched indirectly through many compromised machines on the Internet. The Purpose behind these attacks is exhausting the existing bandwidth and makes servers deny from providing services to legitimate users. Most detection systems depend on some type of centralized processing to analyze the data necessary to detect an attack. In centralized defense, all modules are placed on single point. A centralized approach can be vulnerable to attack. But in distributed defense, all of the defense modules are placed at different points and do not succumb to the high volume of DDoS attack and can discover the attacks timely as well as fight the attacks with more resources. These factors clearly indicate that the DDoS problem requires a distributed solution than the centralized solution. In this paper, we compare both types of defense mechanisms and identify their relative advantages and disadvantages. Later they are compared against some performance metrics to know which kind of solution is best.

Index Terms—DoS, DDoS, Distributed Denial of Service Attacks, Comparison, Distributed Defense, Centralized Defense.

I. Introduction

Nowadays, many attacks are based on the so-called distributed denial-of-service (DDoS) attacks. The DDoS attack is launched by sending a large number of attack packets to a target machine/network through the use of some compromised machines distributed throughout the Internet. The attack happens when multiple machines on the internet consume the bandwidth or exhaust the resources of particular system/network by sending a large number of attack packets [1, 2, 3]. DDoS attacks came into existence in February 2000 when some famous websites like CNN.com, Yahoo.com etc. goes down by this attack. In July 20019, some major websites from the United States and South Korea will also get affected by this attack. Some social networking sites, including Facebook, Twitter, Live journal, etc. were also got affected by this attack. In December 2010, the famous financial houses like Mastercard, PayPal, Visa [4] are also get affected by DDoS attacks. Online internet banking sites of some major banks of United States are always being under threat against powerful DDoS attacks [5]. In today's scenario, everybody will get dependent on the internet and computer to perform various day to day activities. Due to lack of appropriate knowledge of internet and its security, networks/servers can easily become the victims of DDoS attack. So DDoS attacks are very dangerous and they need to be handled properly.

The four entities involved in a DDoS attack are attacker, agents, master control program and victim. The attacker is the person which is responsible for the execution of the attack. It can choose any particular machine or network on the internet against which attack is to be performed. It further recruits some master control programs which mask it's existence and helps in performing the attack. Master control programs further identify and compromise some machines on the internet which can be used as attacking agents. Master control program acts as a bridge between the attacker and the attacking agents. The agents are compromised machines capable of sending an attacking stream to a particular victim on the internet. The attacker asks master control program to perform an attack against a particular victim. Further master control program instructs agents to send attack stream to a particular target. The agents then start sending a flood of attack packets to the intended victim. The amplification of attack can be increased by recruiting more number of agents. Figure 1 illustrates the various phases in the process of executing a DDoS attack on a victim.

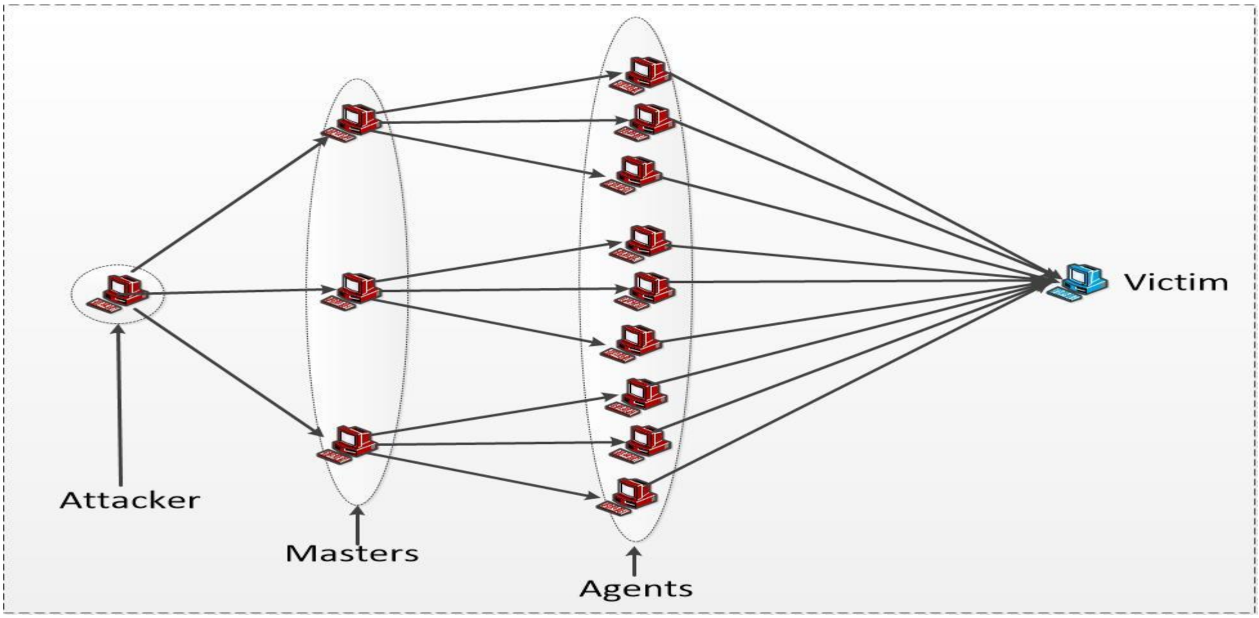

Fig.1. Execution of a DDoS attack

II. Classification of DDoS Attack & Defense Mechanisms

To understand DDoS attacks, it is necessary to understand their classification. A detailed classification of DDoS attack and defense mechanisms is already identified in [16]. In this section, we will discuss various DDoS attack and defense mechanisms.

A. DDoS Attack Mechanisms

There are a wide variety of DDoS attacks but we put them into two important categories. The main categories of DDoS attacks are bandwidth depletion and resource depletion. Figure 2 shows various categories of DDoS attacks.

(1) Bandwidth Depletion:

In *Flood attack*s, the agents send large volumes of IP traffic to the target in order to congest the target's system bandwidth. Some of the well-known flood attacks are UDP and ICMP flood attacks. The *Amplification attack* uses the broadcast IP address feature available in routers to increase and reflect the attack. This feature allows sending messages to a broadcast IP address. It instructs the routers servicing the packets to send them to all IP addresses within the broadcast address range. This creates attack traffic and thus shrinks the target system's bandwidth. Some famous amplification attacks are fraggle and smurf attacks.

(2) Resource Depletion:

The *Protocol exploit attack*, exploits some implementation bug or a specific feature of some protocol installed on the victim's machine. A good example of this attack is TCP SYN attack. It exploits the inherent weakness of 3-way handshake involved in the TCP handshake. An attacker can initiate an SYN flooding attack by sending a lot of SYN packets and never acknowledges any of the replies, so putting the server waiting for ACK's which does not exist. Other examples are PUSH + ACK, CGI request, and authentication server attacks. The *Malformed packet attacks* rely on incorrectly formed IP packets that are sent from agent to the victim's machine. It can be divided into types: IP address and IP packet options attack.

B. DDoS Defense Mechanisms

The importance of the DDoS problem and the amplified rate of DDoS attacks require the introduction of various DDoS defense techniques. Many of these techniques solve different type of DDoS attack at different locations on the internet with a different degree of cooperations. We can classify the DDoS defense mechanisms based on three different criteria: activity level, deployment location and degree of cooperation as shown in figure 3.

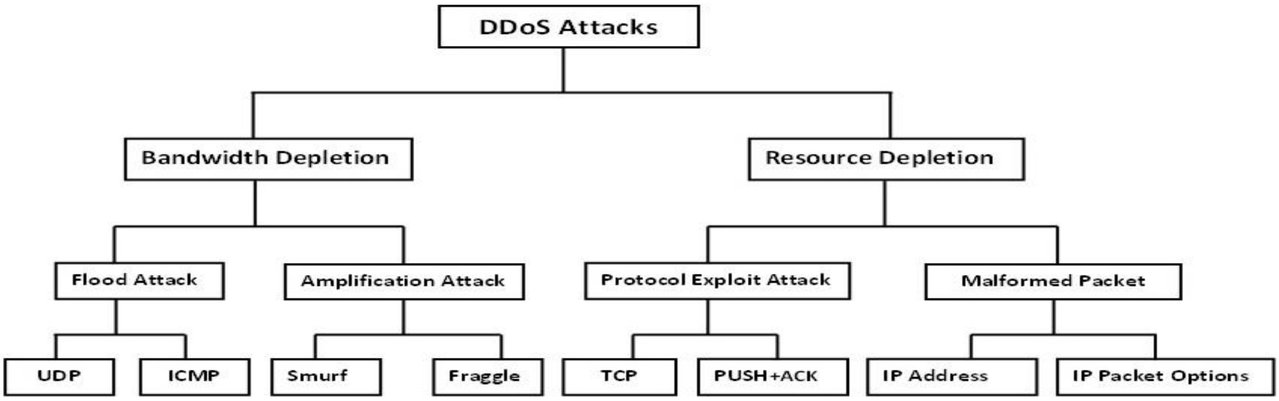

Fig.2. Categories of DDoS Attacks

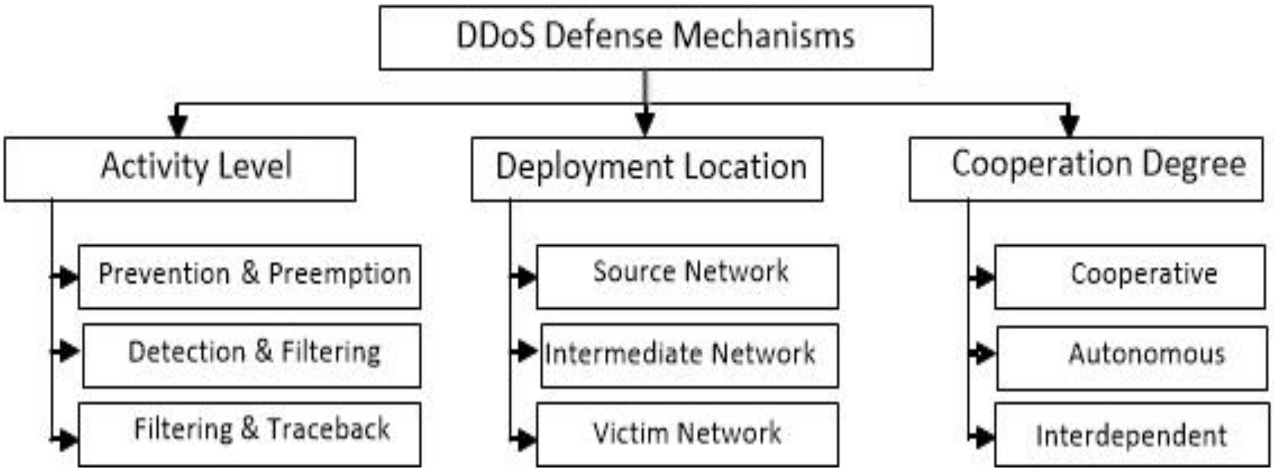

Fig.3. Classification of DDoS defense mechanisms

(1) Activity level based defense:

DDoS attacks can be handled in the following three ways. They are:

1. Attack prevention and pre-emption (to be done before the attack happens),
2. Attack detection and filtering (to be done during the happening of attack),
3. Attack source traceback and identification (to be done after the attack happens).

The first line of defense prevents from the happening of DDoS attacks. This can be done by securing hosts and networks from attacker's activity by using software's like antivirus, anti-trojans, and firewalls. Attack detection mainly deals with the identification of DDoS attacks and filtering is used to drop attack packets identified during detection phase. Many traffic monitoring systems have been developed to detect signs of attacks either by verifying the presence of attack signatures or by detecting variances in the traffic characteristics. Attack source traceback and identification are used to find out the real source of the attacker. The effectiveness of attack defense relies on false positive ratio and false negative ratio. The false positive ratio is the number of packets categorized as attack packets but in reality they are the legitimate one. The false negative ratio is the reverse case.

(2) Deployment location based defense:

The attack traffic originates from different distributed attacker machines. This traffic is then forwarded by intermediate routers and converges at victim's network. This process involves three kinds of networks: source side networks which generate attack traffic, many intermediate networks that forward the attack traffic towards the victim and finally the victim network containing the victim. The DDoS defense system can be deployed at any of these participating networks (i.e. source network, intermediate network or victim network). Victim network-based defense solutions increase the victim capability to identify that it is the victim of an attack and having more time to react. Intermediate networks are more effective in handling traffic and trace back to the attack source. Source networks are to the best place to stop attacks at the early stages and it also prevents them to enter in the intermediate networks.

(3) Cooperation degree based defense:

There are three methods of defense based on the degree of cooperation. They are autonomous, cooperative and interdependent mechanisms. Autonomous defense mechanism performs the task of attack detection and response independently. These defense systems are normally placed at any single place on the internet to defend that local network. Firewalls perform as an autonomous defense mechanism. Cooperative defense mechanisms can perform better through the cooperation with other defense entities. Interdependent mechanisms cannot operate autonomously. For attack detection and response they depend on other entities.

III. Comparison between Centralized & Distributed Defense

There exist many defense systems in literature which work either in a centralized manner or distributed manner. In centralized defense, all the defense components are deployed at a single location as compared to distributed defense in which defense components will be placed on many deployment points/networks on the internet. The various components of distributed defense work collaboratively with each other to provide DDoS defense. Centralized defense solutions are normally deployed in the victim networks due to economic reasons. Centralized solutions are mostly not able to detect and stop attack traffic in the early stages. Sometimes centralized solutions itself become the victim of DDoS attacks due to their single instance. So centralized defense systems are mostly not able to handle DDoS attacks efficiently. A distributed defense system overcomes all the shortcomings of centralized defense systems. Table 1 illustrates some differences between centralized and distributed defenses based on some important characteristics of DDoS defense mechanisms.

Table 1. Centralized vs Distributed Defense

Characteristics	**Centralized Defense**	**Distributed Defense**
Security modules deployment	All the security components are deployed to a central location.	In this defense system, the security components are deployed at multiple places.
Fault isolation	The defense system is centrally located, making it easy to recover from a crash.	As the defense system is distributed making it difficult to recover.
Communication	No communication among modules is required because defense modules are located at the same place.	Communication among various modules distributed at multiple places is required.
Configurability	Easy, because a small number of components are required.	Difficult, because each component must monitor a set of host locally
Reliability	If any of the security components stop working then defense system comes to halt and will not work.	If any of the security components stop working then it will stop monitoring only a part network, not the rest.
Deployment location	Normally these defense systems are deployed at the source or victim end.	Deployed throughout the internet

IV. Defense Locations for DDoS Attacks

The attack traffic mostly originates from the source networks by the attackers. Source networks are further connected with intermediate networks. Intermediate networks are needed to connect source network with the target network. Intermediate networks forwards that attack traffic to the target network in which victim lies. The target network is also called a victim network. There can be more than one source networks which originate the attack traffic. So there are three networks which are responsible for the transportation of attack traffic from source to victim network. These networks are source network, intermediate network and victim network. If we combine all these networks together then it will be called a hybrid network. Figure 4 shows the various networks where a DDoS defense system can be deployed.

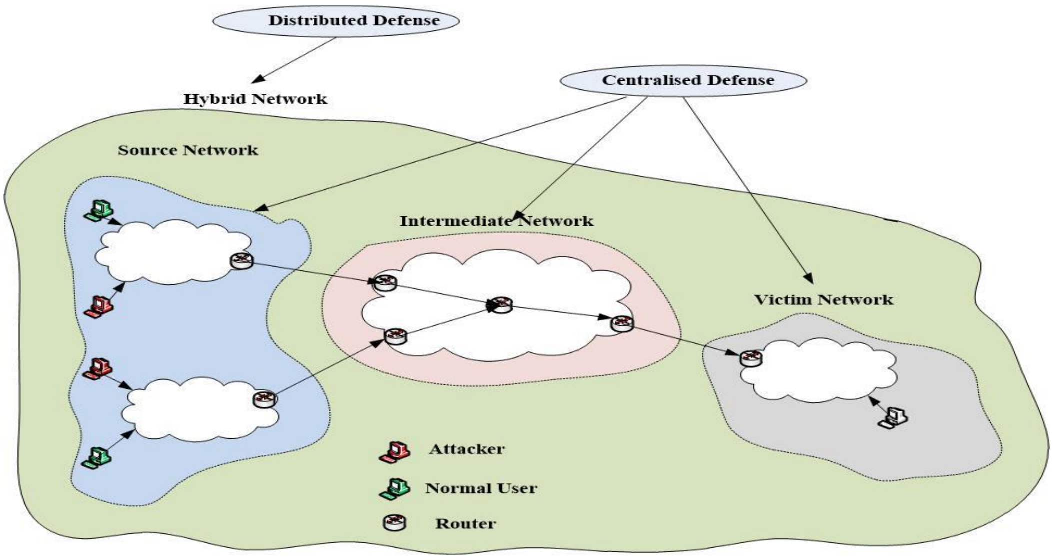

Fig.4. Different Deployment Locations for DDoS defense [6]

In literature, there exist many defense systems which work in centralized or distributed environment. A DDoS attack can be mitigated by putting the defense system on either of these three network locations i.e. source, victim or intermediate network. If we put a defense system in these locations then it is called a centralized defense system. The another method is to combine all these networks locations to form a hybrid or distributed network. If we put the defense components at all these locations (i.e. source, intermediate and victims networks) then it is called a distributed defense. Table 2 illustrates the various features, advantages and disadvantages of various deployment based centralized and distributed defense systems.

Table 2. Comparison of Different Location-Based Defense Systems

	Scheme Name	Features	Advantages	Disadvantages
Centralized Defense	Source-End Defense System	Defense system is deployed in the source networks	• It detects and filters attack traffic in the source network before it overwhelms the network • Less traffic needs to be checked in source networks which in terms consumes fewer resources	• Sometimes legitimate traffic will be misjudged as attack traffic • It is difficult to deploy defense system in source networks
	Victim-End Defense System	Defense system is deployed in victim's network	• Low cost and easy to deploy and manage • It is easy to detect attacks because high rate of resource consumption	• It waits for the attack traffic to reach the victim and hence it waste a lot of bandwidths • It results in overwhelming victim resource
	Intermediate Network Defense System	Defense system is deployed in the intermediate network on core routers	• More effective as all attack traffic will pass through core routers • It is the suitable place to filter attack traffic	• Difficult to process each packet as traffic volume is large • Implementation is difficult because it needs router reconfiguration
Distributed Defense	Hybrid Network Defense System	Defense system will be deployed on all above mentioned locations (i.e. source, victim and intermediate networks)	• Robust amongst the all as defense components will cover every network location • The task of detection and response can be distributed to achieve better defense	• It is difficult to manage as it needs cooperation between defense components • Complex and create extra overhead for networks

Each kind of deployment location has its advantages and disadvantages. But if we talk in terms of strong defense then distributed defense will be the only solution.

V. Existing DDoS Defense Mechanisms

A DDoS defense mechanism can be deployed at any of three above mentioned locations i.e. source network, victim network, intermediate network or on all these three locations. In this section, we will discuss some existing defense mechanisms from literature related to these categories.

A. Source Based Defense Mechanisms

Source based defense mechanisms are deployed in the source networks from where the attack originates. The can be placed on the edge router of the source network connecting. The source end defense methods have some advantages as compared to the victim and intermediate defenses. The attack traffic can be detected at the early stages which can reduce the further damage. Due to the low volume of attack traffic, it can be handled with less overhead. But it suffers from some drawbacks such as deployment issue and low volume of attack traffic sometimes cause collateral damage.

D-Ward is one of the popular source end based DDoS defense methods [7]. It detects and blocks attack traffic originating from source networks. But it has some issues like low attack volume sometimes punish legitimate traffic also. MULTOPS [15] is a data structure which detects and filter ongoing bandwidth attacks by monitoring the rate of incoming and outgoing traffic to a particular host or network. But this method cannot differentiate between a flash crowd and DDoS attack.

B. Victim-based Defense Mechanisms

There exist many defense mechanisms protects a victim's networks by monitoring and filtering attack traffic on the edge router or access router. These systems are desired to protect a particular network or individual hosts. These methods are easy to deploy but it wastes a lot of bandwidths.

Wang [9] proposed a victim based defense mechanism which can be installed on the edge routers connecting customer network to the ISP. This method detects traffic anomalies by monitoring the abnormal SYN-FIN pair. Chang [10] proposed a hop count filtering methods which use the TTL field in the IP header to count the hop count for every packet to detect DDoS attacks. It builds an IP to hop count mapping table to identify and filter spoofed IP packets.

C. Intermediate network based Defense mechanisms

Intermediate network-based defense mechanisms are basically placed on the core routers of internet service providers. They can effectively handle DDoS attack but at the cost processing, which can degrade the network performance.

Pushback [11] defense can be placed on the core routers to control high bandwidth attacks. If attack rate is high then it can request its upstream routers to control the flood. The main drawback of this scheme is that sometimes it can inflict to collateral damage. In [12] Dongwon proposed a probabilistic scheduling filter based method to detect DDoS attacks. In this filters can be put on core routers to identify attacks using probabilistic packet marking technique. The only drawback of this scheme is that it put extra overhead in the IP header.

D. Hybrid Defense Mechanisms

In hybrid defense mechanisms, the components of defense system are to be deployed in various locations on the internet. The components cooperate with each other to carry the DDoS defense. They provide a strong defense against any kind of DDoS attack but difficult to deploy and manage.

Defcom [13] put its defensive components on the source, victim, and intermediate network. The defense components communicate with each other to detect and response DDoS attacks. The effectiveness of defcom depends on how accurately the victim detects the traffic anomaly and the exchange of attack information during the defense process by the participating nodes. Speak-up [12] mechanism attempts to lower the attack request by encouraging all the clients to spontaneously send a high volume of traffic. The main purpose of this technique is that a major part of their upload bandwidth is already being taken by the attackers.

VI. Performance Evaluation

Here we have identified some performance parameters which be used to comparatively evaluate the performance of different deployment based defense techniques. The performance measurement metrics are as follows:

A. Attack Detection Accuracy

The accuracy of DDoS attack detection depends on many factors like the deployment location, the volume of attack traffic, and the techniques used for attack detection. There is mainly three kinds of techniques used for attack detection. They are anomaly based, attack signature based and third party attack detection tools. Each kind of technique has its own advantages and disadvantages like anomaly based techniques are more reliable as compared to signature based but they are not fast.

B. Network Performance

It is related to change of network protocols and resources during the deployment of DDoS defense system. Sometimes a defense system needs to do these changes which in result affect its performance. One example is the use of a router for packet marking during the defense process. It consumes some processing power and memory to carry out the marking process.

C. Reliability

It is the ability of a DDoS defense to remains available during the defense process. Sometimes attacker initially attacks the defense system to remove it from the way and later attack the victim. Centralized defense system is more prone to DDoS attack then distributed DDoS defense system because they centralized defense systems are deployed to a single location.

D. Implementation Complexity

It is related with issues like deployment of defense system will put a minimum effect on various networks devices like routers and network protocols. Sometimes in the case of distributed defense it difficult to convince an ISP to adopt a new defense system.

E. Robustness

It is the strength by which a defense method can handle DDoS attacks. The robustness depends on many components of defense method like its capability to accurately characterize the attack traffic, attack detection, attack response, attack traceback etc.

F. Scalability

It refers to the ability of a defense system to manage a number of attacks and networks if they grow in the future. Scalability is required when an organization needs to expand its business, which further increases its network size.

Table 3. Performance Comparison between Centralized and Distributed Defense Locations

	Type of Defense	**Attack Detection Accuracy**	**Network Performance**	**Reliability**	**Implementation Complexity**	**Robustness**	**Scalability**
Centralized Defense	Source-End Defense System	Low	Moderate	Low	Difficult	Low	Low
	Victim-End Defense System	High	Good	Low	Easy	Low	Low
	Intermediate Network Defense System	Medium	Moderate	Medium	Medium	Medium	Medium
Distributed Defense	Hybrid Network Defense System	High	Poor	High	Difficult	High	High

Table 3 gives the detailed comparison between different DDoS defense locations based on some performance metrics. The comparison clearly shows that distributed defense schemes can detect DDoS attacks with more accuracy than others. Distributed defense methods are more reliable as compared to centralized because their defensive components are placed in many locations. The centralized defense methods can easily become the target of DDoS attack due to their single location. Distributed defense are more robust and easily scalable as compared to centralized methods. The only drawback of distributed defense systems is that their implementation is difficult and they put some effect on the performance of the network. So in order to effectively defend a DDoS attack, the defensive components of a defense method need to put on source, intermediate and victim network. Distributed defense system will cover all the drawbacks of the centralized solution and hence they will be best if they can be implemented.

VII. Conclusion

DDoS is one of the biggest threats to the internet and its resources. This problem should be tackled with an appropriate defense method. Here we have discussed the classification of DDoS attack and defense mechanisms. Based on deployment location, a DDoS defense method can be put either in a centralized or distributed defense systems. These defense locations are compared against their features, advantages, and disadvantages. The comparison shows that distributed defense system are little more effective than centralized defense. But this comparison was not sufficient to prove their efficiency. We have also identified and discussed some existing defense mechanisms of each category from the literature.

Later in order to prove the effectiveness of distributed defense, we compared them against some performance metrics. The comparison clearly shows that distributed defense are better than centralized defense system. So in order to effectively control the DDoS attack, we must choose a distributed DDoS defense solution.

REFERENCES

[1] R. Chang, "Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial", In Telecommunications Network Security, IEEE Communications Magazine, pp. 42-51, October 2002.

[2] Y. Kim, W. Lau, M. Chuah, and H. Chao, " PacketScore: Statistics-based Overload Control against Distributed Denial-of-Service Attacks", IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 2, pp. 141-155, April-June 2006.

[3] F.Lau, S. Rubin, M. Smith, and L. Trajkovie, "Distributed Denial-of-Service Attack". In Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, USA, pp. 2275-2280, October 2000.

[4] "Operation Payback cripples MasterCard site in revenge for WikiLeaks ban", Dec. 8, 2010, [online] http://www.guardian.co.uk/media/2010/dec/08/operation–payback–mastercard–website–wikileaks

[5] T. Kitten, "DDoS: Lessons from Phase 2 Attacks", Jan. 14, 2013, [online] http://www.bankinfosecurity.com/ddos-attacks-lessons-from-phase-2-a-5420/op-1

[6] K. Singh, N. Kaur, and D. Nehra, "A comparative analysis of various deployment based DDoS defense schemes", In proceedings of 9th international conference on Quality, Reliability, Security and Robustness in Heterogeneous Network, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 115, pp. 606-616, January 2013

[7] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source", In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), pp. 312–321, 2002

[8] Y. He, W. Chen, W. Peng, and B. Xiao. "An efficient and practical defense method against DDoS attack at the source-end", In Proceedings of the 11th International Conference on Parallel and Distributed Systems, Washington, DC, USA, 2005 Vol. 02, pp. 265–269, July 2005

[9] H. Wang, D. Zhang, and K. Shin, "Detecting SYN flooding attacks", In Proceedings of IEEE INFOCOM, 2002

[10] J. Cheng, W. Haining and K. G. Shin. "Hop-count filtering: An effective defense against spoofed DDoS traffic", In Proceedings of the 10th ACM conference on Computer and communications security, pp. 30–41, October 2003.

[11] J. loannidis and S. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks", In Proceedings. of Network and Distributed System Security Symposium, San Diego, California, 2002.

[12] D. Seo, H. Lee, and A. Perrig, "PFS: Probabilistic filter scheduling against distributed denial-of-service attacks", In Proceedings of the IEEE 36th Conference on Local Computer Networks (LCN), Bonn, Germany, pp. 9–17, October 2011.

[13] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A Framework for a Collaborative DDoS Defense", In Proceedings of the 22nd Annual Computer Security Applications Conference, Miami, FL, USA, pp. 33-42, December 2006.

[14] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "DDoS defense by offense", SIGCOMM Computer Communications Review, Vol. 36, no. 4, pp. 303-314, August 2006.

[15] T. M. Gil, and M. Poleto, "MULTOPS: a data-structure for bandwidth attack detection", In Proceedings of 10th Usenix Security Symposium, Washington, DC, pp. 2338, August 2001

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

Authors' Profiles

Karanbir Singh is doing his Ph.D. in the field of Network Security from I. K. Gujral Punjab Technical University, Kapurthala, Punjab, India. He obtained his M.C.A degree from Kurukshetra University, Kurukshetra (Haryana), India. He has a teaching and research experience of more than 12 years. He is the member of various professional bodies like IAEME, UACEE, and IACSIT. He has authored more than 6 publications in the proceedings of various national and international conferences. His research interests are in the fields of Computer Networks, Network Security, and Adhoc Networks.

Kanwalvir S. Dhindsa is working as Professor in the department of CSE & IT at Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib (Punjab). He obtained his Ph.D. in Computer Engg. (In the field of Information Systems and Mobile Computing), and also M.Tech. degree from Punjabi University, Patiala (Punjab). He has been awarded the 'Best Ph.D. Thesis Award' in International conference held in association with Computer Society of India (CSI) at COER, Roorkee (Uttarakhand) in November 2014. He has guided more than 20 M. Tech. students and is currently guiding 8 Ph.D. scholars. He has authored more than 50 publications in various esteemed international journals and proceedings of national and international conferences. His current research interests are Big Data, IoT, Cloud Computing, Mobile Computing, Security and Networks.

Bharat Bhushan is employed as Head and Associate Professor in Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar, India. He has done Ph.D. in Computer Science & Applications from Kurukshetra University, Kurukshetra, India. His qualification also includes M.C.A and Master of Science (Physics). He has teaching and research experience of more than 26 years. He is professional Member of various National and International Associations. He has more than 30 research papers to his credit in various international/national journals and conferences. His research interests are in the fields of Software Quality and Mobile Networks.

How to cite this paper: Karanbir Singh, Kanwalvir Singh Dhindsa, Bharat Bhushan,"Distributed Defense: An Edge over Centralized Defense against DDos Attacks", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.3, pp. 36-44, 2017.DOI: 10.5815/ijcnis.2017.03.05