Shielding techniques for Application Layer DDoS Attack in Wireless Networks: A Methodological Review

Kiran Salunke · U Ragavendran

Received: date / Accepted: date

Abstract In today’s world the wireless networks are widely preferred as a communication medium as these are infrastructure less networks. The application layer of these networks is targeted by attackers because it is responsible for actual data exchange with privacy of end users. As human dependency on wireless networks is increasing the DDoS attacks i.e. distributed denial of service attack which becomes a nightmare for the researchers. This attack is one of the most devastating attacks that can be executed on web-servers and congest the network keys like socket connections, CPU cycles, and memory database. In this current mobile computing world the necessity of DDoS attack management is significantly increased because this attack can degrade the entire web experience. Further, this DDoS attack is commenced along with the legitimate requests so it is also important to differentiate DDoS attack from other similar Events. This review endeavors to explore with more emphasis on various privacy preservation scheme for application layer DDoS attack and its management stages like prevention, detection, mitigation and Differentiation along with comparative statement of prominent techniques discovered in each stage. This methodological survey report shall lead the way to researchers and network designers to suit the specific management scheme to provide the complete protection of wireless networks from DDoS attack.

Keywords Network Security · DDoS attack management · Mobile Adhoc network · Wireless networks · Privacy preservation · Data Security · Data Encryption · Machine Learning

Kiran Salunke
SVKM's NMIMS MPSTME Shirpur(India)
E-mail: kiran.salunke@nmims.edu

U. Ragavendran
SVKM's NMIMS MPSTME Shirpur(India)
E-mail: U.Ragavendran@nmims.edu
1 Introduction

Now-a-days vital services like Banking, E-commerce and browsing information is available to user via web applications without time and space constraints. Even business owners and individual governments of large number of countries made their service available to user on their websites. Seeking Help from these applications we can perform numerous task like buying and selling, performing financial transactions, setting up a small or large E-Commerce business and availing schemes from governments. Due to these web applications become very much important to all these service providers. As these web applications becomes important ultimately they become prime target of attackers. These attackers might be influenced by several factors like financial gain, business competition, a part of cyber warfare or policy disagreement. The prime aim of attackers is to make web services inaccessible to genuine users by disturbing web applications. Average Financial Loss per hour Due to downtime to institutions is $52000 to $440000. These types of attack is called as DoS attacks. DoS stands for Denial of Service Attacks. DoS is evolving every day ever since it was coined first. The most efficient way to execute this DoS attack is Distributed Denial of Service (DDoS attack). Number of Distributed Denial of Service Attacks are increased by 240% in 2018 from 2014. 2019 is worse than 2018 in trending of DDoS Attack. There is almost 200 % hike in DDoS Attack Execution in 2019 from year 2018. Attack volume is also increasing manifold in 2019 as compare to 2018.

Government websites regularly becomes victim of these types of DDoS Attacks which inherently exposes lack of security measures in these websites. The official websites of govt. like India, USA, Brazil and Ireland were severely affected due to DDoS attacks. Banking websites are also on target list of attackers as it is directly affecting economy of a country. Latest examples are HSBC bank, bank of America etc. and it is due to fact that now customers do not hesitate to buy or sell online. DDoS attack is very much capable of disturbing internet connectivity of million number of users as it can also affect DNS service Provider. In the latest happenings a large DDoS attack executed on Telegram with 200-400 Gbps during Hong-Kong Protest. In August 2018 The Bank of Spain experienced DDoS attack which took it offline for few hours[1]. Amazon cloud computing division AWS recently experienced a long DDoS attack which lasted around 8 hours.[2]. In the first quarter of 2019 March was busiest month in terms of DDoS Attack. March 16 with 699 attacks was pick for the attackers along with noteworthy upwelling occurred on January 17 with 532 attacks[3]. according to latest report in every 60 seconds 16 DDoS attacks take place at a rate of 622 Gbps[31].

Now with the terms like IoT more and more devices are coming on online platform, so other systems like Transportation, Heating System also gets affected by DDoS attack. DDoS evolving as time is ticking that’s why it is major threat to world’s opulence. Table 1 illustrate some important events occurred in last 5 years in aspect of DDoS Attacks.
Fig. 1 Dynamics of the number of DDoS attacks in Q1 2019 [4]

Table 1 Impact of DDoS Attack in recent time

| Victim                          | Role of victim | Year  | Motive                                      |
|--------------------------------|----------------|-------|---------------------------------------------|
| Telegram[3]                    | messenger      | 2019  | To take down communication service          |
| Bank of Spain[1]               | Banking website| 2018  | To block Financial transactions             |
| Github [5]                     | Hosting service Provider | 2018  | To make Servers offline                     |
| Amazon AWS [6]                 | Cloud Computing Division | 2019  | Parts of AWS Services were taken offline     |
| Brazilian sport ministry[7]    | Govt. Website  | 2016  | To take down Rio Olympics site              |
| Spanish constitutional website | Government Website | 2017  | To take down Several websites               |
| HSBC [9]                       | Banking website| 2016  | To block Financial transactions             |
| Bank of America [35]           | Banking website| 2016  | To block Financial transactions             |
| Dyn [10]                       | DNS Service    | 2016  | To take down Twitter                        |
| European ISPs [11]             | Internet Service Provider | 2020  | To make server unavailable                   |

2 Background

A focused work by hackers to bound or totally remove web traffic to a specific website, server or online service is called as a Denial of Service attack or DoS attack. It can be performed in numerous ways but the DDoS or “Distributed denial of service” attack is very famed plus ubiquitous, which contains compelling or tricking a cluster of computers into overflowing a server with data until the point where it become unusable. A DDoS attack downpours a server
with lot of requests that it becomes insensitive effectually shutting its service down. A DDoS attack are efforts to crowd a server with meaningless traffic so the websites on which it operates runs slowly or take down it completely.

A DDoS attack will either back sites off to a slither, or make them altogether difficult to get to on the grounds that it top off a server’s transmission capacity with so much information and for that aggressor need a great deal of information. Which implies that to arrange such an attack you either need a great deal of all around composed frameworks around the world. To accomplish this assailants use "Botnet"

To accomplish an objective a system of contaminated Computer which, under the order of a solitary ace Master, cooperate called as botnet. An additional layer of inconvenience included by misleading Computer into DDoS attack. These blameless Machines known as "reflectors", are sent a tricky association request from one of the "zombie" System in the botnet. That contact solicitation will fool the reflector into intuition the objective server is attempting to connect with them, and like a decent machine it will attempt to reach back so as to perceive what it needs. You get enough guiltless "reflectors" all pinging the server simultaneously, and you have yourself a DDoS attack. A botnet depends on two things: for one, it needs a huge system of contaminated gadgets, known as "zombies", to do the snort work and hard work for whatever plot the programmer has arranged. Also, you need somebody to really order them to accomplish something, habitually called the Command and
Control focus, or “bot herder” (yet not "the warlock" for some crazy explanation). When those things are set up, a botnet ought to be all set reason some commotion.

US remain frontier in aspect of distribution of Botnet Servers in the world. The Netherlands slides up to runner up from third in Q4 2018. Third position taken by to Russia rises from seventh. China (7.51%) is now on fourth position. Greece and Germany moves out of top 10 as their position is taken by Vietnam in seventh, and South Korea respectively.

There are three different types of DDoS attack. Volumetric or volume based, protocol based and Application layer DDoS Attack. All these type are having different aim or goal to achieve. The goal of Volumetric DDoS attack is to saturate Bandwidth, goal of protocol based DDoS Attack is to consume server Assets and application layer DDoS Attack is to crash web server.

There are essentially two classes of DDoS Attacks Network layer DDoS Attacks and Application DDoS Attacks. The aim of the network or transport layers’ attacks is to over-burdens a system or server and devours the entirety of its accessible assets. While Application DDoS Attacks explore the rupture or helplessness in a website composition of an application to overpower the server or database driving a web application with the expect to push it down to the edge of total collapse. Such Attacks copy genuine client traffic, constructing them tougher to recognize.

Fig. 3 country wise distribution of botnet servers Q1 2019
A Flash Event is a kind of system traffic that likewise makes a refusal of administration authentic clients of a web administration. According to [50], a Flash Event (FE) is like HR-DDoS (high-rate DDoS) Attack where a huge number of real clients attempt to get to a specific processing ability. This unexpected flood in genuine rush hour gridlock is basically because of some breaking news occurring the world over like the distributing of Olympic calendar or new item dispatch by organizations like Apple, Samsung, and so forth. It causes the less than ideal conveyance of reactions from web administration and along these lines, requires quick activity. As there are just a couple of parametric contrasts among FE traffic and DDoS Attacks, it’s very difficult to separate the two[92].

Many common characteristics shared by Together HR-DDoS attacks and FEs like a delay in responses from the webserver modification in the rate of traffic volume etc. but there are some parametric alterations among them. The request rate per source IP is higher in HR-DDoS attacks than FEs (Flash events). Network flow, Data traffic per IP Throughput are the aspects on which we can categorize FE DDoS attack.

3 DDoS Attack Management

To defend webserver from DDoS attack, defence strategy consist of four different stages namely prevention, detection, differentiation and mitigation.
Fig. 5 Different Stages of DDoS Protection

Fig. 4 shows entire taxonomy in DDoS Attack Management and fig. 5 shows when to apply different level of Defences in DDoS attack time span. First we will discuss about prevention.

3.1 Prevention

Ingress and egress filtering which consider packet evenness as the measures to avoid from DDoS attacks. It have little employment difficulty and is apparent to the client-side but however it leads to wastage of resources and it unable to prevent web servers from forged IP address.

Route Based distributed packet filtering prevents spoofed DDoS attack packets from getting their objectives before they can divulge loss by using routing information but its lack in terms of scalability.

History-based IP filtering approach can obstruct the attacking traffic while enabling the authentic users to pass the filters. It shows that the proposed methodology can improve the CPU use fundamentally during the DoS attacks, contrasted with a current protection stage and the first SIP usage however it neglected to address the issue of intrusion detection.

Honeypot plot recognizes the intruders at numerous points of the system. When the swayed territory is discovered, the data is sent to a staggered design to stop the range of the influenced section to the honeypot by making a barrier framework against the Intruders. Recreation results show that the proposed strategy diminishes the false positives and enhances the Packet rate and throughput however it expects attackers will utilize conventional technique to launch Attack.

SoS (Secure Overlay Services) used a hash based routing and clustering-based detection algorithm to resist the threat of intelligent DDoS attack but its responses are limited for public servers.

The privacy-preserving and Readily deployable DDoS prevention amenities is offered by Umbrella. To provide real time DDoS prevention, with only autonomous placement at the victim’s ISP and without changing Internet core or end-host, umbrella can be implemented which makes it immediately deployable however it’s not useful for small websites.
Table 2 DDoS prevention Schemes

| Technique               | Author & Year | Approach                                                | Findings                          | Constraints                                |
|-------------------------|---------------|---------------------------------------------------------|-----------------------------------|--------------------------------------------|
| Umbrella [71]           | Liu et. al. 2019 | Multi-layer defense architecture                        | Can deal with large scale attacks along with privacy | Only useful for small websites |
| Ingress filtering [54]  | Ping Du et. al 2010 | Dropping IP packets not matching domain Prefix & Eliminate IP Spoofing | Does not prevent Forged IP Address |                                           |
| Egress Filtering        | Ping Du et. al 2010 | Outbound filter make sure that only assigned IP address is used | Protect other domains             | Wastage of resources                       |
| Route Based distributed packet filtering [79] | Kihong Park 2003 | Use of Routing Information | Synergistic filtering               | Not scalable                               |
| IP filtering based on history [107] | Zhaou et al 2009 | Already built IP Address database is used | No need to study entire network | Intrusion detection not possible |
| SoS [63]                | Chi Hyun In 2005 | Hash based Routing is used                              | Distributed System                | Not recommended for public servers          |
| Load Balancing [46]     | M. Belyaev 2014 | Increasing Bandwidth on critical connections           | Multiple server Architecture      | Costly & Complex                           |
| Honeypot[88]            | Selvaraj et. al. 2016 | IP allow attacker to attack honeypot not actual system | Detect attackers                  | It assumes attacker will use traditional method to launch attack |

Even though lot of research work has been carried out in DDoS Attack prevention schemes but still they are not sufficient to break DDoS attacks since there are always susceptible to innovative and mixed attack types for which attack patterns are not exist in the database. Table 2 illustrates different DDoS attack prevention Schemes along with their findings and constraints.

3.2 Detection

This phase of DDoS attack defence is need to perform during ongoing DDoS Attack so that it can successfully eliminated using mitigation techniques. Anomaly-based, Signature-based and combination of these i.e. Hybrid detection are the Detection tactics which are categorized by considering analysis
methods. We will discuss about Signature Anomaly based detection schemes in review.

3.2.1 Signature Based Detection Scheme

Pattern detection, Misuse detection, and Rule-based detection or Knowledge-based are the alternative names to Signature-based detection schemes. This method gathers facts about numerous attacks and system experiences catches the essential behaviour such as network traffic occurrences, protocol stipulations from the available datasets.

Garcia et. al. makes use of the developed knowledge to recognise the happening of abnormal events and fixed an alarm if an DDoS attack is recognised. To instances the attack occurrences Agarwal et. al. counterparts the inward traffic with the stored patterns with the help of used index of ‘patterns or signatures’ of public attacks. This methodology is successful just if there should arise an occurrence of known attacks in light of the fact that fresh attacks or marginally altered from the past and referred to attacks not get recognized as they are not having marks inside database. The marks and examples of different attacks comprise a few fields of IP packets like the keywords inside payload of a packet, ports and source and target IPs. Such frameworks are too slow and rely upon the deficiency conditions (or conduct) of the unfortunate casualty framework. Flaw conditions may emerge because of an enormous number of open TCP connections, unnecessary use of data transfer capacity and because of the surpassed complete throughput. Techniques like SNORT, BRO, IDES, and INBOUNDS are the some of the signature based detection approaches. The network administrator follows this approach nowadays.

Wu et. Al. Proposed a recognition technique comprises of a traffic pattern corresponding algorithm sorting trees. It discrete the DDoS traffic from normal traffic by examining transmission rate, the outgoing & incoming packet rate & SYN, TCP and ACK flag rate the classification trees.

Limwiwatkul Rungsawang proposed a pattern corresponding algorithm is utilized to identify the traffic stream which is indistinguishable from attack stream and searches for the source of the attack. In this authors break down the TCP/IP packets in contradiction of some well-checked guidelines and circumstances to recognize the attack and normal traffic.

Thapngam et. al proposed a scheme in which it attack traffic is recognized use the transmission rate. This investigation shows that high transmission rate of attack traffic when contrasted with genuine system traffic in light of the fact that the slave specialists under the order of their master produce the attack traffic in a brief timeframe outline while the normal traffic sits tight for the server’s reaction in this way expand the timespan. Such techniques can’t identify effectively in light of the fact that the attackers can without much of a stretch direct the copy attack traffic headed for the object utilizing FE.

Thomas et. al. proposed a recognition scheme known as NetBouncer that readies a database of real clients. On the off chance that the approaching packets don’t have a place with an authentic client, at that point the packets
Table 3 DDoS prevention Schemes

| Technique | Author & Year | Approach          | Constraints                                      |
|-----------|---------------|-------------------|--------------------------------------------------|
| SHIELD    | Garcia et. al. 2004 | Traffic Pattern | only useful for known attack                     |
| SNORT     | Gupta et al. 2012 | Traffic Pattern | only useful for known attack                     |
| BRO       | Gupta et al. 2012 | IP Address        | System is too slow                                |
| INBOUNDS  | Xia et al. 2005 | Transmission Rate | does not work in case of Mimicked traffic         |
| Netbouncer| Thomas et. al. 2003 | Legitimacy Test | It’s a time consuming Task                        |

want to demonstrate their authenticity through a progression of authenticity tests. The novel clients are included in database in the event that they finish the assessment and send a suitable amount of packets up to point where session window terminates.

Signature-based detection approach effects in good recognition accuracy with the little false warnings as it can reveal only known attacks. However by adjusting the attack patterns or by launching attacks with minor deviations which is called as zero day DDoS attacks continue to be undisclosed by this method. Table 3 illustrates Signature Based DDoS Attack Detection Schemes along with constrains. Table 3 Signature Based DDoS Attack Detection Schemes

3.2.2 Anomaly Based Detection Scheme

Novelty detection, behaviour based, outlier detection or one class learning scheme are the other names of anomaly based detection which is proficient of identifying novel, unfamiliar and fresh (anonymous) attacks.

Wang et. al. proposes skyshield technique which protect from application layer DDoS attacks, they structure and actualize such a framework by taking preferences of the sketch strategies. First by computing Hellinger distance it figured the disparity between outlines in two sequential discovery cycles after that they utilize the anomalous sketch got from the last identification cycle to keep away from the turnaround computation of IP addresses and finally they have utilized bloom filters and the CAPTCHA systems to ensure the adequacy of SkyShield. The test results show that SkyShield can adequately moderate application-layer DDoS attacks and represent a restricted effect on ordinary clients however given plan Unable to identify attack when request rate is expanded slowly.

Bhuyan et.al. Developed a DDoS attack detection by increasing the gap among genuine traffic and bogus traffic. False alarm frequency drops considerably in identifying DDoS attacks. It makes use of proximate real-time IP traffic traces on testbed network for research validation which show that the IP traceback scheme can efficiently catches all attacks from zombie network.
Behal et al. proposed D-Face scheme which D-FACE defense system consist of an ISP network of various boundary level PoPs. As part of defense solution to these PoPs, memory computational overheads of a victim-end are distributed with the help of a comprehensive entropy based distributed mathematical model. D-FACE is adaptable as it kills the effect of genuine FEs bit by bit as well as it hinders the DDoS attack promptly. It is mechanized as without human intercession it portrays and channels the attack traffic. it is community-oriented as every one of the PoPs collaborate with one focal PoP implementer where the multifactorial recognition metric is figured.

Behal et al. come up with D-FAC system which utilizes processing summed up Divergence between arrange traffic streams to distinguish various kinds of FEs and DDoS attacks based on source IP address. D-FAC is conveyed at various limit level PoPs of an damaged individual system to disperse the memory computational overheads between these PoPs.

Zhao et al. addresses this issue with CDA classification detection algorithm. The tale technique can adequately recognize AL-DDoS attacks, which has incredible reference an incentive for further investigation of DDoS attack and its successful identification. As we have examined, there is at present an absence of investigation on major bot-net attacks, a huge number of zombie machines.

Hameed et al. proposes scheme called as HADEC which captures live network traffic, forms it to log applicable data to sum things up structure, and uses MapReduce and HDFS to track recognition calculation for DDoS flooding attacks. HADEC settles the adaptability, memory wastefulness, and procedure unpredictability concerns of ordinary arrangement by using parallel data handling guaranteed by Hadoop. The assessment results demonstrated that HADEC would require under 5 min to process (from catching to distinguishing) 1 GB of log document, created from approximately 15.83 GBs of live traffic traces. The general identification time can be additionally decreased to couple of seconds with the help of little log record.

Musa et al. Recommended a detection of HTTP DDoS centered on cloud with the help of arithmetic method with the covariance matrix. The recognition phase perceive an alternate sort of HTTP flooding attack dependent on attack conduct by 2 algorithms branded as preparing and testing. A preparation calculation was utilized to build typical examples of system traffic, and the analysis calculation was utilized to decide the kinds of traffic got. The results acquired from this exploration had been assessed by utilizing the disarray grid to quantify recognition execution and give consequences of internal and outside cloud conditions.

Hoque et al. recommended a technique which detects DDoS at the victim end in real time at the application layer. The planned work used programming and equipment embraced from the system made to recognize typical from counterfeit traffic continuously. Pre-processor, equipment module, and security director were three fundamental segments consolidated into the system, which handled Packet rate, source IPs and source IPs file variety to identify the attack.
Johnson Singh et al. Presented a recognition plan to figure low and high Rate of DDoS attack. Registering various HTTP GET solicitation, entropy, and change for every link performs the discovery. The 20 s time window utilized for counting HTTP GET demands.

Liao et al. recommended a scheme to identify application layer DDoS attacks which consist of user access frequencies, frequency request and time interval. Specially concentrating frequency request as well as on request time interval. As compare to an attacker Time span for a regular user may be higher, as a usual used to devote additional period for browsing interesting pages. The time interval for the current and following requests is shorter which is not considered in technique.

Singh et al. Presented a technique that use machine-learning approach to detects HTTP DDoS attack by distinguishing botnet from genuine users in identifying attack traffic, genuine traffic, and trash traffic. The given system performs scrutiny versus user behaviour in place of observing the whole traffic as it’s deployed as proxy. The recommended work inspects consumer conduct to identify mischievous request detects the botnet source against the web server.

Singh and De detects HTTP DDoS attack using used a genetic algorithm (MLP-GA) with the help of multilayer perceptron. A typical client has an explicit time interval, as a real client searches and peruses while getting to a page and when stirring to different pages. The recognition system recommended by the analysts tallies the quantity of HTTP GET demands got by the web server and ascertains the quantity of IP addresses focusing on the server more than 20 seconds. The recommended identification additionally reviews the port number utilized by HTTP DDoS, as ports utilized by HTTP DDoS attackers are shifted and stay open. The discovery strategy utilized fixed edge length to direct recognition, as indicated by these specialists, static convention lengths utilized by HTTP DDoS assailants.

False signal ratio increases due to online investigation, handling a huge amount of data and the due the occurrence of ambiguity in data which are the crucial defies for this approach. Unverified methods are embraced for catching unacquainted attacks while verified and unverified techniques are pictured for monitoring the enormous quantity of data. Real-time detection is not performed by such schemes. Table 4 illustrates Anomaly Based DDoS Attack Detection Schemes along with findings and constrains.

3.3 Mitigation

This phase of DDoS Defence is need to execute after confirming that the DDoS Attack is executed on a web server. Mitigation process ensures that the all legitimate users will complete request by reducing severity of DDoS attack. Mitigation phase again classified into two type’s i.e. Filtering Based mitigation System and Capability Based mitigation System.
| Technique     | Author & Year | Approach                  | Findings                                      | Constraints                                                                 |
|---------------|---------------|---------------------------|-----------------------------------------------|-----------------------------------------------------------------------------|
| Skysheild[98] | Wang et. Al. 2018 | Divergence of Sketch      | Able to detect app layer DDoS attack          | Unable to detect attack when request rate is increased at slow rate         |
| EL-DAT[50]    | Bhuyan et. Al. 2016 | Extended Entropy          | Able to detect DDoS Flooding attack           | Unimpressive false positive rate                                           |
| D-FACE[45]    | Behal et. al. 2018 | Source IP Entropy         | Early detection of App layer DDOS Attack      | Suffers from computational & memory overhead                               |
| D-FAC[44]     | Behal et. al. 2018 | Divergence                | Able to detect app layer DDoS attack          | Suffers from problem of secure communication & Cost                        |
| CDA[105]      | Zhao et. al. 2018 | Entropy of URL per IP     | Able to detect HTTP flood attack              | Does not work for leveraging Attack workload                               |
| HADEC[61]     | S. Hameed et. al. 2018 | Source IP Entropy       | Able to detect HTTP flood attack              | Does not address False alarm Rate issue                                    |
| CBDA[37]      | S. Musa et. al. 2017 | Co-variance Matrix       | Able to detect HTTP flood attack in Cloud     | Does not work for Flash crowd workload                                       |
| FPGA[?]       | N. Hoque et. al. 2017 | Source IP Entropy        | Able to detect HTTP flood attack              | Does not talk about True Negative rate                                     |
| ANN[64]       | K. Johnson et. al. 2016 | Source IP Entropy & Variance | Provides high Detection Rate                  | Take long time to converge reasonable fitness value for weights           |
| Feature Extraction[68] | Q. LIAO et. al. 2015 | Time interval for HTTP GET Request | Able to detect HTTP flood attack              | Does not talk about True Negative rate                                     |
| MLP-GA[89]    | Singh & De 2016 | HTTP get Count            | Able to find Low rate DDoS attack             | Take long time to converge reasonable fitness value for weights           |
| ASVM[76]      | Oo et. al. 2016 | Packet Variance          | Able to detect HTTP flood attack              | Does not Work for Sophisticated attacks                                    |
### Table 5 Filtering Based Mitigation Techniques for DDoS Attack

| Technique | Approach | Findings                  | Constraints                     |
|-----------|----------|---------------------------|---------------------------------|
| Integrated inter-serves[73] | RR protocol | bandwidth is assured      | Overconsumption of bandwidth   |
| Differentiated Services[73] | IP Header | Allocation of resources   | Co-operation of multiple domain required |
| Class based queuing[73] | IP header | Maintain QoS during DDoS  | Difficult to maintain Queues   |
| Resource Pricing[73] | DGAP protocol | Desirable client get access | Prices for legitimate user increases |
| Pushback[73] | attack signature | Effectively Mitigate DDoS Attack | Not effective for DDoS attack |
| Throttling[73] | Throttle Rate | Prevent server from going Down | Hard to decipher to traffics    |
| StopIT[70] | End host based traffic analysis | Has less deployment overhead | Need to build filters          |
| AITF[40] | Construct level Path | Has less deployment overhead | Have high false positive rates |

### 3.3.1 Filtering Based System

This is amid the initial work to report DDoS attack. This section discusses eight different works like integrated inter-serves, IP trace back, class based queuing, resource pricing, pushback and throttling. These systems mitigate DDoS attack by filtering attack traffic. These systems are not widely adopted due to their deployment hurdles. Table 5 illustrates Filtering Based DDoS Attack mitigation Schemes along with findings constraints. These systems do not work for large scale attack as filtering mechanism depend upon capacity of filtering device.

### 3.3.2 Capability Based System

These systems are completely different from filtering based system as their goal is to confirm that the sender receive explicit permission before sending any message to destination. While message is traversing from source to destination every router in between puts its own signature on it and these sequence of signatures is assisted as a capability which will receiver give it to sender.

J. yu et. al. proposed scheme called as trust management which acquainted lightweight component TMH with relieve session flooding attack utilizing trust assessed from clients’ meeting history. Contrasting with other protection components, TMH is lightweight, autonomous to the administration subtleties, versatile to the server’s asset utilization and extendable to permit coordinated effort among servers. They checked its viability with reproductions under various attack methodologies. However it suffers from high Computations and data transmission overhead.
Somani et al. proposed a scheme to block DDoS attack in which during attack the number connections rises so that attack will be get captivated. The proposed plan likewise functions admirably with the administrations having resources restrictions. Proposed work shows another heading of DDoS mitigation and gives a novel arrangement dependent on the decrease in “resource usage factor” per demand during the attack. This scheme is not suitable for webservers as they have constrained resources.

Liu et al. proposed scheme which is MiddlePolice. The first readily deployable scheme unambiguously discourses three issues. The issue of deployment from the cloud solved by capability mechanism. Second, it can only work either vendor or protocol defined traffic governing rules as it is fully destination-driven. In last it addresses the traffic bypass vulnerability. Due to Widespread evaluations on the Internet for enormous victims like government it may be confidentiality offensive.

Bharot et al. proposed scheme which perform attack mitigation by misguiding the attacker with the help of ICRPU which detect source of the attack restrict them for future request. Hellinger distance function utilized for mitigation model using Intensive Care Request Processing Unit (ICRPU) and feature selection method, if certain space is establish, then every packets are analysed and classified in two types, as legitimate request DDoS requests. Normal Request Processing utilized for the entire legitimate requests. ICRPU processes all the DDoS request were these request got tiring in question and answer. Simultaneously these request are blocked but this scheme leads to high Computation overhead.

Pillutla et al. proposed a scheme based on Kohonen neural network model called as FSOMDM scheme which is an enhanced fuzzy rule recommended for mitigating DDoS attack to upsurge the vital features of SDN in cloud computing. By deriving a singleton output function that inspects the supervised input data traffic through the characteristics of traffic scrutiny strategy which is software inspired for categorizing them into mischievous and trustworthy traffic it mitigate DDoS attack. Suggested scheme does not address application layer DDoS Attack. Table 6 illustrates Capability Based Based DDoS Attack mitigation Schemes along with findings constrains.

3.4 Differentiation

This phase of DDoS defence employed during attack. Distinguishing a DDoS attack from genuine traffic is uphill task for researchers since the attackers attack with more sophisticated techniques to the victim every time. The popular websites are the principal victims of such DDoS attacks. It means there is no symptom to encounter against such attacks effectively in near future too.

To distinguish DDoS attacks from Flash events, researchers already proposed various methods and They can be divided into three types based on the type of detection metric used namely: based on information entropy, information divergence/distance, coefficient of correlation
Table 6 Capability Based Mitigation Techniques for DDoS Attack

| Technique          | Author & Year | Approach                     | Findings                  | Constraints                          |
|--------------------|---------------|------------------------------|---------------------------|--------------------------------------|
| Trust Management   | J. Yu. et. al. 2010 | User History                 | Able to mitigate HTTP Flooding attack | Leads to high Computation & bandwidth overhead |
| Scale inside out   | Somani et. al. 2018 | Resource utilization of each request | Quick absorption of attack at victim end | Webserver does have limited amount of resources |
| Feature selection  | Bharot. Et. al. 2018 | Hellinger distance function | Able to mitigate HTTP Flooding attack | Leads to high Computation overhead |
| Middle police      | Liu et. al. 2018 | Endpoint driven network traffic control protocol | Readily deployable scheme | It may be privacy invasive for large victims like government |
| FSOMDM             | Pillutla & Arjunan 2018 | Neural network                | Able to mitigate HTTP Flooding attack | Does not address application layer DDoS Attack |

3.4.1 Entropy Based techniques

To discriminate DDoS attacks from FEs Many authors have proposed solutions based on human behavior modeling. By analyzing the logs of web servers researchers found the underneath semantics of human behavior.

Prasad et al. proposed a technique comprising of distribution of source IP addresses, access points and speed of increased/decreased traffic to separate the traffic behaviour of FE and DDoS attack. for differentiation of FEs from DDoS attacks they proposed ITM (an Internet threat monitoring) system utilized central data centre and a group of monitors for the modelling. To discriminate FEs from DDoS attacks entropy variations and Information theoretic framework were utilized.

Tao et al. proposed a scheme which administer the network traffic by supervising the network traffic by using a flow entropy based system on the edge routers of the network. if the flow entropy drops considerably in a short period the Potential attack alarms will be on. To discriminate the attack traffic and FE traffic the Sibson distance between different network flows is utilized.

Saleh et al. proposed a scheme in which the three layers of the framework i.e. flexible, collaborative, multi-layer DDoS framework (FCMDPF) for avoiding application layer DDoS attacks. the outer blocking (OB) layer blocks the source IP if If the source IP source is present in already built black list table, service traceback oriented architecture (STBOA) layer checks Whether the incoming request is launched by a human or by an automated tool. The third
flexible advanced entropy based (FAEB) layer differentiates HR-DDoS attacks and FEs. However, the framework suffers from low false negative rate.

Sachdeva et al. proposed a scheme to distinguish DDoS attacks from FEs which use combination of cluster entropy and source IP entropy. As most of the traffic comes from already visited source networks, traffic cluster entropy is more in the case of HR-DDoS attacks as entire of the traffic comes from comparatively new source networks but small in the case of flash events. NS2 simulations and emulations in DETER testbed are used to validate the results.

Bhandari et al. proposed a scheme in which calculation of entropies of alteration in request rate, the number of dissimilar sources IP's, page access entropy along with of new source IP addresses to find the similarity between flows and sharing of request rate among source IPs is done to differentiate DDoS and FEs. Real datasets of FIFA, CAIDA and synthetically generated datasets are utilized for research validations.

for discriminating APP layer DDoS attack and flash event Behal et. al. proposed Entropy which subtracts the entropies of attack traffic from the normal traffic. Using the same approach as mentioned in [46], accuracy of - Entropy metric for discriminating DDoS attacks and FEs is more as compare to Renyi's generalized information entropy metric.

Singh et. al. detects and distinguishes AL-DDoS attack from FE by using a well-organized fuzzy-GA method. They optimized parameters with genetic algorithms as well as fuzzification is done to give range of DDoS attack and flash event using membership function. With accuracy of 98.4% and FPR of below 2% the fuzzy-GA method shows consistency in distinguishing DDoS attack from FE, with an estimated accuracy of 97.3% the Planned model can also distinguish FEs. Table 7 illustrates Entropy Based DDoS Attack Differentiation Schemes along with findings constrains. Table 7 Entropy Based DDoS Attack Differentiation Schemes.

3.4.2 Information Divergence based Techniques

Yu et al. found that the DDoS attack flows are intensely similar as likened to FE flows as to launch attack traffic alike pre-built programs are used by all the nodes in the botnet by calculating the information distance centred on the impression. Three information distances namely Sibson, Jeffrey and Hellinger are utilized for distinguishing App Layer DDoS attack and FE and They witnessed that Sibson distance is best fit for discriminating DDoS attacks and FEs and detection accuracy of 65% achieved in this technique.

Saravanan et al. distinguishes DDOS FEs by user behavior model based on the client legality and pages surfed which use approach of flow similarity. They calculate Hellinger distance metric between attack and FE flows. Information distance amid attack flows is close to zero while it is close to one for FE. By using CAIDA and FIFA World Cup dataset they validate their planned method by simulating the DDoS attacks and FEs correspondingly.

Behal et al. calculates the information distance among dissimilar kinds of network by using Renyi’s generalized information distance to distinguish
DDoS and FEs. They calculate the information distance between probability distributions of attack and FE flows and They found that attack flows are deviated more from the normal flows for DDoS attacks, while FEs flows are alike to normal flows. With less false positives and more detection accuracy from other methods. Real datasets of FIFA, CAIDA and synthetically generated DDoSTB datasets are utilized for research Validations.

Further, Behal et al. also proposed a generalized divergence metric which compile the information distance among dissimilar types of network flows. The detection accuracy of this Divergence metric in differentiating DDoS attacks and FEs is high with respect to Renyi’s generalized information divergence metric. Table 8 illustrates Divergence Based DDoS Attack Differentiation Schemes along with findings constrains.

### Table 7 Entropy Based DDoS Attack Differentiation Schemes

| Technique       | Author & Year | Approach                  | Findings                                                                 | Constraints                                                                                           |
|-----------------|---------------|---------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| $\phi$ Entropy  | Behal et.al. 2017 | Source & Destination IP | Better Accuracy as compare to Renyi entropy                              | System is not scalable in case of large volume attacks, Does not give any information about various categories of FE |
| Source Entropy  | Bhandari et.al. 2016 | Flow similarity           | Able to discriminate DDoS & Flash Event on various parameters             | Does not give any information about various categories of FE                                          |
| Cluster Entropy | Sachdeva et. al. 2016 | Flow Similarity           | Can Operate in Three Different Defensive Modes                            | Does not meet QoS Requirements                                                                        |
| FCMDPF          | Saleh et. al. 2014 | Flow Similarity           | optimal solution that addresses all sorts of HTTP DDoS/DDoS attacks       | Does not Prevent from all kinds of FE Attacks                                                          |
| ITM             | Prasad et.al. 2013 | Source IP                 | Able to identify Genuine Flash Crowd                                     | Fails to recognize low rate Flash Crowd, Does not address the issue of multiple attacks at same time |
| Sibson Distance | Tao et. al. 2013 | Flow Similarity           | Can be implemented Easily                                                 |                                                                                                        |
| FUZZY–GA        | Singh et. Al. | Optimization              | Gives best accuracy among all techniques                                  | Takes too much time to get fitness value                                                               |
Table 8 Divergence Based DDoS Attack Differentiation Schemes

| Technique          | Author & Year | Approach               | Findings                     | Constraints                                           |
|--------------------|---------------|------------------------|------------------------------|-------------------------------------------------------|
| $\phi$ Divergence[42] | Behal et. al. 2017 | Source and Destination IP | High Accuracy                             | fails in case of large volume attacks                 |
| Hellinger distance[87] | Saravanan et.al. 2016 | Flow Similarity        | Low false positives and false negative rates | Don't consider multiple botnets operating at same time |
| Three metric[104]   | Yu et.al. 2009  | Flow Similarity        | Finds best information distance       | Accuracy of 65%                                       |

3.4.3 Correlation Coefficient based Techniques

Apart from using information theory based metrics, many authors have proposed correlation based methods to discriminate DDoS attacks from FE.

Yatagai et al.[102] recommended an algorithm which operates in two different phases by analysing HTTP-GET requests they modeled the page access behaviour of genuine users. Analysing the web IP address with the similar browsing order is released and clogged in first while computing correlation amongst browsing time and page info size in second phase. They detect that the browsing time increases in proportion to information size for normal users. Network gateway is utilized for implementation of scheme.

Li et al.[67] proposed an scheme to distinguish DDoS and FE by amalgamation of total deviation and coefficient of correlation. Firstly a flow anomaly detector recognise them by calculating the hybrid detection metric by stated router for detecting anomalies of incoming flows thereafter by computing total deviation and resemblance coefficient’s values by a flow dissemination estimator sample the flows based on pertinent traffic features. FE, DDoS and normal flows are distinguished by a decision device. MIT Lincoln Laboratory (DDoS) 2.0.2 and HTTP log files from a busy server are utilized for research validation to represent DDoS attacks and FE correspondingly.

Thapngam et al. proposed a behavior-based detection scheme to discriminate DDoS and FE. To distinguish DDoS attack from FE they have used the logic of packet arrival rate and They calculate Pearson’s correlation coefficient. High amount of automation expectable transmission rate found for DDoS Attack which leads to correlation value nearby to 0 or 1. For an FE They detected that the request rate is random which brings correlation value less than 1. 1998 FIFA world cup dataset are used for assessment of their proposed method.

Bhatia et al. proposed a scheme in which they calculate variation in the new source IPs as well as variation in incoming traffic rate and number of requests per source IP to explore the behavioural change amid FE and DDoS attack. CAIDA and FIFA Dataset are used for research Validation.
Zhou et al. proposed a scheme which consist of framework of three different module namely traffic FM (filter module), DADM (DDoS attack detection module) and ATDM (traffic detection model). They calculate the proportion of entropies of source IPs click rate of a web page for identifying application layer attacks. For FE ratio was small while for DDoS attacks ratio was high.

Some other authors like Poornima et al. [81], Patil et al. [66], Tinju et al. [97] and Roa et al. [83][57] also proposed correlation based methods using the idea of flow similarity to discriminate attack flows from FE flows.

Xiao et al. implemented k-nearest neighbour algorithm to group the flows generated from the same malicious code or bots with the help of approach of flow similarity between the flows generated by the similar mischievous attack software and correlation between them. High classification rate and low response time are the merits of scheme. The given scheme fail if an attacker modifies the configuration parameters to start producing different attack flows. KDD’99 dataset was used for evaluation.

Chawla et al. recommended correlation based DDoS attack and flash event detection and discrimination (CoDFEDD) which is a structure based on Pearson’s product moment correlation method. FIFA, CAIDA, MIT Lincoln and synthetically generated datasets using GENI (Global Environment for Network Innovations) testbed are utilized for research validations. Value of CoDFEDD indicator is close to 1 suggests the flow similarity of attack flows is key observation of scheme.

Durga et al. implemented as scheme in which to discriminate reflector DDoS attacks and FE the Kendalls tau rank correlation method is utilized. By combining network traffic analysis with server load analysis techniques for discriminating DDoS attacks and FE is proposed by Bhatia et al. which is an ensemble-based model. They also calculate coefficients of correlation to identify flow similarity. Table 9 illustrates Correlation Based DDoS Attack Differentiation Schemes along with findings constrains. Apart from correlation, entropy and Divergence few researchers use other methods to differentiate DDoS attack from flash events [78][69][65][53].

In current generation of heterogeneous and dynamic networks like mobile crowd-sourcing network the issue of privacy preservation and DDoS attack is more severe [106]. there are few researchers who have also proposed solution for DDoS attack management which can utilized to protect webservers from DDos attack. each solution have there own merits as well as limitations. [39][58][77][74][36][60][51] [95][62][38][86][41]

4 Testing DDoS Attack Defences

To prove the novelty and superiority of their proposed schemes with respect to existing schemes There are various Datasets as well as tools are utilized by researchers. We will see those tools and dataset in this section.
Table 9: Correlation Based DDoS Attack Differentiation Schemes

| Technique                  | Author & Year | Approach          | Findings                                      | Constraints                                      |
|----------------------------|---------------|-------------------|-----------------------------------------------|--------------------------------------------------|
| variation in new source IPs [49] | Bhatia et al. 2016 | Network features | Distinguished DDoS Attack & FE on multiple parameters | Does not address DDoS Attack with variable packet rate |
| RCD [55]                   | Durga et al. 2016 | Flow Similarity   | Discard malicious flow of Traffic             | High false positive rates                         |
| CKNN [101]                 | Xiao et al. 2015 | Flow Similarity   | Reduces Overhead of KNN correlation           | Fails to address issue of multiple attacks        |
| CoDFEDD [52]               | Chawla et al. 2015 | Flow Similarity   | Efficiently detect DDoS Attack                | Does not tested on Real time environment’s        |
| Traffic Pattern [94]       | Thapngam et al. 2011 | Flow Similarity | Protect the server from crashing during a DDoS attack | Suffers from Delay & complexity issue             |
| ATDM [108]                 | Zhou et al. 2014 | Source IP         | Able to detect application layer DDoS Attack | Response rate is sluggish                         |

4.1 Datasets and tools

For training and testing of application layer DDoS defense mechanisms, there are a numerous number of datasets available. It is been found that the most of the available datasets are old. While there is wealth of network traces available, among which there are comparatively few application layer traces available. There is a number of sources of attack free HTTP traces provided by the Internet Traffic Archives. Analysis on these datasets have led some researchers to suggest it does not resemble real network data. Table 10 illustrates existing datasets for DDoS defense evaluation [75].

The most of the research works have trusted upon generated attack traces with the help of existing DDoS attack generation tools as these datasets are not very dependable. Table 11 illustrates existing tools for DDoS defense evaluation.

4.2 Performance Metrics

All researchers use few performance metrics to show superiority of their proposed scheme. These performance metrics show the originality of proposed scheme. Few performance metrics are listed below.

Let a be total number of attacks, b be the total malicious connection reported, and c be malicious connections reported correctly.
Table 10  Existing Dataset for DDoS defence evaluation

| Name of Dataset          | Content                                                                 |
|-------------------------|-------------------------------------------------------------------------|
| WorldCup98[15]          | Web request recorded during 1998 FIFA world cup which are around 1.3 billion |
| EPA-HTTP[16]            | HTTP log of entire day from busy WWW server                              |
| SDSC-HTTP[17]           | HTTP log of entire day from busy WWW server                              |
| Calgary-HTTP[18]        | HTTP log of entire year from busy CS departmental WWW server             |
| ClarkNet-HTTP[19]       | HTTP log of two weeks from busy ISP WWW server                           |
| NASA-HTTP[20]           | HTTP log of two months from busy WWW server                              |
| Saskatchewan-HTTP[21]   | HTTP log of seven month from university WWW server                       |
| CAIDA[34]               | Approximately one hour of anonymised traffic traces from DDoS Attack on 4th August 2007 |
| DARPA[22]               | Dataset of varying Complexity attacks                                    |

Table 11  Existing Tools for DDoS defence evaluation

| Name of Tool                      | Type of Attack                              |
|-----------------------------------|---------------------------------------------|
| Low Orbit Ion Cannon: LOIC[23]    | TCP, UDP or HTTP flood Attack               |
| HULK[24]                          | random flood attack                         |
| DDoSim[25]                        | HTTP or TCP flood                           |
| R-U-D-Y aRe yoU Dead Yet[26]      | low POST attack                             |
| Tor’s Hammer[27]                  | slow POST attack                            |
| Pyloris[28]                       | connection exhaustion DoS                   |
| Golden Eye[29]                    | HTTP protocol attack                        |
| SIPp-DD[30]                       | SIP flooding attacks.                       |

Detection Rate is given by
\[ DR = \frac{c}{a} \]

False Negative Rate is given by
\[ FNR = \frac{a-c}{b} \]

False positive rate is given by
\[ FPR = \frac{b-c}{b} \]

along with these performance metrics which are explained below are also considered while examining DDoS attack management schemes.

Detection Speed: a long delay can degrade user experience so detection scheme should manage the connection swiftly.

Low computation overhead: firewall can be castoff as a bottleneck by the attackers which is a new kind of attack if computation overhead should be as low as possible.

Detection Accuracy: Detection accuracy can be calculated by using two elements: detection rate and false negatives. How much of the attack connections
the firewall recognized is Detection rate. How much of the incoming attack traffic did the firewall pass on to the Web server is false negative rate.

5 conclusion

In this paper, a review of the prevailing research scope in the aspect of DDOS attack and their shielding techniques with the different stages of prevention, Detection, Mitigation and Differentiation is described in detail. This review found that the prevention schemes will be always vulnerable to modified and sophisticated types of DDoS attacks. The Anomaly based schemes give best results for detection with high accuracy, the capability based schemes are suitable for mitigation while divergence based schemes gives better results in aspect of differentiation with Flash Events. The reviewed research work has proposed different types of shield mechanisms against the DDoS attacks but due to deficit of standards against the performance the optimal protection system is indeterminate. In future, world shall experience more sophisticated attack with heterogeneous traffic. So upcoming security and privacy protection schemes shall be robust, scalable, and also heterogeneous in the way of combining these reviewed management schemes to challenge the modern days DDoS attack and realize the secure wireless networks.

6 Declarations

Funding: Not applicable.

Availability of data and material: Not applicable.

Code availability: Not applicable.

Conflict of interest: Authors declare that they have no conflict of interest.

References

1. https://www.bankinfosecurity.com/bank-spain-hit-by-ddos-attack-a-11430. Accessed on: 2018-07-28.
2. https://www.darkreading.com/cloud/eight-hour-ddos-attack-struck-aws-customers/d/d-id/1336165. Accessed on: 2018-09-13.
3. https://www.reuters.com/article/telegram-cyber/messaging-service-telegram-hit-by-ddos-cyber-attack-idUSL4N23J2QX. Accessed on: 2019-12-13.
4. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2019/05/20135454/en-candc.png. Accessed on: 2019-11-12.
5. https://www.theregister.co.uk/2018/03/01/github_ddos_biggest_ver. Accessed on: 2019 - 12 - 23.
6. https://www.ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack. Accessed on: 2019-10-18.
39. Muhammad Ejaz Ahmed, Saeed Ullah, and Hyoungshick Kim. Statistical application fingerprinting for ddos attack mitigation. *IEEE Transactions on Information Forensics and Security*, 14(6):1471–1484, 2018.
40. Katerina J Argyraki and David R Cheriton. Active internet traffic filtering: Real-time response to denial-of-service attacks. In *USENIX annual technical conference, general track*, volume 38, 2005.
41. Narmeen Zakaria Bawany, Jawwad A Shamsi, and Khaled Salah. Ddos attack detection and mitigation using sdn: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 42(2):425–441, 2017.
42. Sunny Behal and Krishan Kumar. Detection of ddos attacks and flash events using information theory metrics–an empirical investigation. *Computer Communications*, 103:18–28, 2017.
43. Sunny Behal and Krishan Kumar. Detection of ddos attacks and flash events using novel information theory metrics. *Computer Networks*, 116:96–110, 2017.
44. Sunny Behal, Krishan Kumar, and Monika Sachdeva. D-fac: a novel $\phi$-divergence based distributed ddos defense system. *Journal of King Saud University-Computer and Information Sciences*, 2018.
45. Sunny Behal, Krishan Kumar, and Monika Sachdeva. D-face: An anomaly based distributed approach for early detection of ddos attacks and flash events. *Journal of Network and Computer Applications*, 111:49–63, 2018.
46. Mikhail Belyaev and Svetlana Gaivoronski. Towards load balancing in sdn-networks during ddos-attacks. In *2014 International Science and Technology Conference (Modern Networking Technologies)(MoNeTeC)*, pages 1–6. IEEE, 2014.
47. Abhinav Bhandari, Amrit Lal Sangal, and Krishan Kumar. Characterizing flash events and distributed denial-of-service attacks: an empirical investigation. *Security and Communication Networks*, 9(13):2222–2239, 2016.
48. Nitesh Bharot, Priyanka Verma, Sangeeta Sharma, and Veenadhari Suraparaju. Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. *Arabian Journal for Science and Engineering*, 43(2):959–967, 2018.
49. Sajal Bhatia, Desmond Schmidt, George Mohay, and Alan Tickle. A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. *Computers & Security*, 40:95–107, 2014.
50. Monowar H Bhuian, DK Bhattacharyya, and Jugal K Kalita. E-ldat: a lightweight system for ddos flooding attack detection and ip traceback using extended entropy metric. *Security and Communication Networks*, 9(16):3251–3270, 2016.
51. Anthony Chadd. Ddos attacks: past, present and future. *Network Security*, 2018(7):13–15, 2018.
52. Shifali Chawla, Monika Sachdeva, and Sunny Behal. Discrimination of ddos attacks and flash events using pearson's product moment correlation method. *International Journal of Computer Science and Information Security*, 14(10):382, 2016.
53. Rup K Deka and Dhruba K Bhattacharyya. Self-similarity based ddos attack detection using hurst parameter. *Security and Communication Networks*, 9(17):4468–4481, 2016.
54. Ping Du and Akihiro Nakao. Ddos defense deployment with network egress and ingress filtering. In *2010 IEEE International Conference on Communications*, pages 1–6. IEEE, 2010.
55. M Durga. Detecting distributed reflection dos attack using kendall’s tau rank correlation. *Int. J. Sci. Technol.*, 1(2):21–23, 2016.
56. Juan M Estevez-Tapiador, Pedro Garcia-Teodoro, and Jesus E Diaz-Verdejo. Anomaly detection methods in wired networks: a survey and taxonomy. *Computer Communications*, 27(16):1569–1584, 2004.
57. V.N. Rao G.R. Rao, A. Konduri. Simulation of rank correlation based detection mechanism for distributed denial of services attacks. *Int. J. Comput. (IJC)*, 16(6):1–8, 2015.
58. Yanpeng Guan and Xiaohua Ge. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Transactions on Signal and Information Processing over Networks*, 4(1):48–59, 2017.
59. BB Gupta, Manoj Misra, and Ramesh C Joshi. An isp level solution to combat ddos attacks using combined statistical based approach. *arXiv preprint arXiv:1203.2400*, 2012.

60. BB Gupta, Manoj Misra, and Ramesh C Joshi. An isp level solution to combat ddos attacks using combined statistical based approach. *arXiv preprint arXiv:1203.2400*, 2012.

61. Sufian Hameed and Usman Ali. Hadec: hadoop-based live ddos detection framework. *EURASIP Journal on Information Security*, 2018(1):11, 2018.

62. Khaled Hamoud and Kamel Adi. Secure and reliable certification management scheme for large-scale manets based on a distributed anonymous authority. *Peer-to-Peer Networking and Applications*, 12(5):1137–1155, 2019.

63. Chi-Hyung In, Choong Seon Hong, Jiang Wei, and Koji Okamura. An enhanced sos architecture for ddos attack defense using active network technology. In *Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPHR/ELETE’05)*, pages 90–95. IEEE, 2005.

64. Khundrakpam Johnson Singh, Khelchandra Thongam, and Tammay De. Entropy-based application layer ddos attack detection using artificial neural networks. *Entropy*, 18(10):350, 2016.

65. Khundrakpam Johnson Singh, Khelchandra Thongam, and Tammay De. Entropy-based application layer ddos attack detection using artificial neural networks. *Entropy*, 18(10):350, 2016.

66. P. Deshmukh K.H. Patil, A. Bagwan. Improving network performance by differentiating ddos attacks from flash crowd. In *Int. J. Adv. Res. Comput. Sci. Manag. Stud. 3*, volume 1, 2015.

67. Ke Li, Wanlei Zhou, Ping Li, Jing Hai, and Jianwen Liu. Distinguishing ddos attacks from flash crowds using probability metrics. In *2009 Third International Conference on Network and System Security*, pages 9–17. IEEE, 2009.

68. Qin Liao, Hong Li, Songlin Kang, and Chuchu Liu. Feature extraction and construction of application layer ddos attack based on user behavior. In *Proceedings of the 33rd Chinese Control Conference*, pages 5492–5497. IEEE, 2014.

69. Qin Liao, Hong Li, Songlin Kang, and Chuchu Liu. Application layer ddos attack detection using cluster with label based on sparse vector decomposition and rhythm matching. *Security and Communication Networks*, 8(17):3111–3120, 2015.

70. Xin Liu, Xiaowei Yang, and Yanbin Lu. To filter or to authorize: Network-layer dos defense against multimillion-node botnets. In *ACM SIGCOMM Computer Communication Review*, volume 38, pages 195–206. ACM, 2008.

71. Zhuotao Liu, Yuan Cao, Min Zhu, and Wei Ge. Umbrella: Enabling ips to offer readily deployable and privacy-preserving ddos prevention services. *IEEE Transactions on Information Forensics and Security*, 14(4):1098–1108, 2018.

72. Zhuotao Liu, Hao Jin, Yih-Chun Hu, and Michael Bailey. Practical proactive ddos-attack mitigation via endpoint-driven in-network traffic control. *IEEE/ACM Transactions on Networking*, 26(4):1948–1961, 2018.

73. Deepika Mahajan and Monika Sachdeva. Ddos attack prevention and mitigation techniques-a review. *International Journal of Computer Applications*, 67(19), 2013.

74. Vincenzo Matta, Mario Di Mauro, and Maurizio Longo. Ddos attacks with randomized traffic innovation: Botnet identification challenges and strategies. *IEEE Transactions on Information Forensics and Security*, 12(8):1844–1859, 2017.

75. Jelena Mirkovic, Sonia Fahmy, Peter Reiher, and Roshan K Thomas. How to test dos defenses. In *2009 Cybersecurity Applications & Technology Conference for Homeland Security*, pages 103–117. IEEE, 2009.

76. Myo Myint Oo, Sinchai Kamolphiwong, Thossaporn Kamolphiwong, and Sangsuree Vasupongayya. Advanced support vector machine (asvm-) based detection for distributed denial of service (ddos) attack on software defined networking (sdn). *Journal of Computer Networks and Communications*, 2019, 2019.

77. Van Linh Nguyen, Po-Ching Lin, and Ren-Hung Hwang. Mcpass: Distributed denial of service defense architecture for mobile networks. *IEEE Network*, 32(1):118–124, 2018.
78. Georgios Oikonomou and Jelena Mirkovic. Modeling human behavior for defense against flash-crowd attacks. In *2009 IEEE International Conference on Communications*, pages 1–6. IEEE, 2009.

79. Kihong Park. Scalable ddos protection using route-based filtering-discex iii demonstration. In *Proceedings DARPA Information Survivability Conference and Exposition*, volume 2, pages 97–vol. IEEE, 2003.

80. Harikrishna Pillutla and Amuthan Arjunan. Fuzzy self organizing maps-based ddos mitigation mechanism for software defined networking in cloud computing. *Journal of Ambient Intelligence and Humanized Computing*, 10(4):1547–1559, 2019.

81. NV Poornima, K ChandraPrabha, and BG Geetha. Adaptive discriminating detection for ddos attacks from flash crowds using flow correlation coefficient with collective feedback. In *Proceedings of International Conference on Global Innovations in Computing Technology (ICGICT’14)*, volume 2, 2014.

82. K Munivara Prasad, A Rama Mohan Reddy, and K Venugopal Rao. Discriminating ddos attack traffic from flash crowds on internet threat monitors (itm) using entropy variations. *African J. Comput. ICT*, 6(2):53–62, 2013.

83. B Durga Rao and K Renuka. Implementation of detection against distributed reflection for rank correlation dos attacks. *Int. J. Adv. Technol. Innovative Res.*, 6(6):516–520, 2014.

84. Manika Sachdeva, Krishan Kumar, and Gurvinder Singh. A comprehensive approach to discriminate ddos attacks from flash events. *Journal of information security and applications*, 26:8–22, 2016.

85. Mohammed A Saleh and Azizah Abdul Manaf. A novel protective framework for defeating http-based denial of service and distributed denial of service attacks. *The Scientific World Journal*, 2015, 2015.

86. Prabakeran Saravanan and T Sethurakari. Optimal hop selection based novel trust based ddos attack removal framework for reliable and secured transmission of data in vanets. *Wireless Personal Communications*, pages 1–29, 2019.

87. Renukadevi Saravanan, Saraswathi Shanmuganathan, and Yogesh Palanichamy. Behavior-based detection of application layer ddos attacks during flash events. *Turkish Journal of Electrical Engineering & Computer Sciences*, 24(2):510–523, 2016.

88. Rajalakshmi Selvaraj, Venu Madhav Kuthadi, and Tshilidzi Marwala. Ant-based distributed denial of service detection technique using roaming virtual honeypots. *IET Communications*, 10(8):929–935, 2016.

89. Khundrakpam Johnson Singh and Tanmay De. Mlp-ga based algorithm to detect application layer ddos attacks. *Journal of information security and applications*, 36:145–153, 2017.

90. Khundrakpam Johnson Singh, Khelchandra Thongam, and Tanmay De. Detection and differentiation of application layer ddos attack from flash events using fuzzy-ga computation. *IET Information Security*, 12(6):502–512, 2018.

91. Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, and Muttukrishnan Rajarajan. Scale inside-out: Rapid mitigation of cloud ddos attacks. *IEEE Transactions on Dependable and Secure Computing*, 15(6):959–974, 2017.

92. Harumaasa Tada, Masayuki Murata, and Masaki Aida. Web service flash crowd mitigation using feedback to users. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*, pages 213–219. IEEE, 2017.

93. Yuan Tao and Shiui Yu. Ddos attack detection at local area networks using information theoretical metrics. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pages 233–240. IEEE, 2013.

94. Theerasak Thapngam, Shui Yu, Wanlei Zhou, and Gleb Beliakov. Discriminating ddos attack traffic from flash crowd through packet arrival patterns. In *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 952–957. IEEE, 2011.

95. Theerasak Thapngam, Shui Yu, Wanlei Zhou, and S Kami Makki. Distributed denial of service (ddos) detection by traffic pattern analysis. *Peer-to-peer networking and applications*, 7(4):346–358, 2014.
96. Roshan Thomas, Brian Mark, Tommy Johnson, and James Croall. Netbouncer: client-legitimacy-based high-performance ddos filtering. In Proceedings DARPA Information Survivability Conference and Exposition, volume 1, pages 14–25. IEEE, 2003.
97. Tinju Grace Varghese and M. Salitha. Model based prediction technique for denial of service attack detection. Int. J. Innovations Adv. Comput. Sci., 4(8):34–39, 2015.
98. Chenxu Wang, Tony TN Miu, Xiapu Luo, and Jinhe Wang. Skyshield: a sketch-based defense system against application layer ddos attacks. IEEE Transactions on Information Forensics and Security, 13(3):559–573, 2017.
99. Patrick Wendell and Michael J. Freedman. Going viral: flash crowds in an open cdn. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 549–558. ACM, 2011.
100. Tao Xia, Guangzhi Qu, Salim Hariri, and Mazin Yousif. An efficient network intrusion detection method based on information theory and genetic algorithm. In PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005., pages 11–17. IEEE, 2005.
101. Peng Xiao, Wenyu Qu, Heng Qi, and Zhiyang Li. Detecting ddos attacks against data center with correlation analysis. Computer Communications, 67:66–74, 2015.
102. Takeshi Yatagai, Takamasa Isohara, and Iwao Sassae. Detection of http-get flood attack based on analysis of page access behavior. In 2007 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, pages 232–235. IEEE, 2007.
103. Jinpeng Yu, C Fang, L Lu, and Z Li. Mitigating application layer distributed denial of service attacks via effective trust management. IET communications, 4(16):1952–1962, 2010.
104. Shui Yu, Theerasak Thapngam, Jianwen Liu, Su Wei, and Wanlei Zhou. Discriminating ddos flows from flash crowds using information distance. In 2009 Third International Conference on Network and System Security, pages 351–356. IEEE, 2009.
105. Yuntao Zhao, Wenbo Zhang, Yongxin Feng, and Bo Yu. A classification detection algorithm based on joint entropy vector against application-layer ddos attack. Security and Communication Networks, 2018, 2018.
106. Sheng Zhong, Hong Zhong, Xinyi Huang, Panlong Yang, Jin Shi, Lei Xie, and Kun Wang. Connecting human to cyber-world: Security and privacy issues in mobile crowdsourcing networks. In Security and Privacy for Next-Generation Wireless Networks, pages 65–100. Springer, 2019.
107. Chenfeng Vincent Zhou, Christopher Leckie, and Kotagiri Ramamohanarao. Protecting sip server from cpu-based dos attacks using history-based ip filtering. IEEE Communications Letters, 13(10):800–802, 2009.
108. Wei Zhou, Weijia Jia, Sheng Wen, Yang Xiang, and Wanlei Zhou. Detection and defense of application-layer ddos attacks in backbone web traffic. Future Generation Computer Systems, 38:36–46, 2014.