Distributed Denial of Service (DDoS) Attacks Comparative Impact Analysis and Mitigation Techniques: A Survey

Snehal Sathwara[1], Chandresh Parekh[2]

[1] *Student M.Tech. in Cyber Security, Dep. of IT & Telecom, Raksha Shakti University, Gujarat, India*
[2] *Assistant Professor (Telecom), Dep. of IT & Telecom, Raksha Shakti University, Gujarat, India*

ABSTRACT

In this digital era, networks and their capacities are continuously growing and significantly increasing their market space. Attackers are improving their skills and developing tools based on new concepts in cyber security to stay ahead in hacker's world by considering how it is powerful, easy to use and cost effective. Distributed Denial of Service (DDoS) attacks are furious problem with the internet services and the networks. This attacks are massively fired by distributing malicious computers. These attacks can be carried out in various forms such as servers crashing, router crashing, overwhelming the network with high traces, damaging server critical resources etc. These attacks have become very complex with respect to time scale such that existing security algorithms are not that much sufficient to counter and protect against this attacks. In North America 50% of companies experienced a DDoS attack. 83% of victims were attacked more than once. 54% of victims were hit more than 6 times. In past, few years DDoS attacks have signed noticeable damage to the targeted network's availability such as websites, online services and applications. Today anyone with black hat mindset can launch the attack. Availability of tools and cost effective attack services have made DDoS attacks more dangerous and more temporal than ever. In order to be in safe side from this attacks, it must be detected and mitigated quickly before the legitimate user access the target of attackers. In this paper, we are carrying out extensive survey of mitigation techniques and impact analysis.

Keyword : - *Cyber Security, Distributed Denial of Service, DoS/DDoS, Mitigation techniques, Botnet, Flooding*

1. INTODUCTION

Distributed Denial of Service (DDoS) attacks are a next version of Denial of Service (DoS) attacks. DoS attacks are traditional version. Several new techniques were deployed in the 90s for DoS attacks. On November 2nd 1988 the first DDOS attack was launched on websites caused almost 15% (about more than 5000) of the systems were infected and function was interrupted [1]. DoS is an attack which affects the legitimate users of the system resources by preventing, reducing or restricts the accessibility. These attacks are achieved by a bulk of packets at the victim side that impact his speed in network or his processing capabilities [2]. It is responsible for the unavailability of the websites and cause slow network performance. A Distributed Denial of Service (DDoS) attacks are performed through multiple compromised systems to the single targeted system. Mostly attackers develop botnets or zombie networks to attack on single target.

1.1 Denial of Service (DoS) attacks

In a Denial of Service (DoS) attack, an attacker produces flood on the system's resources by applying malicious packets to the targeted system which causes slow down the system performance or bringing the system down. Below listed are the example of DoS attacks:

- Flooding the victim with more traffic
- Flooding a service with more events
- Hanging a system by putting into infinite loop
- Crashing a TCP/IP by corrupt packets

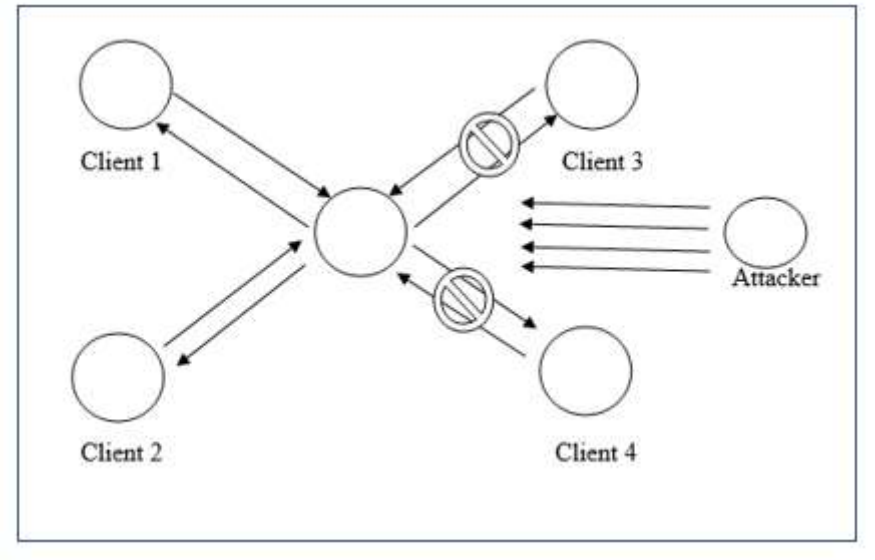

Fig -1: DoS Behavior in a Network

1.2 Distributed Denial of Service (DDoS) attacks

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents further process the connection request to the large number of the reflector systems with the spoofed IP address of the victim. They revert the response to the victim system and due to this flood will be generated at the victim system. With effect of this flood system of victim will ne shut down or may reduce the performance.

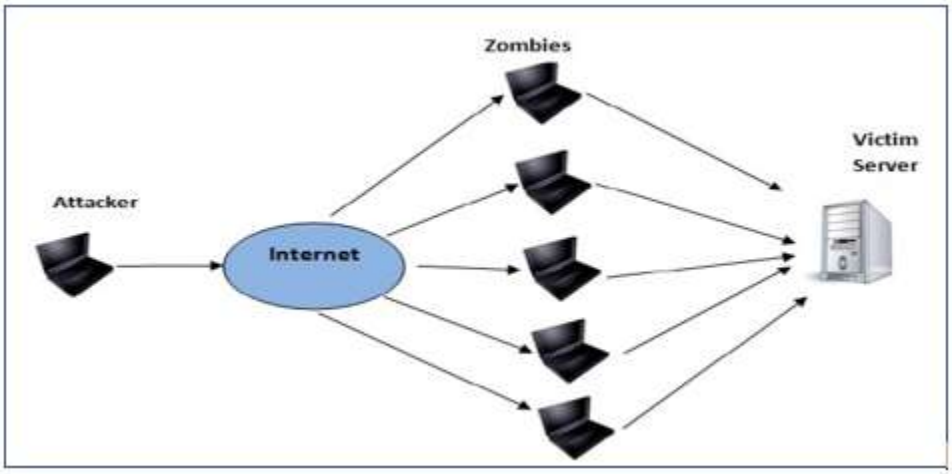

Fig -2: DDoS Behavior in a Network

2. CLASSIFICATION OF DDoS ATTACKS

Attackers deal with various techniques to launch DDoS attacks on the targeted system or networks. This techniques include Peer to Peer attack, SYN flooding, application level flooding, ICMP flooding, service request flooding, bandwidth attack, Permenant DoS and Distributed reflection Denial of Service. Following are the classification of the DDoS attacks.

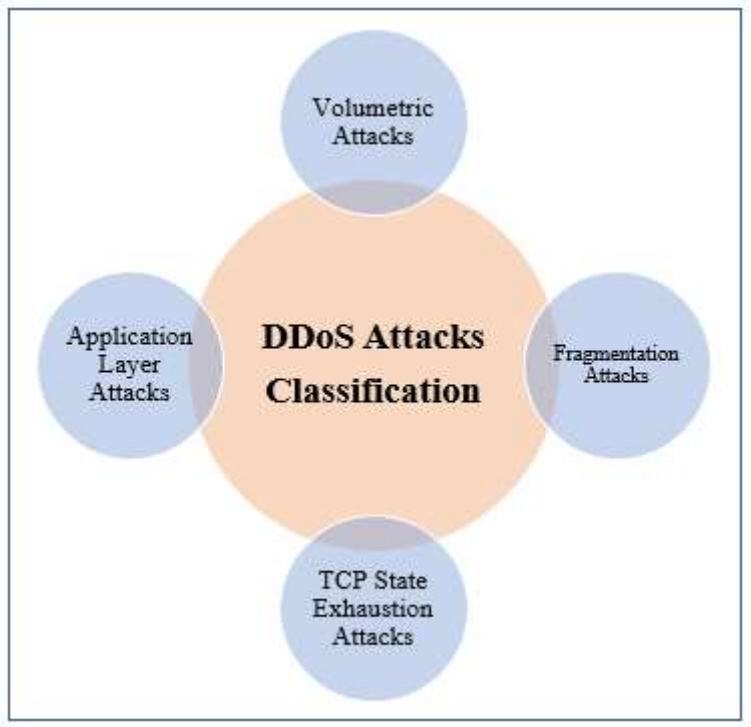

Fig -3: Classification of DDoS attack

- **Volumetric Attacks:** These attacks are based on bandwitdth which is used to generate the flood over the victim networks or targeted systems. Volumetric Attacks are measured in bits per second. System will be hang or shut down due to these attacks[3].

- **Fragmentation Attacks:** These kind of attacks are generated by flooding of TCP or UDP fragments which is very difficult to re-assemble for the victim system, resulting the reduce performance of the system [4][5].

- **TCP State Exhaustion Attacks:** These attacks applied the state of connection tables which are present in the network components like firewalls, load balancers and application servers. Unit of measurement is packets per second [5].

- **Application Layer Attacks:** These attacks are generated to destroy specific application or user services and resulting very slow performance or producing a low traffic rate which is measured in requests per second[6].

3. TECHNIQUES OF DDoS ATTACKS

DDoS attacks techniques are widely divided into three main types Bandwidth depletion attacks, Resource depletion attacks and Application attacks. The following are the techniques of DDoS Attacks[7].

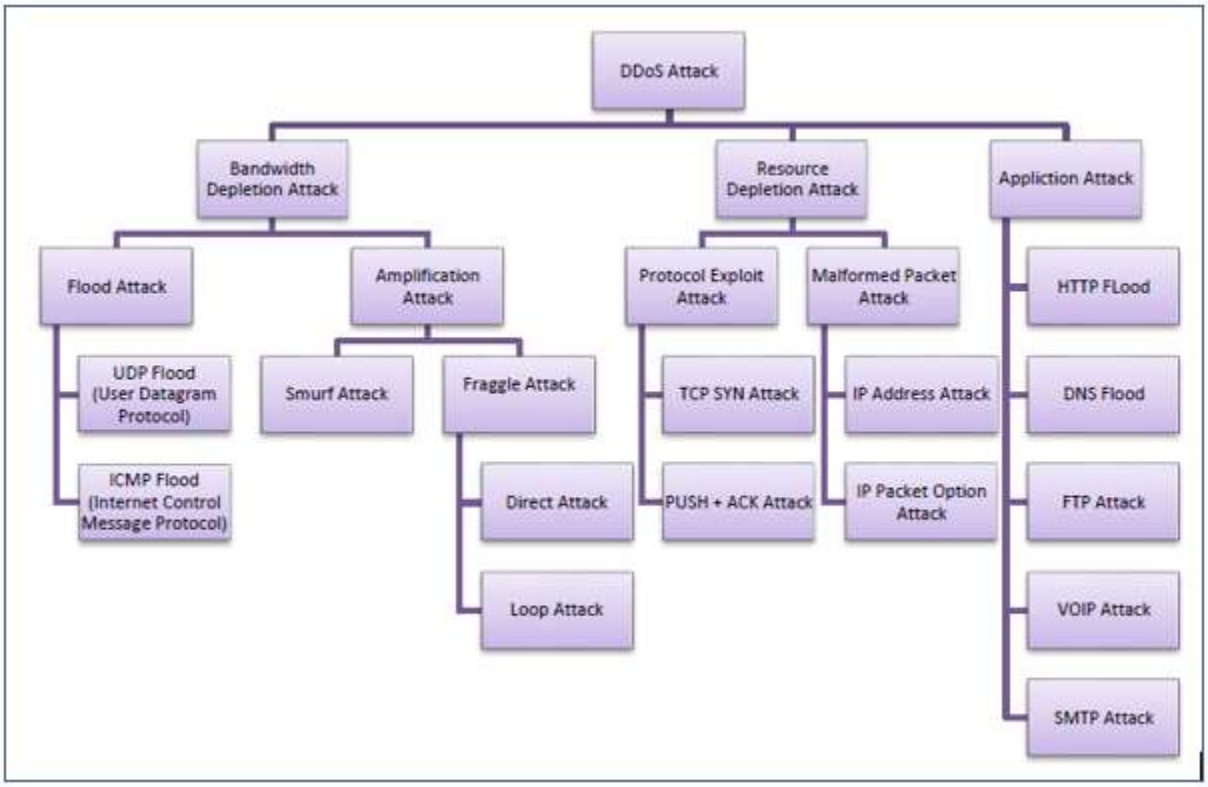

Fig -4: DDoS attacks techniques

- **Bandwidth Deplation Attacks:** This techniques are widely use to generate heavy flood by using higher bandwidth to the networks. It is unwanted traffic to prevent the legitimate traffic from reaching the victim's network. Trinoo is the one of the popular tools that cause the bandwidth depletion attacks in the network. These attacks can be further classified as flood attack and amplification attack [8].

- **Resource Depletion Attacks:** The resource depletion attack is targeted to band the resources of the victim's system. These attack can be further classified as Protocol Exploit Attack and Malformed Packet Attack. In which TCP SYN attack and IP address attack are most used in DDoS attack [7]. In Malformed packet attacks, packets contain malicious information or data to crack the victim's system. Malformed packets attacks are performef in two ways:
  a) IP address attack: In this attack, malformed packets are merged into origin and destination IP that cause slow down and significantly crashes the system and networks.
  b) IP packet option attack: Attacker will use optional fields in IP packet to generate malformed packets. This is more vulnerable once it is attacked by more than one zombie.

- **Applications Attacks:** In this attack, application layer protocols are exploited by the attacker. They finds weakness in HTTP, HTTPS, DNS, SMTP, FTP and VOIP and exploits on the basis of the targeted damage[6].

4. IMPACT ANALYSIS OF DDoS ATTACKS

4.1 Arbor Networks Report

In 20 years, Distributed Denial of Service attacks have marked dramatically changes. As per Arbor Networks security report related to DDoS attack analysis based on bandwidth attack, it is increasing year by year [9].

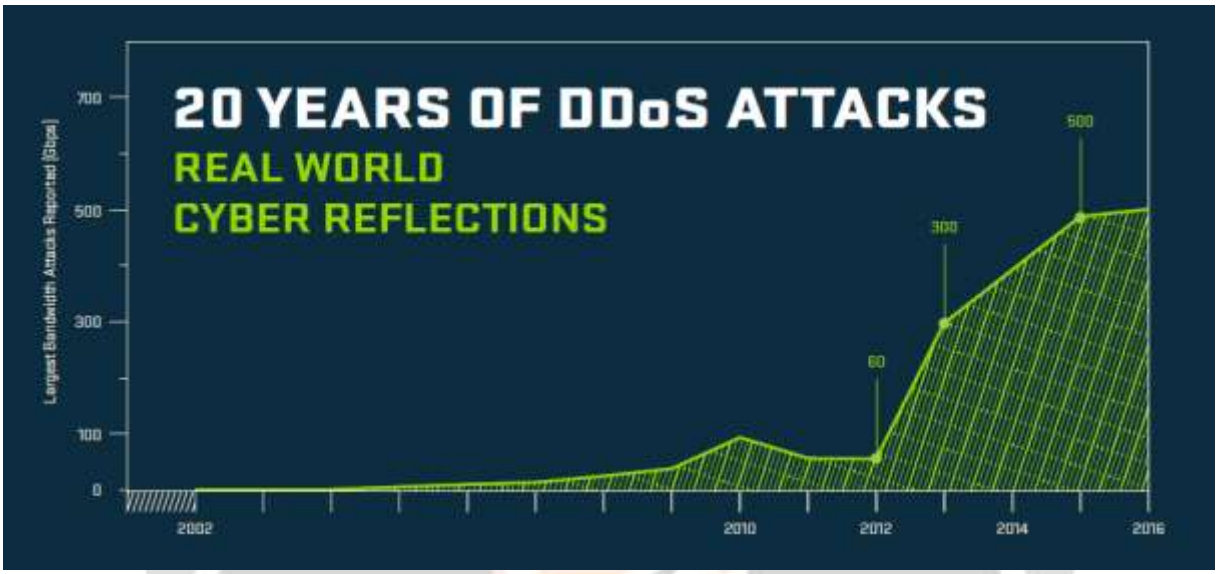

Chart -1: Arbor Networks DDoS analysis report for 20 years

Table -1: Major DDoS attacks are reported by Arbor Networks [9]

Year	Attack details	Impact
1996	ISP Panix targeted by Sustained DDoS Attack	Affected business
1998	Mafiaboy Attacks Yahoo, Fifa.com, Amazon.com, Dell Inc, E trade, ebay and CNN	Major e-commerce sites and their business
2002	Root DNS Server attack	Significant “Smurf” attacks that cause outages for some sites
2007	Estonia DDoS attack	Increasing diplomatic tensions with Russia.
2011	Sony Data Breach Camouflaged With DDoS	Data breach for playstation network users.
2012	DDoS Attack Impacts Canadian Political Party Elections	Delayed voting in election
2012	MI5 And MI6 Websites Attacked By Assange Protesters	US an UK government websites down
2014	Anonymous Shuts Down Cleveland City Website	Anonymous shut down the Cleveland, Ohio city website and posted a video
2014	PlayStation Network and Xbox Live attacked on Christmas Day	Problem in online gaming service
2015	Turkish Internet hit with massive DDoS attack	Internet down
2016	#OpTrump	The trump campaign is targeted
2016	IoT Botnet Targets Global Events	500 gb/sec in attack traffic for the duration of the event
2016	Mirai IoT Botnet	1Tbps multi vector DDoS attack against DNS infrastructure, world's most popular websites offline.

4.2 Kaspersky Lab Securelist Report on DDoS attack in Q4 2016

As per securelist report for Q4 2016, 80 countries were targeted by DDoS attacks. In which more than 50% were targeted in China. The longest DDoS attack marked for 292 hours in Q4 2016 which is greater than the previous year and set the record for the year 2016 [10].

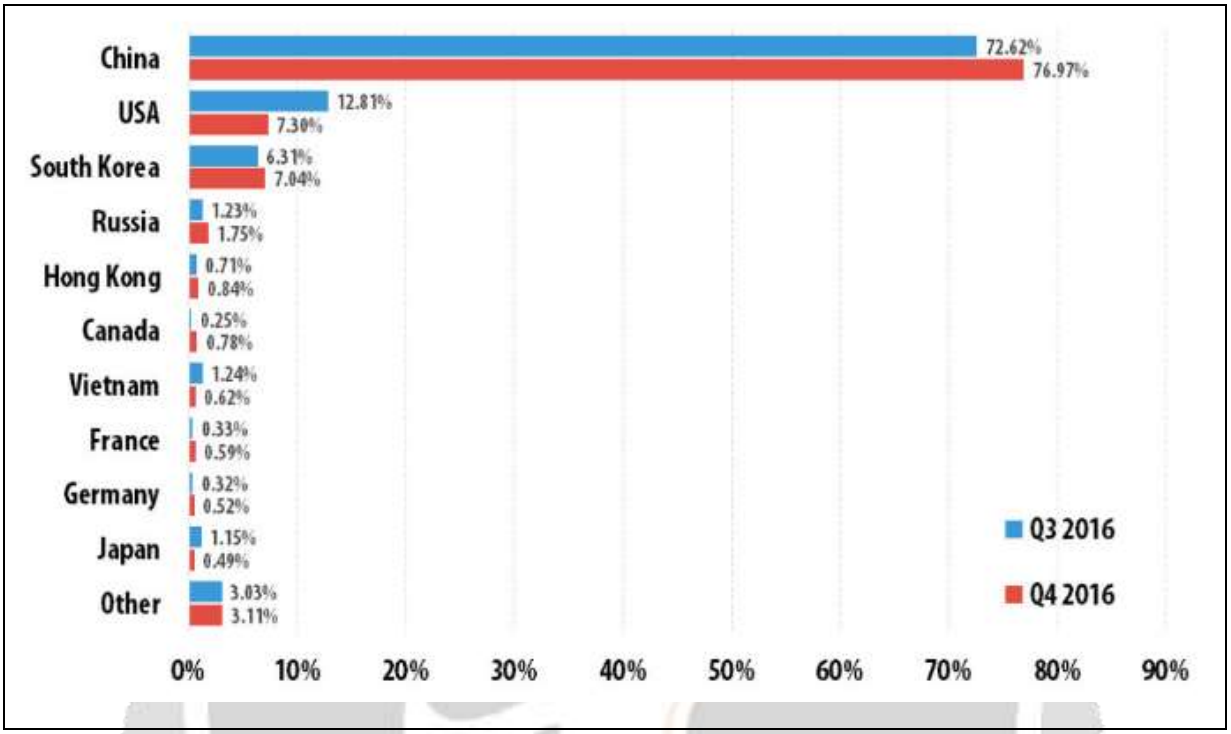

Chart -2: Securelist Report of countrywise DDoS attack in Q3 2016 Vs Q4 2016 [10]

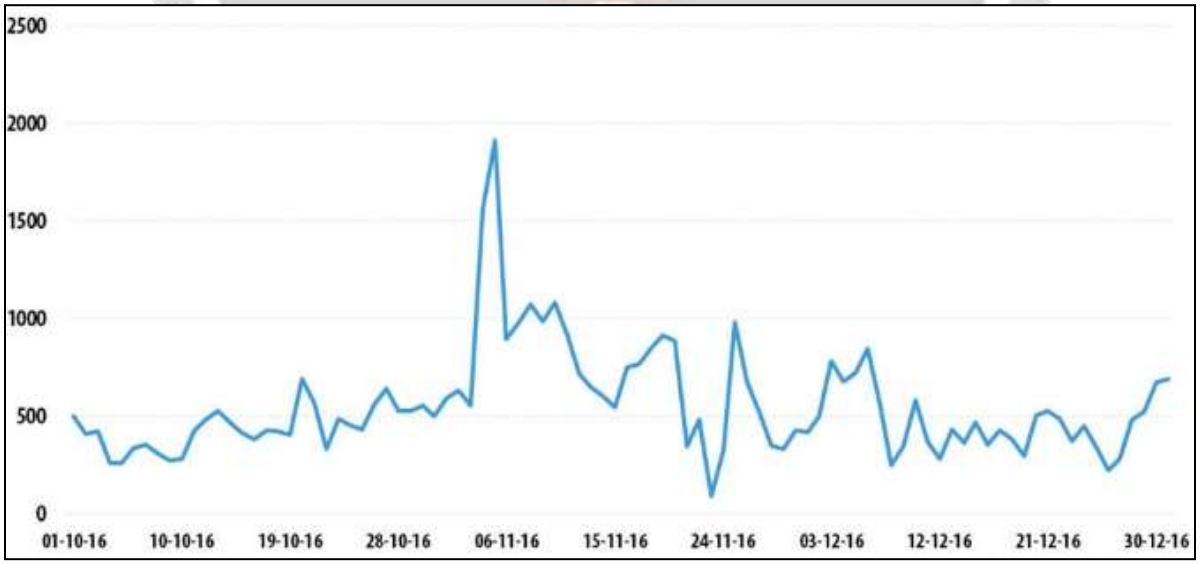

Chart -3: Secure List Report on Number of DDoS attacks overtime in Q4 2016 [10]

As per Kaspersky Lab securelist report for Q4 2016, which contains depth analysis of number of times that DDoS attack insist and generate monthly monitoring reports to identify the types of DDoS attack. As per popular monitoring by IoT devices it is predicted that in year 2017 linux system would be targeted operating system.

5. ANALYSIS OF DDoS MITIGATION TECHNIQUES

This analysis shows that the variety of various security measurements had been developed to mitigate the effect of DDoS attacks. These techniques have advantages and few limitations or disadvantages which are also highlighted based on literature review survey.

Table -2: DDoS Attacks Mitigation Techniques Analysis

Mitigation Techniques	Advantage	Disadvantage
Route based packet filtering [11]	• Random IP spoofing • Static routing compitable	• Not compatible when dynamic routing is used. • Wide implementation is needed. • Not robust to dynamic changes. • Modification of Border Gateway Protocol (BGP) is required.
Secure Overlay Service (SOS) [12]	• Reducing the burden of filtering • Proactive techniques • Compitable communications between predefined source nodes	• It is not secure because location and IP can be reached. • New routing protocol introduction required. • Not applicable to web server.
Hash based IP traceback [13]	• Low storage requirements • Easy to identify the true source attack	• Router Overhead • 28 byte of hash overhead generation.
Deterministic Packet Marking [14]	• Easy to implement • Computational overhead is less • Less packets involved	• Overhead prevention is not there. • Computational work is medium. • Package header size is higher.
Probabilistic Packet Marking [15]	• Path information mark in router • Reconstruction of attack graph • Support incremental deployment.	• High computational work is required for path reconstruction • No overload prevention • Source tracing probability is low.
Hop count filtering [16]	• Low storage required • Lightweight	• It is not compatible with dynamic IP
Pushback [17]	• Effective for different path from legitimate user.	• Costly • All routers are involved

6. CONCLUSION

In this paper a comprehensive survey of DDoS mitigation techniques ate focused and presented. The impact analysis of DDoS attacks are providing the idea of how these attacks are furiously growing and affecting the networks and damage the business revenue generation. Major impact of DDoS attacks such as loss of goodwill, network shutdown, financial loss, disabled organization etc. The survey also focusing on the limitation and vulnerabilities of existing security mechanisms such as routers, traceback etc. to differentiate between the legitimate traffic and the attack traffic which is forcing to get further dedicated mitigation techniques through which ratio of impact can be decreased. This paper is intended to take effective counter measures against DDoS attack.

7. REFERENCES

[1]. H.K.Orman- "The Morris Worm: A Fifteen-Year Perspective" IEEE Security and Privacy, 2003.
[2]. Christos Douligeris and Aikaterini Mitrokotsa- "DDOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION" Signal Processing and Information Technology, 2003. ISSPIT 2003. Proceedings of the 3rd IEEE International Symposium.
[3]. http://www.cisco.com/web/about/security/intelligence/guide_DDoS
[4]. http://www.microsoft.com/security/sir/story/default.aspx#!ddos-attacks
[5]. https://security.radware.com/ddos-knowledge-center/ddospedia/http-fragmentation-attack/
[6]. Mohammad Faruk Alam- "Application Layer DDoS: A Practical approach and Mitigation techniques" Apricot2014, Petaling Jaya, Malaysia
[7]. Arun Raj Kumar and P. and S. Selvakumar- "Disributed Denial of Service (DDoS) Threat in Collaborative Environment A survey on DDoS Attack Tools and Traceback Mechanism" 2009 IEEE International Advance Computing Conference (IACC2009)
[8]. K C Okafor, Joy Anulika Okoye and Gordon Ononiwu- "Vulnerability Bandwidth Depletion Attack on Distributed Cloud Computing Network: A QoS Perspective" International Journal of Computer Applications(0975-8887), March 2016
[9]. https://www.arbornetworks.com/blog/insight/wp.../20yrs_v2_FINAL-20160912.pdf
[10].https://securelist.com/analysis/quarterly-malware-reports/77412/ddos-attacks-in-q4-2016/ - Alexander Khlimonenko, Jens Strohschneider, Oleg Kupreev on February 2, 2017
[11]. K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets," SIGCOMM Comput. Commun. Rev., vol. 31
[12]. A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: An architecture for mitigating DDoS attacks," IEEE J. Sel. Areas Commun., vol. 22, no. 1, pp. 176–188, Jan. 2004.
[13]. Alex C. Snoeren, et al., "Hash-Based IP Traceback", ACM Sigcomm, Aug. 2001
[14]. A. Belenky, and N. Ansari, "Tracing Multiple Attackers with Deterministic Packet Marking (DPM)", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2003
[15]. K. Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack", IEEE INFOCOMM, Apr. 2001
[16]. C. Jin, H. Wang, and K. G. Shin, "Hop-count filtering: An effective defense against spoofed DDoS traffic," in Proc. 10th ACM Conf. Comput. Commun. Security, 2003
[17]. R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," ACM SIGCOMM Comput. Comm.