Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 7 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey

By K. Munivara Prasad, A. Rama Mohan Reddy & K.Venugopal Rao
JNTUH University, India

Abstract- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are typically explicit attempts to exhaust victim's bandwidth or disrupt legitimate users' access to services. Traditional architecture of internet is vulnerable to DDoS attacks and it provides an opportunity to an attacker to gain access to a large number of compromised computers by exploiting their vulnerabilities to set up attack networks or Botnets. Once attack network or Botnet has been set up, an attacker invokes a large-scale, coordinated attack against one or more targets. Asa result of the continuous evolution of new attacks and ever-increasing range of vulnerable hosts on the internet, many DDoS attack Detection, Prevention and Traceback mechanisms have been proposed, In this paper, we tend to surveyed different types of attacks and techniques of DDoS attacks and their countermeasures. The significance of this paper is that the coverage of many aspects of countering DDoS attacks including detection, defence and mitigation, traceback approaches, open issues and research challenges.

Keywords: denial of service (DoS), distributed denial of service (DDoS), detection mechanisms and trceback approaches.

GJCST-E Classification : D.4.6

Strictly as per the compliance and regulations of:

DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey

K. Munivara Prasad [α], A. Rama Mohan Reddy [σ] & K. Venugopal Rao [ρ]

Abstract- Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are typically explicit attempts to exhaust victim's bandwidth or disrupt legitimate users' access to services. Traditional architecture of internet is vulnerable to DDoS attacks and it provides an opportunity to an attacker to gain access to a large number of compromised computers by exploiting their vulnerabilities to set up attack networks or Botnets. Once attack network or Botnet has been set up, an attacker invokes a large-scale, coordinated attack against one or more targets. As a result of the continuous evolution of new attacks and ever-increasing range of vulnerable hosts on the internet, many DDoS attack Detection, Prevention and Traceback mechanisms have been proposed, In this paper, we tend to surveyed different types of attacks and techniques of DDoS attacks and their countermeasures. The significance of this paper is that the coverage of many aspects of countering DDoS attacks including detection, defence and mitigation, traceback approaches, open issues and research challenges.

Keywords: denial of service (DoS), distributed denial of service (DDoS), detection mechanisms and trceback approaches.

I. Introduction

Denial-of-service (DoS) attacks exploit internet to target critical Web services [1, 2, 3, 4, 5,6]. This type of attack is intended to prevent legitimate users from accessing a specific network resource or degrade normal services for legitimate users by sending huge unwanted traffic to the victim (machines or networks) to exhaust services and connection capacity or the bandwidth. Increasing flow of these DoS attacks has made servers and network devices on the internet at greater risk.

Denial of service attack programs are around for several years. Previous single source attacks are currently countered simply by several defense mechanisms and therefore the source of those attacks will be simply rejected or blocked with improved tracing capabilities. However, with the amazing growth of the internet throughout the last decade, an increasingly large amount of vulnerable systems are currently available to attackers. Attackers will currently use a huge range of those vulnerable hosts to launch an attack rather than employing a single server, an approach that is not terribly effective and detected easily.

A distributed denial of service (DDoS) attack [7, 12] is a large-scale, coordinated attack on the provision of services of a victim system or network resources, launched indirectly through a large number of compromised computer agents on the internet. Before applying an attack the attacker takes large number of computer machines under his control over the internet and these computers are vulnerable machines. The attacker exploits these computers weaknesses by inserting malicious code or some other hacking technique so that they become under his control. These vulnerable or compromised machines can be hundreds or thousands in numbers and these are commonly termed as 'zombies.' The group of zombies usually formed the 'botnet.' The magnitude of attack is depends on the size of botnet, for larger botnet, attack is more severe and disastrous.

DDoS attacks in the Internet can be launched using two main methods. In the first method the attacker send some malicious packets to the victim to confuse a protocol or an application running on it (i.e., vulnerability attack [8]). The Second method essentially include the network/transport-level/ application-level flooding attacks [8], in which an attacker to do one or both of the following: (i) interrupt a legitimate user's connectivity by exhausting bandwidth, network resources or router processing capacity or (ii) disrupt services of a legitimate user's by exhausting the server resources such as CPU, memory, disk/database bandwidth and I/O bandwidth.

Nowadays, DDoS attacks are often launched through well organized, remotely controlled, and widely distributed Zombies or Botnet computers of a network, that are continuously or simultaneously sending a huge amount of traffic or service requests to the target system. The attack results the target system either responds so slowly, unusable or crashes completely [8],[9] [10]. Zombies of a botnet are usually recruited through the use of Trojan horses, worms, or backdoors [11]–[13]. It is very difficult for the defense mechanisms to identify the original attacker because of the use of spoofed IP addresses by zombies under the control of the attacker with botnet [14].

Earlier DDoS attacks were manual, in which attacker had to implement many steps before the launch of final attack, which includes port scanning, identifying compromised machines or zombies in the internet to

Author α: Research scholar, Department of CSE, JNTUH, Hyderabad. e-mail: prasadkmv27@gmail.com
Author σ: Professor, Department of CSE, SVUCE,SV University, Tirupati
Author ρ: Professor and Head, Department of CSE, GNITS, Hyderabad.

create botnet, deploying malware etc. Nowadays, sophisticated and automated DoS or DDoS attack tools been developed to assist attackers in implementing all or some steps automatically with minimal human effort to launch these attacks. The attackers can just configure desired attack parameters for a specified attack and the rest is managed by automated tools. Some of the common automated attack tools available are TFN (Tribe Flood Network), Trinoo, TFN2K, Shaft, Stacheldraht, Knight and Trinity. Many of them work on IRC (Internet Relay Chat) in which handlers and zombies communicate indirectly without revealing their identities. The others are agent based where handlers and zombies know each other's identity and communicate direct [9].

II. DDoS Attacks Classification and Architectures

a) *DDoS Motivation*

DDoS attackers are usually motivated by various reasons. We categorized these DDoS attacks based on the motivation of the attackers into seven main classes:

1. *Financial/economical gain:* Attacks launched for financial gain are often, the most dangerous and difficult to stop. These are mainly concern of corporations and require more technical skills and experience.
2. *Invariably slow network performance:* The attacker launches an attack to block the resources of victim system, which slowdowns the performance of the system and intern to the network.
3. *Revenge:* Attackers of this kind are normally with lower technical skills and are frustrated individuals, carry out these as a response to a perceived injustice.
4. *Ideological belief:* Attackers in this category are inspired by their ideological beliefs to attack their targets. This category is currently one of the major incentives for the attackers to launch DDoS attacks.
5. *Intellectual Challenge:* In this, attack the targeted systems for experiment and learn how to launch various attacks. They are usually young hacking enthusiasts who want to show off their competencies.
6. *Service unavailability:* In this attacker overloads the services offered by the victim system through unwanted or fake traffic.
7. *Cyberwarfare:* Attackers of this class is normally belong to the military or terrorist organizations of a country and they are politically motivated to attack a wide range of critical sections of another country.

b) *Classification*

Various classifications of DDoS attacks have been proposed in the literature, when DDoS attacks are classified based on the degree of automation, they are defined as Manual, Semi-automatic and Automatic attacks. In manual approach the attacker had to complete many steps before the launch of final attack, such as port scanning, identifying available machines in the public or private network to build botnet, inserting malware etc. For Semi-automatic or Automatic attacks, various sophisticated attack tools have been developed to support attackers in carrying out all or some steps automatically to reduce human effort. The attackers can configure desired attack parameters and the rest is done by automated tools.

Another classification of DDoS attacks by attack rate i.e., how the rate of attack varies with respect to the time. The classes are Continuous Rate and Variable Rate attacks. The attack has constant flow in continuous rate after it is executed. But as in, variable rate attack changes its impact and flow with time, making it more difficult to detect and respond. Within variable rate, the attack rate can further be applied as Fluctuating or Increasing. Additionally, based on the data rate of attack, traffic in a network is also categorized as high rate and low rate DDoS attacks.

DDoS attacks further classified as 'by impact' i.e., in which the normal service is completely unavailable to users known as Disruptive, or it can be Degrading the services of victim system in which it is not completely unavailable or decrease in the efficiency.

In direct attacks, agents or zombie machines directly attack the victim system as shown in the in Figure. 1. But in reflector attacks, zombies send request packets to a number of other compromised machines (PCs, routers etc.) called Zombies or Bots and the reply generated Zombies is targeted towards the victim system for an impact desired by the attacker. Example for this attack is sending huge amount of traffic as 'ping' request with spoofed IP address to the victim system to saturate bandwidth.

The main classification of DDoS attacks is 'by exploited vulnerability' through which an attacker launches attack on the victim. The classification is given in Fig. 2 .In this classification, flood attack is used to block the victim's machine or network's bandwidth. This can be performed as TCP flood, UDP flood and ICMP flood. In general, all flooding attacks generated through DDoS can as direct attacks or reflector attacks.

c) *DDoS attacks architectures*

DDoS attack networks uses three types of architectures: the Agent-Handler architecture, Internet Relay Chat (IRC)-based architecture and the Web based architecture.

i. *Agent-Handler Architecture*

The Agent-Handler architecture is also referred as Botnet based architecture, in which the attacker uses the botnet to launch an attack. Generally a group of

zombies or bots that are controlled by an attacker (also called as bot Master) form a botnet. Botnets consist of masters, handlers, and bots as shown in Figure 3. The handlers are means of communication that attackers use to command and control indirectly the bots. The handlers can be programs installed by the attackers on a collection of compromised systems (e.g.,Network servers) to send commands to carry out the attack. Bots are devices that have been compromised by the handlers and that will carry out the attack on the victim's system. Figure 4 shows all the elements of a botnet. The owners and users of the bot systems are generally unaware of the situation.

ii. *IRC-based architecture*

The bot master or controller launches an attack through the bots by sending the commands to them which intern behave according to the master instructions. At the other end the bot sends the response or the status information to the master. Their communication is done through public chat systems instead of doing these with their original addresses. If they use the original identity or private channels, the detection system easily track and block the location and system. Internet relay chat (IRC) is the one which allows the users to communicate without performing any authentication check and no security to user communications. IRC provides a text-based command syntax protocol to define the rules and regulations to the users and that is installed widely across the network. There is huge number of existing IRC networks available in the internet and which can be used as public exchange points, but the majority IRC networks doesn't contain any strong authentication. The wide variety of tools in the internet is available to provide anonymity on IRC networks. Therefore, IRC provides simple, low-latency, widely available, and anonymous command and control channel for botnet communication. An IRC network is a collection of one or more IRC servers as depicted in figure 4.

iii. *Web-based architecture*

Botnets are using HTTP as a communication protocol to send commands to the bots making it more difficult to track the DDoS command and control structure. Like IRC-based botnets web-based botnets do not maintain connections with command and control servers or handlers. The Web bots downloads the instructions using web requests periodically. Web-based botnets are stealthier since they hide themselves within legitimate HTTP traffic. Advanced web development languages (PHP, ASP, JSP, etc.) through encrypted communication over HTTP or HTTPS protocol are used to configured and control the bots.

d) DDoS Strategy

A Distributed Denial of Service (DDoS) attack consists of several elements as shown in Figures 1. There are four steps in launching a DDoS attack. These are shown in Figure 5.

1. *Discover vulnerable hosts or agents:* The attacker selects the agents to perform the attack. Any systems which is running with no antivirus software or pirated copies of software in internet is vulnerable and operated as a compromised system. Attackers utilized these compromised hosts or bots for further scanning and compromises .Attacker generates the attack stream by using the abundant resources of these compromised machines.
2. *Compromise:* The attacker exploits vulnerabilities and security holes of the agent machines and installs the attack code.
3. *Communication:* The attacker communicates with the handlers to identify the active agents, to schedule attacks or to upgrade agents. The communication among the attackers and handlers

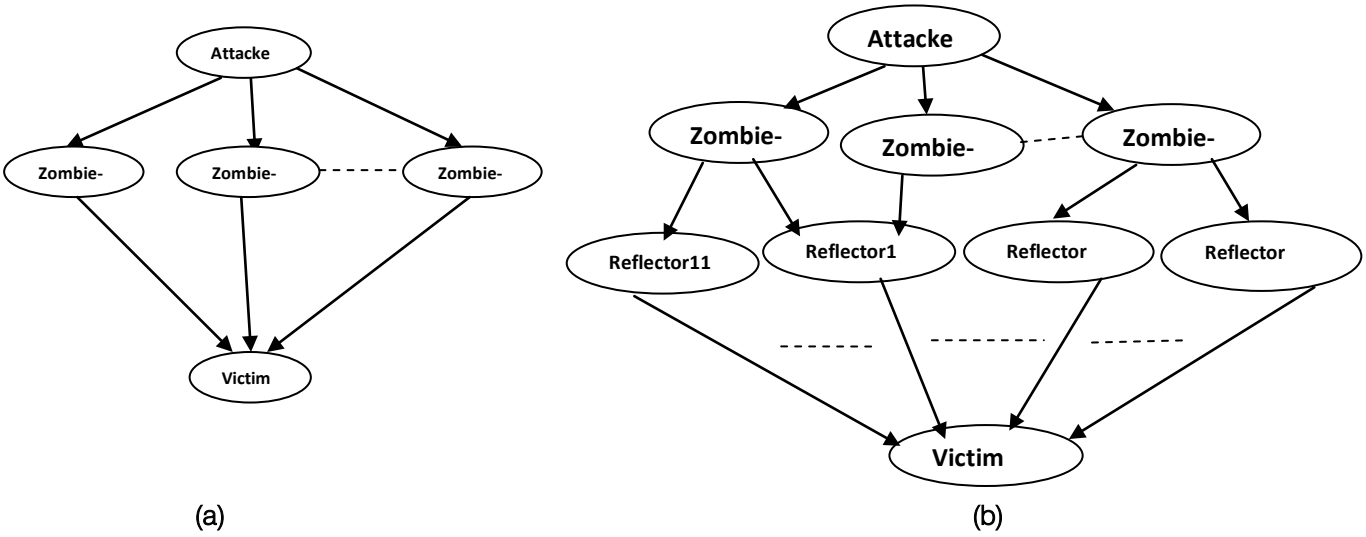

Figure 1 : (a).Direct attack, (b).Indirect attack

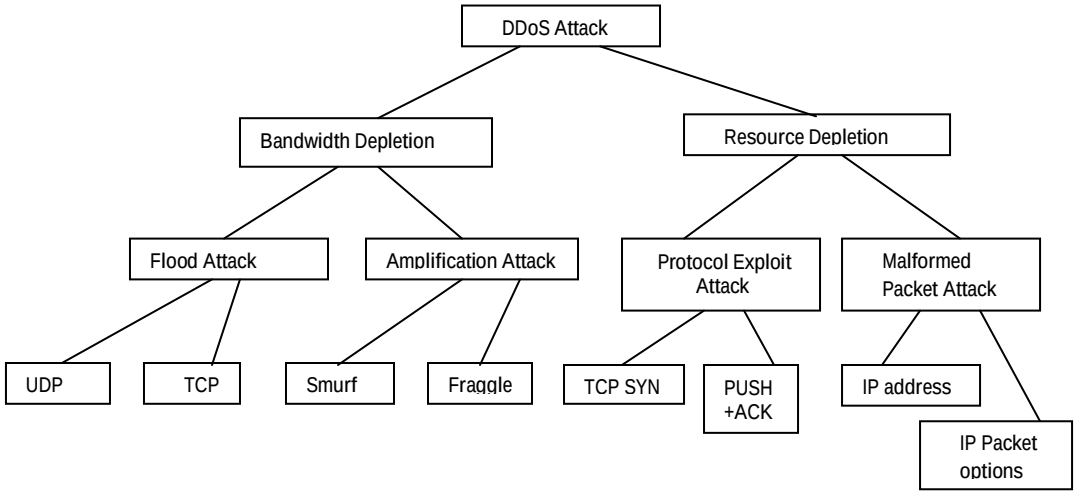

Figure 2 : DDoS attacks Classifications

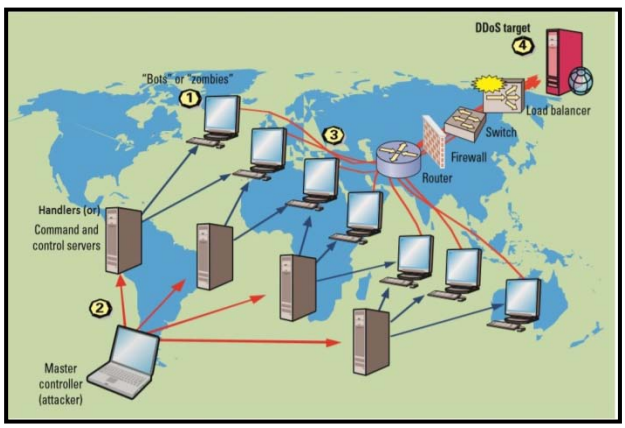

Figure 3 : Agent handler Architecture Figure

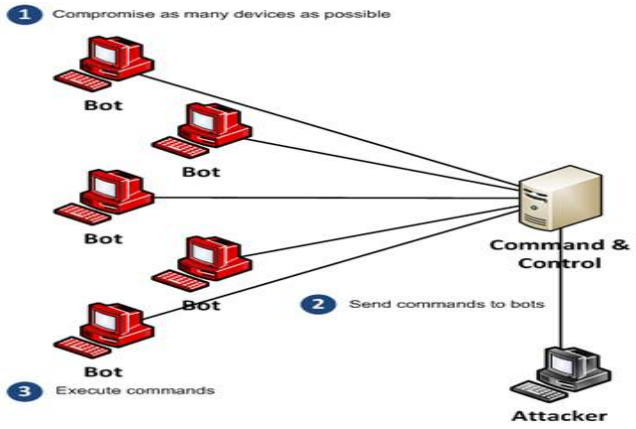

Figure 4 : IRC- based Architecture

can be done through various protocols such as TCP,UDP or ICMP and based on the network configuration with single handler or multiple handlers.

4. *Launching an Attack:* The attacker launches an attack by selecting the victim system, attack duration and adjusting the features of the attack

such as the type, length, Time to Live(TTL), and port numbers.

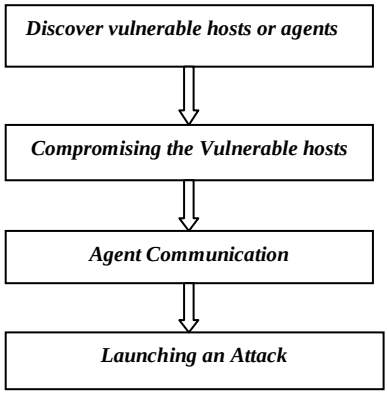

Figure 5 : Phases of performing DDoS attacks

III. DDoS Defense, Detection and Mitigation

a) DDoS Defense Architectures

When a DDoS attack is detected, there is nothing that can be done except manually fix the problem and disconnect the victim system from the network. DDoS attacks blocks a lot of resources such as CPU power, bandwidth, memory, processing time, etc., on the paths that lead to the targeted system. The main goal of any DDoS defense mechanism is to detect DDoS attacks as soon as possible and stop them as near as possible to their sources. DDoS defense schemes are divided into four classes based on the locality of deployment: source-end, victim- end, Core-end or intermediate router and Distributed or Hybrid defense mechanisms. The advantages and disadvantages of all these approaches are given in the table1.

i. *Source-end defense mechanism*

Source-end defense mechanisms are deployed at the sources of the attack to prevent network users from generating DDoS attacks. In this approach, source devices identify malicious packets in outgoing traffic and filter or rate-limit the traffic. Detecting and stopping a DDoS attack at the source is the best possible defense as minimum damage is done on legitimate traffic.

ii. *Victim-end defense mechanism*

In the victim-end defense mechanism, the victim system detects, filter or rate-limit malicious incoming traffic at the routers of victim networks, i.e., networks providing Web services. The legitimate and attack traffic can clearly be distinguished from either online or offline, using either misuse based intrusion detection or anomaly based intrusion detection. However, attack traffic reaching the victim may denied or degraded services and bandwidth saturation.

iii. *Core-end or Intermediate router defense mechanism*

In core-end or intermediate network defense scheme, any router in the network can independently attempt to identify the malicious traffic and filter or rate-limit the traffic. It also balances the trade-offs between detection accuracy and attack bandwidth consumption. Detection and traceback of attack sources becomes easy, due to collaborative operation. In this point of defense, the traffic is aggregated i.e., both attack and legitimate packets arrive at the router and it is a better place to rate-limit all the traffic.

iv. *Distributed-end or Hybrid Defense architecture*

Attack detection and mitigation at distributed ends can be the best strategy against DDoS attacks. The hybrid defense mechanisms are deployed at (or their components are distributed over) multiple locations such as source, Victim or intermediate networks and there is usually cooperation among the deployment points. The core-end is best to rate-limit all kinds of traffic whereas the victim-end can accurately detect the attack traffic in a combination of legitimate and attack packets. Therefore, distribution of methods of detection and mitigation at different ends of the network can be more beneficial.

b) DDoS Detection and Mitigation Strategies

In this section, we present a summary of existing methods on DDoS attack detection and mitigation. These methods are based on the architectures discussed above namely source-end, Victim-end, Core-end and Hybrid mechanisms in the network. We classify methods for DDoS attack detection into four major classes as shown in Figure 6.

i. *Statistical Methods*

Statistical properties of normal and attack patterns can be exploited for detection of DDoS attacks. Generally a statistical model for normal traffic is calculated and then a statistical inference test is applied to determine if a new instance of the traffic or flow belongs to this model. Instances that do not follow the learnt model, based on the applied test statistics results, traffic or flows are classified as anomalies.

Chen et al. [19] develop a distributed change point (DCP) detection architecture using change aggregation trees (CATs). The pre-change and post-change network traffic was described using non-parametric CUSUM approach. The cumulative deviation is higher than random increase when a DDoS flooding attack is launched and CAT mechanism is designed to detect abrupt changes in traffic flows work at router level. The traffic change patterns were detected at the domain server uses attack-transit to construct the CATs, which represent the attack flow pattern.

D-WARD [20] detects an attack based on constant monitoring of bidirectional traffic flows between

the network and the Internet and based on the periodic deviation analysis with the normal flow patterns. Abnormal flows are rate limited in proportion to their arrival rate. D- WARD offers a good detection rate along with the reduction of DDoS attack traffic significantly. It uses a predefined model for normal traffic and detects anomalies in the two-way traffic based on the deviation statistics. Finally, D-WARD notices the traffic for either confirmation of the attack or refutation. If confirmed, D-WARD further controls the rate limit. However, if refuted, it gradually allows increased traffic rate.

Saifullah [21] proposes a defense mechanism by using distributed algorithm that performs weight-fair throttling at upstream routers. The throttling is weight-fair because the traffic intended for the server is controlled (increased or decreased) by using leaky buckets at the routers based on the number of users connected, directly or indirectly to the routers. In the beginning of the algorithm, the survival capacity is underestimated by the routers so as to protect the server from any sudden initial attack. The survival capacity is initialized to minimal or normal values at the beginning of the algorithm and the rate is updated (increased or decreased), based on the server's feedback sent to its child routers and ultimately propagated downward to all routers, in the successive rounds of the algorithm with an assessment to converging the total server load to the acceptable capacity range.

Peng et al. [22] describe a new approach to detect bandwidth attacks by observing the arrival rate of new source IP addresses. The detection system is based on an advanced non-parametric change detection scheme, CUSUM. Cheng et al. [23] propose the IP Flow Feature Value (FFV) algorithm using the vital features of DDoS attacks, such as flow dissymmetry, abrupt traffic change, distributed source IP addresses and concentrated target IP addresses. ARMA prediction model is established for normal network flow using a linear prediction technique. Then a DDoS attack detection scheme based on anomaly detection techniques and linear prediction model (DDAP) is used.

Udhayan and Hamsapriya [24] defines a Statistical Segregation Method (SSM), by sampling the flow in consecutive intervals and compares the samples with the attack state condition and sorts them based on the mean parameter. Attack flows from legitimate flows are segregated using correlation analysis.

In [25], a generic DoS detection scheme was introduced based on maximum likelihood criterion with random neural networks (RNN). This approach initially selects a set of traffic features in offline mode to obtain pdf estimates and to evaluate the probability ratios. It measures the features of incoming traffic and attempts to decide according to each feature to take decision. Lastly, it obtains an overall decision using both feed-forward and recurrent architectures of the RNN. A brief summary of these methods is given in Table 1.

In [26], authors present a lightweight tunnelling protocol called LOT, to prevent network traffic against IP spoofing and flooding attacks. It is deployed at network's communication gateways. Two gateways with LOT implementation can detect each other and create the tunnel between them to secure communication. The protocol allows the gateway to discard spoofed IP packets which specify source addresses in other gateway and vice versa and communication can be protected from any type of DDoS attacks. The use of per-flow quotas to identify flooding of packets from different networks mitigation the DDoS attacks. The LOT protocol not only passes restricts spoofed packets to destination and also filter packets based on filtering rules determined by destination gateway.

In [27], authors attain DDoS detection with enhanced time limits through non-asymptotic fuzzy estimators. The estimator is deployed on mean packet inter-arrival times. The problem is divided into two parts; one is actual DDoS detection and the other is identification of victim IP addresses. The first part is achieved using strict real time limits for DDoS detection. The second part i.e., identification of victim IP addresses is attained through comparatively relaxed constraints. The goal is to identify victim IP addresses in a timely manner to launch added anti intrusion applications on offended hosts using packet arrival time as the main statistic of DDoS attack determination.

A game theoretic approach is followed in [28] to offer defense against DoS/DDoS cyber-attacks. The DDoS attack is modelled as a one-shot & zero-sum game with non-cooperation. To perform an attack, multiple features are investigated in terms of cost with malicious traffic distribution and number of attackers. It is validated in analytical terms that a single optimal strategy of defense is available to defender in which upper boundaries are set to attacker payoff depending upon the rational or irrational attackers. Table 2 presents a brief summary of the Statistical based DDoS detection methods.

ii. *Soft computing based methods*

Learning paradigms, such as Artificial Neural Networks (ANNs), radial basis functions and genetic algorithms are widely used in DDoS attack detection because of their ability to classify intelligently and automatically. Soft computing is a method of describing a set of optimization and processing techniques that are tolerant of imprecision and uncertainty.

Artificial Neural Networks (ANNs) are widely used learning models with their ability to cope with demands of a changing environment [32]. These ANNs are self-learning and self-organizing models with the features like robustness, fault tolerance and parallelism. ANNs are good to identify and resist unknown

disturbances in a system because of its self-learning characteristic.

In [33], authors use Linear Vector Quantization (LVQ) model of ANN. It is same as self-organizing maps and applied the techniques of pattern recognition, multi-layer classification and data compression. In supervised learning, it knows the target output against different forms of various input patterns. After testing the system with LVQ model, authors use the same dataset with Back propagation (BP) model of ANN for comparative study. On the basis of comparison results, they claim that LVQ is more accurate in determining DDoS attacks than BP. They show that LVQ is 99.723% accurate on average against tested dataset whereas the average accuracy of BP is 89.9259% for the same dataset. Accuracies are computed on the basis of percentages of obtained false positives and false negatives against each sample of testing data. There are 10 samples used to test the systems for each of the LVQ and BP models.

In [34], authors train the BP neural network with a traffic entropy variations dataset as inputs and DDoS strengths as outputs. 20 different samples in the dataset are used for training with 10Mbps attack strength as the lowest and 100Mbps being the highest in the dataset. The entropy variations are calculated based on an assumption that the attack traffic is seen different in the network from normal traffic. The model is tested with random inputs of four entropy variations and calculated attack strengths respectively as 20, 50, 70 and 95Mbps. The BP neural network's output is obtained with little errors. False positives and false negatives are very less and also the system is tested with variations in network size i.e., number of neurons in processing layer but in real cases, increasing the network size also increases both training time and implementation cost.

In [35], authors propose Time Delay Neural Network (TDNN) to acquire early warning system against DDoS attacks. TDNN is a neural network in which time delay factor is hidden inside the representative signal. The authors created a Demilitarized Zone (DMZ) and TDNN is implemented in two-layer pattern. The node action is monitored by neighboring nodes and attack information is sent to the expert module for integrated analysis. The layered structure enables the system to ensure some appropriate actions as a proactive strategy against DDoS attacks. The detection results on deployed architecture show that proposed scheme is able to give 82.7% correct detection rate as compared to 46.3% with general Intrusion Detection System (IDS).

Jalili et al. [36] introduce SPUNNID as DDoS attack detection system based on a statistical pre-processor and unsupervised artificial neural network. It use statistical pre-processing to extract features from the traffic, and uses an unsupervised neural network to analyse and classify traffic as an attack or normal traffic.

Karimazad and Faraahi [37] propose an anomaly-based DDoS detection method using Radial Basis Function (RBF) neural networks based on features of attack packets analysis. It is applied to classify data as normal or attack categories. If the incoming traffic is identified as attack traffic, the attack packets source IP address are sent to the Filtering Module and the Attack Alarm Module performs further actions. Otherwise, if the traffic is normal, it is directed to the destination.

Gavrilis and Dermatas [38] present a detection method for DDoS attacks in public networks based on statistical features estimated in short-time window analysis of incoming data packets. A small number of statistical parameters are used to define the behavior of the DDoS attacks. An accurate classification is achieved using Radial Basis Function neural networks than this.

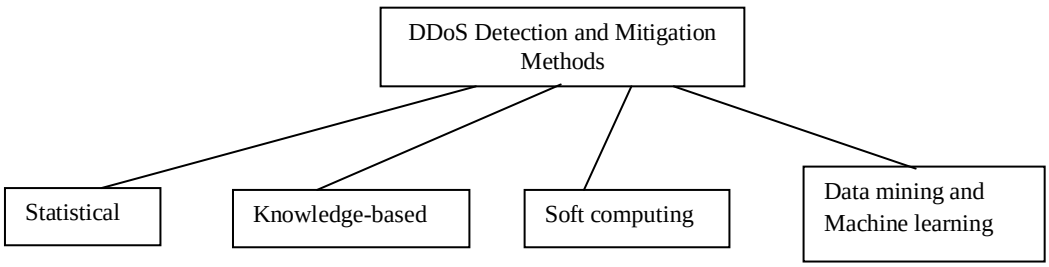

Figure 6 : DDoS Detection and Mitigation methods

Table 1 : Comparison of DDoS attack Defense architectures

Defense Method	Advantages	Disadvantages
Source-end Defense Architecture	• Detecting and stopping a DDoS attack at the source provides best possible defense as minimum damage is done on legitimate traffic. • Minimum amount of traffic to be checked at source point for which fewer resources are required by the detection & mitigation mechanism.	• Detecting DDoS attacks at source end is difficlut because sources are widely distributed across the network and a single source behaves like a normal traffic. • The difficulty of deploying system at the source end.
Victim-end Defense Architecture	• Detecting DDoS attacks in victim routers is relatively easy because of the high rate consumption of resources. • Best practically applicable type of defense scheme as Web servers providing critical services always try to secure their resources for legitimate users.	• During DDoS attacks, victim resources, e.g., network bandwidth, often gets over- whelmed and these approaches cannot stop the flow beyond victim routers. • Detect the attack only after it reaches the victim and detecting an attack when legitimate clients have already been denied is not useful.
Core-end Defense Architecture	• Detection and traceback of attack sources are easy in this approach due to collaborative operation. • The traffic is aggregated i.e., both attack and legitimate packets arrive at the router and it is a better place to rate-limit all the traffic.	• Deployment is the main difficulty with this approach. • To attain full detection accuracy, all routers on the Internet will have to follow this detection scheme, because unavailability of this scheme in one router may cause failure to the detection and traceback process. • Full practical implementation is extremely difficult because it requires the reconfiguration of all the routers on the Internet.
Distributed-end or Hybrid Defense architecture	• Detection can be done at the victim side and the response can be initiated and distributed to other nodes by the victim. • Distribution of methods of detection and mitigation at different ends of the network can be more beneficial.	• Strong cooperation among the deployment points is required. • Complexity and overhead because of the cooperation and communication among distributed components scattered all over the Internet.

Wu et al. [39] proposes detection of DDoS attacks using decision trees and grey relational analysis. The detection of the attack from the normal state is defined as a classification problem. They use 15 attributes, to monitor the incoming/outgoing packet/byte rate, and also collect the TCP, SYN, and ACK flag rates, to define the traffic flow pattern. The decision tree method is used to develop a classifier to detect abnormal traffic flow and also use a novel traffic pattern matching procedure to identify traffic flow similar to the attack flow and to trace back the origin of an attack.

In [42] the authors proposes ensemble of classifiers which uses the Resilient Back Propagation (RBP) neural network as the base classifier for DDoS Detection. They are mainly focussed on improvement of the performance of the base classifier. The RBPBoost combines the output of the ensemble of classifier outputs and Neyman Pearson cost minimization strategy [43], for final classification decision. Table 3 presents a brief summary of the soft computing.

Table 2 : Statistical based DDoS Detection methodsReference

Reference	Objective	Deployment	Working Mode	Remarks
Mirkoviac al. et[20]	Attack prevention	Source side	Centralized	Statistical traffic modelling is used to Detect DDoS attacks and blocks the attack traffic when it is detected at source end.
Akella.et al.[31]	Attack detection	Source and victim side	Distributed	A profile is constructed from normal traffic and detects anomalies in the traffic using stream sampling. In general this approach used in the network routers.
Prasad, ARMReddy, KVGRrao[41]	Attack detection	victim side	Distributed	Modeling and Counter measures of Flooding attacks to ITM using Botnet and Group Testing.
Peng.et al.[22]	Detecting bandwidth attacks	Victim side	Centralized	Sequential nonparametric change point detection method is used to improve the detection accuracy and employed at victim end.
Chen.et al.[19]	Attack detection and Traceback	Between source and destination network	Distributed	Hybrid approach which is used to detect and trace back the attack source.
Oke and Loukas [25]	Attack detection	Victim side	Centralized	Defines a set of attack specific input features that captures the behavior and the long term statistical properties of the traffic during detection.
Saifullah[21]	Attack prevention	Between source and destination network	Distributed	Prevention method which protects Internet servers and routers from DDoS attacks using distributed weight-fair throttling from the upstream routers.
Chen[29]	Attack detection	Victim side	Centralized	Detects DDoS attacks using two-sample t-test by integrating the statistics of SYN arrival rate.
Zhang.et al.[30]	Attack detection	Victim side	Centralized	Uses an Auto Regressive Integrated Auto Regressive (ARIMA) model for protecting servers from DDoS attacks.
Cheng.et al.[23]	Attack detection	Victim side	Centralized	Activities four flow features: asymmetry of the flow, burst in the traffic volume, distributed source IP destination IP address while detecting DDoS attacks.
Udhayanand Hamsapriya[24]	minimize false alarm	Victim side	Centralized	Statistical segregation method is used to detect DDoS attacks based on sampling of traffic flow in consecutive time interval.

Table 3 : Soft computing based DDoS Detection methods

Reference	Objective	Deployment	Working Mode	Remarks
Jalili.et al[36]	Attack detection	Victim side	Centralized	Statistical preprocessor and unsupervised neural network classifier methods were used for DDoS attack detection.
Gavrilis &Dermatas[38]	Attack detection	Victim side	Centralized	Detects DDoS attacks using statistical features estimated in short time interval in public network with Radial basis function of neural network.
Nguyen and Choi[40]	Attack detection	Intermediate network	Centralized	K-nearest neighbour based technique is used to detect only known attacks.
Wu et al. [39]	Attack detection and traceback	Victim side	Distributed	Trace back to the attacker location based on traffic flow pattern matching using decision trees.

Karimazad And Faraahi[37]	Attack detection	Victim side	Centralized	Low false alarm rate can be achieved using Radial Basis Function (RBF) neural networks.
Kumar and Selvakumar[42]	Attack detection	Victim side	Centralized	High detection rate in RBP Boost can be achieved using the combination of an ensemble of classifier outputs and Neyman Pearson cost minimization strategy.

methods presented in this section. Table 3 presents a brief summary of the soft computing methods presented in this section.

iii. *Knowledge based Methods*

In knowledge-based approaches, network events or actions are tested against predefined rules or patterns of attack. In these, general representations of known attacks are called as attack signatures and these are formulated to identify actual occurrences of attacks. Knowledge-based approaches include expert systems, signature analysis, self-organizing maps, and state transition analysis.

Gil and Poletto [44] present a heuristic data structure named as MULTOPS (MUlti-Level Tree for Online Packet Statistics), that monitor traffic characteristics of network devices like routers to detect and eliminate DDoS attacks. MULTOPS is a tree of nodes which includes traffic rate statistics for subnet prefixes at different aggregation levels and was expansion and contraction of the tree occurs within a pre-specified memory size. A MULTOP of network device detects bandwidth attacks by the occurrence of a significant difference between traffic rates going to and coming from the victim or the attacker. Routers or network monitors equipped MULTOPS may fail to detect a bandwidth attack that is fixed by attackers that randomizes IP attack source addresses on malicious packets. It also fails to detect attacks that deploy a large number of attack flows to explode a victim.

Thomas et al. [45] introduces a practical approach with high performance DDoS defense mechanism called as NetBouncer. It distinguishes legitimate and illegitimate use of resources and ensuring that are made available only for legitimate use. It allows traffic to flow with respective to a long list of recognized legitimate clients and if packets are received from a source not on the legitimate list, a NetBouncer device invite administer to perform variety of legitimacy tests to test the client to prove its legitimacy. If a client proved its authorization, it is added to the legitimacy list and subsequent packets from the client are accepted.

Wang et al. [46] present a methodical way of modeling DDoS attacks using Augmented Attack Tree (AAT), and implemented an AAT-based attack detection algorithm. It explicitly captures the specific subtle incidents triggered by a DDoS attack and the corresponding state changes from the observation of the network traffic transmission on the primary victim server. With reference to the conventional attack tree (CAT) modeling method, AAT is advanced because it provides additional information like the state transition process. It overcomes the limitations of CAT modelling.

Limwiwatkul and Rungsawang [47] discover DDoS attack signatures by analysing the TCP/IP packet header against pre defined rules and conditions, and differentiating the difference between normal and abnormal traffic flow. These mainly focus on ICMP, TCP and UDP flooding attacks.

Zhang and Parashar [48] introduced a distributed approach to defend against DDoS attacks in the Internet. To detect DDoS attacks independently, defensive systems are deployed in the network, unlike traditional IDS, this method detects and stops DDoS attacks within the intermediate network. An IRC communication is used between these independent detection nodes to exchange information about network attacks and combined this information for aggregate network attacks. Individual defence nodes obtain estimated information about global network attacks and stop the attacks more effectively and accurately using the aggregated information of network. An earlier approach depends on monitoring the volume of traffic received by the victim and these are incompetent of distinguishing a DDoS attack from a flash crowd.

Lu et al. [49] defines a perimeter-based DDoS defese system, in which the traffic is analyzed at the edge routers of an Internet Service Provider (ISP) network. The DDoS defense system consists of two major components: (1) temporal-correlation based feature extraction and (2) spatial-correlation based detection. It accurately identifies and detect DDoS attacks without changing existing IP forwarding mechanisms at routers. A brief summary of these knowledge based methods is given in Table 4.

iv. *Data mining and machine learning methods*

In [50] the authors proposed an effective defensive system called as NetShield to protect client hosts, network routers and network servers from becoming victims, zombies and handlers of DDoS flood attacks. It protects any IP-based public network on the Internet and uses preventive and rate limiting to eliminate system vulnerabilities on target machines. It enforces dynamic security policies for protecting network resources against DDoS flood attacks.

Chen et al. [51] introduces DDoS Container as a comprehensive framework for DDoS attack detection. It uses a network based detection method to defense complex and simple types of DDoS attacks and works in parallel to inspect and control ongoing traffic in real time. It covers stateful inspection on traffic flow streams

and correlates actions among different sessions by continuous monitoring of both DDoS attacks and legitimate applications. It terminates the session when it detects a DDoS attack.

Lee et al. [52] propose proactive detection method for DDoS attacks by exploiting an architecture comprising of a selection of handlers and agents that communicate, compromise and attack. It performs cluster analysis. The authors presented the results using the DARPA dataset, were each phase of the attack scenario is segregated well and can detect originators of a DDoS attack as well as the attack itself.

Sekar et al. [53] inspect the design space for in-network DDoS detection and propose a triggered, multi-stage approach that addresses both scalability and accuracy. They designed and implemented the LADS (Large-scale Automated DDoS detection System), which makes effective use of the data readily available to an ISP.

Rahmani et al. [54] designed a joint entropy analysis of for DDoS attack detection using multiple traffic distributions. The time series of IP- flow numbers and aggregate traffic sizes are statistically dependant and were this occurrence of an attack affects the dependence and causes a break in the time series for joint entropy values.

A low-rate DDoS attack detection difficult compared with the Normal attacks because of its similarity with normal traffic. In [55] defined two new information metrics: (i) generalized entropy metric and (ii) information distance metric, to detect low- KK DDoS attacks. The attack is detected based on the distance between legitimate and attack traffic. The generalized entropy metric is more accurate than the traditional Shannon metric [56].

In [57] early detection of flooding DDoS attacks are defined using FireCol, which is based on information theory. It is deployed in Internet service provider (ISP) level as a part of intrusion prevention system (IPS). The IPSs create virtual protection rings around the hosts to defend and cooperate by exchanging specific traffic information.

The approach described in [58] analyses characteristics of DDoS and flash crowd attacks and provides an efficient way to distinguish between the two in VoIP networks. The authors validated the method through simulation.

In [59] the authors present a wavelet transformation and probability theory based network anomaly detection approach. It is able to identify known as well as unknown DDoS attacks.

Zhong and Yue [60] implemented a DDoS attack detection model which extracts a network traffic and a network packet protocol status models and defines the threshold for the detection model. K-Means clustering algorithm is used to build initial threshold values for network traffic of Captured network traffic values. Packet protocol status model is built using Apriori [61] and FCM [62] for captured packets. When the current network traffic exceeds the threshold value, the network packet protocol status is checked to identify abnormal packets. If there are no abnormal packets exist, a new threshold value model is build based on the current network using k-means module.

A two-stage automated detection system is proposed in [63] for DoS attacks in network traffic. It is the combination of traditional change point detection method with wavelet transforms [64]. In [65], Li and Lee present a systematic wavelet based method for DDoS attack detection. DDoS attack traffic is detected using energy distribution based on wavelet analysis. Energy distribution over time has limited variation if the traffic keeps change its behavior over time.

Gupta et al. [66] use ANN to identify the number of zombies in a DDoS attack. Sample data is used to train a feed-forward neural network created using the NS-2 network simulator. The generalization capacity of the trained network is capable and it is able to calculate the number of zombies involved in a DDoS attack with test error.

Cheng et al. [68] proposes the IP Address Interaction Feature (IAI) algorithm considering abrupt traffic changes, interactions among addresses, many-to-one asymmetries among addresses, distributed source and concentrated target addresses. The IAI algorithm is designed to describe the critical characteristics of network flow states. A support vector machine (SVM) classifier, which is trained by an IAI time series with normal and attack flows, is applied to classify the state of current network flows and identify the DDoS attacks. It has higher detection and lower false alarm rates compared to competing techniques.

The method defined in [69] identifies flooding attacks in real time and also assess the strength of the attackers based on fuzzy reasoning. This process consists of two stages: (i) statistical analysis of the network traffic time series and (ii) identification and assessment of the strength of the DDoS attack based on an intelligent fuzzy reasoning mechanism.

Zhang et al. [70] define a Congestion Participation Rate (CPR) based approach for flow level network traffic to detect

Table 4 : Knowledge based DDoS Detection methods

Reference	Objective	Deployment	Working Mode	Remarks
Gil and Po-Letto [44]	Attack prevention	Between source and destination network	Centralized	Each network device maintains a MULTOPS data structure to detect attacks that deploy a large number of DDoS attack flows using a large number of agent and IP spoofing attacks.
Thomas et al.[45]	Attack detection	Victim side	Centralized	Inline packet processing is used by the Net Bouncer to differentiate DDoS traffic from flash crowd based on network processor technology.
Limwiwatkul & Rung-Sawang[47]	Attack detection	Victim side	Distributed	Attack signature models are constructed using TCP packet headers for DDoS attack detection.
Zhang and Parashar[48]	Proactive	Intermediate network	Distributed	A gossip based scheme uses global information about DDoS attacks by information sharing to detect attacks.
Lu et al.[49]	Attack detection	Edge router	Distributed	Exploits spatial and temporal correlation of DDoS attack traffic for detecting anomalous packet.
Wang.et. al[46]	Attack detection	Victim side	Centralized	Augmented Attack Tree model is used for the detection of DDoS attacks.

Table 5 : Datamining and machine learning based DDoS Detection methods

Reference	Objective	Deployment	Working mode	Remarks
Hwang et al.[50]	Attack prevention	Victim side	Centralized	Protects network clients, routers and servers from DDoS attacks using protocol anomaly detection
Li and Lee[52]	Attack detection	Victim end	Centralized	An energy distribution based wavelet analysis technique defined for the detection of DDoS traffic.
Sekar.Et.al[53]	Attack detection	Source side	Distributed	A triggered multi-stage approach is defined to acquire scalability and accuracy for DDoS attack detection.
Gelenbe and Loukas[73]	DDoS defense	Victim end	Centralized	Detects attack by tracing back flows automatically.
Lee et al.[62]	Attack detection	Source side	Centralized	Agent handler architecture along with cluster analysis is used to Detects DDoS attack proactively.
Rahmani et al[54]	Attack detection	Victim side	Distributed	A joint entropy analysis used for multiple traffic distributions to detect DDoS attacks.
Li and Li[65]	Attack detection	Victim end	Centralized	Wavelet transformation and probability theory are used to detect DDoS attacks
Dainotti et al[63]	Detection of DoS attack anomalies	Victim end	Centralized	Detects attacks accurately using combination of traditional change point detection and continuous wavelet transformation.
Zhong and Yue[60]	Attack detection	Victim side	Centralized	Unknown DDoS attacks are detected using fuzzy c-means clustering and Apriori techniques.
Xia et al. [69]	Detects flood attack and its intensity	Victim end	Centralized	Detection of DDoS flooding attack using fuzzy logic.

Xiang et al[55]	Detects low rate flooding attacks	Victim end	Centralized	New information metrics used to detect low-rate DDoS flooding attacks.
Gupta et al.[66]	Number of zombies identification	Victim end	Distributed	Uses ANN to evaluate the number of zombies in a DDoS attack.
Francois et al.[57]	DDoS flooding attack detection	Source end	Distributed	A DDoS flooding attack detection technique supports incremental deployment in real network.
Jeyanthi and Iyengar[58]	Flash crowd Detection	Victim end	Centralized	Detects DDoS attacks using entropy based analysis.
Prasad, ARMReddy ,KVGRao[15]	Flash crowd Detection	Router/ITM level	Distributed	Detects DDoS attacks using entropy variations.

low-rate DDoS (LDDoS) attacks. A flow of higher CPR value leads to LDDoS and subsequent dropping of the packets. It identifies DDoS attacks with high detection accuracy using correlation of subset of features.

In [71], authors defined an approach to detect botnet and their activities based on traffic behaviour analysis. Machine learning strategies are used to classify traffic behaviour and proved experimentally that botnet activities can be identified in smaller time windows with high accuracy.

In [72], low-rate DDoS attacks are detected using anomaly based approach. In low-rate DDoS attacks methods, attackers send malicious traffic at lower transmission rate to mislead traditional anomaly based DDoS detection techniques. The authors proposed two information metrics, generalized entropy metric and information distance metric. These metrics are used to measure difference between legitimate traffic and attack traffic to detect DDoS attacks.

In [73], a mathematical model is proposed to provide the benefits of DDoS defence based on dropping of attack traffic. The authors used an autonomic defence mechanism based on Cognitive Packet Network (CPN) protocol to tracing back flows coming into a node automatically. A summarized presentation of these methods in this category is given in Table 5.

IV. Traceback Mechanisms

Identifying attack source(s) through some mechanism to block or mitigate the attack at origin is referred as Traceback in DDoS defense. Implementing the traceback to identify DDoS source accurately is difficult because of, easy spoofing of source IP addresses, stateless nature of IP routing without knowing the complete path, link layer or MAC address spoofing and modern attack tools provides to implement intelligent attack techniques easily [74].

In [75], authors calculated entropy variations of network traffic to implement a traceback scheme. To detect an attack the difference of entropy values between normal traffic and the DDoS attack traffic is calculated. If the attack is detected, the traceback is initiated towards its upstream routers. The proposed scheme provides an advantage over traditional traceback approaches in terms of scalability and storage requirements in victim or intermediate routers. It stores only short-term information i.e, entropy values of successive time intervals in order to detect the DDoS attack.

In [76], authors presents a method for detection and traceback of low-rate DDoS attacks ,where low-rata attacks are very much similar to normal traffic and have more ability to hide their attack related identities in the aggregate traffic. Two new information metrics were introduced to detect low-rate DDoS attacks, which are generalized entropy metric and information distance metric. In this approach, difference between legitimate and attack traffic is identified through the proposed information metrics and are capable to detect the attack in prier hops earlier than counts mentioned in proposed schemes. These information metrics increase detection accuracy of the system and is capable of identifying low-rate DDoS attacks effectively by reducing false positive rates.

In addition to entropy variation scheme, other traditional reactive methods also exist to traceback DDoS attack sources [74]. In packet marking scheme, trace the path through upstream routers towards the attack sources i.e., zombies. It is a standard technique used in traceback implementations, however contains some inherent drawbacks. There exits two types of packet marking schemes i.e., probabilistic and deterministic packet marking.

In probabilistic packet marking (PPM), every router inserts its IP address probabilistically into the packets moving from source to destination. The method relies on the assumption that attack packets more frequent than legitimate packets. Once the attack is detected, the victim requests sufficient range of packets to reconstruct the path upto the attack source through embedded information within the packets. There is no specific fields defined in an IP packet for markings. Therefore, it utilizes infrequently used 16-bit fragment ID in IP packets for the markings [78]. However, this method has some major drawbacks. For instance, it is valid just for direct attacks. It cannot detect the original location of attack source just in case of reflector attacks

because the traced location is of reflector machines and not the actual zombies. Moreover, in a well distributed attack with a reasonably sizable amount of zombies, the possibility of wrong construction of the path increases. It's additionally an acknowledged indisputable fact that nowadays, due to large number of zombies, the attackers reveal real IPs of zombie machines and hence the sources are already discovered. The packet marking scheme places computational overhead on intermediate routers when traceback is initiated. In addition that victim remains available during the process of traceback to send control messages to upstream routers. The bandwidth is saturated due to attack impacts the control messages are dropped, it leads to wrong construction or misconstruction of attack path.

Table 6 : Trceback mechanisms of DDoS attacks

Existing mechanisms	Traceback Working Principle	Advantages	Drawbacks
Hash Based IP Traceback	20 byte IP header and first 8 bytes of payload is logged for every packet by the Intermediate routers. Hashing is performed on the logged data.	It requires low storage and protects from eavesdropping.	Increases the false positives and Overhead in generating 28 byte hash for the packets.
Algebraic approach to IP traceback	Polynomial functions are used to generate traceback data and stores in unused bits of IP header.	Noise elimination and multiple path reconstruction are possible and robustness is improved.	Variations will occur in random full path tracing schemes and poor scaling.
Enhanced ICMP traceback-Cumulative path[77]	Intermediate routers generate Itrace-CP message. The victim uses this message to trace the attack path and source.	In less time it constructs an entire attack path.	A change to be made to the router and space is required to process packets.
Advanced and Authenticated scheme for IP Traceback.	Traces the origin of IP packet with 11 bit hash and distance field of 3 bits are generated using 32 bit IP address and stored in IP header.	Low overhead on router and network and computational complexity is very less.	No time synchronization between victim and the router and Secret key is shared between routers.
Fast Internet Traceback	A packet marking scheme and path reconstruction algorithms are used at routers and end hosts to receive the packet markings.	Minimal Processing time is required to traceback the attack source for less flow.	False positive rates are high.
Deterministic packet marking [78]	The source of an attack flow is identified by employing tracing information inscribed in the packet.	Traceback process requires small number of packets.	No overload prevention and Increase in packet header size.
Probabilistic packet marking [78]	Routers mark the packets with probabilistic path information and victim reconstructs the attack graph.	Efficiency and easy implementabilty over Deterministic Packet Marking.	More number of packets and computational work involved in traceback process. Probability of finding the source traced is low.
Flexible Deterministic Packet marking [74]	Large scale IP Trace back scheme which encodes the information and reconstruction the attack path using mark recognition.	Traceback process requires relatively less number of packets and minimal Computation work. Probability of finding a source is high.	Packet processing consumes more resources.
IP Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots[16]	Honeypots are used as the proxy servers and the attack source is traced through honeypot entries.	Low overhead on server and no direct damage to the server.	Processing delay and cost consuming process for honeypots.
Decision tree and grey relational	Decision trees are constructed for the traffic flow with respective upstream routers and analyses the	Upstream routers can be easily identified for attack strength.	Complicated process when for the large size network.

analysis[18]	attack strength.		
New information metrics[17]	Information distances are calculated for each flow in the network.	Less computational complexity for calculating the information distance.	Accurate detection is not possible.

In deterministic packet marking (DPM), the router inserts its IP address deterministically into the IP packets. This scheme was introduced to overcome the drawbacks of probabilistic packet marking, because it has easy implementation and needs less computational overhead on intermediate routers. However, it also has the limitations. In this scheme, packets are marked only by first ingress edge router with the information i.e., the entire is not stored as in PPM. Therefore, it needs even additional packets to reconstruct the attack path [74]. Furthermore, it additionally has some limitations similar to PPM scheme discussed above. This approach is less efficient than traditional schemes.

In packet logging scheme [74] which is also referred as Source Path Isolation Engine (SPIE), the information of each packet is stored or logged at routers through which the packet is passed. The routers in this approach are termed as Data Generation Agents (DGAs). The stored information of the packet includes constant header fields and first 8 bytes of the digests (payload hashed through many hash functions). Bloom filters are used to store these DGAs, which is a space-efficient data structure and is capable of reducing storage requirements by large magnitude.

In ICMP messaging scheme [77], routers are programmed to send ICMP messages together with the network traffic. The ICMP packets contain path information such as source address, destination address and authentication parameters etc. A typical router with this scheme normally sends one ICMP messaging packet for every 20,000 packets passing through it i.e., a traceback message is sent with the proportion of 0.005 percent of the network traffic [74]. A summarized presentation of these methods in this category is given in Table 6.

V. Conclusion and Future Work

In this paper, we have presented a broad classification of various DDoS attacks, DDoS Defensive architectures such as Source-end, Victim-end and Intermediate architectures. We have also presented various Detection and mitigation mechanisms such as Statistical based, Soft-computing based, Knowledge based and Data mining based approaches along with their advantages and disadvantages based on where and when they detect and respond to DDoS attacks. Finally, we presented an overview of traceback mechanisms of DDoS attacks such as packet marking schemes, information distance, honey pots and entropy variations. Practically it is very difficult to design and implement DDoS defense and detection. In real time networks, fulfilling all the requirements for DDoS detection is not possible and to accomplish this, various performance parameters need to be balanced against each other delicately and appropriately.

References Références Referencias

1. T. Peng, C. Leckie, , and RMrao, K. “Survey of network-based defense mechanisms countering the DoS and DDoS problems.”, ACM Computing Survey, 39, 3:1–3:42. (2007),
2. V. Chandola,, A. Banerjee, , and V. Kumar, ,“Anomaly detection: A survey. ACM Computing Survey,” 41, 15:1–15:58. (2009)
3. G. Loukas, and ¨G. Oke, “Protection against denial of service attacks: A survey.” Computer. Journal. 53, pages-1020–1037. (2010)
4. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita “Surveying port scans and their detection methodologies.” Computer. Journal., 54, Pages-1565–1581. ,(2011)
5. H. J. Kashyap, and D. K. Bhattacharyya “,A DDoS attack detection mechanism based on protocol specific traffic features.”, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India, 26-28 October, pp. 194–200. ACM. , (2012)
6. S.Lin, and T.C.Chiueh “A survey on solutions to distributed denial of service attacks.”, Technical Report TR201. Department of Computer Science, State University of New York, Stony Brook. ,(2006)
7. 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.
8. 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.
9. Ranjan. S, Swaminathan. R, Uysal. M, and Knightly. E, “DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection”, IEEE INFOCOM’06, 2006.
10. 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.
11. Puri. R, “Bots and Botnet – an overview,”, Aug. 08, 2003, [online] http://www.giac.org/practical/GSEC/Ramneek Puri GSEC.eps

12. Todd B., "Distributed Denial of Service Attacks," Feb. 18, 2000, [online] http://www.linuxsecurity.com/resource files/intrusion detection/ ddos–whitepaper.html
13. CERT, "Denial of Service Attacks," June 4, 2001, [online] http://www.cert.org/tech tips/denial of service.html
14. 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.
15. K Munivara Prasad, Dr. A Rama Mohan Reddy and Dr K Venugopal Rao, Discrimination of Flash crowd attacks from DDoS attacks on internet threat monitoring (ITM) using *Entropy variations*, IEEE African Journal of Computing & ICT , Vol 6. No. 2, pp- 53-62, June 2013.
16. K Munivara Prasad, Dr. A Rama Mohan Reddy , IP *Traceback for Flooding attacks on Internet Threat Monitors (ITM) Using Honeypots* , International journal of Network Security & Its Applications (IJNSA),ISSN : 0974 - 9330, Vol.4, pp 13-27, No.1,Jan 2012.
17. Y. Xiang., Li, K., and Zhou,, "Low-rate DDoS attacks detection and traceback by using new information metrics, " IEEE Transaction on Information Forensics. Vol: 6, pages: 426–437, 2011.
18. Y. C Wu,., Tseng, H. R., Yang, W., and Jan, R. H., "DDoS "detection and traceback with decision tree and grey relational analysis.,", International Journal of Ad Hoc and Ubiquitous Computing, Vol-7, 121–136.2011.
19. 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),
20. 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)
21. 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)
22. 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)
23. 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)
24. 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)
25. 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)
26. Y. Gilad., and A. Herzberg, A., ''LOT: A defense against IP spoofing and flooding attacks,'' ACM Transaction on Information. Systems. Se, 15: (2012).
27. S. N. Shiaeles,., Katos, V., A. S Karakos, , and Papadopoulos, B. K., ''Real time DDoS detection using fuzzy estimators,'' Computer. Security., 31: pages:782–790 (2012).
28. 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).
29. C.L. Chen "A new detection method for distributed denial-of-service attack traffic based on statistical test",. Journal of Universal Computer Science, 15, 488–504. ,(2009)
30. 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) "
31. A. Akella, , 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)
32. 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).
33. 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).
34. 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).
35. 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).
36. 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.
37. 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)
38. 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)
39. 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)
40. 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)
41. K Munivara Prasad, Dr. A Rama Mohan Reddy ,Modelling and Counter measures of Flooding attacks to ITM using Botnet and Group Testing, Global journal of Computer Science and Technology (GJCST), Volume11, Issue 21,pp-15-24,Dec 2011,
42. P. Kumar, and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier." Computer Communication, 34, pages-1328– 1341. (2011)
43. C. Scott, and R.Nowak, A neyman-pearson approach to statistical learning." IEEE Transaction on Information Theory, 51, pages-3806–3819. (2005)"
44. 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)
45. 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)
46. 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
47. 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)"
48. G. Zhang, and Parashar, M. "Cooperative defence against DDoS attacks." Journal of Research and Practice in Information Technology, 38, 1–14. (2006)
49. 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)
50. 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)
51. 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)
52. 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)
53. 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)
54. 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)
55. 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)
56. Shannon, C. E. (1948) "A mathematical theory of communication." Bell system technical journal, 27, 397– 423.

57. 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)
58. 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)
59. 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)
60. 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)"
61. 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)
62. 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)
63. 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.
64. A. Haar, A. (1910) Zur "Theoriederorthogonalen Funktionensysteme." Mathematische Annalen, 69, 331– 371.
65. 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)
66. B. 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)
67. R. Yan, Q. Zheng, Niu, G., and Gao, S "A new way to detect DDoS attacks within single router." Proceedings of the 11th IEEE Singapore International Conference on Communication Systems, Guangzhou, China, 19-21 November, pp. 1192–1196. IEEE CS. . (2008)
68. 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)
69. 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)
70. C. 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)
71. D. 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).
72. 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).
73. E. Gelenbe, and G. Loukas,. "A self-aware approach to denial of service defence." Computer Networks, 51, pages:1299–1314. (2007)
74. K. Kumar, A.L. Sangal, and A. Bhandari, "Traceback Techniques Against DDoS Attacks: A Comprehensive Review," Proceedings of IEEE 2nd International Conference on Computer and Communication Technology (ICCCT), 491–498 (2011).
75. Yu, S., Zhou, W., Doss, R., and Jia, W., ''Traceback of DDoS Attacks Using Entropy Variations,'' IEEE Transactions on Parall. Distr., 22: pages:412–425 (2011).
76. Y. Xiang, Li, K., and Zhou, W., ''Low-rate DDoS attacks detection and traceback by using new information metrics,'' IEEE T Inf. Foren. Sec., 6: 426–437 (2011).
77. H.F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," CERT Coordination Center, Special Report: CMU/SEI-2002-SR-009 (2002).
78. K. Subhashini, and G. Subbalakshmi, ''Tracing sources of DDoS attacks in IP networks using machine learning automatic defence system,'' International. Journal. Electron. Commun. Comput. Eng., 3: 164–169 (2012).