A Review on Detection, Defensive and Mitigation of DDoS Attacks with Traceback Methods

Mr K Alluraiah[a], Manna Sheela Rani Chetty[b]
[a] Research Scholar, [b] Professor
[a, b] Department of Computer Science and Engineering, KoneruLakshmaiah Education Foundation, Vaddeswaram, AP, India
[a] alluraiah.svcolleges.edu.in, sheelarani_cse@kluniversity.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: The most tremendous attacks in the globeis Distributed Denial of Service (DDoS) attacks, which is the very powerful and typical external attempts to weak bandwidth of the victims or interrupt legitimate users to access the services. The traditional Internet services of architecture is unsafe to DDoS attacks and the collection of internet connected devices affected by the malwares, then it allows the intruders to control all the internet connected devices is a Botnet or attacked networks.In Botnet, one disadvantage is that if the Botnet is set up then the intruder creates the large-scale networks to attack on more number of victims.As anoutcome of the permanentgrowth of latest attacks and constantly growingcollection of weak sources on the internet, the Detection, Prevention of DDoS attack and Trace back methods have been proposed.In this paper, we have reviewed various types of classification methods for DDoS attacks and its countermeasures. Finally,this survey paper assesses and illustrates the efficiency of variousDDoS attacks including detection, defense and mitigation, trace back methods. These methods rely on better router functionality or changes to existing protocols. The advantages and disadvantages of existing research methods in this problem are also described..

Keywords: Machine Learning, Naïve Bayes, Distributed Denial of Service (DDoS) Attack, Botnet, Fuzzy logic.

1. Introduction

Recently, Distributed Denial of Service (DDoS) attacks have acquired enormous money related adversities to trade and governance all over the world, as appeared in Worldwide Infrastructure Security Report [1]. In most Internet conditions, gadgets help out applications that run by thought on the affiliation, which interfaces with hazardous experts to see responsibility concerning contraptions. Appropriately, it is reachable to have the impedance of affiliations or the utilization of contraptions as a starting inspiration driving attacks for different region, similar to the event of the DDoS attacks [2], which has been accumulated for various considerations, for example, (I) straightforwardness and office of execution, not needing enormous unequivocal data on the aggressor side, and (ii) arrangement of stages and operations for related attack union. Possibly the most hazardous malevolent traffic on the web is the DDoS volumetric attack, which is in hazard for over 65% of aforesaid attacks [3]. In a volumetric DDoS, a couple of aggressors arrange the sending of a high speed of pointless information attempting to over-bother the disasters figuring resources or the close by association joins. As shown by one perspective, the high achievement rates for such an attack happen pondering when the distracted Internet switches reliably utilize the FIFO (First-In-First-Out) and DROP-TAIL lining areas. Solid traffic is besides destroyed [3]. Intensely hot clear domain and control of DDoS attacks has gotten earnestly testing as aggressors keep utilizing novel techniques to dispatch DDoS attacks [4]. The ever-increasing number of DDoS attacks, concurred with making gathering in their sorts, generating bad effect, has undertaken DDoS attack Detection, disavowal, and help the foremost need.

The DDoS attack [5,6] has a huge growth, associated with attack on the strategy of relationship of a maddening turn of events or network resources, dispatched by suggestion through unlimited coordinated PCs on the web. Going prior to implementing an attack the assailant undertakes command over giant uncountable PC machines over the web and these PCs are frail machines. The assailant abuses these PCs deficiencies by embedding harmful code or other different hacking strategy so that he could easily overpower them. These delicate or bargained machines conceivably scands in numbers and these are expectedly named as 'zombies.' The gathering of zombies when in doubt spread out the 'Botnet.' The scale of the attack relies upon the amount of the Botnet, used for logical Botnet, the attack is ensured greater along with shocking. Within the Internet DDoS attacks may be dispatched with the usage of two huge strategies. In the key strategy the attacker ships a few risky packs to the trouble to stupefy a show or software strolling on it. The Second method from an overall perspective joins the network/transport-level/application-level flooding attacks [7], wherein an assailant does each going with: (i) interfere with an authentic customer's straightforwardness by exhausting exchange speed, network resources or switch supervising cutoff or (ii) upset relationship of an ensured clients by obliterating the master assets, as an example, CPU, memory, plate/database record transmission and I/O move pace. Nowadays, DDoS attacks are reliably dispatched through competent, by suggestion controlled, and all around included Zombies or Botnet PCs of anetwork, which are never-endingly or concurrently sending a massive degree of traffic or association alluding to the goal plan. The attack consequences the goal configuration either react powerfully or abend absolutely [7],

[8], [9]. Zombies of a Botnet are normally picked utilizing Trojan horses, worms, or discretionary segments [10], [11]. It is exceptionally hard for the protect portion to see the genuine attacker considering the utilization of sign IP addresses by zombies immensely influenced by the attacker with Botnet [12].

In Figure 1, depicted as, the attacker assistants with control server to make the control and dominate the design. The control server has stacks of resources and which is an amazing trained server, the control cut off may contains the different form like memory, bandwidth and processing power. Regardless of taking the commands from the attacker, the middle people, furthermore referred to as Agents are liable for looking through Botnets. They send instructions identified with models and amend the same to the Botnets. In this, the owner makes the undermined frameworks for the malwares introduced on their PCs on the off chance that they are one of the parts in the Botnets. Always attackers utilize the specialists as work locale leaps to begins the attacks against the target systems (victims) [13]. Therefore, this is required to locate the Botnet DDoS attacks to intrude with the designs of several assets from being crushed. Machine Learning methods when presented to information are in shape for adjusting autonomously and gaining from prior calculations to decipher the accessible information for recognizing hidden patterns.

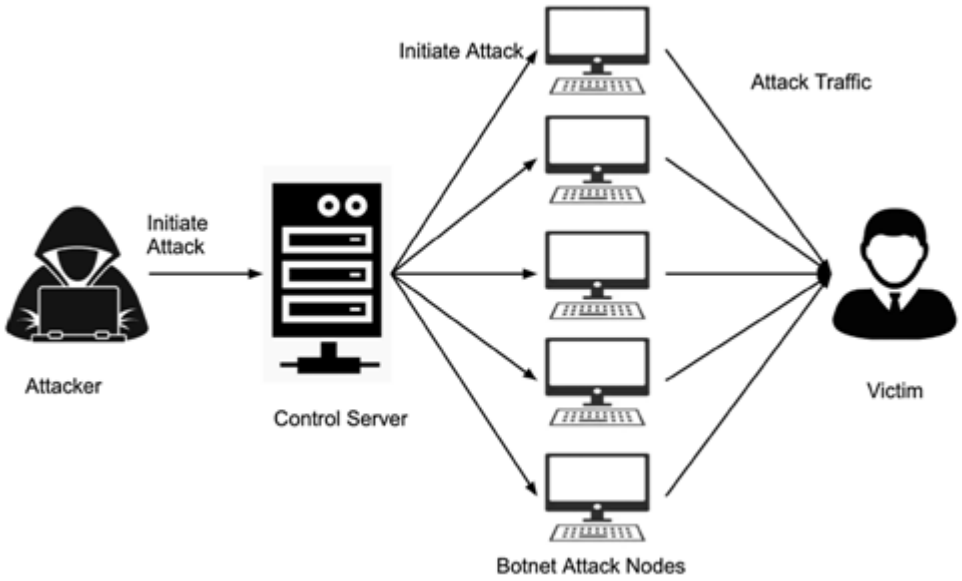

Figure. 1. The Illustration of DDoS attack.

2. The DDoS Attacks of the Classification Methods

The DDoS attacks, being dispersed in nature makes them incredibly unbelievable to fight or trace back mechanism. Knowing and seeing all the properties of [14],[15] DDoS attacks is one of the significant steps towards the progress of historic and skilled DDoS defensive mechanism described the essential for understanding DDoS attack and their impact in cloud environment. Figure 2 illustrates the classification methods for DDoS attacks dependent on the mode, stream, impact and consumption of the attack.

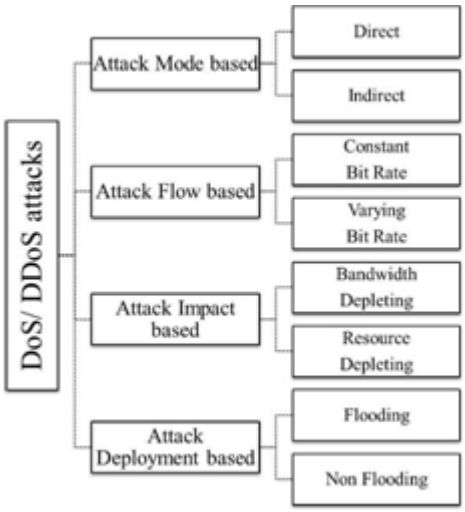

Figure 2: The Classification methods for DDoS Attacks

DDoS have different appearances, but flooding attack, the most outstanding form of DDoS is the guideline purpose of assembly of this research work. The Flooding attack is an attack wherein it covers the network with unnecessary packets, for example either the node may send different packets or the middle point may send the entrancing gatherings which beat its rate limit. A DDoS attack has been mentioned here into two, considering the show level that it attacks and dependent on Botnets. Considering the flooding attacks, protocol level could be classified into two categories. 1) Transport/Network level or 2) Application level. In Transport/Network layer, ICMP, DNS, TCP and UDP protocol packets are usually used to launch the attacks. Thinking about the Botnets, DDoS attacks can be classified into attacks because of IRC based Botnets and attacks considering internet-based Botnets. The following with Figure 3 obviously depicts the classification methods of DDoS flooding attacks.

1. Network /Transport Level Flooding DDoS Attacks

Such forms of attacks are launched utilizing DNS, ICMP, TCP and UDP protocol packets. Here we've got four kinds of attacks on this group.

a. Normal flooding attacks

The association of the legitimate users is the major point of the flooding attacks. Attackers mainly attempt to tire out the victim's network bandwidth. Illustrations of flooding attacks are VoIP flood, DNS flood, ICMP flood, UDP flood and so on all these flooding can be accomplished either by spoofed or non-spoofed IP addresses.

b. Protocol exploitation flooding attacks

The utilization bugs of a touch of the victim's protocols are the primary agenda here. Attackers use some particular features to consume majority of the victim's resources. Instances of protocol exploitation flooding attacks are RST/FIN flood, ACK& PUSH ACK flood and TCP SYN flood and so on.

c. Reflection-based flooding attacks

Rather than sending direct requirements to the reflectors, attackers traditionally send conveyed ICMP repeat request. Considering that the reflectors will send their reactions to the individual being victim. In this manner, the reflectors exhaust the requirements of the individual being victims. The Models are Smurf and Fragile attacks.

d. Amplification-based flooding attacks

For each message they get, attackers misuse services to make more prominent and different messages to build the traffic towards the individual being victims. Reflection and improvement techniques are consistently utilized by the assistance of Botnets. For instance, attackers send spoofed requests to vast number of reflectors in smurf attack, which is the reflection and this is finished by mauling IP broadcast feature of the groups and that is the expansion. The entire of the above kinds of attack were introduced in [26], [27], [28].

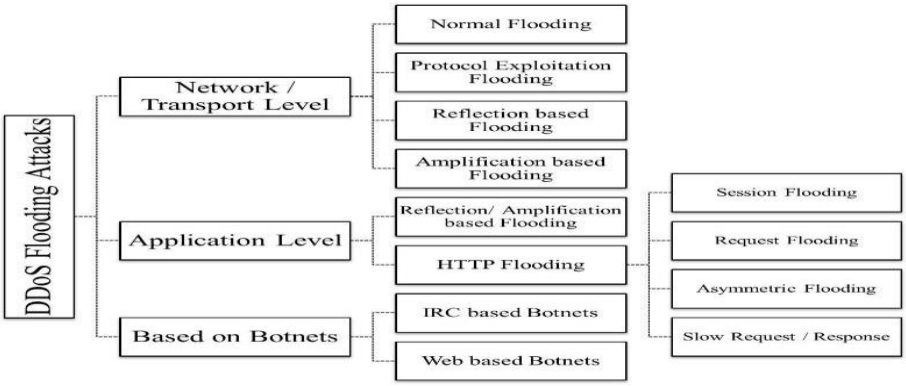

Figure 3. Classification of DDoS Flooding Attacks

2. Application-Level DDoS Flooding Attacks

Upsetting valid user's facilities with killing the server services includes CPU, memory, I/O bandwidth, Sockets and disk bandwidth is the center of application-level DDoS attacks. Being like to legitimate traffic, they are stealthier than numerous attacks. Due to the fact that the application layer attacks target the Hypertext Transfer Protocol (HTTP) or Session Initiation Protocol (SIP), DNS they typically contain the same collision to the resources. Now, SIP flooding attacks and DNS amplification flooding attacks are briefly described like the two well-known application-level flooding attacks in this group exploiting DNS as well as SIP protocols.

a. Reflection/Amplification based flooding attacks

These types of attacks used to send fake application-level protocol requests. DNS amplification attack used to rent both reflection and amplification techniques. With respect to DNS, reply messages are constantly significantly better than the uncertainty messages. So, the attackers who make a huge amount of network traffic use fake source IP addresses to produce small DNS queries. This generated large quantity of data traffic is going to the sufferer system to make it partially or completely incapable.

VoIP flooding attack, a new example that uses reflection technique is a difference of UDP flooding.

In this, attacks send VoIP packets from fake source IP addresses through SIP at a extremely high rate. The array of the source IP address will also be extremely large. The fake connections use large number of resources. The victim VoIP server should be able to distinguish authentic and fake VoIP connections. The VoIP flooding will destroy a network with packets from random source IP addresses or even permanent.

b. HTTP flooding attacks

In this category, the subsequent are the four types of attacks.

i. Session flooding attacks

Attacker's meeting correlation request rates are higher than the genuine users' requests in this kind of attack. This consumes a lot of the server resources and causes flooding attack. In this group, HTTP get/post flooding attack plays most vital role in this category in which a huge number of legal HTTP requests are generated by the attackers in the structure of get/post, to a victim web server. Such an attack is likewise called as extreme VERB and uses non-spoofed IP addresses.

ii. Request flooding attacks

In this group, sessions that include several requests than normal are sent by the attackers. Single-session HTTP get/post flooding attack (also known as excessive VERB Single session) is the famous attack in this category. This is different from the earlier attack and permits different requests in a particular HTTP session using the quality of HTTP 1.1. Therefore, attackers can bound the HTTP attack session rate and may keep away from the session rate constraint method of different defense mechanisms.

iii. Asymmetric attacks

Sessions that include high volume requests are sent by attackers.

3. Botnet-Based DDoS Attacks

The most essential mechanisms that enhance DDoS flooding attacks are Botnets. Present days application layer attacks have almost utilized Botnets. A complete introduction of Botnets and tools made utilizing botnets

near to the central focuses and preventions are related with the survey [33]. A short study of the planning of Botnet near to tools used to dispatch DDoS flooding attacks is introduced in this part. Progress of a efficient and effective defense mechanism winds up being all the additional testing when attackers use zombies or Botnets.

A Botnet is formed by group of bots or zombies so as to manage by means of an attacker. The bots or zombies are called as the Agents and the attacker is also called as the Master of the Botnet. Alongside master and agents, there are controllers in the botnet through which the masters analyze by recommendation with their representatives to ask for and control the network. Figure 4 illustrates the elements of a Botnet during a DDoS attack.

Botnets are developed in different ways. Botnets can be categorized into three major categories like P2P, Web and IRC depends on how bots are restricted by the masters [34], [35].

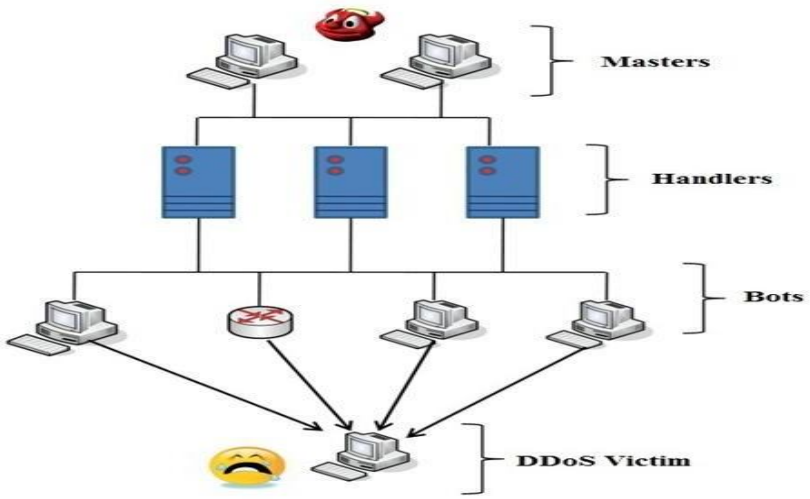

Figure 4: Botnet based DDoS Attack

a. IRC-based Botnets

Internet pass on Chat is a instant online messaging protocol dependent on text. It has customer server design and can interface innumerable customers through different expert servers. Attackers can utilize authentic IRC ports by manhandling IRC channels as controllers to send commands to the bots. For the explanation that IRC servers consistently have huge volume of traffic, an attacker can easily cover his quality and pass on the harmful code through file sharing.

Instead of retaining up the list regionally at their site, attackers can take a look at the rundown of every open bot, by checking into the IRC server. Centralized command and control (C&C) structure restraints the IRC based Botnets and their basic drawbacks is that, servers are the essential issues of dissatisfaction.

b. Web-based Botnets

To launch commands to the bots, Botnets have begun utilizing HTTP as a communication protocol and in this manner, it is commonly called HTTP based Botnets. Correspondence through HTTP makes the course towards following back to the command-and-control structure additionally testing. Not at all like IRC-based Botnets, has web-based Botnets don't keep up relationship with a command-and-control server and rather than that each web Bot downloads the principles which sometimes utilizes web demanded. Complex PHP scripts are utilized to organize and control web-based bots and for correspondence in addition, they use encryption over HTTPS (port 443) or HTTP (port 80) protocol. Web based Botnets are likewise stealthier than IRC based Botnets in nature since they can cover themselves inside legitimate HTTP traffic. Low-Orbit Ion Cannon (LOIC) 4, Dull Energy and Aldi are the three conspicuous and broadly utilized Web-based Botnet tools. The hazardous tool can destroy the attacked hosts, at whatever point needed by affecting the conventionality of all the information on the hard drive.

3. Detection, Defensive and Mitigation of DDoS Attack

a). DefenseArchitectures of DDoS

Accurately when a DDoS attack is seen, there is nothing that ought to be conceivable except for to really fix the issue and separate the victim system from the network. DDoS attacks change a lot of resources, for example,

CPU power, data transmission, memory, processing time, and so on, in ways that lead to zero in on the objective system. The fundamental objective of any DDoS attacks divide is to perceive DDoS attacks as right on time as could be viewed as regular and stop them as near their sources as could really be viewed as ordinary. DDoS protection plans are amassed into four classes subject to the improvement district: source endpoint, victim endpoint, key endpoint or intermediate router, and distributed or hybrid defense techniques. These trades off approaches are appeared in Table 1.

i. Defense mechanism for source end

Source protection mechanisms are passed on to the attack source to prevent DDoS attacks from network clients. Thus, the original plans perceive malicious packets in one-time active filter as well as traffic or traffic rate-limit. Executing and Detecting a DDoS attack by the resource is the good defense because legitimate traffic does less damage.

ii. Defense mechanism for victim end

The ultimate victim defense mechanism and victim detection systems or filter malicious traffic that pushes free throughput to the victim's network router such as networks that provide web services. The visibility and transfer online attack could be a real audience online and not through the intervention of an abusive anomaly, according to an intrusion detection. But the impulse seems to be a victim of traffic, they can be lowered, that they cannot deny that the speed of the service of the altar, and on the saturation species.

iii. Defense mechanism of Core-end or Intermediate router

In a relationship with main or brief protection, any switch/router on the network can naturally attempt to see malicious traffic and channel or cutoff its rate. It moreover balances the tradeoff between identifying evidence precision and the use of attack data transmission. Recognizing evidence and tracing the sources of an attack is ultimately critical due to adaptability. For this purpose, behind the protection, traffic equals that both the attack and the actual packets are detected on the switch, and this is a stimulating place away from all traffic.

iv. Hybrid Defense architecture or Distributed-end

Detecting and mitigating end-of-flow attacks might be the good approach for DDoS attacks. The cross-defense mechanism is transmitted (or parts of it are appropriate) in different domains, for example, in the interaction networks of origin, victim or general, and all this is seen as a joint effort of sending points. The medium is ideal outside of what many might consider a high volume of traffic;however, the victim side can see the attacking traffic in its entirety in a group of legitimate and attacking packets. Therefore, extending detection and mitigation approaches to various ends of the network could be furthervaluable.

b) Detection and Mitigation Strategies of DDoS

In this part, we provide an overview to detect and prevent DDoS attacks of the existing methods. These strategies build scheduled the patterns discussed above to express the origin, end, sacrifice, heart, and hybrid approaches on the web. We describe a methodology to detect DDoS attacks in four main modules, as shown in Figure 4.

i. Statistical Methods

The authentic properties of standard/standard and attack models can be cracked to detect DDoS attacks. Regularly, a quantifiable model is made plans to work with normal traffic, and after some time an evident interpreting test is applied to pick whether a substitute traffic or stream profile is fitting for that model. Occasions that don't adapt to the scholarly model, thinking about the inevitable results of applied assessments, traffic or streams, are classified as anomalies.

[26] Design a Distributed change point detection (DCP) project utilizing change aggregation trees (CAT). The affiliation traffic when the change was clarified utilizing the non-parametric CUSUM approach. The joined deviation is more basic than the trivial improvement when a DDoS flood begins, and a CAT structure is depended upon to see unforeseen changes in the amazing time gridlock streams working at the exchanging layer. The traffic change plans were recognized on the space worker utilizing attack dispatches to make CATs that recommend the attack stream plan.

D-WARD [27] believes a to be as the subject of an unexpected gander at bidirectional traffic streams between the network and the Internet and is reliant on a proportion of the intruded-on deviation with standard stream plans. Odd streams are destitute upon obstacles subject to their rehash of event. D-WARD offers a wonderful region rate that is close for the most part lessening DDoS traffic. It utilizes a predefined plan for standard traffic and sees deviations from the norm in two-manner traffic subject to deviation data. At last, the D-WARD checks the traffic

to check whether the assault is affirmed or dropped. Whenever ensured, D-WARD will keep on testing past what many would envision. Regardless, at any destroyed second, it truly permits a speed up.

[28] Proposes a distributed algorithm discovery approach that controls a sensible weight limit on upstream switches. The smothering is sensibly weighted, taking into account how the ordinary expert traffic is controlled (expanded or diminished) utilizing partitions that disregard changes dependent no nonsense of related customers, plainly or wrongly to the switches. Near the beginning of the check, it isn't suggested that changes be made far enough to defend the worker from any amazing right off the bat assault. You surely know the unessential or ordinary credits toward the beginning of the figuring, and the speed is restored (expanded or diminished), since the master information sent by your optional switches at last incited the rushed utilization, all things being equal, in the going with periods of the assessment with a look at standing out from the whole stack of the worker outside of numerous' assessment on a potential space.

[29] Describe another approach to manage oversee transmission capacity disclosure and insight assaults by seeing the progression of new source IP addresses. The affirmation framework depends upon a CUSUM ensured non-parametric change zone plan. In this [30], we propose a FFV (IP Flow Characteristic Value) calculation that mistreats the fundamental attributes of DDoS attack, for example, stream imbalance, unexpected traffic changes, inevitable source and target IP addresses. The ARMA request model is acquainted with the mysterious network stream utilizing the quick guess methodology. A DDoS detection plan is then utilized detection procedures and a linear prediction model (DDAP).

In [31], he defines a statistical segregation method (SSM), through an awesome stream at dull reaches, separates the models and the attack state and sorts them as indicated by very far. attack streams are isolated from authentic streams utilizing identical assessment.

In [32], an overall DoS affirmation strategy dependent on most likelihood rules with random neural networks (RNN) was introduced. This framework essentially picks a great deal of traffic limits in a substitute way to oversee reason PDF checks and measure probabilities. Measure the qualities of the advancing toward traffic and attempt to settle on a choice on the entirety of the credits to appear at an objective. At last, the general outcome is gotten utilizing both brief and common RNN structures. A short depiction of these systems is introduced in Table 1.

In [33], suppliers present a lightweight passage program called LOT to cover network traffic from IP hating attacks and flooding attacks. It is shipped off the fitting areas of the networks. Two areas utilizing a LOT can consider one another and join each other to pass on. The show permits the doorway to drop scrutinized IP apportions highlight source addresses in another zone and the converse route around, and the match can be shielded from DDoS attacks. Utilizing archives for each stream to show stream packs from various affiliations helps DDoS attacks. Bundle goes past passing obstacles from social execution gatherings to target channel groups, and it moreover agrees to channel rules mentioned by the objective entryway.

In [34], the authors endeavor to see DDoS attacks with updated time objectives utilizing non-asymptotic fluffy assessments. The assessor is sent in the mean bundle get time. The issue is restricted to two spaces; one is the genuine DDoS detection and the other is the indisputable affirmation of the victim's IP address. The hidden segment is overhauled by utilizing boundlessness and silly cutoff centers to perceive DDoS attacks. The following part, expressly the particular check of the difficulty's IP addresses, is refined for commonly inconspicuous purposes. The goal is to decipher the victim's IP addresses in a positive manner for dispatching adversary applications, including obstruction or end, utilizing the appearance time of the bundles as a fundamental evaluation of the target.

The theoretical betting thinking is preceded in [35] to ensure against DoS/DDoS progressed attacks. A DDoS attack happens as a solitary, non-steady issue. To complete an attack, various qualities are investigated, like the expense of making noxious traffic and the measure of attackers. It is believing it or not displayed that the protector has an outstanding ideal security procedure that sets most limit cutoff centers for attack works out, dependent upon standard or dumb attackers. Table 2 gives a theoretical of pieces of statistical based DDoS detection methods.

ii. Methods based on soft computing

Ideal learning models like artificial neural networks (RNAs), deceptive illustrative constraints, and genetic algorithms are consistently used to detect DDoS attacks because of their intelligent and automatic coordination capabilities. Soft computing is a strategy for depicting a set of processing and optimization frameworks that are liberal with respect to imprecision and uncertainty.

Artificial neural networks (RNAs) are routinely utilized learning models that can adjust to the necessities of a

changing environment [36]. These ANNs are self-learning and self-organizing together models with limits like parallelism, reliability, and fault tolerance. ANNs are unimaginable for social event and managing dull issues in a framework because of their self-learning characteristics.

In [37], the authors utilized the ANN linear vector quantization (LVQ) model. It is fundamentally relative masterminded depictions and applies strategies like support, tiring, and data compression. In supervised learning, you comprehend the objective outcome basically indistinguishable from various kinds of various entry plans. In the wake of testing the arrangement with the LVQ model, the authors utilize a comparable ANN back propagation model (BP) edifying collection for the sensible assessment. Contemplating the inevitable results of the relationship, they guarantee that LVQ is more cautious than BP in detecting DDoS attacks. They show that the LVQ is 99.72% correct for a standard data set compared to the expert data set, while the conventional precision of blood pressure is 89.92% for an essentially indistinguishable data set. Precision is evaluateddependent upon the level of false positives and false negatives got for each review data submission. There are 10 models that are utilized to test the edges of all LVQ and BP models.

In [38], the authors use a BP neural network with traffic entropy of different kinds of datasets as information sources and DDoS attack powers as outputs. For training, 20 remarkable models are utilized against the dataset, with an attack speed of 10 Mbps as the least and 100 Mbps as the best in the dataset. Entropy changes are settled ward with the arrangement that attack traffic on the network isn't actually identical to normal traffic. The model was tested with safe responsibilities of four self-confidently picked combinationsof entropy and force values of 20, 50, 70 and 95 Mbps. The output of BP's neural networks is gotten with moderately couple of errors. There are essentially less falsepositives and false negatives, likewise, the arrangement is tested with various network sizes, and that is, the measure of neurons in the relationship of the layer, at any rate in genuine cases, the improvement of the network size is further developing. Boththe preparation time and the cost of use.

In [39], the authors propose that a time-delayed neural network (TDNN) receives a DDoS plan. TDNN is a neural network wherein the delay factor is covered up in an extraordinary signal. The authors made a demilitarized zone (DMZ) and TDNN ended up on a two-level course of action. The advancement of node is checked by neighboring nodes and data on attacks is sent to the expert module for analysis. The layered arrangement permits the development to make a sensible move as a proactive framework against DDoS attacks. The detection results of the integrated system show that the proposed plan can accomplish the correct detection speed of 82.7% when bound from 46.3% utilizing the General Intrusion Detection System (IDS).

[40] The execution of SPUNNID as a DDoS detection structure depends upon a statistical preprocessor and a unsupervised artificial neural network. It utilizes statistical preprocessing with to remove traffic functionality and utilizations an unsupervised neural network to review and classify traffic as standard or attack traffic. [41] propose a penetrate based DDoS detection method utilizing Radial Basis Function (RBF) neural networks dependent on the qualities of a packetattack study. It is utilized to sort information as regular or by attack class. In the event that the pushing toward traffic is viewed as attack traffic, the primary IP address of the attack packs is shipped off the Filter area and further move is made in the Attack Alert part. Something other than what's expected, if the traffic is moderate, it goes to the target.

[42] To give a method to detect DDoS attacks in open networks dependent on the genuine attributes expected in a short-term window study.

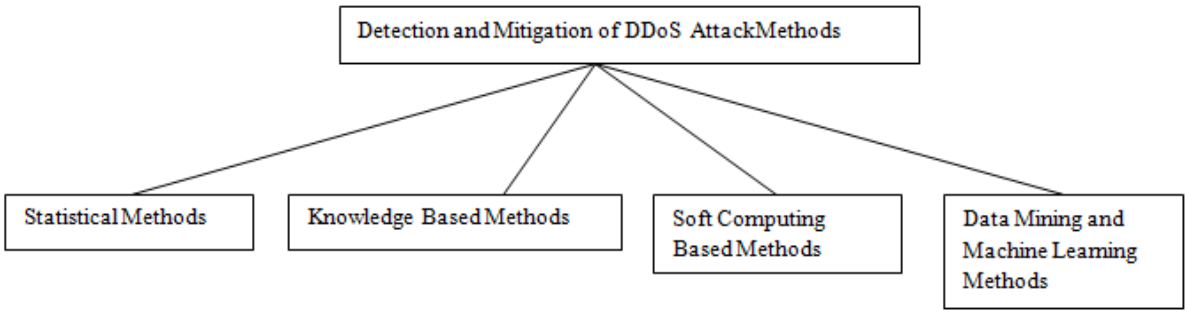

Figure 5: Detection and Mitigation Methods of DDoS Attacks

Defense Methods	**Advantages**	**Disadvantages**
Defense Architecture (Source-end)	• Source-side DDoS detection and prevention provides the best possible protection while minimizing validtransfer. • The least amount of traffic to be tested on the source side, for which the detection and mitigation mechanism requires fewer resources.	• Detection of DDoS attacks on the source side is difficult because sources are extensively spread crosswise the network and one source acting like standard traffic. • Complexity of source-side circuit assignment.
Defense Architecture (Victim-end)	• Detection of DDoS attacks on victim routers is moderatelysimple due to high source usage. • This is the best practical defense method because web servers that provide malicious services constantlyattempt to protect their resources from legal users.	• In DDoS attacks, the victim's resources, such as bandwidth network, are frequently overloaded and these approaches cannot prevent traffic from passing through the victim's routers. • Detect an attack justfollowing it has reached the victim, and there is no point in detecting an attack when valid customers have previously been rejected.
Defense Architecture (Core-end)	• Locating and tracing attack sources with this method is very easy through mutual operation. • Traffic is aggregated, which means that valid packets and attacks arrive at the router together, which is the best place to throttle all traffic.	• The biggest challenge with this method is the expense. • For maximum discovery accuracy, all Internet routers should use this discovery method, as being unavailable on a router could interfere with the discovery and spy method. • A fully usable implementation is very difficult because it requires reconfiguring every router on the Internet.
Defense architecture (Hybrid or Distributed-end)	• Discovery can be made on the victim side and the reply could be routed and circulated to further nodes with the victim. • The sharing of detection and mitigation techniques at different close of the network may be more favorable.	• Tough support between points of consumption is essential. • Complexity and transparency due to support and declaration among distributed mechanisms prevalent on the Internet.

Table 1:Evaluation of DDoS attack with Defense architectures

[43] Provides DDoS attack detection utilizing decision trees and relational grayscale analysis. Testing an attack from a run of the typical state is depicted as a classification issue. They utilize 15 credits to check the speed of incoming /outgoing packets/bytes what's more collect the rates from the TCP, SYN and ACK flags to depict the traffic stream plan. The decision tree is utilized to make a classifier to detect unusual traffic streams what's more uses another traffic plan coordination system to treat the traffic stream as an attackstream and follow the source of the attack.

In [44], the authors propose a great deal of classifiers that utilization the Resilient Back Propagation (RBP) neural network as an associate classifier for detecting DDoS attacks. They generally rotate around the progress of the base classifier adjustment. RBPBoost joins the outcome of the classifier's outcome dataset and Neumann Pearson's cost minimization technique [45] to make the final classification outcomes. Table 3 outfits a format of soft computing with the strategies introduced in this part. Table 3 is an outline of the soft computing techniques introduced in this part.

References	Objective	Deployment	Mode of Working	Remarks
Mirkoviacet.al [27]	Prevention of Attack	Source end	Centralized	Numerical traffic shaping is utilized to detect DDoS attacks and prevent detected traffic attack on the source side.
Akella.et al. [46]	Detection of Attack	Sourceend and victim end	Distributed	The report be based on standard traffic and detects traffic anomalies by sampling the flow. This method is commonly used on network routers.
Peng.et al. [29]	Detection of attacks bandwidth	Victim end	Centralized	Thenon-parametricmodify detection method is therefore utilized to recover the detection precision and is used on the victim's side.
Chen.et al. [26]	Detection of Attack and Trace back	amongnetworks of source and destination	Distributed	It is utilized to detect and outline the origin of an attack using a hybrid process.
Oke and Loukas [32]	Detection of Attack	Victim end	Centralized	Defines a set of precise attack input capabilities that capture long-term statistical properties and traffic activity during detection.
Saifullah[28]	Prevention of Attack	among networks of source and destination	Distributed	That Prevention technique protects Internet servers and routers from DDoS attacks by distributing the load fairly. Regulation of upstream routers.
Chen [30]	Detection of Attack	Victim end	Centralized	Detect DDoS attacks with two t-tests that combine incoming SYN statistics.
Zhang.et al. [47]	Detection of Attack	Victim end	Centralized	It utilizes a built-in Automatic Regression Method (ARIMA) to defend servers from DDoS attacks.
Cheng.etal. [30]	Detection of Attack	Victim end	Centralized	The actions of the four characteristics of the flow: flow irregularity, increased traffic volume, destination IP address, source IP address allocated during DDoS detection.
UdhayanandHamsapriya[31]	Falsealarm reduction	Victim end	Centralized	The statistical partitioning technique is utilized to detect DDoS attacks depends on a traffic flow incident during a later time interval.

Table 2: DDoS detection based on statistics reference

Reference	Objective	Deployment	Mode of Working	Remarks
Jalili.et al[40]	Detection of Attack	Victim end	Centralized	To detect DDoS attacks, we used classification methods for uncontrolled neural networks and a statistical preprocessor.
Gavrilis&Dermatas [42]	Detection of Attack	Victim end	Centralized	DDoS attack Detection using arithmetical functions expected at small intervals in aopen network with the neural networkof a radial basis function.
Nguyen and Choi [48]	Detection of Attack	Intermediate network	Centralized	According to the adjacent neighbor method, to detect only known attacks by using K-means.
Wu et al. [43]	Detection of Attack andtraceback	Victim end	Distributed	Using decision trees return to the attacker's location based on the appropriate traffic flow model.

Table 3: DDoS Detection methods based on soft computing

iii. Methods of Knowledge based

In data-driven strategies, network events or exercises are performed against predetermined attacking rules or techniques. In them, common images of well-known attacks are called attack signs are designed to recognize real-life attacks. Data-driven strategies combine expert systems, signature learning, map self-assembly, and state change assessment.

[49] present a heuristic information structure called MULTOPS (Layered Packet Statistics Tree) that monitors network device traffic credits as changes to detect and mitigate DDoS attacks. MULTOPS is a hub tree that aggregates traffic rate estimates for subnet prefixes at different full levels as the tree grows and weight occurs within a predefined memory size. The MULTOP network device detects bandwidth attacks

[49] Present a heuristic information structure called MULTOPS (Layered Packet Statistics Tree) that screens network contraption traffic credits as changes to detect and mitigate DDoS attacks. MULTOPS is a middle tree that sums traffic rate checks for subnet prefixes at different full levels as the tree makes and weight occurs inside a predefined memory size. The MULTOP network device detects bandwidth attacks when there are significant opportunities between the inbound and outbound traffic speeds of the victim or attacker. The network monitors or switches, organized by MULTOPS, may not recognize the bandwidth attack defined by the attackers who randomize the source addresses of the IP attack in malicious packets. Furthermore, it cannot detect attacks that send out countless streams of attacks to blow up the victim.

[50] Offers a useful way of thinking about a general DDoS protection mechanism called Net Bouncer. This appears to be a valid and unacceptable utilize of resources with ensures that they are only obtainable for proper utilize. Open the transfer to a stream with a relevant, but irrelevant legitimate user profile, and if any packets are received from an invalid source, the Net Bouncer appliance, welcome, understand how to run various validation results to validate the user for to confirm your credibility. If the customer has indicated their subscription, it is included to the validity record and the customer's packages are acknowledged.

[51] Provide a logical framework for organizing DDoS attacks utilizing an extended attack tree (AAT) and a broad attackdetection algorithm dependent on AAT. It obviously gets the particular direct events accomplished by the DDoS attack and the relating state changes dependent on the perspective on the transmission of network traffic to the major victim's server. Concerning the conventional attack tree (CAT) showing the cycle, the AAT is given above considering the way that it gives extra data, for example, the state progress framework. This overcomes the constraints of the CAT process.

[52] Detects DDoS subscription by identifying the TCP / IP packet header based on a predefined set of laws and circumstances and distinguishing between regular and irregular traffic. They primarily consider on TCP, UDP, and ICMP flood attacks.

[53] Introduction of a dissipated process to ensure against Internet DDoS attacks. For the independent detection of DDoS attacks in the network, defense methods other than conventional IDS are executed; this technique detects and prevents DDoS attacks in the intermediate network. These independent unmistakable detection nodes focus utilize the IRC message to replace data about network attacks and offer that data for absolute network attacks. Specific protect nodes focuses acquire expected data about wide network attacks and prevent attacks considerably more effectively and conclusively using aggregated network data. The above approach depends after inspecting the amount of traffic got by the individual being victim and they are irrelevant for a single DDoS attack from a multitude of outbreaks.

[54] Describes a perimeter-based DDoS defense method that analyzes traffic on the edge switches/routers of an Internet Service Provider (ISP) network. The DDoS defense technique contains two fundamental processes: (1) feature suppression depends on temporal correlation and (2) detection based on spatial correlation. It reasonably detects a DDoS attacks without changing the IP sending partitions open on the switches. An outline of these knowledge-based methods is introduced in Table 4.

iv. Methods of Machine learning and Data mining

In [55], the authors developed an efficient defense method known as Net Shield to ensure that clients, network switches, and ultimately network servers become victims, zombies, and controllers of DDoS flood attacks. Provides several open networks with an Internet bound IP address configuration and exploits prevention and speed limiting to trigger infrastructure weaknesses in tracking machines. It adopts dynamic security approaches to protect network resources from DDoS flood attacks.

[56] Introduces the DDoS container as a completestructure for detecting DDoS attacks. It utilizes a network discovery procedure to protect the most multifaceted and important types of DDoS attacks, and it also mechanism

to identify faults and consistently manage the flow of traffic. It describes stateful traffic flow assessment and analyzes practices of changed groups by continuously checking for DDoS attacks and genuine / legitimate applications. Kill session instances upon detection of DDoS attacks.

[57] Propose a practical technique for detecting DDoS attacks by mishandling a mechanism that contains the recognition of administrators and malicious agents, compromises and attackers. Perform pack review. The authors introduced the outcomes utilizing the DARPA dataset, where every time of the attack state is crippled and can detect the initiators of the DDoS attack, also as the genuine attack.

[58] Explore the proposed space for intranet DDoS attacks and come up with a dedicated, multi-step approach that offers measurable and precision. They organized and developed LADS (Large Scale Automated DDoS Attack Detection System), this uses information quickly exposed to the ISP.

[59] Examination of joint entropy estimation to detect DDoS attacks using different traffic distributions. The timing of the number of IP flows and the total size of the traffic depends on whether this attack event affects reliability and reasons a split in the timeline of the combined random values. Its resemblance to regular traffic.

In [60], two new data estimates are presented: (i) the complete entropy metric and (ii) the data distance metric for survey DDoS attacks with a low KK. The attack is detected dependent upon the distance between the genuine traffic and the attacking traffic. The full-scale entropy metric is more exact than the standard Shannon metric [61].

[62] Describes past detection of continuous DDoS attacks utilizing FireCol, which is hypothetical information. It is dispatched off the Internet Service Provider (ISP) layer as Intrusion Prevention System (IPS) encryption. IPS makes virtual security rings around has for security and exchange by transmitting basic necessity traffic information.

The mindset described in [63] assesses the qualities of DDoS and flash attacks and provides a suitable strategy for viewing them on VoIP networks. The authors adopted this method by magnification.

In [64], the authors proposed an approach to network anomaly detection based on wavelet changes and probability theory. It can be detected by known and unknown DDoS attacks.

[65] Development of a DDoS detection strategy that concentrates network traffic and network traffic protocol class models and shows a limit a helper for the detection model. A K-Means clustering algorithm is utilized to make the essential intrude with values for network traffic the attributes forgot network traffic. A packet protocol state model is assembled utilizing Apriori [66] and FCM [67] to get packets. It is the place where the current network traffic beats the cutoff respects that the protocol condition of the network packets is determined to see unusual packets. In the event that there are no custom packages; another cutoff respect model subject to the current network is compiled utilizing the k-means an area.

In [68], a two-step robotic framework is proposed to detect DoS attacks on network traffic. This is a combination of the standard procedure for detecting a switching point with wavelet changes [69]. In [70], Lee and Lee present an efficient wavelet-based framework for testing DDoS recognition. DDoS transfer is detected by force scattering depends on the wavelet score. The force challenge will continue to accumulate in the long term if the traffic continues to change its long-term advantage.

[71] Use ANN to see the measure of zombies in a DDoS attack. The data from the test is utilized to design a forward neural network worked with the NS-2 Network Simulator. The assessed furthest reaches of the prepared network is acceptable and permits calculating the size of the zombie according to a DDoS attack with a test fault.

[72] Proposed an IP Address Interaction Function (IAI) algorithm that takes into account unexpected traffic changes, the relationship between addresses, the disproportionate many-to-one relationship between addresses, the source of transmission and destination addresses. The IAI algorithm wants to represent the key qualities of the states of a network flow. To collect current network flow status and display DDoS attacks, a Support Vector Machine (SVM) classifier is applied, based on IAI's time course of action with standard flow and attack flow. It has a higher detection rate and a lower false alarm rate, which manifests itself in different ways depending on the strategies of the competitors.

The methodology illustrated in [73] predicts progressive flood attacks and also estimates the strength of attackers subject to open to deduction. This cycle joins two phases: (i) valid evaluation of network traffic. Improvement history and (ii) conspicuous confirmation and evaluation of the strength of the DDoS attack dependent on the intellectual method of fuzzy reasoning.

[74] Establish a method that is Congestion Participation Ratio (CPR) methodology used for network traffic of the flow-level to enable low-frequency DDoS (LDDoS) attacks. A higher CPR compliance flow encourages

LDDoS and packet dropping. Identify high detection accuracy with DDoS attacks using a separation of duties ratio.

In [75], the authors described a way to combat Botnet surveillance and drills depend on behavior traffic analysis.Approachesof Machine learning are used to describe traffic behavior and have shown that botnet exercises are likely to be recognized in more modest high accuracywith time windows.

In [76], low-speed DDoS attacks are detected utilizing an anomaly-based approach. In low-speed DDoS attack moves close; Attackers send harmful traffic at the most insignificant bit rate to mislead standard anomaly-based DDoS detection structures. The authors proposed two information metrics, extra entropy metric and a data distance metric. These metrics are utilized to quantify the contrast between real traffic and attacktraffic to detect DDoS attacks.

In [77], author proposed a numerical model is that shows the advantages of protecting against DDoS attacks, depending on the drop in traffic attack. The authors utilized a self-contained protection mechanism dependent on the Cognitive Packet Network (CPN) protocol to track the return streams that regularly arrive at the node. A review of these methods in this group is presented in Table 5.

Reference	**Objective**	**Deployment**	**Mode of working**	**Remarks**
Gil and Po- Letto [49]	Prevention of Attack	network among source and destination	Centralized	Each machine in the association maintains a MULTOPS data development to recognize attacks that set up a huge number of DDoS attack streams using endless trained professionals and personifying attacks.
Thomas et al. [50]	detection of Attack	Victim end	Centralized	Net Bouncer uses sequential packet distribution to distinguish flash based from DDoS traffic on multiple processors network. The technology.
Limwiwatkul&Rung-Sawang[52]	detection of Attack	Victim end	Distributed	Attack signature plans are made using TCP group headers to detect DDoS attacks.
Zhang and Parashar [53]	practical	network of Intermediate	Distributed	The voice-based plan leverages generic DDoS intelligence in the distribution of information to detect attacks.
Lu et al. [54]	detection of Attack	boundary router	Distributed	Use the spatial and transient association of DDoS traffic to perceive the packaging of encroachment.
Wang.et.al [51]	detection of Attack	Victim end	Centralized	The Extended model of Attack Tree is used to detect DDoS attacks.

Table 4: Knowledge based Detection methods of DDoS

Reference	**Objective**	**Deployment**	**Mode of Working**	**Remarks**
Hwang et. al [55]	Attack Prevention	Victim end	Centralized	Protects clients, routers and servers on your network against DDoS attacks by detecting protocol anomalies.
Li and Lee [70]	Attack detection	Victim end	Centralized	A defined power allocation wavelet analysis method to detect DDoS traffic.
Sekar.et.al [58]	Attack detection	Source end	Distributed	A multi-step approach is described and enabled to achieve flexibility and precision in DDoS attack detection.
Gelenbe and Loukas [77]	defense DDoS	Victim end	Centralized	Detect the attack mechanically. monitoring of return flows
Lee et al. [57]	Attack detection	Source end	Centralized	The Agent Manager architecture with Cluster Analytics is used to proactively detect DDoS attacks.

Rahmanial et [59]	Attack detection	Victim end	Distributed	Collaborative entropy analysis used for several traffic distributions to detect DDoS attacks.
Li and Li [64]	Attack detection	Victim end	Centralized	Wavelet transformation and probability assumption are used to detect DDoS attacks.
Dainottial et [68]	Detection of DoS attack anomalies	Victim end	Centralized	Totally detect attacks by joining standard weather point revelation and tireless wavelet change.
Zhong and Yue [65]	Attack detection	Victim end	Centralized	Anonymous DDoS attacks are detected using fuzzy clustering c-means and Apriori methods.
Xia et al. [73]	Detects floodattack and itsstrength	Victim end	Centralized	Detection of DDoS flood attacks used by fuzzy logic.
Xiang al et [60]	Detects low-ratefloodingattacks	Victim end	Centralized	New logical metrics used to detect low frequency DDoS flood attacks.
Gupta al. et [71]	Number ofzombies classification	Victim end	Distributed	To compute the number of zombies in a DDoS attack used by ANN.
Francois et al.[62]	Flooding DDoSattackdetection	Source end	Distributed	One of the methods for detecting DDoS flood attacks supports incremental deployment on a real network.

Table 5: Machine learning and Data mining-based DDoS Detection methods

Evolution and Analysis of Various Traceback Methods

In this part, evaluation of various traceback methods is finished on the sources of metrics described in earlier sector and shown in the Table 1 and Table 2. Every scheme is evaluated with the new classification of traceback methods such as Packet logging input debugging, DPM, link testing, PPM, ICMP trackback, reposition and Entropy difference. Its Advantages and Drawbacks has been shown in the Table 7.

Category	**Link Testing**	**Control Flooding**	**ICMP Traceback**	**Packet Logging**
ISP involvement	High	None	Low	Moderate
Range of attack packets wanted for traceback	N-A	Huge	Very large	1
Processing overhead	Low	None	Low	Low
Storage requirement	Low	Low	Low	Fair
Ease of implementation	Yes	Yes	Yes	Yes
Scalability	High	N-A	High	Fair
Bandwidth overhead	High	Huge	Low	None
Number of functions had to enforce the scheme	None	1	2	3
Ability to address most important DDOS attack	Yes	No (only DDoS attack)	Yes	Yes
Classification	IDS based	IDS based	Proactive	IDS assisted

Table 6: Evaluation of Traceback Methods

Category	**Traceback using IP-Sec**	**PPM**	**Pushback**	**Traceback using Entropy variation**
ISP involvement	High	None	No	No
Range of attack packets wanted for traceback	Fair	Very large	Large	Very large

Processing overhead	High	Low	High	High
Storage requirement	No	High	N-A	Fair
Ease of implementation	Yes	No	Yes	No
Scalability	Poor	High	High	Highest
Bandwidth overhead	High	None	Very Low	High
Number of functions had to enforce the scheme	None	2	2	2
Ability to address most important DDOS attack	No	Poor	Yes	Yes
Classification	IDS assisted	Proactive	Proactive	Proactive

Table 7: Evaluation of Traceback Methods

S.NO	Traceback Methods	Benefits	Drawbacks
1.	Input debugging/ Controlled Flooding with Link Testing [3][14][21][22]	✓ Suitable with accessibleprotocols ✓ It accepts the incremental execution ✓ Convenient to available routers and network communications ✓ Examination of post packetstudy is allowed ✓ ISP assistance isn't alwaysessential.	✓ This approach is utilized for DOS Attacks no longer for DDOSAttacks ✓ This method isn't always feasible for broad operation. ✓ It can't sketch the attack when it's far ended i.e., attack should wait dynamic til the trace back is concluded. ✓ Bandwidth slide could be very high whilst tracing the attacksource. ✓ It obtains regenerated plan of the internet topology.
2.	Traceback for ICMP [12]	✓ Suitable with accessibleprotocols ✓ This helps the incremental execution. ✓ Permits previous packetstudy ✓ Not required ISP support ✓ Suitable with network infrastructure and existing routers	✓ It produces additional networktraffic by the Bandwidth overhead. ✓ Low defensive as there may be noencryption approach carried out with key allocation.
3.	Detection method DPM/PPM [4][6][7]	✓ This is simply toexecute ✓ This has no bandwidth overhead and less processing ✓ It is suitable for a collection of attacks not now(D) DoS ✓ It doesn't have the absolute security defects. ✓ It can't tell internal topologies of the ISPs ✓ This ismeasurable	✓ Some packets will leave the switch without being isolated, since each switch marks disperses ✓ This is also costly to execute this method on behalf of memory overhead ✓ However, this speculation that isn't huge when attack is amazingly appropriated for instance in reflector attacks. One crucial thought for PPM to work is that DOS attack traffic could have more noteworthy volume than general standard traffic.

4.	Hash based Logging Scheme [8]	✓ Suitable with presentedrules ✓ maintain for incrementalexecution ✓ Permits previous packetstudy ✓ irrelevant network trafficis suspended ✓ Suitable with network infrastructure and existing routers	✓ Storagerequirements and Resource motivation in terms of processing ✓ Allocation of classification information between various ISPs leads to legal issues and logistic ✓ Low appropriate for DDoS attacks
5.	IP-Sec Using IP Traceback [16]	✓ Suitable with accessibleprotocol ✓ Permits previous packetstudy ✓ It is secured highly	✓ ISP connection is necessary ✓ Low measurable
6.	Pushback [9][10]	✓ This is simple toexecute ✓ It makes use of collective based congestion control algorithm which has been formerly carried out. ✓ Appropriate with network communications and current routers.	✓ Precisely whilst a switch taking a reposition signal, it is going to check and control the aggregate showing up rate from the various associations and discover the relations which provides to the plug up. Anyhow, this technique is not suitable if the traffic attack is dependably spread throughout the inbound relations. ✓ Due to the fact that arriving aggregate rate is comparative in every link, switch can't see the virulent traffic and basic traffic which prompts the problem of fake negative and fake positive in this regard.
7.	Traceback with Disorder form [11]	✓ It executes functions which can be far-flung of intruders to perform IPtraceback. ✓ This scheme ismeasurable ✓ It will not sicken from the packet pollution wrangle ✓ The router level isn't always atrouble at Storage space requirement ✓ This scheme can process as a free software program module with the current routing software which performs satisfactoryexecution.	✓ The separation of DDOS Attacks and flash crowds are not taken into account in this method, it would see flash crowd as DDOS Attack engaging false positive

Table 8: Benefits and drawbacks of various Traceback Methods

4. Conclusion

In this survey paper, we provided various classification methods for the division of various DDoS attacks and defensive architectures of DDoS like a source end, the victim end, the base end and the end is distributed. We have presented different methods for detecting and mitigating DDoS attacks, such as knowledge-based methods, arithmetical methods, methods based on soft computing, methods of data mining and machine learning, alongside with its advantages and disadvantages based on when and where they are detected in response to DDoS attacks. lastly, we provided an evaluation of various DDoS traceback methods such as correlation testing, flood control, ICMP traceback, packet recording, PPM, reverse tracking, and universe tracking. It is practically complex to create and execute DDoS detection and defense. Therefore, in actual networks, we will not meet all requirements until DDoS discovery is not performed, and to complete this type of network it is necessary to balance the different performance parameters with each other in a smooth and adequate manner.

References

1. D. Anstee, C. F. Chui, P. Bowen, and G. Sockrider, Worldwide Infrastructure Security Report, Arbor Networks Inc., Westford, MA, USA, 2017.

2. S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," IEEE Communications Surveys and Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.
3. Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, "Understanding internet DDoS mitigation from academic and industrial perspectives," IEEE Access, vol. 6, pp. 66641–66648, 2018.
4. Hoque, N.; Bhattacharyya, D.; Kalita, J.: Botnet in DDoS attacks: trends and challenges. IEEE Commun. Surv. Tutor. 99, 1–1 (2015).
5. P. J. Criscuolo, "Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319,", Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.
6. Todd B., "Distributed Denial of Service Attacks," Feb. 18, 2000, [online] http://www.linuxsecurity. com/resource files/intrusion detection/ ddos–whitepaper.html.
7. J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communications Review, vol.34, no. 2, pp. 39-53, April 2004.
8. Ranjan. S, Swaminathan. R, Uysal. M, and Knightly.E, "DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection", IEEE INFOCOM'06, 2006.
9. Chang R. K. C., "Defending against flooding-based distributed denial of service attacks: A tutorial,", Computer Journal. IEEE Communication Magazine,Vol. 40, no. 10, pp. 42-51, 2002.
10. Puri. R, "Bots and Botnet – an overview,", Aug. 08, 2003, [online] http://www.giac.org/practical/GSEC/ RamneekPuriGSEC.eps
11. CERT, "Denial of Service Attacks," June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html
12. Liu. J, Xiao. Y, Ghaboosi. K, Deng. H, and J. Zhang, "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures,", EURASIP Journal. Wireless Communications and Networking, vol. 2009, Article ID 692654, 11 pages, 2009.
13. Rodríguez-Gómez RA, Maciá-Fernández G, García-Teodoro P (2013) Survey and taxonomy of Botnet research through life- cycle. ACM ComputSurv (CSUR) 45(4):45
14. V. Jean Shilpa, P. K. Jawahar (2019)" Advanced Optimization by Profiling of Acoustics Software Applications for Interoperability in HCF Systems", Journal of Green Engineering, Alpha publishers,9(3), pp.462-474.
15. P.Radha, B.MeenaPreethi,"Machine Learning Approaches For Disease Prediction From Radiology And Pathology Reports", Journal of Green Engineering, Alpha publishers,9(2),pp. 149-166
16. Higgins, K.J 2010, 'Researchers to Demonstrate New Attack That Exploits HTTP, [online] http://www.darkreading.com/vulnerability-management/167901026/security/attacks-reaches/228000532/index.html
17. A.Suresh Kumar, 2018, 'Obfuscating Software puzzle for Denial of Service attack mitigation', International Journal of Pure and Applied Mathematics.
18. M. Kowsigan and S. Priyadharshini, 2018, 'Security in Data & Dissemination of Distributed Data in Wireless Sensor Network', International Journal of Pure & Applied Mathematics, Volume 118.
19. Higgins, K.J 2010, 'Researchers to Demonstrate New Attack That Exploits HTTP, [online] http://www.darkreading.com/vulnerability-management/167901026/security/attacks-reaches/228000532/index.html
20. Shekyan, S 2012, 'Are you ready for slow reading?' Retrieved from https://community.qualys.com/blogs/security labs/2012/01/05/slow-read
21. Bhuvaneswari K., and Rauf H.A., 2009, 'Edgelet based human detection and tracking by combined segmentation and soft decision', International Conference on Control Automation, Communication and Energy Conservation, Issue 5204487.
22. Poornaselvan K.J., Gireesh Kumar T., and Vijayan V.P., 2008, 'Agent based ground flight control using type-2 fuzzy logic and hybrid ant colony optimization to a dynamic environment', Proceedings - 1st International Conference on Emerging Trends in Engineering and Technology, ICETET, Issue 4579922, PP: 343 - 348.
23. Hoque, N, Bhattacharyya D.K &Kalita, J.K 2015, 'Botnet in DDoS Attacks: Trends and Challenges', IEEE Communications Surveys & Tutorials, Vol. 17, no. 4, pp. 2242-2270.
24. Alomari, E, Manickam, S, Gupta, B.B, Karuppayah, S &Alfaris, R 2012, 'Botnet- based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art', International Journal of Computer Applications, Vol. 49, no. 7, pp. 24-32.
25. R.Kanmani and A. Jameer Basha, 2016, 'Performance analysis of wireless OCDMA system using OOC, PC and EPC codes', Asian Journal of Technology, Vol-15(12), PP: 2083-2089.

26. Y Chen, K. Hwang, and W. S. Ku, "Distributed change-point detection of DDoS attacks over multiple network domains.", Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems, Las Vegas, NV, 14-17 May, pp. 543–550. IEEE CS. (2006),
27. J. Mirkoviac, Prier, G., and Reiher, P. "Attacking DDoS at the source.", Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12-15 November, pp. 1092–1648. IEEE CS. (2002)
    A. M. Saifullah, ", Defending against distributed denial-of-service attacks with weight-fair router throttling." Technical Report 2009-7. Computer Science and Engineering, Washington University, St. Louis, USA. (2009)
28. T. Peng, C.Leckie, and RM Rao, K. "Detecting distributed denial of service attacks using source IP address" monitoring. Proceedings of the 3rd International IFIP-TC6 Networking Conference, Athens, Greece, 9-14 May, pp. 771–782. Springer- verlag. (2004)
29. J. Cheng, Yin, J., Wu, C., Zhang, and Li, Y. "DDoS attack detection method based on linear prediction model." Proceedings of the 5th international conference on Emerging intelligent computing technology and applications, Ulsan, South Korea, 16-19 September, pp. 1004–1013. Springer- Verlag. (2009)
30. J. Udhayan, and T. Hamsapriya, "Statistical segregation method to minimize the false detections during DDoS attacks." International Journal of Network Security, 13, pages 152–160. (2011)
31. G. Oke, G. and G. Loukas, G "A denial of service detector based on maximum likelihood detection and the random neural network." Computer. Journal., 50, 717–727. (2007)
32. Y. Gilad., and A. Herzberg, A., ''LOT: A defense against IP spoofing and flooding attacks,'' ACM Transaction on Information. Systems. Se, 15: (2012).
33. S. N. Shimeles,Katos, V., A. S Karakas, and Papadopoulos, B. K., ''Real time DDoS detection using fuzzy estimators,'' Computer. Security., 31: pages:782–790 (2012).
34. T. Spyridopoulos, G. Karanikas, T. Tryfonas, T., and Oikonomou, G., ''A game theoretic defence framework against DoS/ DDoS cyber-attacks,'' Computer Security., DOI: 10.1016/j.cose.2013. 03.014 (2013).
35. Y. Liu., B.Cukic, and Gururajan, S., ''Validating neural network-based online adaptive systems: A case study,'' Software Quality. Jounal., 15: pages- 309–326 (2007).
36. Liu, Y, Li, J. and Gu, L., "DDoS Attack Detection Based on Neural Network," Proceedings of IEEE 2nd International Symposium on Aware Computing (ISAC), 196–199 (2010).
37. P.K. Agarwal, B. Gupta, Jain, S., and M.K. Pattanshetti, "Estimating Strength of a DDoS Attack in Real Time Using ANN Based Scheme,", Communications in Computer and Information Science (Springer), 157: 301–310 (2011).
38. T. Chang-Lung, A.Y. Chang, and Ming Szu, H., "Early Warning System for DDoS Attacking Based on Multilayer Deployment of Time Delay Neural Network," Proceedings of IEEE 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pages- 704–707 (2010).
39. R. Jalili, F. Imani-Mehr, M. Amini, and Shahriari, H.R. (2005) "Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks." Proceedings of the International conference on information security practice and experience, Singapore, 11-14 April, pp. 192–203. Springer-verlag.
40. R. Karimazad, and A. Faraahi, A "An anomaly- based method for DDoS attacks detection using rbf neural networks." Proceedings of the International Conference on Network and Electronics Engineering, Singapore, pp. 44–48. IACSIT Press. (2011)
41. D. Gavrilis, and Dermatas, E "Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features." Computer Networks and ISDN Systems, 48, pages-235–245. (2005)
42. Y. C Wu, Tseng, H. R., Yang, W., and Jan, R. H "DoS detection and traceback with decision tree and grey relational analysis.", International Journal of Ad Hoc and Ubiquitous Computing, 7, 121–136. (2011)
43. P. Kumar, and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier." Computer Communication, 34, pages-1328– 1341. (2011)
44. C. Scott, and R.Nowak, A neyman-pearson approach to statistical learning." IEEE Transaction on Information Theory, 51, pages-3806–3819. (2005)"
    A. Akela,Bharambe, M. Reiter, M., and Seshan, S "Detecting DDoS attacks on ISP networks." Proceedings of the Workshop on Management and Processing of Data Streams, San Diego, CA, 8 June, pp. 1–2. ACM. (2003)
45. G. Zhang, S. Jiang., Wei, G., and Guan, Q. A prediction-based detection algorithm against distributed denial-of-service attacks.", Proceedings of the International Conference on Wireless Communications

and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germany, 21-24 June, pp. 106–110. ACM. (2009) “
46. H.Nguyen and Choi, Y “Proactive detection of DDoS attacks utilizing k-NN classifier in an Anti- DDoS framework.” International Journal of Electrical, Computer, and Systems Engineering, 4, 247–252. (2010)
47. T. M. Gil, and M. Poletto, “MULTOPS: a data- structure for bandwidth attack detection.” Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Berkeley, CA, USA, 13-17 August 3. USENIX Association Berkeley. (2001)
48. R. Thomas, B. Mark, T. Johnson, and J. Croall, “Net Bouncer: Client-legitimacy-based high-performance DDoS filtering”. Proceedings of the 3rd DARPA Information Survivability Conference and Exposition, Washington, DC, 22-24 April, pp. 111–113. IEEE CS, USA. (2003)
49. J. Wang, R. C. W. Phan, Whitley, J. N., and Parish, D. J.) “Augmented attack tree modelling of distributed denial of services and tree-based attack detection method.” Proceedings of the 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July, pp. 1009–1014. IEEE CS. (2010)
50. L. Limwiwatkul, and A. Rungsawang, A. Distributed denial of service detection using TCP/IP header and traffic measurement analysis.” Proceedings of the IEEE International Symposium Communications and Information Technology, Sapporo, Japan, 26-29 October, pp. 605–610. IEEE CS. (2004)”
51. G. Zhang, and Parashar, M. “Cooperative defence against DDoS attacks.” Journal of Research and Practice in Information Technology, 38, 1–14. (2006)
52. Wu, D., Lu, K., Fan, J., Todorovic, S., and Nucci, A “Robust and efficient detection of DDoS attacks for large-scale internet.” Computer Networks, 51, 5036– 5056. (2007)
53. Hwang, K., Dave, P., and Tanachaiwiwat, S. “Net Shield: Protocol anomaly detection with datamining against DDoS attacks”. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, 8-10 September, pp. 8–10. Springer-verlag. (2003)
54. Chen, Z., Chen, Z., and Delis, A. “An inline detection and prevention framework for distributed denial of service attacks.” Computer. Journal. 50, 7–40. (2007)
55. Lee, K., Kim, J., Kwon, K. H., Han, Y., and Kim, S.”DDoS attack detection method using cluster analysis. Expert Systems with Applications, “34, 1659– 1665. (2008)
56. Sekar, V., Dueld, N., Spatscheck, O., van der Merwe, J., and Zhang, H. “LADS: large-scale automated DDoS detection system.” Proceedings of the annual conference on USENIX Annual Technical Conference, Boston, MA, 30 May-3 June, pp. 16–29. USENIX Association. (2006)
57. H. Rahmani, N. Sahli, and Kammoun, F “Joint entropy analysis model for DDoS attack detection.” Proceedings of the 5th International Conference on Information Assurance and Security - Volume 02, Xian, China, 18-20 August, pp. 267–271. IEEE CS. (2009)
58. Y. Xiang, K. Li, and Zhou, W. “Low- rate DDoS attacks detection and traceback by using new information metrics.” IEEE Transactions on Information Forensics and Security, 6, 426–437. (2011)
59. Shannon, C. E. (1948) “A mathematical theory of communication.” Bell system technical journal, 27, 397– 423.
60. J. Francois, Aib, I., and Boutaba, R. “Fire Col: A collaborative protection network for the detection of flooding DDoS attacks.” IEEE/ACM Transaction on Networking, 20, pages-1828–1841. (2012)
61. N. Jeyanthi, and N.C.S.N. Iyengar, “An entropy-based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks.” International Journal of Network Security, 14, 257– 269. (2012)
62. Li, M. and Li, M. “A new approach for detecting DDoS attacks based on wavelet analysis.” Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17-19 October, pp. 1–5. IEEE. (2009)
63. R. Zhong, and G. Yue DDoS detection system based on data mining.” Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2-4 April, pp. 062–065. Academy Publisher. (2010)”
64. R. Agrawal, and R. Srikant, “Fast algorithms for mining association rules in large databases.” Proceedings of the 20th International Conference on Very Large Data Bases, Santiago de Chile, Chile, 12-15 September, pp. 487–499. Morgan Kaufmann. (1994)
65. J.C. Dunn “A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters.” Journal of Cybernetics, 3, 32– 57. (1973)
    A. Dainotti, A. Pescap´e, and Ventre, G. (2009) “A cascade architecture for DoS attacks detection based on the wavelet transform.” Journal of Computer Security, 17, 945–968.
66. Haar, A. (1910) Zur “TheoriederorthogonalenFunktionensysteme.” MathematischeAnnalen, 69, 331–371.

67. Li, L. and Lee, G. "DDoS attack detection and wavelets." Proceedings. of the 12th International Conference on Computer Communications and Networks, Dallas, Texas, USA, October 20-22, pp. 421–427. IEEE. (2003)
68. B.Gupta, R. C. Joshi, and Misra, M. "ANN based scheme to predict number of zombies in DDoS attack." International Journal of Network Security, 14, pages:36–45. (2012)
69. J. Cheng, Yin, J., Y. Liu, Cai, Z., and Wu, C. "DDoS attack detection using IP address feature interaction." Proceedings of the 1st International Conference on Intelligent Networking and Collaborative Systems, Barcelona, Spain, 4-6 November, pp. 113–118. IEEE CS. (2009)
70. Xia, Z., Lu, S., Li, J., and Tang, J. "Enhancing DDoS flood attack detection via intelligent fuzzy logic." Informatics (Slovenia), 34, pages-497–507. (2010)
71. Zhang, Z. Cai, W. Chen, Luo, X., and Yin, J. "Flow level detection and filtering of low-rate DDoS. Computer Networks," 56, pages:3417–3431. (2012)
72. Zhao, I. Traore, B. Sayed, W. Lu, Saad, S., Ghorbani, A., and Garant, D., ''Botnet detection based on traffic behaviour analysis and flow intervals,'' Computer Security, DOI: 10.1016/j.cose.2013.04.007 (2013).
73. P. C. Senthil mahesh, S. Hemalatha, P. Rodrigues, and A. Shanthakumari, "DDoS Attacks Defense System Using Information Metrics," Proceedings of 3rd International Conference on Trends in Information, Telecommunication and Computing, Lecture Notes in Electrical Engineering (Springer, New York), 25–30 (2012).
74. Gelenbe, and G. Loukas, "A self-aware approach to denial-of-servicedefence." Computer Networks, 51, pages:1299–1314. (2007).