Research Inventy: International Journal of Engineering And Science
Vol.9, Issue 10 (October 2019), PP 27-35
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Analysis Of Distributed Denial Of Service Defense Mechanisms

J. Britto Dennis[1], Dr.M.Shanmuga priya[2]
[1]*Ph.D Scholar & Assistant Professor (IT Department),*
Dhanalakshmi Srinivasan Engineering College, Perambalur.
[2]*Professor & Supervisor (ECE Department),*
MAM College of Engineering, Tiruchirappalli.

Abstract: *Denial of Service (DoS) and Distributed Denial Service (DDoS) attacks are a large scale and coordinated attack on availability of a network resource or a victim system. Researchers have come up with more suitable solutions to the DoS and DDoS problems. However, attackers are enriching their capability of DoS attacks and develop the new attacks. This paper lays down the survey of DoS attacks and its different countermeasures that are available in the literature. We discuss and analyze these real time attacks based on the solitude mechanism used, methods, ease of deployment and the network overhead involved. Our onerous survey study presented in this paper provides a platform for the study of evolution of DDoS attacks and their defense mechanisms moreover, a proposed method for avoiding DDoS attacks is also included in this summary.*
Keywords: *Firewall, DDoS attack, Ingress monitoring, CAPTCHA, Puzzle, Countermeasure.*

I. Introduction

A Denial of Service (DoS) attack on the Internet aims to make a resource unavailable to the permissible users by sending spurious requests. Distributed Denial of Service attack is a large-scale and coordinated attack on the availability of a network resource or a victim system, floated diffusely through many compromised computers on the Internet. "Primary victims" are those services that are under the attack, while "secondary victims" are compromised systems that are used to launch the attack. An attacker controls the primary victims, which in turn control the secondary victims (Zombies). The attackers require only a few resources and bandwidth for execution to launch the attack.

In 1996, DDoS became an impuissant attack to cyber security. And then many types of DDoS were revised with the rapidly increasing popularity of DDoS. The first documented DDOS attack was reported in August 1999 against a university in United States which lasted for 2 days. On Monday, 7 February 2000, Yahoo, the most popular site on the web was hit by high-profile DDoS attacks which led to high revenue losses to Yahoo. In October 2002, Domain Name System (DNS) service to Internet users around the world that are provided by the 13 root servers were shut down for an hour because of a DDoS flooding attack. Most recently, since September 2012, online banking sites of 9 major U.S. banks e.g. Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, and HSBC have been continuously the targets of series of a powerful DDOS flooding attacks launched by a hacktivist.

Preventing Denial of Service attacks is extremely hard, if not impossible, to precisely differentiate all the attackers requests from other benign requests. Thus, solutions that depend on detecting and filtering attackers' requests have limited effectiveness. There have been a number of protected mechanisms and solutions to the Denial of Service attacks were proposed. However, still there is no wide solution which can defend against all the known forms of DDoS attacks. This paper tries to analyze and classify the current solutions to the Denial of Service attacks. By examining the merits and demerits of each solution, we can come to know about the effectiveness of the solutions.

In this paper we have done a detailed survey on the DoS attack strategies that have come into existence till date. It also MapQuest the different preventive mechanisms, and makes a comparison based on the factors such as basic architecture or mechanism used, modification on infrastructure, ease of deployment, and the overall network overhead involved. In section II, we describe the countermeasures for DoS attacks proposed till date from 1996. Section III makes an analysis of the proposed solutions. Finally, in section IV we have the conclusion of our analysis.

II. Countermeasures Of Dos

Various classifications and solutions have been proposed over the past decade, in order to secure the networking environment from venomous attackers. The following section deals with the countermeasures proposed by different experiments conducted by different authors so far to diminish DoS attacks from 1996 to till date.

A. Firewall Based Mechanisms

Firewall was the basic means of protection for all types of network based attacks, until the year of 1996. Rule sets are followed by a Firewall to allow or deny protocols, ports or IP addresses. Firewalls were also used to diminish DoS attacks, which have been explained below.

1) TCP SYN Flooding Attack and the FireWall-1 SYNDefender (1996)

Firewall is proposed as a solution [1] to prevent denial of service attacks based on more secure packet forwarding Syndefender defends against the TCP SYN flood attacks by interrupting all SYN packets and mediating the connection attempts before they reach the operating system. Syndefender helps to prevent the target host from becoming flooded by unresolved connection attempts, which causes the operating system and the host, stop receiving new connections. As a result, the host system is effectively isolated from the SYN flood attack.

B. Filtering Mechanism

This category of solutions addresses the core of the problem by limiting the amount of traffic presented to target and it requires some set of rules to filtering the packets. In ingress filtering, it assures that incoming packets are essentially from the networks from which they claim to originate.

1) Network Ingress Filtering (1998)

Ingress traffic filtering technique is used to describe a simple, effective, and straightforward method [3] to prohibit DoS attacks which use forged IP addresses to be propagated behind an Internet Service Provider's (ISP) aggregation point. This type of filtering method does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules.

C. Overlay Networks

Overlay networks are used to design secure communication services among application sites of a geographically distributed control system against DoS attack. Nodes in the network are connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network.

1) Center Track: An IP Overlay Network for Tracking DoS Floods (2000)

Overlay network of Center Track [5], consisting of IP tunnels or other connections that are used to selectively reroute fascinating datagrams directly from edge routers to special tracking routers. The tracking routers, or associated sniffers, can easily regulate the ingress edge router by perceiving from which tunnel the datagrams arrive. The datagrams can be observed, then dropped or forwarded to the appropriate egress point.

2) *SOS: Secure Overlay Services (2002)*

This architecture is designed by a combination of secure overlay tunneling, routing via consistent hashing, and filtering specifically to support for emergency services [7]. The effect of attack is reduced by performing intensive filtering and introducing randomness and anonymity into the architecture.

3) An Overlay Protection Layer against Denial-of-Service Attacks (2008)

This paper assists a new architecture namely overlay protection layer that proactively prevents application sites from DoS attacks. The key point is to hide application locations behind an overlay (proxy) network [13]. Application sites have the capability to hide their IP addresses, by preventing DoS attacks, which depend on knowledge of fatality IP address. As a result attackers cannot easily trace and locate the application sites to launch attacks.

D. Active Monitoring

Active monitoring involves injecting test traffic (TCP/IP traffic) onto a network and monitoring the flow of that traffic. It can watch for particular conditions to arise and react appropriately.

1) Active Ingress Monitoring (AIM): An Intrusion Isolation Scheme in Active Networks (2001)

The source address spoofing denial of service attacks remain the most powerful threat in the Internet. This paper employs the method of Active Ingress Monitoring (AIM), to effectively insulate DoS attacks that use randomly forged source IP addresses [6] by effectively detecting and identifying interference in an active networks environment.

E. *Capability Based Approaches*

Capability based security mechanisms are used to mitigate denial of service attacks. Capabilities or tokens are used for authentication purposes and also to classify between an authentic and an attacker.

1) Preventing Internet Denial-of-Service with Capabilities (2003)

This paper proposes a new approach to preventing and limiting Denial of Service attack (DoS) by restriction on the exchange of information without prior permission from the target. This architecture demands [8], that the nodes must first get "permission to send" from the destination; a receiver provides tokens, or capabilities, to those senders whose traffic it agrees to accept. Then senders can include these tokens in packets. Thus only those packets with the tokens are permitted to pass the network.

2) Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks (2007)

This approach offers a strong protection for Denial-of-Capability (DoC) attack, which thwarts new capability-setup packets from reaching the destination, restricts the value of these systems [12]. Portcullis used to diminish DoC attacks by allotting scarce link bandwidth for connection establishment packets based on *per-computation* fairness. This approach ensures that a valid sender can establish a capability with high probability regardless of an attacker's resources or strategy and that no system can recover on our guarantee.

3) Using Web-Referral Architectures to Mitigate Denial-of-Service Threats (2010)

WRAPS [15], permits a client to attain greater privilege to access web service by assigning to it a secret fictitious URL called privilege URL with a capability token entrenched in part of the IP and port number fields. Through that URL, the client can establish a privileged channel with that website (target website) even in the existence of flooding attacks. A website offers a client a privileged URL if the client is referred by one of the site's trusted neighbors, or is otherwise qualified by the site's policies that are used to identify valued clients. A qualified client will be readdressed to the privilege URL generated automatically using that client's identity, service information, and a server secret.

F.CAPTCHA Based Mechanism

CAPTCHA stands for Completely Automated Public Turing test to differentiate robots from humans. CAPTCHA is a distorted letters or image containing short text, to prevent automated relocation blogs and forums and it can be used to avoid spam mails.

1) Image Flip CAPTCHA (2009)

CAPTCHA is an efficient defensive mechanism of DoS attacks. It is an automated test that humans can pass, but current computer programs can't pass: any program that has high success over a CAPTCHA can be used to solve an unsolved Artificial Intelligence (AI) problem [14]. A Human Interaction Proof (HIP) like Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) offers a way to make such a distinction. Reverse Turing test of CAPTCHA is used by Web service providers to secure human interaction assumed services from Web bots.

2) GeoCAPTCHA - A Novel Personalized CAPTCHA Using Geographic Concept to Defend Against 3rd Party Human Attack (2012)

This paper introduces a new CAPTCHA scheme namely GeoCAPTCHA, which exploits the personalized contents such as geographical information to thwart the 3rd party human attack [18]. GeoCAPTCHA is a personalized image-based CAPTCHA, which is used to recognize and insulate human from robots. This scheme is good to be used to prevent automatic programming attacks and defend against third-party human attacks.

3) A new avatar dynamic image based CAPTCHA service on cloud for mobile devices (2014)

CAPTCHAs are used as one of the guaranteed technology in cyber security. This paper proposes a new solution called an image-based avatar CAPTCHA for mobile devices. Users correctly identify the visually distorted human faces embedded in a complex background without selecting any non-human avatar face [20]. CAPTCHA is generated on cloud, so that it improves efficiency and reduces response time for use to authenticate as human.

G.Puzzle-Based Mechanisms

Puzzle-based defense mechanisms were tried to correct the imbalance between the costs to the attacker for generating a bogus request and cost to the server for processing a request by demanding a computation or memory access, in the form of a puzzle solution, from each client.

1) The Design and Implementation of Network Puzzles (2005)

This paper proposes a client puzzle at IP layer, which allows any device inside the network to push load back onto those it is servicing [10]. Network layer puzzles can be applied to all traffic from spiteful clients, making it possible to prevent against arbitrary attacks. As a result network puzzles are used to mitigate the DoS attacks by slow down the flooding and port scanning activity.

2) Non-Parallelizable and Non-Interactive Client Puzzles from Modular Square Roots (2011)

This paper proposes a novel scheme for client puzzles which rely on the computation of square roots modulo a prime. Using this scheme solution of the puzzle cannot be obtained faster than scheduled by distributing the puzzle to multiple machines or CPU core [16]. This scheme provides polynomial granularity and compact solution and verification function against DoS attacks. This is not always true; it fails in the case of CPU-GPU integration.

3) Rate Limiting Client Puzzle Schemes for Denial-of-Service Mitigation(2013)

This paper introduces a novel mechanism called leaky bucket rate limiting queue to puzzle difficulty according to a queue delay. By rate limiting, the numbers of incoming requests were used to prevent the server overloading [19]. As a result, attackers had to spend expensive time to solve harder puzzle which reduces their rate of prosperous attacks.

4) Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks (2015)

This paper introduces a novel architecture for a client puzzle called as software puzzle. Algorithm of the puzzle is randomly generated only after the client request is arrived at the server side [21]. Software puzzle prevents the DoS attack by ensuring that 1) an attacker must need a significant effort to translate CPU functions to GPU functions and 2) An attacker is unable to predict the implementation to solve the puzzle in advance.

H. *Network layer based mechanisms*

Here we present recent mechanisms deployed on network layer.

1. Detection Based on Self- Similarity (2010)

Analysis on various incoming traffic patterns has led to a conclusion that most of the attacks have a self-similar nature [22]. The models thus developed helps in identifying changes in the energy levels which in turn helps in the detection of the malicious packet flow. Backtracking at each affected router locates the attacker and helps in distinguishing normal TCP flow from the attack flow.

2) SAP (Shrew Attack Protection)(2010)

Shrew Attack Protection is a protection method, rather than a detection method. Each flow is analyzed to identify the drop rate of them. A fair preset threshold is compared with the estimated drop rate, and if it is found severe, then such packets are given higher priority for transmission .As a result, their drop rate is probabilistically reduced. So even if a DoS attack occurs the impact of that attack on legitimate users is reduced [29].

3) Deficit Round Robin (DRR) algorithm(2010)

If an average packet length is known ahead, ordinary round robin will be effective, in case of different packet sizes. The major issue with traditional round robin service is that packets from different classes can have different sizes. DRR assigns a quantum of service to each class in each round .This technique tries to serve packets from each class on a per round

basis [24]. Drawback of this approach is that it is a destination based defense mechanism and hence a network resource gets inflated prior to detection.

4) Software based mechanism(2011)

A light weight software based method that compares average traffic per timeslot with traffic in the current time slot. If traffic in current time slot is greater than the target average traffic per time slot, then the processing is continued. If timeouts in that timeslot is twice the number of discarded packets and no. of discarded packets is greater than threshold, then also the normal processing is carried out. If inter arrival time is reduced, the flow is detected to be a DoS attack [23].

5) Robust RED (RRED)(2012)

RRED was developed focusing on enhancing the TCP throughput during a DoS attack. RRED is applied to incoming flows to detect and filter out attack packets before a normal RED algorithm is applied [26]. These

approach emphases on performance of TCP flows. Hence the performance of this system with UDP flows is unpredictable.

6) EBDT: An DoS attack detection method based on EWMA(2012)

EBDT is an anomaly detection mechanism which has lower missing report and higher false positive rate than the misuse detection. Based on the TCP traffic abnormal characteristics produced by DoS attack on network flow EBDT is deployed. Exponential Weighted Move Average (EWMA) algorithm is used to analyze TCP traffic. EBDT is a two-step procedure including sampling and statistical of TCP traffic, and attack judgment [25]. According to researches, EBDT failed to provide considerable attack detection precision.

7) Multiple Sampling Averaging Based on Missing Sampling (MSABMS)(2012)

This approach is used to detect DoS attacks based on the model of small signal [27]. A statistics on the packets are taken within 30 s with the sampling interval of 10 ms (3000 sampling points in total), and the statistical results are compared with a threshold for identifying the DoS attacks. An Eigen value estimating matrix is established to estimate the attack period after the detection of DoS attacks. Major issues with this approach includes: (i) increase of network bandwidth and network scale reduces the accuracy and the efficiency of entropy calculation (ii) lower detection rate, and higher false positive rate and higher false negative rate. (iii) Higher computational complexity.

8) MultiFractal Detrended Fluctuation Analysis (MF-DFA) (2015)

This mechanism explores the change in terms of multifractal characteristics over a small scale of network traffic caused by DoS attacks. Using wavelet analysis, the singularity and bursty of network traffic under DoS attacks are estimated through Holder exponent. The difference values (D-value) of Holder exponent of network traffic between normal and under DoS attack situations are identified. The D-value is used as the basis to determine DoS attacks. A detection threshold is set
based on the statistical results. Comparison of D-value with detection threshold confirms DoS attack [28].

9) LAAEM: A Method to Enhance LDoS Attack (2016)

This LAAEM (LDOS attack ability for enhancing method) contrivance explains TCP's retransmission timeout mechanism can be oppressed by using spitefully chosen low-rate attack flow to make TCP throughput plunge to a very low rate. LDoS attacks will debase the performance of web traffic, TCP services and condense TCP throughput to zero. Based on LDoS, bots multiplexing in multi-targets attack circumstances is anticipated, and then nearby the LDoS attack ability attractive method. In simulation, the method shows good performance and malleability, it can enhance attack ability efficiently under assortment of interrelated parameters. With this method, the assailant may use a small botnet to origin very great destruction which only large botnet can cause by habitual method.[29]

H. *Other Solutions*

Here we present other solutions that use mechanisms apart from the ones listed above.

1) A Defense against address spoofing using Active Networks (1997)

This paper presents active networks as a defense against DoS attacks. Active networks afford an increased computational power within the network itself [2]. Here, filter is built that can be dynamically organized to filter out duplicate packets within the network. ANTS is an active network toolkit were assist to build and maintain active network applications.

1) Defending Against Denial of Service Attacks in Scout (1999)

This paper describes a two-dimensional architecture [4] for defending against denial of service attacks. In one dimension, the architecture accounts for all resources consumed by each I/O path in the system and this accounting mechanism is implemented by Scout operating system. In the second dimension, different modules that define each path can be configured in separate protection domains. The resulting system is called the Escort protects against resource based denial of service attacks. This paper describes the Escort architecture and its implementation in Scout, and reports a collection of experiments that measure the costs and benefits of using Escort to protect a web server from denial of service attacks.

2) SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding (2004)

This paper assists a Stateless Internet Flow Filter (SIFF) to allow an end-host to selectively stop individual flows from reaching its network, without any of the common inference [9]. The network traffic can be divided into two classes, privileged (prioritized packets subject to recipient control) and unprivileged (legacy traffic). Privileged channels are established through a capability exchange handshake. Capabilities are dynamic and

verified by the routers in the network, and can be quashed by quenching update messages to an aberrant host. SIFF is transparent to legacy clients and servers, but only updated host will relish the benefits of it. Both the filtering and the capability mechanisms are involved in mitigation of DoS attacks.

3) Eagle Eyes: Protocol Independent Packet Marking Scheme to Filter Attack Packets and Reduce Collateral Damage During Flooding Based DoS and DDoS Attacks (2012)

This paper propose a novel packet marking mechanism [17], which mitigates the Denial of service attacks by filtering and also reducing collateral damage significantly by selectively dropping attack packets based on its packet mark. Fingerprint of the path in each packet used to identify the attack packets coming from various source even in case of IP spoofing

4) DDoS Defense by Offense (2006)

This paper presents the design, implementation, experimental evaluation and analysis [11], a protection against application level distributed denial-of-service (DDoS), in which attackers cripple a server by sending legitimate-looking requests that consume computational resources. Under the various conditions, offended server encourages all clients, resources permitting, to automatically send higher volumes of traffic. Here, an attacked server gives a client service only after it pays in some currency. Ex., CPU or memory cycles and the evidence of payment is the solution to a computational puzzle. In this way DoS is controlled.

III. Comparative Analysis

Here we focus the key discoveries which provide solutions to the problem of DoS over the past 19 years. Table I gives a comparison among various popular DDOS tools, based on the basic architecture used, the isolation mechanism used to isolate the legitimate traffic or the level where the isolation is done, the ease of deployment and the overall network overhead involved.

Phase 1: Early 90's to 2000

Internet services are unexpectedly busted or denied by DoS attacks, and it was originated suddenly in early 90's. But, this ultimately came to a virtual standstill in the mid 90's due to the sound effects of DoS attacks. Thus during this phase, resistance against DoS attacks was done with the aid of firewalls. But as the strength of DoS attacks enlarged and leads to DDoS attacks. In the end of 90's, Number of monitoring agents were introduced to monitor the network. An agent can collect communication control information and it can sentry for certain conditions to arise and react appropriately. We can derive from the table that in this phase, solutions proposed for firewalls and active monitoring as their basic architecture was easy or fairly moderate to deploy and involved a low and moderate overhead. The end of this phase also leads to the evolution of filtering techniques.

A. Phase 2: 2000 to 2005

The 1st phase countermeasures were still inadequate to defend a DDoS attack and the need for proactive and reactive mechanism was crucial. In this phase, overlay network approaches were used to defend the DDoS attacks. Overlay networks involved selective overlay nodes that form a protection perimeter over the network that needs to be secured. These approaches had some kind of packet marking schemes; it also had moderate deployment properties. The overhead involved varies depending on the isolation mechanism used.

B. Phase 3:2005 to 2010

In this phase, capability based mechanisms are used to diminish DoS/DDoS attacks. Defense based on network capabilities supports fundamental changes to the Internet, so that senders must get explicit authorization from the receiver before they are allowed to exchange the data. Here, filtering technique was also used to mitigate the denial of service attacks by some set of filter rules. The network overhead involved basically is low in this phase whereas the deployment might be complex at times due to the usage of an integrated architecture of previously proposed mechanisms.

C. Phase 4: 2010 to 2013

This is the most important landmark in the journey to mitigate DoS attacks, because in this period more number of solutions was proposed to meet the crack in security of both the application level and the network level. In application level, with infer of the table CAPTCHAs were used to defend against DoS attacks. And puzzles were introduced in order to precisely raise the cost of using a service, through computation (client puzzles). In order to overcome network level attacks, an integrated architecture of filtering techniques with capabilities were used to identify and differentiate between legitimate and the bad traffic. The ease of deployment and overhead involved varies on the isolation mechanisms used. Most of these approaches require memory to hold predetermined models for comparison. Techniques with higher processing complexities were also deployed focusing on packet lengths, inter-arrival time, protocol etc.

D. Phase 5: 2013 to 2016

The fifth phase portrays a clearer picture of a solution to the problem of DoS attacks. Unlike the previous phases, where the problem of DoS was solved by a central entity having control of the overall mechanism, here the process of mitigating DoS becomes distributed. In case of the application level protection, CAPTCHAs are made more complex from ordinary text recognition to complex image recognition CAPTCHAs. Client puzzles become weakened by fast puzzle solving techniques or using built-in GPUs. However hackers inflate their capability of DoS attack year-by-year. Software puzzle is a promising technique to mitigate DoS attacks by making attackers unable to prepare an implementation to solve the puzzles in advance using randomly generated algorithms. These algorithms can be any of the conventional cryptographic algorithms. During this phase, appreciable advancements evolved in network layer based DoS/DDoS detection. The characteristic of the traffic is subjected to analysis and efficient backtracking along with it, provided better detection of malicious sources. The ease of deployment, less processing overheads and memory management favors these approaches in the present network scenario. Denial of service attacks mainly focus on the application layer rather than other layers. In recent years, Internet has faced many problems on the application level and many solutions are proposed for application level DoS attacks. Software puzzle became an efficient technique to reduce the GPU inflated DoS attacks by making attackers unable to predict the puzzle solution or spend much time to translate CPU functions to relevant GPU functions, such that translation cannot be done in real time. From this study, it is concluded that a software puzzle is a promising mechanism to mitigate the DoS/DDoS attacks. Thus in future, the rounds in the algorithms, which are used to generate the puzzles, are shuffled to enhance the defense of DoS attacks.

Table I: Comparison of DoS Defense Mechanisms

Year	Paper	Authors	Basic Architecture/Mechanism	Isolation Mechanism	Ease of deployment	overhead
1996	TCP SYN Flooding Attack and the Firewall-SYNDefender [1]	Mary L. Bailey, Burra Gopal , Michael A. Pagels, Larry L. Peterson, Prasenjit Sarkar	Firewall	IP Level, Access Control List	Moderate	Low
1997	A Defense against address spoofing using Active Networks [2]	Van c Van	Active networks	Selective filtering	Easy	Moderate
1998	Network Ingress Filtering [3]	P. Ferguson.	Filtering Mechanism	IP Level, Filtering	High	Moderate
1999	Defending Against Denial of Service Attacks in Scout [4]	Oliver Spats check, Larry L. Peterson	Escort security architecture	End-to-end resource accounting	Moderate	Moderate
2000	Center Track: An IP Overlay Network for Tracking DoS Floods [5]	Robert Stone	Overlay Networks	Hop by hop central tracking system	Moderate	Moderate
2001	Active Ingress Monitoring (AIM): An Intrusion Isolation Scheme in Active Networks [6]	Gitae Kim and Tony Bogovic	Active monitoring	Active Ingress Monitoring	Moderate	Moderate
2002	SOS: Secure Overlay Services[7]	Angelos D. Keromytis, Vishal Misra, Dan Rubenstein	Overlay network	Secret destination. IP level	High	High
2003	Preventing Internet Denial-of-Service with Capabilities [8]	Tom Anderson, Timothy Roscoe, David Wetherall	Capability approach	Dynamic filtering	Less	Moderate
2004	SIFF: Stateless Internet Flow Filter to Mitigate DDoS Flooding [9]	Abraham Yaar, Adrian Perrig, Dawn Song	Filtering mechanism & capability Mechanism	IP Level, Packet marking & path identification	Moderate	High
2005	The Design and Implementation of Network Puzzles[10]	Wu-chang Feng Ed Kaiser Wu-chi Feng Antoine Luu	Network puzzle scheme	Hint-based hash-reversal	High	Low
2006	DDoS Defense by Offense [11]	Michael Walsh, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenkery	Speak-up a currency scheme	Application level, CAPTCHA, Capability	Moderate	Moderate
2007	Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks [12]	Bryan Parno, Dan Wendlandt, Elaine Shi, Adrian Perrig, Bruce Maggs, Yih-Chun Hu	Anti-denial of Capability (DoC) approach, Capability based	Scarce link bandwidth allocation, computational proofs of work (puzzles), capability	High	High
2008	An Overlay Protection Layer	Hakem Beitollahi, Geert	Overlay network	Location hiding	Moderate	Moderat

	against Denial-of-Service Attacks [13]	Deconinck, Katholieke Universiteit Leuven		technique		e
2009	Image Flip CAPTCHA[14]	M. Tariq Banday, Nisar A. Shah	Image CAPTCHAs	Application level, CAPTCHA with sub images	Easy	Low
2010	Using Web-Referral Architectures to Mitigate Denial-of-Service Threats [15]	XiaoFeng Wang, Michael K. Reiter	Web referral architecture	capability based approach, (tokens)	Easy	Low
	The Taming of The Shrew: Mitigating Low-Rate TCP-Targeted Attack [29]	Chia-Wei Chang, Seungjoon Lee, Bill Lin and Jia Wang	Drop rate monitoring method	Bandwidth share based technique	Moderate	Lows
	The DRR-based Approach of Defending against LDoS [24]	Jin LEI, Xingchen LIU	Memory requirement	Destination based LDoS detection	Moderate	High
2011	Non-Parallelizable and Non-Interactive Client Puzzles from Modular Square Roots[16]	Y. I. Jerschow and M. Mauve,	Client puzzle scheme	bandwidth-based cost factor	High	moderat e
	Software based Low Rate DoS Attack Detection Mechanism [23]	Rejo Mathew , Vijay Katkar	Distributed real time detection	Inter arrival time of packets are focused	Moderate	Low
2012	Eagle Eyes: Protocol Independent Packet Marking Scheme to Filter Attack Packets and Reduce Collateral Damage During Flooding Based DoS and DDoS Attacks[17]	Samant Saurabh and Ashok Singh Sairam	Protocol based mechanism	Packet marking scheme	Moderate	Moderat e
	GeoCAPTCHA - A Novel Personalized CAPTCHA Using Geographic Concept to Defend Against 3rd Party Human Attack[18]	Te-En Wei, Albert B. Jeng, Hahn-Ming Lee	CAPTCHA based mechanism	Geo CAPTCHA for 3rd party	Moderate	Moderat e
	RRED: Robust RED Algorithm to Counter Low-Rate Denial-of-Service Attacks [26]	Changwang Zhang, Jianping Yin, Zhiping Cai, and Weifeng Chen	Detection and filtering mechanism	Centralized detection approach	Moderate	Moderat e
	EBDT:A Method for Detecting LDoS Attack [25]	Kai Chen, Huiyu Liu, Xiaosu Chen	Depends on EWMA algorithm	Approximate detection method	Moderate	Low
	MSABMS-based approach of detecting LDoS attack [27]	Wu Zhi-jun ,Zhang Hai-tao , Wang Ming-hua , Pei Bao-song	Network scale and bandwidth based mechanism	Precise detection for smaller attack signals	Moderate	High
2013	Rate Limiting Client Puzzle Schemes for Denial-of-Service Mitigation[19]	Jing Yang Koh, Joseph Teo Chee Ming, and Dusit Niyato	Client puzzle	leaky bucket rate limiting queue mechanism	High	Moderat e
2014	A new avatar dynamic image based CAPTCHA service on cloud for mobile devices[20]	Mr. Prasad V. Kalne	Image CAPTCHA	Dynamic image	Moderate	Moderat e
2015	Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks[21]	Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng	Client puzzle mechanism	Software puzzle	Easy	Low
	Low-Rate DoS Attacks Detection Based on Network Multiracial [28]	Wu Zhi-jun, Zhang Liyuan, Yue Meng,	Distributed attack detection mechanism	MF-DFA algorithm deployed	Moderate	Low
2016	LAAEM: A Method to Enhance LDoS Attack	Heshuai Li, Junhu Zhu, Qingxian Wang, Tianyang Zhou, Han Qiu, and Hang Li,	Tcp's retransmission timeout mechanism	Multi target bot multiplexing algorithm	Moderate	Low

IV. Discussion

DoS and DDoS attacks were attempted to deplete resources such as network bandwidth, memory and computational power by overwhelming the service with bogus requests. In order to mitigate the DDoS attacks, several techniques have been proposed in the past by various researchers. However, most of the project research were focusing either on Application Layer or Network Layer and are mostly providing only a single layer of defense. In application layer, the attacks over-exercise specific functionality or features of a website with the intention of disabling them. Mitigation of DDoS attacks at application layer requires identification of human traffic from human-like bots and hijacked browsers. The majority of DDoS attacks focus on targeting the network layers, where malicious traffic (TCP / UDP) is used to flood the victim. Hackers achieved. LDoS by

inflate traffics and consuming the network bandwidth. One of the major threats in the network layer is low rate denial of service attacks. LDoS attacks send packets periodically in a short interval of time there by denying or consuming resources until the server goes offline. Hence, we have planned to propose a combination of both the Application Layer and Network Layer approaches to produce a comprehensive frame work for the minimization of DDoS attacks by using a software puzzle mechanism called Random algorithm with random puzzles which provides more guarantee in terms of increased performance for security and reduced computational complexity.

V. Conclusions

The distinct mitigation techniques for Denial of service attacks were proposed. A comparative analysis of DDoS defense mechanisms evolved from 1996 to till date is presented. With the evolution of attacks, it is observed that distinct countermeasures have been proposed and are implemented. While the methods differ in their region of action, the type of mechanism/architecture used, modification to the infrastructure, their ease of deployment, and overall overhead, each method has certain features that make it more suitable to implement in one situation from another. Further software shows a promising future to mitigate the DoS/DDoS attackes.

References

[1]. Mary L.Bailey, Burra Gopal, Michael A. Pagels, Larry L.Peterson, Prasenjit Sarkar,"TCP SYN Flooding Attack and the FireWall-SYNDefender" 1996.
[2]. Van c Van, "A Defense against address spoofing using Active Networks" IEEE/ACM Transactions on Networking, 1997.
[3]. P.Ferguson and D.Senie, "RFC 2267: Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing," ftp://ftp.internic.net/rfc/rfc2267.txt, Jan 1998.
[4]. Oliver Spats check, Larry L. Peterson, "Defending against Denial of Service Attacks in Scout" Proc of the 3rd Symposium on OS Design and Implementation, Feb 1999.
[5]. Robert Stone, "Center Track: An IP Overlay Network for Tracking DoS Floods" 9th USENIX Security Symposium, Aug 2000
[6]. Gitae Kim and Tony Bogovic, "Active Ingress Monitoring (AIM): An Intrusion Isolation Scheme in Active Networks", 2001.
[7]. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services," Proc. ACM SIGCOMM '02, Aug. 2002.
[8]. T. Anderson, T. Roscoe, and D. Wetherall, "Preventing Internet Denial-of-Service with Capabilities", Nov. 2003.
[9]. Abraham Yaar, Adrian Perrig, Dawn Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding" 2004.
[10]. Wu-chang Feng Ed Kaiser Wu-chi Feng Antoine Luu "The Design and Implementation of Network Puzzles", 2005.
[11]. Michael Walsh, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenkery, "DDoS Defense by Offense", 2006
[12]. Bryan Parno, Dan Wendlandt, Elaine Shi, Adrian Perrig, Bruce Maggs, Yih-Chun Hu, "Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks", 2007.
[13]. Hakem Beitollahi, Geert Deconinck, Katholieke Universiteit Leuven, "An Overlay Protection Layer against Denial-of-Service Attacks", 2008.
[14]. M. Tariq Banday, Nisar A. Shah, " Image Flip CAPTCHA", The ISC Int'l Journal of Information Security, vol. 1, no 2, July 2009.
[15]. X. Wang and M. Reiter, "Using Web-Referral Architectures to Mitigate Denial-of-Service Threats" IEEE transactions on dependable and secure computing, vol. 7, no. 2, april-june 2010.
[16]. Y.I.Jerschow and M.Mauve, "Non-parallelizable and non-interactive client puzzles from modular square roots," in Proc. Int. Conf. Availability, Rel. Secur., Aug. 2011.
[17]. Samant Saurabh and Ashok Singh Sairam, "Eagle Eyes: Protocol Independent Packet Marking Scheme to Filter Attack Packets and Reduce Collateral Damage During Flooding Based DoS and DDoS Attacks", 2012.
[18]. Te-En Wei, Albert B. Jeng, Hahn-Ming Lee, "GeoCAPTCHA– ANovel Personalized CAPTCHA Using Geographic Concept to Defend Against 3rd Party Human Attack", 2012.
[19]. Jing Yang Koh, Joseph Teo Chee Ming, and Dusit Niyato, "Rate Limiting Client Puzzle Schemes for Denial-of-Service Mitigation", 2013
[20]. Prasad V.Kalne, Vaishali L.Kolhe, "A new avatar dynamic image based CAPTCHA service on cloud for mobile devices", 2014.
[21]. Yongdong Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng, "Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks", 2015.
[22]. Wuhan, Hubei, "Detection of Low-rate DDoS Attack Based on Self-Similarity", China in 2010 Second International Workshop on Education Technology and Computer Science (March 06-March 07).
[23]. Rejo Mathew, Vijay Katkar, "Software based Low Rate DoS Attack Detection Mechanism", International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.
[24]. Jin LEI, Xingchen LIU, "The DRR-based Approach of Defending against LDoS", 2010 International Conference on Intelligent Computing and Intelligent Systems (October 29-October 31).
[25]. Kai Chen, Huiyu Liu, Xiaosu Chen, "EBDT:A Method for Detecting LDoS Attack", IEEE International Conference on Information and Automation Shenyang, China, June 2012.
[26]. Changwang Zhang, Jianping Yin, Zhiping Cai, and Weifeng Chen, "RRED: Robust RED Algorithm to Counter Low-Rate Denial-of-Service Attacks" , IEEE Communications Letters,May 2010.
[27]. Wu Zhi-jun ,Zhang Hai-tao , Wang Ming-hua , Pei Bao-song, "MSABMS-based approach of detecting LDoS attack" vol. 31, pp. 402-417, 2012.
[28]. Wu Zhi-jun, Zhang Liyuan, Yue Meng, "Low-Rate DoS Attacks Detection Based onNetwork Multifractal", IEEE Transactions on Dependable and Secure Computing, 2015.
[29]. Chia-Wei Chang, Seungjoon Lee, Bill Lin and Jia Wang, "The Taming of The Shrew: Mitigating Low-Rate TCP-Targeted Attack", AT&T Labs-Research, Florham Park, 2010.
[30]. Heshuai Li, Junhu Zhu, Qingxian Wang, Tianyang Zhou, Han Qiu, and Hang Li, " LAAEM: A Method to Enhance LDoS Attack"2016