Classification of Cooperative Distributed Denial of Service Defense (DDoS) Schemes

Author Prachi Gulihar

Abstract

Distributed denial of service(DDoS) attack is one of the biggest challenges faced by the internet community today. DDoS attacks attempts to disrupt the availability of resources to the legitimate users by overwhelming the network and server resources. In this paper we discuss the importance of cooperative mechanisms over the centralised ones and various existing cooperative techniques to defend against DDoS attack. We also discuss their major drawbacks. The major disadvantage of centralised defense mechanism is single point of failure when the central kingpin node itself comes under attack. What we realise is that although these techniques have been developed but are rarely deployed in the real world because the researchers have long ignored the economic incentive part in the working of cooperatives DDoS mechanisms. Due to lack of incremental payment structures the cooperation between the nodes fails. Sometimes the payment structures are non-existent and in some cases the payment structure is in place but the incentives are not lucrative enough for the nodes to share their resources. The DDoS attack scenario can be divided into attack phase, detection phase and response phase. When the attacker machines perform in cooperation then for the defense mechanism to be stong it should also be in cooperation.This work gives an overview of the existing cooperative defense mechanisms at different layers of the Open Systems Interconnection (OSI) model and an overview of mechanism using third-party for any of these three phases.

Keywords

Distributed Denial of Service (DDoS) attack, defense mechanisms, cooperative third party defense schemes.

1. Introduction

Distributed denial of service attacks are the ones in which the attacker gains control of the system by exploiting its vulnerabilities. In this manner the attacker is able to compromise several machines which then together form an army of zombies who act as slave machines. The attacker or the master machine then commands the slave machines to begin the attack either by sending malicious packets to the victim's address or by flooding exhausting the connectivity bandwidth and server resources. When the attacker‘s target is connection bandwidth then the attack takes place in network and transport layer whereas when the target is on exhausting the server resources then the attack takes place on the application layer. Distributed denial of service attack differs from the denial of service attack in a way that the former attack involves the execution of the attack by the coordination of numerous zombie machines and internet connections whereas the latter only involved a single machine and single connection in control of the attacker [1]. When the attacker performs the attack it is doing that with the collaborative efforts of hundreds and thousands of machines then why not defend the system in the similar way, by achieving collaboration between several nodes which are ready to pool their resources in exchange for some economic incentive.

When combating DDoS attacks the industry and the academia have always ignored the economic incentive part of the problem which has been the key aspect in defeating DDoS attacks. Incentives are the cornerstones of the race of humans. The problem is that although there are many distributed cooperative defense mechanisms but

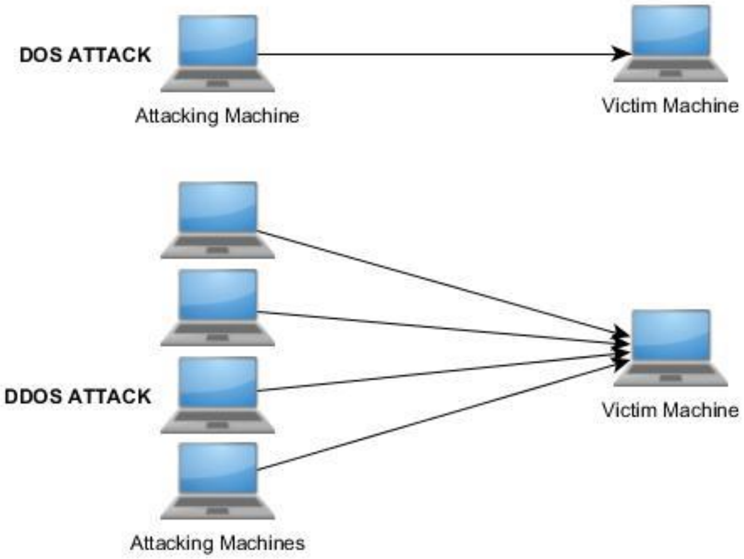

Figure 1 DoS vs DDoS attack

still the systems are being victims of DDoS attacks. This is because no solution has been able to lure ISPs to pool their free cache memories in order to perform collaborative defense. They have been rarely deployed on the Internet because their payment structure is either non-existent or it lacks an incremental pattern. This has led failure of cooperation. Another closely related challenging problem is the deployment of the distributed solutions because detection and responses are scattered at different locations.

The DDoS attack defense mechanisms can be classified by the strategy used to detect the attack. It can be classified as anomaly based, pattern based and third-party detection. In pattern based attack detection technique, the signatures of known attacks are stored in the database and then the traffic is matched with the signatures stored, if the signature matches then the DDoS attack is successfully detected. The main drawback of this approach is its vulnerability to zero day attacks. Every then and now new attacks are launched, new viruses are made so if the stored database is not updated in real time then the system is bound to surpass many new attack types. In anomaly based attack detection technique, an ideal model I defined and the incoming traffic is then compared with that ideal model. If the deviations go beyond the defined acceptable limits then the attack id detected. The advantage of this technique over pattern detection is that here the system can be trained to detect the new types of malicious traffic.

2. Motivation

The Internet Service Providers (ISPs) are facing a problem of increased volumes of illegitimate traffic. The main purpose of this malicious traffic is to exhaust the limited network resources like storage, bandwidth. The level of resources required to maintain the network performance falls short and the Quality–of-Service (QoS) provided by the network degrades rapidly. Avery large volume of malicious traffic is produced by misbehaving users who either knowingly or unknowingly launch flooding Distributed Denial of Service attacks from their systems. Congestion control mechanisms are executed at network level to prevent the traffic from reaching its peak value by throttling mechanism. Throttling means regulating the rate of traffic being transferred over a network link to prevent it from collapsing due to traffic overload.

But this mechanism fails to maintain the required level of QoS. The ability of DDoS attack to generate massive volumes of unwanted traffic has made it one of the biggest threats the internet is vulnerable to [17]. The main targets of DDoS attack are the websites. They attack the benign user’s ability to access the website or server [18]. The primest marks of DDoS attack which went on for two days can be traced back to year 1999 [19]. Since then a lot of DDoS detection techniques and response strategies have been developed. A more advanced kind of DDoS attack is known as amplification attacks like Domain Name Server(DNS) amplification attack, NTP amplification attack etc in which these servers play the role of reflectors and create a stronger attack. In these attacks the servers are not attacked directly but instead these multiple servers are used to generate large traffic against small requests which is directed towards the spoofed IP address provided by the attacker who sent the request to these servers. The response data is used as unwanted traffic. As observed [20] there are two main characteristics because of which the DDoS defense mechanisms have been unable to provide reliable protection. Firstly, the inability to distinguish between the malicious and benign traffic. There is no such mechanism which efficiently differentiate the traffic with minimum collateral damage to the legitimate requests. Secondly, DDoS attack sources are distributed across different sites which is why it becomes very difficult to trace them.

3. Statistics

The largest reported DDoS attack was of volume 400 Gpbs in year 2014[21]. Since then the DDoS attacks are growing in volume. There efficiency and implementation techniques are getting more sophisticated day by day making it a big challenge for the security professionals. The below pie chart shows the distribution of various kinds of DDoS attacks the systems are prone to. The volumetric DDoS attack type is the most common one with 65% of the attacks being the volumetric attacks. They are performed by the slave machines which are a part of botnet and act on the commands of the master machine. The volumetric attacks are done by floods like User Datagram Protocol (UDP) floods, Internet Control Message Protocol (ICMP) floods etc. The second popular attacks are the state exhaustion attacks standing at 18%. This type od DDoS attack is also known as protocol attack because it exploits the vulnerability present in network protocols. Ping of Death exploiting buffer overflow has most instances in state-exhaustion attacks.

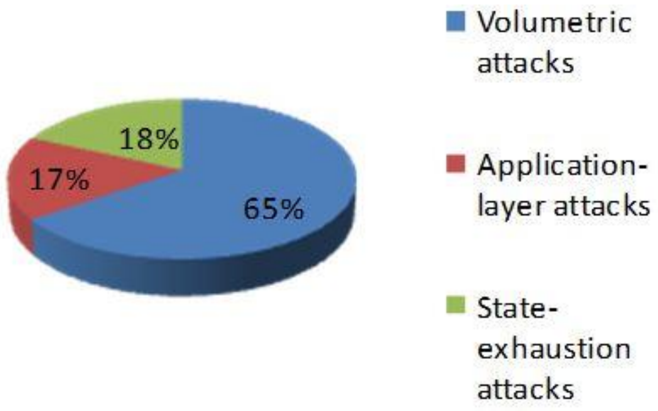

Figure 2 Types of DDoS attacks

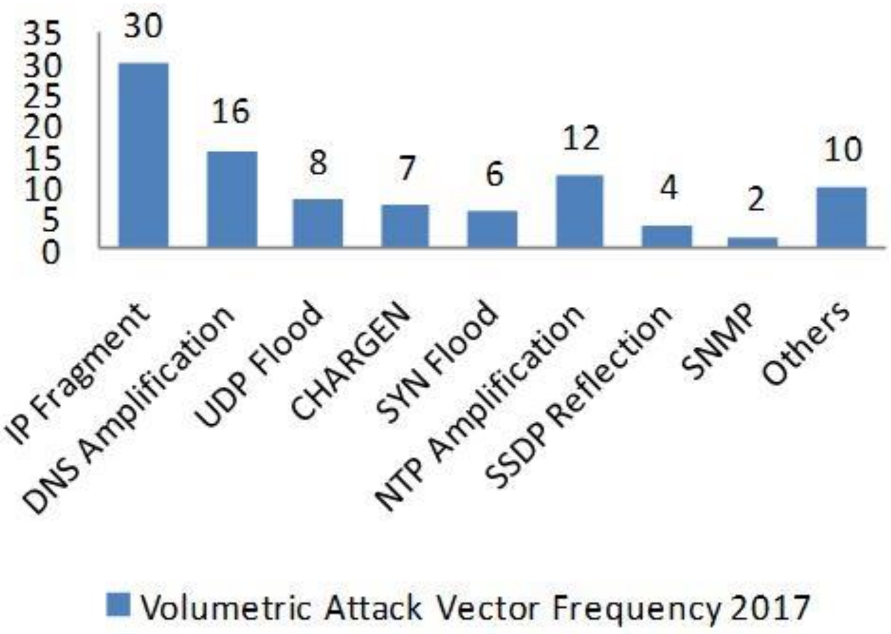

Figure 3 DDoS attack vectors recorded

The next kind of attacks are the application layer attacks standing at
17%. HTTP flood is the most popular kind in this subset. The following graph shows the various volumetric attack types prevalent in year 2017 [22]. They include both infrastructure and application attack vectors. The percentage share of IP fragmentation is the most at 30 percent followed by amplification attack done using Domain Name Servers (DNS). A jump of 69 percent was recorded from August 2017 to December 2017 peaking in September. Probably the reason is that the any person having a computer and internet acces is now able to generate volumetric DdoS attack from its location. The other vectors shown in the graph includes PUSH, POST and GET floods.

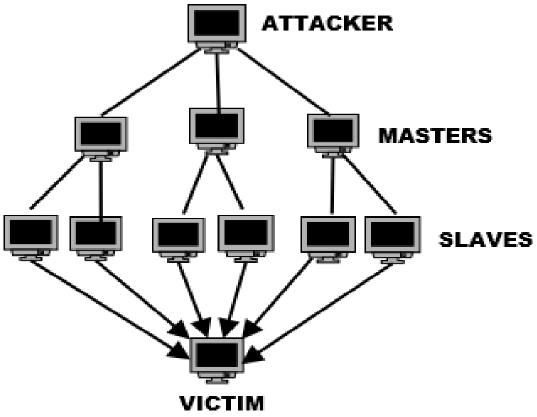

Figure 4 Master-slave model

4. Taxonomy of DDoS Attacks

The first kind of DDoS attack exploits the vulnerabilities in the network protocol and software [26]. And the second kind of DDoS attack focuses on exhausting the network resources by generating huge volumes of attack traffic. This kind of attack is known as flooding attack which is further divided into two types- simple DDoS attack and amplified DDoS attack. Amplified DDoS attack is harder to defend because the sources of attacks are not traceable. In simple DDoS attack an attacker makes an army of several zombie machines by exploiting the vulnerabilities in them. In amplified DDoS attacks, the use of reflectors is made. For example a DNS server, web server, Network Time Protocol (NTP) server can behave as reflector nodes. They all return response packets based on the request packet. A DDoS network comprise of attackers, agents, victim and control messages whose flow is denoted by dotted arrows in the below figures. It is via control messages that the attacker conveys the commands to the zombie army.

4.1 Architecture of DDoS Attack Network

The DDoS attack network is of three types [27]. Agent-handler model, IRC and reflector based model. The agent handler model has three components- attacking machine, zombie machine and the agents. The attacker sends control messages to other zombie machines commanding them to send malicious traffic to the victim node. The below figure explains the Internet Relay Chat (IRC) model in which the zombie machines are replaced by handlers. The function of handlers is to flood the victim on the command of the attacker machine.

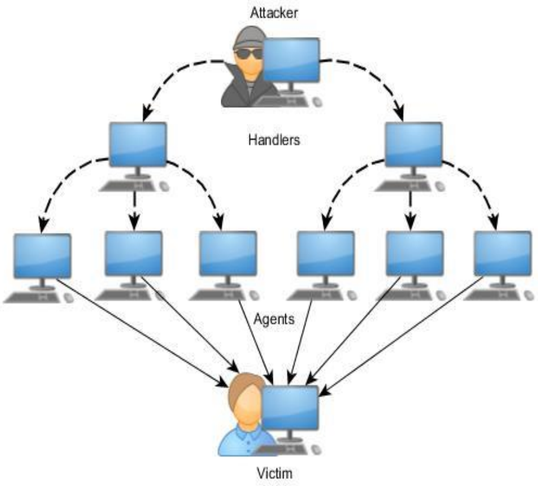

Figure 5 IRC model of DDoS attack network

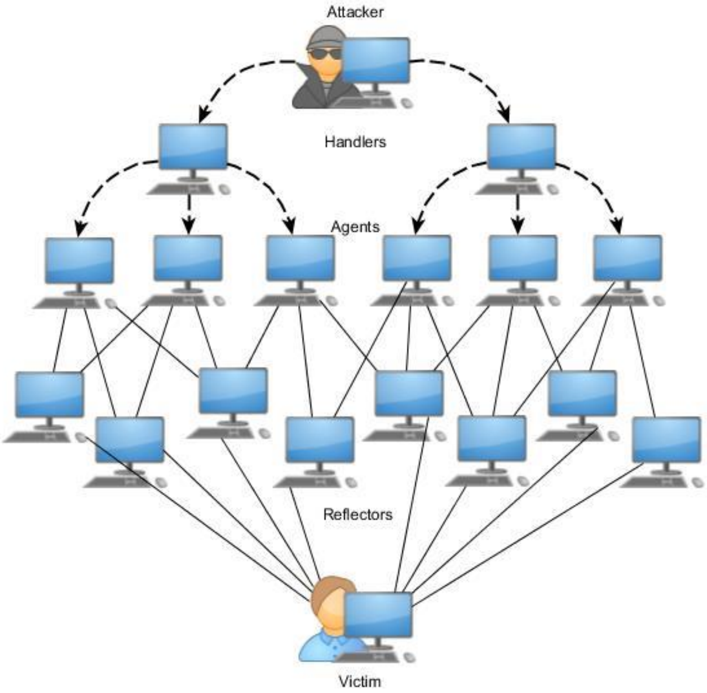

Figure 6 Reflector model DDoS attack network

4.2 Reflector Based Flooding Attack

The above figure explains the reflector based architecture of the DDoS attack. In this attack lies a big difference from the traditional DDoS attack scenario- the use of reflectors. A reflector is a kind of server which responds the client with the replies in accordance with the queries received. The reflector based DDOS attack is always diffused across the network and may further be of two types- Amplified or non-Amplified. Not all reflectors serve as amplifiers [28]. Reflectors are able to generate the attack traffic by catering to legitimate requests only.

4.3 IP Spoofing Based

IP Spoofing is the fundamental technique used in almost all kinds of DDoS attacks. It is done to prevent the location of the attacker from getting revealed. In the IP header there is a filed for source address, which is changed by the agent machines. In the reflecting DDOS attack, the attacking agent replaces its source address by the IP address of the victim machine. These victim machines may be existent or non-existent. For a DDoS attack to be successful it is better to use existent IP addresses so that they can pass through ingress filtering defense mechanism. If the number of zombie machines in the attacker's army is large in count then DDOS flooding attack can be performed without spoofing the IP address. This becomes more untraceable if the chain of zombie machines is spread across different geographical regions. The flooding based DDoS attacks are broadly classified into direct attacks and reflector attacks [29]. The following figure 7 represents another perspective of flooding mechanism.

4.4 Direct Flooding Attack

In direct flooding type DDoS attack, the architecture remains as of simple DDoS attack. The agent machine sends packets like Transmission Control Protocol (TCP), User Datagram Protocol (UDP) and ICMP directly to the victim machine and the reply generated by the victim instead of going to the attacking machine, it goes to the IP address which the attacker had spoofed in the IP header. Whereas in the reflector flooding mechanism the attacker spoofs its IP address as that of the victim. It then sends query packets to the reflector server but the reply packets instead of coming to the attacking machine are diverted to the victim machine. The following are some typical flooding attacks.

4.5 Smurf Attack

This attack is also known as ICMP echo flooding attack. It aims to exhaust the bandwidth of the victim machine by sending multiple echo reply packets. This attack can also make use of amplifiers. The ICMP messages are used to get the status of the nodes in path. The amplifier will broadcast echo request message to the hosts in its subnet. So if its subnet comprise of 100 nodes then the victim will be getting echo reply message from 100 nodes. This is called amplification effect [30].

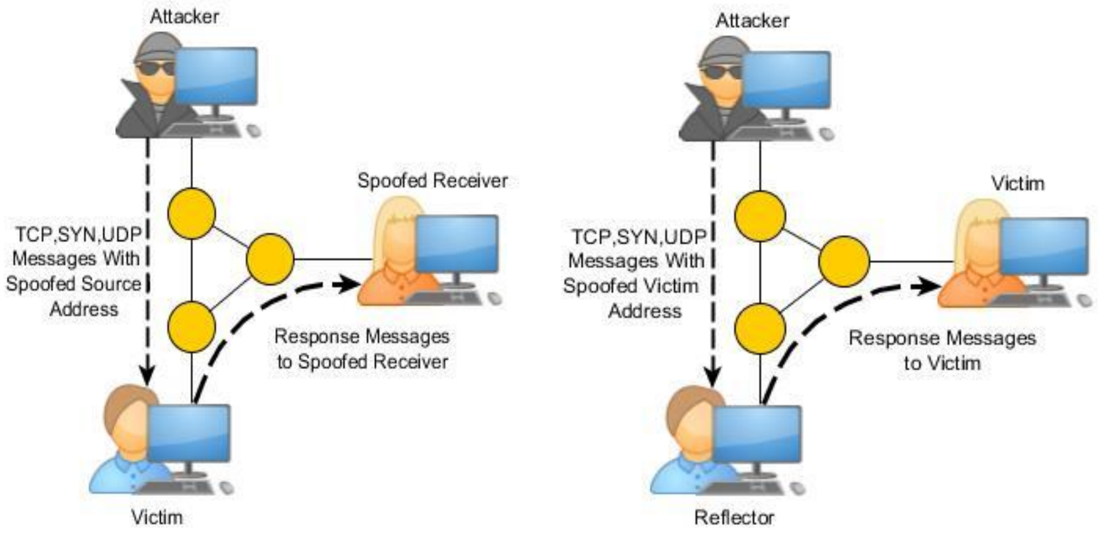
Attacker
TCP,SYN,UDP Messages With Spoofed Source Address
Spoofed Receiver
Response Messages to Spoofed Receiver
Victim
Attacker
TCP,SYN,UDP Messages With Spoofed Victim Address
Victim
Response Messages to Victim
Reflector

Figure 7 Direct vs Reflective flooding mechanism

4.6 TCP SYN Attack

TCP SYN flood [26] is a kind of direct DDoS attack. In this attack the attacker attacks the ability of the victim machine to accept any new TCP connections by leaving them in open state due to incomplete handshake protocol execution. In setting up of a TCP connection, the client initiates by sending TCP SYN packet to the server which replies with TCP SYN-ACK packet. The third step is when the client who requested the TCP connection, sends back TCP ACK packet to the server hence completing the three-way handshake. The server has only limited number of TCP connections, the attacker exploits this vulnerability and sends numerous TCP SYN packets without sending TCP ACK packets for the earlier requested connections, hence leaving open connections. This inhibits the server's ability to accept any TCP connection requests from the legit users.

4.7 UDP Flood Attack

UDP flooding DDoS attack aims at exhausting the bandwidth resource of the victim machine by diverting numerous UDP packets to it. The attacks which target the bandwidth are not completely curbed by increasing the bandwidth links of the victim machine, only its resistance can be increased. UDP protocol is a connectionless protocol. In a UDP flood attack the victim receives numerous UDP packets at different ports. The victim machine then checks for the application on that port, finding none it replies back the sender with Destination Unreachable message packet. Due to absence of any kind of negotiation, spoofing a packet becomes much easier.

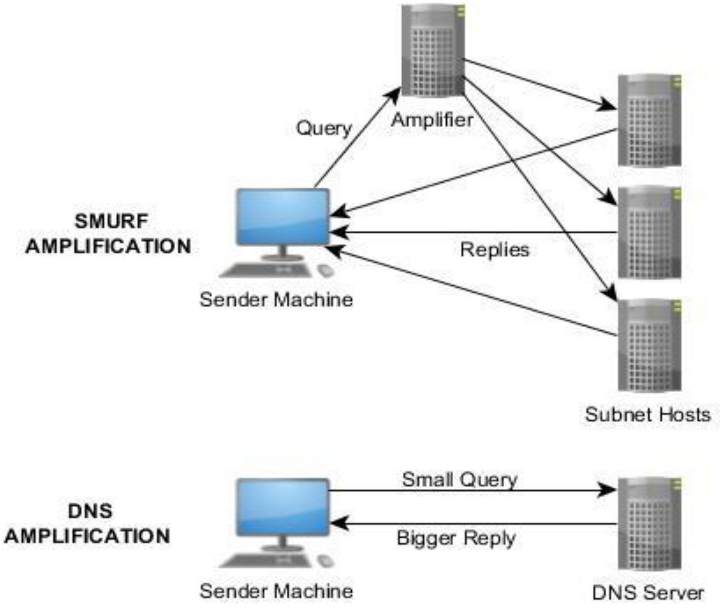

Figure 8 Smurf vs DNS Amplification

4.8 DNS Amplification Attack

Any network protocol which generates a reply to the query can be used in reflector flooding attack. But what empowers this characteristic is the technique of amplification. An amplifier is used to broadcast the query packet to all the servers in its range which aids the attacker to generate a bigger response to a small request as shown in the above figure 8. This way the volume generated as reply to the query becomes multi-fold and using the technique of IP spoofing, this response is diverted to the victim machine which gets overburdened and hence cannot serve legitimate requests making the DDoS attack successful. Figure 9 illustrates the attack mechanism. The largest on record DDoS attack is caused by DNS amplification. The ratio of query to reply of DNS server is 1:70 whereas for NTP server it ranges from 1:20 to 1:200.

DNS amplification attack is a recent type of reflector based DDoS flooding attack. Complicated interaction mechanisms exist between clients and name servers. On comaring the smurf amplification attack with DNS amplification attack one must notice the significant difference in their attacking mechanisms. In smurf attack the echo request messages are broadcasted to multiple hosts in the subnet using amplifiers because of which the amplification effect is achieved, whereas in DNS amplification the server itself magnifies the volume of traffic diverted to the victim machine by generating larger response packets to very small query packets. Smurf attack performs flooding by generating multiple replies to a request whereas DNS amplification generates a single big reply. This helps the attackers in getting more work done in doing less efforts which is why this is a very popular and hard to defend flooding DDoS attack caused by DNS servers as amplifiers.

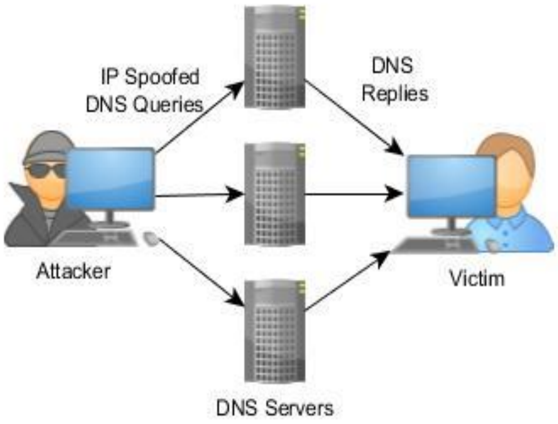

Figure 9 DNS Amplification Attack

5. Taxonomy of DDoS Defense Mechanisms

We can categorize DDoS defense mechanisms in two categories- centralised and distributed. This depends on whether the defense mechanisms phases- detection, mitigation and response are deployed at the same location or different locations. In the centralised mechanisms the whole DDoS defense mechanism is either set up at source, destination or the intermediate network. But in centralised mechanisms the detection might take place at the victim node, mitigation at the intermediatory nodes and response at the source of the attack traffic generation. This means that the whole process is scattered at various locations in the internet but to successfully combat against the DDoS attack all these parties need to work together in collaboration with one another [3].

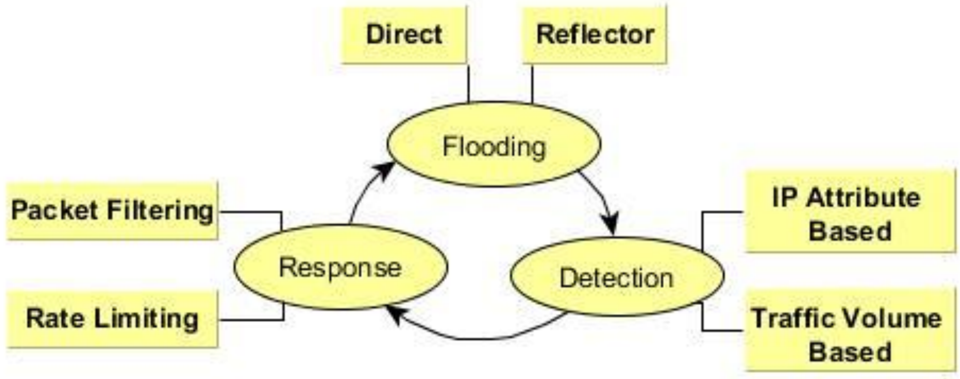

Figure 10 DDoS attack scheme

In this write-up the focus is on several cooperative defense mechanisms available but first we explain the need of such mechanisms when centralised ones are already in place. In centralised systems the main issue is single point of failure. It means the whole of the defense system can crash if the only site where all its components are deployed comes under attack. The cooperative system is able to solve this problem by having multiple nodes in action for defense at different locations. These nodes have similar functionalities so even if the nodes in one location are compromised still we have numerous set of nodes in place to defend the victim site. Secondly, internet does not have any central control authority over its autonomous systems so a defense model which does not have a central authority in control will prove beneficial.

5.1 Pushback and Packet Marking

Chen et al. [5] proposed a cooperative mechanism by combining the techniques of pushback messages and packet marking. It is called Attack Diagnosis(AD) in which the victim machine first detects the DDoS attack and then sends AD commands to the upstream routers in the network. It is a reactive defense mechanism. It makes use of AD enabled routers which then starts marking each packet deterministically with the interface information it is passing through. The victim machine then then uses this attached interface information to traceback the source of malicious packets.

The AD related commands are authenticated using the Time To Live(TTL) field of the IP packet header. AD scheme is ineffective when the DDoS attack is performed at a large scale so an extension to AD called Parallel Attack Diagnosis(PAD). AD can stop the traffic from single router at a time, whereas PAD diagnoses and stops the traffic from multiple routers simultaneously.

5.2 IP Traceback and Port Marking

Chen et al. [6] have proposed one more distributed DDoS mechanism based on the concept of router port marking and packet filtering. These are presented as two modules used. The function of router port marking module is to mark the packets probabilistically by appending router’s interface port number to the packets. It is a six digit number which is locally unique. When the victim machine is flooded with the malicious packets then it makes use of this appended information to traceback the source of the malicious packets.

The function of packet filtering module comes next which then filters the malicious incoming packets at the upstream routers. This mechanism has low computation and communication overheads. But it has two limitations. Firstly, as there is no authentication used so the attackers can forge the marking fields so that their actual location is never revealed. Secondly, although this technique effectively traces back the IP but it fails to identify the master behind the DDoS attack who is in control of the army of zombies or compromised machines.

5.3 Signature Based Defense

Papadopoulos et al. [8] proposed Coordinated Suppression of Simultaneous Attacks (COSSACK) mechanism. It uses a software system called watchdog which is built on the edge routers. It is based on a critical set of assumptions like existence of attack signatures, edge router’s capability to filter packets on the basis of these signatures and continuous connection availability. The watchdog software does ingress and egress filtering on the edge routers to stop DDoS attack flow and it also sends multicast notifications to the source side. It is unable to withstand DDoS attack traffic generated from the legacy networks that have not deployed COSSACK.

5.4 Capability Based Defense

Anderson et al. [9] have proposed distributed defense mechanisms based on the capabilities. In these mechanisms firstly the sender has to obtain the rights to send from the receiver. These rights are kind of short-term contracts, tokens or authorizations. To understand this better we can understand it through an analogy of sticking on the postage stamp onto the letter before posting. The only difference here is that the postage stamp is bought from the post office whereas the sending rights will be obtained directly from the receiver. Another analogy will be of receiver defining the window size beforehand in sliding window protocol of data link layer. The major drawback of this scheme is that the capability setup channel is not secure. These mechanisms always have to be kept active hence increasing the processing and memory overheads.

5.5 Datagram Based Defense

Argyraki et al. [11] proposed an alternative to capability based filtering mechanism which is datagram filtering mechanism in which instead of denying all the traffic by default only that traffic is denied which is identified as malicious. This is called Active Internet Traffic Filtering(AITF). In this the receiver is able to contact the misbehaving senders and ask them to stop. Every ISP polices its misbehaving nodes or else they are at a risk of losing connectivity to the victim machine which may be an important point of access. So there lies as strong incentive for the participating ISPs to cooperate. AITF is affordable to be deployed by the ISPs because it preserves the receiver’s bandwidth at per-connection cost. The legitimacy of the traffic is verifies using three-way handshake which may not be completed because the handshake packets and the DDoS attack traffic are flowing through the same flooded link. This mechanism also has several deployment issues because it is not relying on edge routers for actual filtering. The routers used are in placed the middle of the network.

5.6 Anomaly Based Defense

X. Liu et al. [12] proposed another distributed defense mechanism against network and transport layer DDoS attacks namely StopIt. In this mechanism each receiver installs a network filter which blocks the undesirable traffic. It makes use of Passport mechanism proposed by X. Liu. for authentication purpose. It has made use of looped and third generation of telecom networks in its architecture. Every autonomous system has a StopIt server for sending and receiving StopIt requests. A filter is installed at the source and the filter requests are exchanged among the peer nodes. In this mechanism the StopIt server can be attacked with packet floods and filter requests if the requests are allowed from neighbouring autonomous systems also. Moreover, StopIt mechanism needs complex detection mechanisms which make it hard to deploy.

5.7 Volume Based Defense

Walfish et al. [13] proposed a distributed DDoS defense mechanisms to prevent application layer level attacks. In this paper the concept of defence by offense is followed. It encourages the honest clients to speak-up by increasing the volume of benign traffic it sends to the server being targeted by DDoS attack. This ensures that the percentage of bandwidth captured by the good clients is increased hence out crowding the one flooded by the attacker. In this work it is not explained how will the server detect the attack. Speak-up mechanism is applicable only in session flooding attacks and not in request flooding or asymmetric attacks.

5.8 Hybrid Defense

J. Yu. et al. [14] proposed a Defense and Offense Wall(DOW) scheme. This is an extension to the Speak-up work by Walfish et al. with addition of anomaly detection method. The anomaly detection method used is based on K-means clustering approach to detect asymmetric, request flooding and session flooding attacks. It has explained the mechanism using two models- the detection model and the currency model. The former's function is to drop suspicious packets while the latter's function is to encourage the increase in session rates by legitimate clients. The major drawback of this mechanism is that it is too resource consuming to be implemented.

6. Literature review/related work

Network and Transport Layer Cooperative Defense	Name of scheme	Author	Scheme description	Limitations
	Aggregate congestion control and Pushback (2002)	R. Mahajan et al.	ACC rate limits the aggregates rather than IP sources	Not effective against uniformly distributed attack sources
	Attack Diagnosis and parallel-AD (2005)	R. Chen, J.M. Park	Combines pushback and packet marking	AD is not effective against large-scale attacks

	TRACK (2006)	R. Chen et al.	Combines IP traceback, packet marking and packet filtering	Not effective for attack traceback
	Passport (2008)	X. Liu, A. Li, , X. Yang, D. Wetherall	Makes use of symmetric key cryptography to put tokens on packets that verify the source	• Attackers may get capabilities from colluders • It only prevents the hosts in one AS from spoofing the IP addresses of other ASs
	Defensive Cooperative overlay mesh (2003)	J. Mirkovic et al.	Defense nodes collaborate and cooperate together	• Classifier nodes require an inline deployment. • Unable to handle attacks from legacy networks
	Stateless Internet Flow Filter (2004)	A. Yaar et al.	Capability-based mechanism	• Always active • Processing and memory costs overheads
	StopIt (2011)	X. Liu, X. Yang, Y. Lu	Novel closed control and open service architecture for filters to be installed	• Vulnerable to attacks in which attacker floods the router • Needs complex verification/authentication mechanisms • Challenging to deploy and manage in practice.
Application Layer Cooperative Defense	Active internet traffic filtering (2009)	K. Argyraki, D.R. Cheriton	Misbehaving sources are policed by their own ISPs	• Several deployment issues • If the flooded link is outside victim's AS, the three way handshake may not complete
	Speak-up (2002)	M. Walfish et al.	Encourage the good clients to out-crowd the bad ones	Not applicable against request flooding and asymmetric attacks

	Defense and offense wall (2005)	J. Yu et al.	Encouragement method with anomaly detection	Very resource consuming to be implemented
	CAPTCHA (2003)	L.V. Ahn et al.	Differentiate DDoS flooding bots from humans	• More delay for legitimate users • Disables web crawler’s access to websites
	Admission control and congestion control (2002)	M. Srivatsa et al.	Port hiding	Requires a challenge server which can be the target of DDoS attacks

Table 1 Layer-wise cooperative DDoS defense mechanisms

Mahajan et al. [4] proposed a distributed DDoS defense mechanism called Aggregate-based Congestion Control(ACC). Aggregates are a part of the network traffic which is identified as malicious. It is characterised by source IP addresses or destination ports. In this mechanism the router detects the aggregates which are overloading its bandwidth rather than the IP sources. On detection of such samples the router sends pushback message to the upstream routers in the network and then sends a rate limit. From then on if the traffic from those upstream routers exceed that rate limit then the packets are dropped and multiple pushback messages are sent. This technique fails to be effective when the attack traffic is uniformly distributed in the network.

Mirkovic et al. [7] proposed a distributed framework called DEFensive Cooperative Overlay Mesh (DEFCOM). This framework supports information and service exchange among the cooperating nodes in the system. They have shown a distributed defense framework architecture of heterogeneous defense nodes which collaborate and cooperate with each other and work as a team to combat DDoS attack. By heterogeneous what is meant is that all the defense nodes do not share the same functionality, like nodes near the victim will do the detection best and the nodes near the source will cater to the response technique.

In this mechanism, the attack alerts from the generator nodes are flooded into the network after which the rate limits are sent to the upstream routers. From then on all the resources requests that are sent to the downstream routers are first classified and the malicious packets are dropped. This works in a P2P network scenario just proper rate limits for both upstream and downstream routers need to be defined and simultaneously the classifier nodes are at work to differentiate malicious traffic and benign traffic. The main disadvantage of this framework is that this is not compatible with the old or legacy networks so if a large portion of the network is a legacy network then the classifier nodes which are deployed in-line malfunction.

X. Liu et al. [10] addressed the drawback of the capability based mechanism scheme by adding secure authentication systems to capability based mechanisms. They called it a Passport system which uses symmetric-key cryptography to encrypt the tokens before appending them to packets being sent. This allows the routers in path to verify that the source address is genuine. Using this technique the ISPs can protect their own addresses from being forged so such schemes offer stronger incentive as compared to other filtering schemes.

This mechanism is vulnerable to colluding attacks in which the attackers get the capabilities from the cheating nodes or they can eavesdrop the packets of the node is honest. Another limitation of this scheme is that although the attackers cannot spoof the IP address of host belonging to other autonomous system but it can easily spoof the IP of some other host in the same autonomous system.

S. Kandula et al. [15] tried to differentiate the DDoS flooding done by humans and bots. They employed a mechanism called Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA). Although it is good technique to differentiate robots and humans but the main disadvantage is that it requires the users to solve different puzzles to pass the authentication test having text, pictures which becomes an annoying task for the users.

Srivatsa et al. [16] proposed an admission control and congestion control scheme which limits the number of clients being served simultaneously. It works on the principle of port hiding which hides the port number on which the service requests are accepted hence making the port invisible to the illegitimate clients. Then congestion control is performed to allocate more resources to good or legitimate set of clients.

7. Performance Evaluation Metrics

Although there are not any standard set of measurements used by the research community but the performance evaluation metrics for volumetric DDoS attack defense strategy can be divided into two according to the level of attack traffic experienced. The first category of the metrics are the ones which measure the performance evaluation under high traffic load and the second one measures the performance under low traffic load. Some commercial products [23] also exist to measure the performance by evaluating a variety of results of the defense technique. The following are discussed below.

7.1 Detection Rate

It measures the number of attacks that are detected from the the number of attacks actually performed by the attacker.

7.2 False Positive Rate

It measures the number of times the legitimate user traffic is wrongly detected as DDoS attack traffic. A similar parameter is true negative which detects the attack even when it is absent. Similary, false negative denotes the inability to find the malicious traffic.

7.3 Ratio between Detection Rate and False Positive Rate

This metric is generated using Receiver Operating Characteristic (ROC) curves over detection rate and false positive rate. ROC curves are widely used to calculate the sensitivity and specificity of the evaluation parameters.

7.4 Failure Rate

It is an application layer level metric [25] which is calculated by finding the ratio of number of requests which go unresponded by the victim to the total number of requests received by the victim.

7.5 Average Latency

It is a measure of application level performance. It is the average of the time delays experienced between the sender initiating the request and the receiver receiving the response message at different instances.

7.6 Throughput

The throughput directly indicates the performance of any defense mechanism. It is the total amount of data transmitted in a unit time.

7.7 Bandwidth

It is the aggregate level of performance measure [24]. Bandwidth denotes the amount of traffic a link can carry under various sates like normal state, attack state.

7.8 Malicious Packet Drop Rate

DDoS defense scheme on packet level aims to lower the volume of malicious packets by selectively dropping them from the whole traffic received. It reflects the capability of any defense mechanism to control the flooding traffic. It is calculated as the ratio of number of packets dropped before reaching the victim to the total number of packets destined for the victim.

7.9 Benign Packet Drop Rate

The main purpose of DDoS defense scheme is to maintain the level of QoS for the benign user traffic. The motive is to be able to forward as many benign packets as possible by preventing the bandwidth to collapse due to congestion. It is calculated as the ratio of number of benign packets dropped before reaching the victim to the total number of packets destined for the victim.

Adjusting the parameters of performance estimation is an important task. Selection of appropriate parameters to judge the performance of any scheme in the network depends on certain rules like he changes in the attack tragic load should be separated into two cases. First, when the variation in traffic rate is very slow and second, when the attack traffic is changing at a rapid rate. The parameters of legitimate data traffic should be collected from the victim side when it is not under any kind of attack, then only a comparative analysis can be done when the developed scheme is enforced.

8. Conclusion

On analysis of various DDoS detection, mitigation and response frameworks the common challenge faced by each on e of them is to quicker detection rate with sustainability of QoS for benign users. In all these techniques the DDoS defense mechanism can be broken down into three parts.- detection, mitigation and response. The mechanisms developed are not only victim-end defense or source-end defense mechanisms but a combination of both across the network. The backbone of these hybrid mechanisms remain a highly effective cooperative mechanism to ensure stable and rigid communication.

9. Scope for Future Research

In the future research, the evaluation of these defense schemes on different topologies of internet will be helpful in deployment of these mechanisms in broader technical areas. For any detection technique developed, setting the value of threshold is very important. Optimization of threshold parameter for any network is an important research area. Inclusion of statistical features for calculating threshold value will enhance its precision. Timely detection of end of DDoS attack is also an important research area having future scope. In fighting against any kind of cyber attack, data plays a very crucial role. The recovery of the legitimate traffic should be very quick and must ensure integrity.

References

1. Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004): 39-53.
2. Rodrigues, Bruno, Thomas Bocek, and Burkhard Stiller. "Enabling a Cooperative, Multi-domain DDoS Defense by a Blockchain Signaling System (BloSS)."
3. Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." IEEE communications surveys & tutorials, pp 2046-2069, 2013.
4. R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, Controlling high bandwidth aggregates in the network, presented at Computer Communication Review, pp.62-73, 2002.
5. R. Chen, and J. M. Park, Attack Diagnosis: Throttling distributed denial-of-service attacks close to the attack sources, IEEE Int'l Conference on Computer Communications and Networks (ICCCN'05), Oct. 2005.
6. R. Chen, J. M. Park, and R. Marchany, TRACK: A novel approach for defending against distributed denial-of-service attacks, Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, Virginia Tech, Feb. 2006.
7. J. Mirkovic, P. Reiher, and M. Robinson, Forming Alliance for DDoS Defense, in Proc. of New Security Paradigms Workshop, Centro Stefano Francini, Ascona, Switzerland, 2003.
8. C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, Cossack: Coordinated Suppression of Simultaneous Attacks, in Proc. Of the DARPA Information Survivability Conference and Exposition, Vol. 1, pp. 2 13, Apr. 2003.
9. T. Anderson, T. Roscoe, and D. Wetherall, Preventing Internet denial-of-service with capabilities, SIGCOMM Comput. Commun. Rev., vol. 34, no. 1, pp. 39-44, 2004.
10. X. Liu, A. Li, X. Yang, and D. Wetherall, Passport: secure and adoptable source authentication, in Proc. of the 5th USENIX Symposium on Networked Systems Design and Implementation (NSDI'08), San Francisco, CA, USA, pp. 365-378, 2008.

11. K. Argyraki, and D. R. Cheriton, Scalable network-layer defense against internet bandwidth-flooding attacks, in IEEE/ACM Trans. Netw., 17(4), pp. 1284-1297, August 2009.
12. X. Liu, X. Yang, and Y. Lu,"To filter or to authorize: network-layer DoS defense against multimillion-node botnets", in Proc. of the ACM SIGCOMM conference on Data communication (SIGCOMM '08), NY, USA, pp. 195-206, 2008.
13. 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.
14. J. Yu, Z. Li, H. Chen, and X. Chen, A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks, the third International Conference on Networking and Services (ICNS'07), pp. 54, June 19-25, 2007.
15. S. Kandula, D. Katabi, M. Jacob, and A. W. BergerBotz-4-sale: Surviving organized ddos attacks that mimic flash crowds, in Proc. Of Symposium on Networked Systems Design and Implementation (NSDI), Boston, May 2005.
16. M. Srivatsa, A. Iyengar, J. Yin, and L. Liu, Mitigating application-level denial of service attacks on Web servers: A client-transparent approach, ACM Transactions on the Web (TWEB), Vol. 2, no. 3, July 2008.
17. K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Reducing unwanted traffc in a backbone network," in Steps to Reducing Unwanted Traffic on the Internet Workshop(SRUTI), 2005, pp. 915.
18. CERT Coordination Center, "Denial of service attacks."Available at http://www.cert.org/tech tips/denial of service.html, March 2007.
19. L. Garber, "Denial-of-service attacks rip the Internet." IEEE Computer, vol. 33, no. 4, April 2000, pp. 12-17.
20. CERT Coordination Center. "CERT advisory CA-98.01 smurf IP denial-of-service attacks." Available at http://www.cert.org/advisories/CA-1998-01.html, March 2007.
21. https://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/ [Last access on 21/03/2018].
22. https://www.akamai.com/us/en/about/news/press/2017-press/akamai-releases-third-quarter-2017-state-of-the-internet-security-report.jsp [Last access on 21/03/2018].
23. A. Hussain, S. Schwab, R. Thomas, S. Fahmy, and J. Mirkovic, "DDoS experiment methodology." in Proceedings of DETER Community Workshop, June 2006, pp. 8-14.
24. W. Feibel, The Network Press Encyclopedia of Networking. Sybex, 2000.
25. C. Ko, A. Hussain, S. Schwab, R. Thomas, and B. Wilson, "Towards systematic IDS evaluation." in Proceedings of DETER Community Workshop, June 2006, pp 20-23.

26. J. MÄolsÄa, “Mitigating denial of service attacks in computer networks". PhD thesis, Helsinki University of Technology, Espoo, Finland, June 2006.
27. S. M. Specht and R. B. Lee, “Distributed denial of service: taxonomies of attacks,tools and countermeasures." in Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, September 2004, pp. 543-550.
28. V. Paxson, “An analysis of using reflectors for distributed denial-of-service attacks." ACM SIGCOMM Computer Communication Review, vol. 31, no. 3, July 2001.
29. R. K. Chang, “Defending against fooding-based distributed denial-of-service attacks: A tutorial." IEEE Commun. Mag., vol. 40, no. 10, October 2002, pp. 42-51.
30. CERT Coordination Center. “CERT advisory CA-98.01 smurf IP denial-of-service attacks." Available at http://www.cert.org/advisories/CA-1998 01.html, March 2007.