Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions

Sajal Bhatia, Sunny Behal, and Irfan Ahmed

Abstract Societal dependence on Information and Communication Technology (ICT) over the past two decades has brought with it an increased vulnerability to a large variety of cyber-attacks. One such attack is a Distributed Denial-of-Service (DDoS) attack which harnesses the power of a larger number of compromised and geographically distributed computers and other networked machines to attack information-providing services, often resulting in significant downtime and thereby causing a denial-of-service to legitimate clients. The size, frequency, and sophistication of such attacks have exponentially risen over the past decade. In order to develop a better understanding of these attacks and defense system against this ever-growing threat, it is essential to understand their modus operandi, latest trends and other most widely-used tactics. Consequently, the study of DDoS attacks and techniques to accurately and reliably detect and mitigate their impact is an important area of research. This chapter largely focuses on the current landscape of DDoS attack detection and defense mechanisms and provides detailed information about the latest modus operandi of various network and application layer DDoS attacks, and presents an extended taxonomy to accommodate the novel attack types. In addition, it provides directions for future research in DDoS attack detection and mitigation.

S. Bhatia (✉)
School of Computing, Sacred Heart University, Fairfield, CT, USA
e-mail: bhatias@sacredheart.edu

S. Behal
Department of Computer Science, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India
e-mail: sunnybehal@sbsstc.ac.in

I. Ahmed
Department of Computer Science, University of New Orleans, New Orleans, LA, USA
e-mail: iahmed4@uno.edu

M. Conti et al. (eds.), *Versatile Cybersecurity*, Advances in Information Security 72, https://doi.org/10.1007/978-3-319-97643-3_3

1 Introduction

Advances in Information and Communication Technology (ICT) over the past two decades has significantly transformed the manner in which data is stored, accessed and communicated, mainly over the network. The variety of services supported by ICT are exponentially expanding and in recent years have even included the control and monitoring of critical infrastructure system such as water, gas, and power. This constant evolution of ICT paired with its ubiquitous nature has brought with it an ever-increasing dependence for storing, processing and transferring information. As a result, any disruption in these systems, even for a relatively short period, directly and adversely affects nearly all key functionalities of a modern society.

A situation, often resulting from a deliberate and malicious attempt by an adversary to intentionally disrupt the normal operations of a service provider (or a server) and render the resources unavailable to its intended clients is known as a Denial-of-Service (DoS) attack. The National Information Assurance Glossary provided by the Committee on National Security Systems (CNSS) gives a more general definition and identifies DoS as [1]:

> Any (series of) actions that prevent any part of an [information system] from functioning.

A DoS attack against an online service provider can target its computing resource such as CPU, memory, or a networking resource such as bandwidth or both. The effects of such an attack can range from a minor delay in service response time to complete inaccessibility. These attacks at times can also have financial implications on organizations heavily dependent on the availability of their services. A report by Amazon suggests that a 100 ms delay in response time can potentially drop their overall sales by approximately 1% [2]. A Distributed Denial-of-Service (DDoS) attack is a distributed variant of the DoS attack where an array of geographically dispersed compromised machines (a.k.a. zombies, bots, slaves) are controlled by an attacker (aka bot-master) and used against a specific target to cause a denial of service. A network of such compromised machines (or bots) is called a *botnet*. In a DDoS attack, individual capability of each compromised machines is utilized and aggregated for use against a common victim, thereby magnifying the effect. Figure 1 demonstrates the working model of a typical DDoS attack. The bot-master compromises an array of bots, commonly by infecting them with a Trojan or a backdoor program, and takes control of them. These compromised bots are then controlled by the bot-master, often via Command and Control (C&C) channels, and simultaneously used to attack a target server using the public network infrastructure. The sophistication, size, volume, and frequency of DDoS attacks have risen exponentially over the years. To develop a better defense system against this ever-growing threat, it is essential to understand their modus operandi, their latest trends, and most widely-used tactics. The motives behind DDoS attacks ranges from fun to financial gain to pushing forward a political agenda, as in the case of the attacks on Estonia and Georgia [3]. A report Arbor Networks on Worldwide Infrastructure Security indicates ideologically-motivated 'hacktivism' and 'vandalism' as the most readily-identified motivations behind DDoS attacks [4].

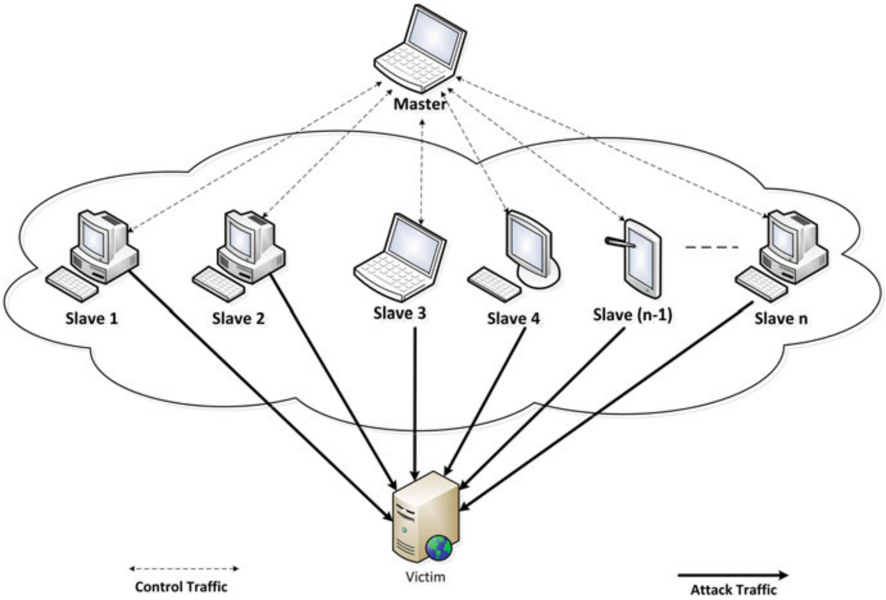


Fig. 1 A typical set-up of a DDoS attack

Moore et al. used their 'backscatter analysis' technique to expose the *worldwide* prevalence of DDoS activity [5]. Their proposed techniques was based on the hypothesis that the attacker often forges or spoofs the source IP address of the packets prior to sending them to the victim. Spoofing of source IP is performed to conceal identity of location. Upon receiving a request from spoofed IP, a response is sent from the victims machine to what is believed to be a genuine host. As the IP address is randomly selected during the spoofing process, the entire IP address space becomes equally likely to receive a response, a phenomenon they referred to as backscatter. Using this backscatter analysis and monitoring the number of replies sent to non-existent IPs over a three-week period 12,805 attacks against an approximately 5,000 distinct Internet hosts from more than 2,000 unique organizations were observed. This widespread nature of DDoS attacks, mainly originating from China, is conformed by a report from Prolexic [6]. A more recent study by Imperva Incapsula shows an increased number of short-lived repeat DDoS attacks such as hit-and-run pulse-wave attacks, Bitcoin as one of the most targeted industries, high-rate and persistent network layer attacks on the rise, and continuous growth of Botnet activity from India and Turkey [7].

The continuous evolving nature, complexity, frequency and magnitude of DDoS attacks implies that the study of such attacks including their detection, characterization, defense and mitigation remain an active area of research and investigation. This chapter focuses on the pertinent DDoS attack detection techniques, defense methods, and launching mechanisms. It also presents an extended taxonomy of

DDoS attacks to include recent attacks, and provides future research directions. Section 2 presents an extended taxonomy of DDoS attacks and describes different methods and mechanisms used to launch DDoS attacks. Section 3 outlines the various reasons for success of these attacks. Section 4 describes in detail some of the pertinent work done in DDoS attack defense methods. The section focuses on attack prevention, detection, traceback, and characterization and mitigation. Finally, Sect. 5 discusses the impact, sophistication and future trends in DDoS attacks and provide directions for research in this important and constantly evolving area.

2 DDoS Attack Taxonomy and Launch Methods

DDoS attack detection research has, not surprisingly, been viewed as a two-dimensional problem – the 'type of attack' and the 'target of attack', as shown in Fig. 2. The classification of DDoS attacks based on the 'target of attack' not only foreshadows the possibility of an attack on any networked system, but also highlights the fact that the magnitude of its impact invariably depends on the resources (computational and communicational) available to the attackers.

In order to exhaust the available resources, an adversary can initiate an attack by overwhelming the target by sending large number of spurious requests. This category of attack is known as the high-rate flooding attack or brute force attack or volumetric attack. These attacks often require attackers to gather sufficient resources both bandwidth and computing to overwhelm the target. Accumulating these computational and networking resources might have been difficult in the past, but with the recent advancements in attacking softwares, availability of high-speed networks, and accessibility of compromised bots that can be 'hired' for as low as $150 per day, it is not particularly difficult [8]. TCP, ICMP, UDP, and HTTP flooding are some of the common types of high-rate flooding attacks.

Contrary to these high-rate flooding attacks, semantic attack exploit the design or implementation flaws of an application or a protocol to cause a denial of service. This can make a semantic attack more challenging to execute as compared to a high-rate flooding attack as it requires the adversary to have comprehensive understanding of the application or protocol being targeted. Semantic attacks are more stealthy in nature and can be launched successfully even with a disproportionate distribution of resources (network bandwidth and processing capacity) between an attacker and the victim. The 'Ping of Death' is a classic example of a semantic attack, executed by sending malformed ICMP packets to the target [9]. Suriadi et al. [10] proposed an application layer semantic attack by exploiting the SOAP format and thereby allowing deeply nested XML to be successfully embedded into the transmitted message, and forcing the XML parser within the service to process the document often causing memory exhaustion and leading to a DoS attack.

It is to be noted that both high-rate flooding and semantic attacks can occur either at the network or application layer of the TCP/IP stack. A TCP SYN flooding attack is an example of a network layer attack exhausting the available network bandwidth

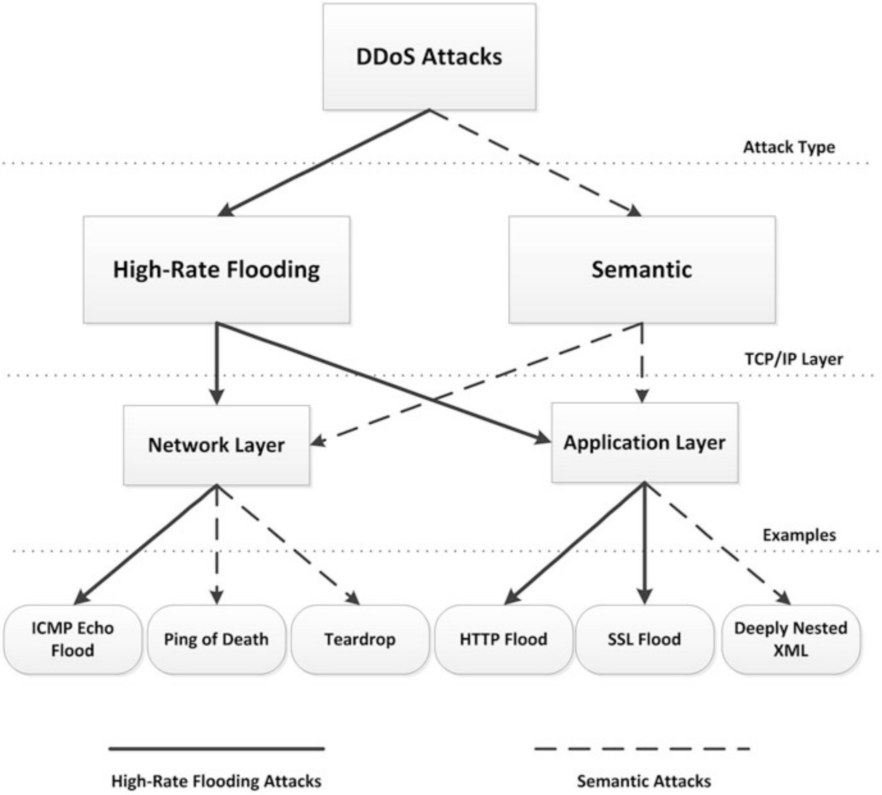


Fig. 2 Two-dimensional view of DDoS attacks

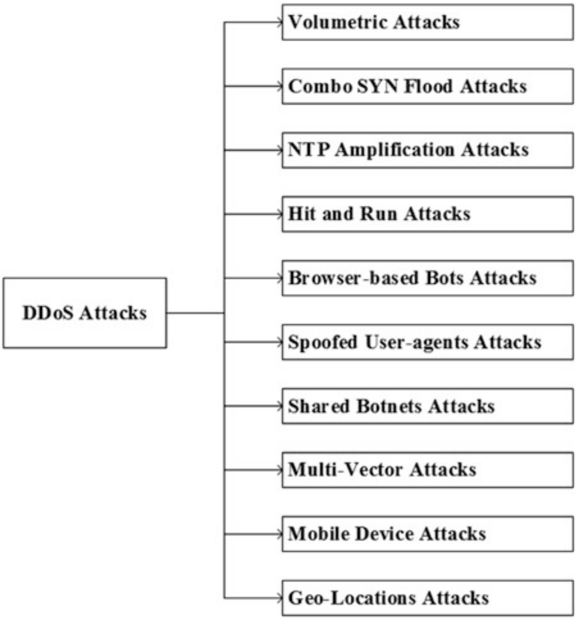
of the victim, while an HTTP flood attack is an example of an application layer flooding attack targeting the application running on the target. Similarly, a deeply nested XML attack and a teardrop attack are examples of application and network layer semantic attack respectively.

2.1 DDoS Attack Taxonomy

Many authors have tried to classify DDoS attacks based on attack launching mechanisms. Jelena et al. [11] classified DDoS attacks (a) by degree of automation wherein they can be categorized into manual, semi-automatic and automatic DDoS attacks, (b) by exploited vulnerability wherein they can be categorized according to type of protocol or type of vulnerability used, (c) by attack rate dynamics wherein they can be categorized into continues or variable rate attacks, (d) by level of impact wherein they can be categorized into disruptive or degrading in nature. Further, Lee et al. [12] classified DDoS attacks into bandwidth or resource depletion attacks according to the type of network resource overwhelmed. Bhuyan et al. [13] extended the taxonomy of DDoS attacks originally proposed by [11] and [12]. They classified DDoS attacks based on the type of architectural model used by the attackers into agent-handler, IRC based, and peer to peer (P2P) based DDoS attacks. According to the authors, there are mainly two types of DDoS attacks in existence (a) network (Layer 3/4) DDoS attacks that target the network and transport layers. These attacks overwhelm and consume whole of the network level resources of a target network or a webserver, (b) application (Layer 7) DDoS attacks exploit a vulnerability in a web-based application. These attacks overwhelm and consumes the resources of a webserver or a database powering a web-based application and shut down its services. Attackers often mimic legitimate user behavior and use authentic ways to launch application layer attacks which make them harder to detect. Xiang et al. [14] characterized DDoS attacks into (a) high-rate DDoS (HR-DDoS) attacks, when the traffic rate of attack flows is more than the legitimate traffic flows, and (b) low-rate DDoS (LR-DDoS) attack when traffic rate of attack flows is similar or less than the legitimate traffic flows [15].

Though the existing set of taxonomies of DDoS attacks are complete in themselves but they did not fit into the ever changing modus operandi of DDoS attackers. The percentage of IoT and mobile devices have increased manifolds over the years [16]. It has changed the trend and type of DDoS attacks being launched nowadays. So, the existing taxonomies of DDoS attacks need to be extended to incorporate these new diversified types of DDoS attack methods as shown in Fig. 3 and described below:

Fig. 3 DDoS attack methods



- **Volumetric attacks:** Such type of DDoS attacks overwhelms the available network bandwidth of a target network with a flood of data packets. These attacks overload the targeted network or server with very high volumes of traffic congestion and cause a denial of service to legitimate users. Such attacks can crash down any business or web service within a few minutes. Examples of volumetric attacks include TCP SYN attack, ICMP attack, Smurf attack, etc. Such network-layer attacks are designed to overwhelm bandwidth, networking resources, and applications that are unable to absorb the increased traffic volumes.
- **Combo SYN Flood Attacks:** In a traditional TCP SYN attack, the requester sends multiple SYN messages to the targeted server without receiving or transmitting ACK messages. As the resources of a web server are limited, it begins dropping out of new connection requests and ultimately, resulting in a denial of service. A combo SYN flood is composed of two types of TCP SYN attacks – one with regular SYN packet size, and the other with larger SYN packet size above 250 bytes. The conventional SYN attack exhausts the server resources (e.g., CPU), whereas the larger packet size in SYN attack causes network saturation. Such attacks can quickly consume the resources of a target server, or of intermediate network devices such as firewalls and load balancers. As per the latest DDoS attacks report from Imperva [16], out of all network layer DDoS attacks occurred nowadays, 75% are Combo SYN flood attacks.
- **NTP Amplification Attacks:** Such DDoS attacks have been used extensively in recent times. The attackers exploit MONLIST feature of Network Time Protocol (NTP) which is used by computers to synchronize their clocks over the internet. Attackers then send redundant MONLIST requests to NTP servers using destination IP of the victim. In this way, a huge volume of useless traffic is sent by the NTP server towards the novice target and overwhelmed it with multiple data packets. There are around 400,000 NTP servers deployed across the Globe that can potentially be exploited using an NTP amplification attack. As per the latest DDoS attacks report from Imperva [16], it is one of the leading attack vectors nowadays and has surpassed frequently accessed SYN flood attacks.
- **Hit and Run Attacks:** In such type of DDoS attacks, attackers randomly generate short packet bursts over an extended period; for days or even weeks. These sophisticated attacks are specifically designed to elude slow-reacting DDoS defense solutions. Such attacks are prevalent among attacker community because of their ease of deployment and low cost. They typically last for 20–60 min in duration. After causing some collateral damage to a target server, such attacks usually occur again after another 12–48 h. They force the anti-DDoS defense solution to be active all the time and can easily elude the existing preventions mechanism such as DNS rerouting and tunneling.
- **Browser-based bot attacks:** Browser-based bots typically become active during a legitimate web browsing session and are sneakily installed on credulous user systems upon visiting a malicious website. Such bots are called Bad bots, and can easily emulate the normal user browsing behavior to elude current DDoS defense solutions. These bots primarily target the application layer and can easily

crash down a web server with mere 50–100 requests per second. Such attacks are difficult to prevent and detect.

- **Spoofed User Agents:** There are Good bots in existence as well, such as Google-bots or Facebook-bots that cannot be stopped to install and, that are critical to ensuring the proper functioning of websites. Bad bots mimic and spoof Good bots to dodge detection. Attackers use this method to pass through low-level filters and proceed to inflict chaos on target webserver. Some of the common spoofed user-agents are Mozilla/5.0 Baiduspider/2.0, MSIE 6.0, Googlebot/2.1, and Linux i686.
- **Shared Botnets:** Nowadays, even a novice and non-technical user can use publically available Botnets either on rent or on sharing basis to launch diversified DDoS attacks. The same machine is sometimes compromised by more than one Botnet. It leads to the generation of sophisticated volumetric attacks with dissimilar traffic patterns which not difficult to identify but also elude the existing DDoS defense system which works on the principle of flow similarity. The trend of latest DDoS attacks is to use more and more shared botnets as they can be accessed cheaply and easily without any technical knowledge.
- **Multi-Vector Attacks:** Traditionally, DDoS attack traffic is composed of a single attack type or a vector. However, the modus operandi of DDoS attacks has been changed drastically using multiple vectors to disrupt the services of a web server. A multi-vector DDoS attack is a blend of (a) volumetric attacks; (b) state exhaustion attacks; and (c) application layer attacks. As per the recent report of Imperva [16], over 81% of DDoS attacks occurred nowadays are multi-vector attacks. Being a combination of different suave techniques, such attacks are difficult to detect and mitigate; and have more success rate as compared to traditional single vector DDoS attacks.
- **Mobile Device Attacks:** The number of mobile users has increased dramatically over the last few years. The cheaper internet bandwidth and faster connectivity leads to more chances for mobile devices to be compromised and inadvertently used to launch mobile DDoS attacks. Mobile phones and tablets are not unaffected by the ever-growing malware as they have weaker security protection as compared to PCs. Lack of awareness of installing anti-virus application, freely available vulnerable mobile applications further adds up the chances of being compromised. So, there is a need to customize existing DDoS defense solutions with the additional layer of complexity in mitigating mobile device attacks. Further, freely available new tools, such as Low Orbit Ion Cannon (LOIC) and High Orbit Ion Cannon (HOIC) intentionally use the mobile devices to participate in ongoing attacks.
- **Geolocations DDoS Attacks:** The presence of insecure IT infrastructure, vulnerable hosting environments, and internet-connected devices have given rise to a series of geolocations DDoS attacks. A DDoS attack may originate in one country but may use the unprotected infrastructure of another country, and later amplified by other environments. The extensive use and deployment of less secure IoT devices have further increased the chances of geolocations DDoS attacks. However, the implementation of sturdier guidelines and security policies

could suggestively lessen the frequency of such kind of DDoS attacks. As per the latest DDoS attacks report from Imperva [16], 52% of the DDoS attacks originate from only ten countries including India, China, Iran, Indonesia, US, Thailand, Turkey, Russian, Vietnam, and Peru.

2.2 DDoS Attack Launch Methods and Mechanisms

DDoS attacks are primarily launched either manually with human coordination or automated using botnets. Manually coordinated attacks require a significant human intervention to be successful and are generally 'ideologically-motivated'. These attacks involve a large army of volunteers, with a common purpose, using their individual machines and a pre-shared tool. Depending on the number of volunteers orchestrated by an attacker, the computing capacity of their individual machines, and the complexity of the attacking tool being used, the aggregated traffic volume targeted to the victim machine can exhaust the available resources and render it unavailable to its intended clients. A recent example of a manually coordinated attack was *Operation Payback*, a name given to attacks launched by a group called *Anonymous* against commercial websites (Mastercard, PayPal,and Amazon) and anti-piracy organizations after they withdrew their ties with WikiLeaks [17–19]. These attacks were launched using a modified version of LOIC (Low Orbit Ion Cannon) tool, an open-source stress testing utility. LOIC was modified and extended to add a new feature called 'Hivemind' which was used to connect volunteers' LOIC tool to 'AnonOps' (a communication platform used by Anonymous) to receive attack instructions [20]. The modified tool had to be later installed on volunteers' machine to enable them to participate in the attack. The Anonymous group also created a web-page requiring volunteers to visit and click on the attack button [20].

Contrary to manually coordinated attacks, automated or Semi-automated DDoS Attacks, usually rely on exploiting network protocol and misusing them to amplify and/or obfuscate network traffic directed towards a victim. These attacks can be fully or semi automated and are generally launched using Botnets. Using browser-based bots is a common launch method in this category of DDoS attacks. Browser-based bots typically become active during a legitimate web browsing session and are sneakily installed on credulous user systems upon visiting a malicious website. Such bots are called Bad bots, and can easily emulate the normal user browsing behavior to elude current DDoS defense solutions. These bots primarily target the application layer and can easily crash down a web server with mere 50–100 requests per second.

Amplification and reflections are two most commonly used attack mechanisms to launch DDoS attacks. An 'Amplification-based DDoS attack' consists of an attacker, an amplification network, and a target victim. An amplification network is a network of host machines which allows broadcast messages to be sent. Any amplification network, when used for communication via a reply-based protocol like ICMP, is potentially prone to amplification-based DDoS attacks. When a packet from a spoofed IP is sent to the broadcast address of such networks, a response from every host is triggered and directed towards the intended victim. Smurf attack is a classic example of a DDoS attack launched using amplification.

Similar to an amplification-based attack, an adversary can also exploit a reply-based protocol such as DNS to launch a ‘reflection-based DDoS attack’ comprising of an attacker, a set of reflectors (reflective network) and a target host. A reflector can be any machine responding to an incoming request with a response sent to the source IP of that request [21]. Common examples of reflectors are web servers, DNS servers and mail servers because they send reply packets to incoming requests. Reflection-based attacks make use of a set of reflectors rather than a single host (broadcast address) in amplification-based attacks to initiate a response and cause the desired effect. A DNS Reflector Attack is a classic example of a reflection-based attack. This attack mechanism was used against Spamhaus, a provider of anti-spam DNS-based Blocklists and Whitelists [22]. Both these attack launch techniques when coupled with the distributed nature of botnets, renders such fully or semi automated DDoS attacks extremely difficult to detect and mitigate.

3 Reasons for Success

The use of latest technology, high level of sophistication, freely available user-friendly attack tools, cheaper Botnets-for-hire services, and advanced tactics have led to the multidimensional growth of DDoS attacks over the years. The traditional cyber security methods like Firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), and Router Access Control Lists (ACL’s) are unable to provide an ideal solution against DDoS attacks. Some of the reasons can be summarized as follows:

1. Firewalls perform state-level monitoring of each incoming connection. When a DDoS attack occurs, a high volume of network packets travels towards a specific destination. For each malicious network packet, a new connection or network flow is established at a Firewall resulting in exhaustion of more legitimate connections in the connection table which is limited in size. It, in turn, causes exhaustion of Firewall resources and leading to degradation of its performance. The Firewalls can shut down specific flows associated with attacks, but cannot perform anti-spoofing tasks similar to a Router. Firewalls are unable to discriminate between legitimate and DDoS attacks due to a similarity of network traffic and legitimate connection setups in application layer DDoS attacks.
2. The IDS/IPS solutions have some anomaly-detection capabilities. They can recognize malicious network packets with valid protocols. They are widely used along with traditional firewalls to block the attack traffic automatically. But they often generate a high number of false positives and false negatives and requires manual configurations specific to a network.

3. Both IDS/IPS and Firewalls are deployed close to the protected web server. They are not the first line of defense where DDoS attacks can be filtered before reaching to the target web server. However, DDoS mitigation techniques can be deployed on the edge routers for early detection.
4. IDS/IPS techniques can be used to detect some known types of DDoS attacks because the majority of them followed signature-based detection approach. However, the signature-based techniques cannot detect zero-day attacks. Even mitigation function is not provided by any of the available IDS/IPS.
5. DDoS attack traffic cannot be filtered by router access control lists (ACLs) alone as they use valid network protocols. Routers can be configured to stop trivial DDoS attacks (e.g., a ping attack) by filtering the nonessential protocols and can also prevent invalid IP addresses through ingress/egress filtering. However, they are typically ineffective against more sophisticated spoofed and application-level DDoS attacks using valid IP addresses.

Apart from the reasons above, there are various other reasons as mentioned below that lead to the successful launching of DDoS attacks and makes these attacks extremely challenging to defend.

- **Automated, user-friendly attack tools:** Availability of user-friendly and freely available attack tools and cheaper Botnets-for-hire services give flexibility to the attackers to launch a variety of diversified DDoS attacks without any technical knowledge. These tools automatically recruit and launch attack traffic with just one click without having any technical knowledge about them.
- **No common characteristics of DDoS streams:** Attackers are becoming more intelligent nowadays. To elude the current DDoS defense deployments, they mimic the characteristics of legitimate traffic and regularly alter the attack patterns. Such a similarity of both types of traffic makes the characterization and filtering very difficult.
- **Hidden identity of participants:** Another important characteristic of DDoS attacks is that they use the technique of IP spoofing to hide, where the attackers make use of fake but legitimate IPs to send the packets to the target. In this way, the attackers try to defeat existing resource-sharing mechanisms which works with valid IP address and also it makes the process of traceback the actual identity of attackers very difficult. In the absence of IP spoofing, malicious IPs could potentially be differentiated from the legitimate ones, and their traffic could be filtered accordingly.
- **Huge volume of traffic:** Under a DDoS attack, a vast number of redundant packets are sent towards the victim to overwhelm its network and server resources which makes the process of traffic profiling tough. Under this considerable network traffic volumes, the defense solutions can merely perform per-packet processing and start dropping the legitimate packets and lead to denial of service to legitimate users.
- **Large number of unwitting and geographically distributed participants:** A DDoS attack involves recruiting of a large number of geographically dispersed attack nodes to generate a massive volume of aggregated attack traffic towards

a victim. It is possible because of the availability of a large pool of unsecured hosts sitting in homes, school, business and governments around the world. The impact of DDoS attack could be controlled if somehow attackers are not able to recruit many agents. But with the ever-increasing number of internet and mobile users over the years, this pool of novice agents being distributed over the globe has also increased manifolds. So, even if we found some ways to secure these novice systems, it requires a long time to deploy such practices in reality to limit the impact of DDoS attacks.
- **Persistent security holes on the Internet:** All the Internet traffic passes through a set of well-connected routers called autonomous systems (ASs) before reaching out to the target. These specialized high-speed ASs are provisioned to forward huge Internet traffic from one hop to another. If some of these ASs become heavily congested or crash down by attackers, the whole of the Internet would slog to cessation and would have a distressing consequence on global connectivity.
- **No administrative domain cooperation:** Since there is no centralized control of the Internet infrastructure and low administrative cooperation between ISPs, deploying a DDoS defense on different parts of the Internet is practically a difficult problem to address. Moreover, to tackle huge volume of DDoS traffic, large amount of resources is also required which cannot be managed by a single victim alone, so a pragmatic DDoS defense solution requires a complete defense infrastructure with autonomous control.

4 DDoS Attack Defense Methods

Many DDoS defense schemes have been proposed in the literature for defending against DDoS attacks but an effective solution is not available till date. Even the attackers also consistently upgrade their skills to circumvent existing countermeasures. The architecture of a typical DDoS defense system is shown in Fig. 4.

As shown, a complete DDoS defense solution is composed of a number of modules namely: Traffic monitoring and analysis, Prevention, Detection, Traceback, Characterization and Mitigation modules. All these modules work in collaboration with each other to defend from a DDoS attack. Accordingly, Peng et al. [23] has classified the DDoS defense methods into following four categories:

- Prevention
- Detection
- Traceback
- Characterization and Mitigation

Traffic monitoring and analysis module sample the network traffic as per the relevant network traffic features. This sampled network traffic is then given as input to the proposed detection algorithm. Attack prevention methods stop the attack traffic before reaching out the specified target. Attack detection method refers to

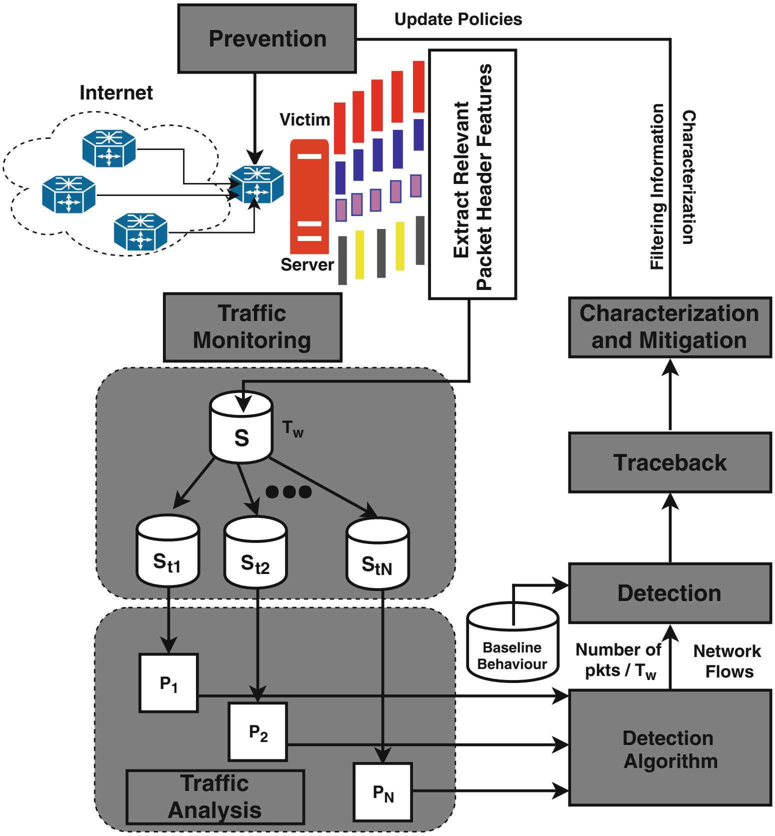


Fig. 4 Modules of a typical DDoS defense system

the detection of attack traffic when it occurs. Traceback of the attack source or its identification is the process of identifying the actual sources of the attack packets. Attack mitigation or response is the last step of a DDoS defense in which techniques are applied to minimize the impact of ongoing attack.

It is worth mentioning that the successful DDoS defense deployments depends on its placement along with the underlying logic of various defense modules [24]. As per [15, 25], a DDoS defense can be deployed at source-end, intermediate network, and victim-end. However, each of these possible deployment location has its own merits and demerits. Traditional security approaches such as Router ACLs, firewalls, IDS/IPSs are not able to protect from against DDoS attacks effectively that has lead to the absence of a perfect solution to combat against DDoS attacks till date; some of the reasons may be the decentralized nature of Internet, collateral damage, lack of collaboration among ISPs, the absence of latest real datasets, infrastructure changes, and obsolete methods used for validation purpose, and deployment issues, etc. [25–30]. The prominent approaches proposed by the fellow researchers for the efficient working of these modules are summarized in subsequent sections.

4.1 Prevention Methods

A prevention is always better than a cure. Attack prevention is the first step to stop an attack before it cause damage to the critical infrastructures and services of a network. Prevention methods aim to fix the security vulnerabilities that are exploited by DDoS attackers to launch attacks. Prevention methods are implemented with a packet filtering technique that is used to drop the malicious incoming packets.

Ingress means the packets that are coming towards the local area network and egress means the packets that are leaving from a local area network as shown in Fig. 5. In the year 1998, Senie et al. [31] proposed an ingress/egress filtering method to prevent DDoS attacks at the edge level routers of the protected network with the aim to allow only those network packets with a pre-specified IP address range. But such methods can be easily eluded by the sophisticated attackers by making use of IP spoofing technique. In this technique, attackers alter the source IP address space in the IP packet headers so that victims are unable to discriminate the attack packets from normal ones. Further, Park et al. [32] extended the concept of ingress filtering originally proposed by [31] to be deployed beyond a LAN. They implemented their proposed Router based packet filtering (RPF) method at the core of the Internet. Their proposed scheme works on the principle that only a limited number of source networks called autonomous systems (ASs) would send traffic on a specific link. Based on this information, traffic with spoofed IP address range can be discarded easily. This technique was then complemented by Li et al. [33] by using a source address validity protocol (SAVE) to store information regarding legitimate source IPs on each interface of the routers and block all other IPs. This scheme continuously propagates updated messages of valid source IPs from source to destination locations. But this scheme requires changes in the well-established routing protocols and universal deployment for better prevention which was very difficult to achieve.

In 2003, Peng et al. [34] proposed a novel scheme to filter attack traffic based on the history of IP addresses. In their scheme, every victim maintained its own list of IP addresses under normal working of a network i.e. under no attack. During a DDoS attack, only those IPs are allowed to send traffic which are available in the previously maintained IP address database. However, such scheme was vulnerable to any sophisticated DDoS attack that mimics legitimate traffic behavior. To overcome this problem, Kim et al. [35] proposed a statistical filtering mechanism called PacketScore, in which every network packet is given a score based on the selected traffic features. Their proposed scheme declared a packet as legitimate packet if the computed score is less than a dynamically computed threshold otherwise declare as attack packet without any human intervention. Their proposed scheme works well for non-spoofed DDoS attacks but the approach itself was vulnerable to performance degradation when the number of attributes used to compute packet score increased.

Further, Liu et al. [36] proposed a hybrid filter-based prevention method called a StopIt to overcome the limitation of IP spoofing. They proposed a passport method by making use of a secure source authentication system. It enable each destination

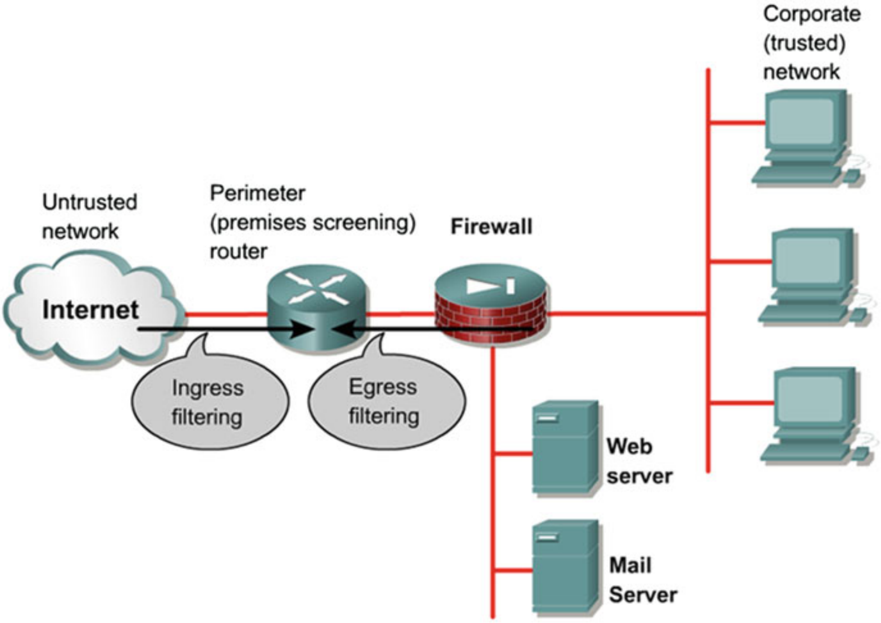


Fig. 5 Prevention of DDoS attacks using Ingree/Egress Filtering

target to install a network filter that blocks the undesirable attack traffic as it receives. However, their proposed method is vulnerable to flooding DDoS attacks. To prevent from such situations, the proposed framework can be configured in such a way that only the requests from nodes within a local AS or from other StopIt servers need to reach to a StopIt server but such manual configurations for an AS with large number of nodes is a very challenging.

Some authors like Saifullah et al. [37] proposed a weight-fair throttling mechanism at the upstream routers to prevent a high profile web server from DDoS attacks. They used a leaky bucket congestion control algorithm to control the network traffic volume destined for a target server based on the connection count. In their proposed scheme, the survival capacity is kept at low initially to protect the target server from any sudden burst of attack traffic. The capacity is increased in each subsequent rounds of the algorithm based on the feedback from the server. The updated capacity is then forwarded to its child routers which then propagated it further to all the routers.

Apart from preventing network layer DDoS attacks, some authors like Saleh et al. [38] proposed a Flexible, Collaborative, Multi-layer DDoS framework for preventing application layer DDoS attacks. Their framework blocks the source IPs based on pre-built black lists. However, their framework suffer produced low FNR. In some recent works, Muharish et al. [39] used neural network learning algorithms and statistical analysis to design a novel packet filtering system. They applied a self-organized-map neural network clustering technique to characterize and classify the different types of traffic. Further, Kalkan et al. [40] proposed a distributed,

Table 1 Comparison of prevention methods

Authors/ year	Deployment type	Working mode	Parameters	Prevention mechanism
Senie et al. 1998	Source-end	Distributed	src/dst IPs	Ingress/egress filtering
Park et al. 2001	Intermediate	Distributed	No. of autonomous systems src/dst IPs	Extension of ingress filtering implement Router based filtering (RBF) BGP routing information
Li et al. 2002	Intermediate	Distributed	src IPs	Proposed a source address validity protocol (SAVE) to overcome the limitations of RBF empower routers to store IPs at local level
Peng et al. 2003	Victim-end	Centralized	src/dst IPs	Filtering based on history of src/dst IPs
Kim et al. 2006	Victim-end	Distributed	src/dst IPs, ports TCP flags, TTL packet size, protocol	Packets are scored based on traffic features
Liu et al. 2008	Intermediate	Distributed	src/dst IPs	Automated characterization Selective packet discarding Overload control
Saiffulah et al. 2009	Intermediate	Distributed	Network traffic volume at upstream routers	Weighted-fair throttling
Saleh et al. 2015	Victim-end	Distributed	Entropy	Multi-layer defense framework
Muharish et al. 2016	Victim-end	Centralized	src/dst IPs, ports Packet transfer rate packet length, count	Applied a self-organized-map neural network clustering technique to characterize and classify the different types of traffic
Kalkan et al. 2016	Victim-end	Distributed	src/dst IPs protocol, packet size No. of packets	Compute score of each connection based on traffic features a realtime filtering mechanism

proactive and collaborative realtime filtering mechanism called ScoreForCore against application layer DDoS attacks. Their proposed scheme compute score of each connection based on the extracted relevant packet header features under normal network conditions. i.e. under no attack. When the network is under attack, the score of each incoming connection is compared with baseline score of connections. Their proposed scheme detect known attacks with 100% accuracy whereas it detect novel unknown attacks with 80% detection accuracy (Table 1).

It is clear from the above discussion of various network level and application level prevention mechanisms that all of the prevention schemes require wider geographical deployment to be more efficient but due to the openness and decentralization of Internet, it is very difficult to implement them.

4.2 Detection Methods

Mainly, DDoS attack detection methods can be categorized based on two approaches: (a) signature-based detection and (b) anomaly-based detection. Signature based approach match a known pattern with the pattern of incoming packets whereas anomaly based approach match the pre-built network traffic model with the incoming network traffic behavior in real-time. As mentioned in [23], anomaly-based detection approach has some inherent limitations as mentioned below:

- **Sophisticated attackers can monitor the network traffic to train their detection systems** There is a possibility that sophisticated attackers can monitor the network traffic to predict the traffic volume, number of source/destination IPs, and source/destination port numbers. This information can then be used by the attackers to launch variety of DDoS attacks in such a way so that there is a minimal deviation in the network traffic features which could effect the working of an anomaly based detection system.
- **Inappropriate selection of threshold values can lead to high false positive rates** Since network traffic is highly dynamic in nature, it is very difficult to set the baseline network traffic parameters. These parameters are used to set the crucial optimal threshold values for the efficient working of an anomaly based detection system. Further, the absence of benchmarked datasets for representing normal traffic also make this selection very difficult.
- **Difficult to extract both qualitatively and precisely appropriate features of legitimate and anomalous network behavior** Existing research have used diversified set of packet header features for the detection of attack traffic but to reduce the overall complexity of computing all of these packet header features, it is necessary to use only those packet header features that are sufficient to detect DDoS attacks.

Fellow researchers have proposed many isolated but effective solutions to detect different types of DDoS attacks. We have summarized these prominent DDoS attack detection methods in Table 2. These methods have been compared on an identified set of attributes such as type of attack detected (LR-DDoS/HR-DDoS), type of deployment (source-end/intermediate/victim-end), detection mode (centralized/distributed), type of network header parameters used, detection metric used, validation mechanism (simulation/emulation/realtime/datasets), datasets used and detection layer (network/application).

Table 2 Comparison of detection techniques for DDoS defense

Authors/ year	Attack type	Deployment type	Detection mode	Parameters	Detection metric	Validation technique	Datasets used	Detection layer
Gil et al. 2001	HR-DDoS	Victim-end	Distributed	Packet rate	CPU cycles Memory size	Realtime	Click tool	Network layer
Feinstein et al. 2003	HR-DDoS	Victim-end	Distributed	src/dst IP src/dst Ports	Shannon Entropy Chi-Square	Simulation	NZIX Bell Labs Ohio University	Network layer
Akella et al. 2003	HR-DDoS	Intermediate	Distributed	src/dst IP packet rate		Simulation	Abiline Backbone Trinoo, TFN	Network layer
Jin et al. 2004	LR-DDoS	Victim-end	Distributed	TCP flags	Correlation Covariance	Simulation	dec-pkt-1 dec-pkt-2	Network layer
Mirkovic et al. 2005	LR-DDoS HR-DDoS	Source-end	Distributed	packet rate connection size	No. of failed transactions No. of dropped packets	Emulation	UCLA Cleo attack tool	Network layer
Zhang et al. 2006	HR-DDoS	Intermediate	Distributed	src/dst IP, ports protocol,drop rate packet size,TTL	Legitimate traffic	Simulation		Network layer

Chen et al. 2007	HR-DDoS	Victim-end	Distributed	CAT change point detection	CUSUM DETER	Emulation		Network layer
Kumar et al. 2007	LR-DDoS	Victim-end	Distributed	src/dst IPs, ports protocol	Shannon Entropy	Simulation		Network layer
Lu et al. 2007	LR-DDoS	Victim-end	Distributed	src/dst IP, Port TCP SYN/FIN(RST) pkt rate	Correlation	Simulation	Auckland university	Network layer
Nychis et al. 2008	HR-DDoS	Victim-end	Centralized	src/dst IPs,ports flow size in/out Degree	Shannon Entropy Correlation	Simulation CMU-2008	GEANT, Internet2	Network layer
Li et al. 2008	HR-DDoS	Victim-end	Centralized	src/dst IPs, ports protocol no. of packets	Euclidian distance Cluster Analysis	Simulation	2000 DARPA	Network layer
Chonka et al. 2009	HR-DDoS	Victim-end	Centralized	flow similarity	Chaos Theory Lypanuv Exponent	Simulation	2000 DARPA	Network layer

(continued)

Table 2 (continued)

Authors/ year	Attack type	Deployment type	Detection mode	Parameters	Detection metric	Validation technique	Datasets used	Detection layer
Xia et al. 2010	LR-DDoS HR-DDoS	Victim-end	Centralized	flow similarity no. of packets	SIC dropped packets	Simulation		Network layer
Sangkatsanee et al. 2011	HR-DDoS	Victim-end	Centralized	src/dst IPs, ports protocol, packets	Shannon Entropy Information gain	Realtime	RLD'09 Weka tool	Network Layer Application layer
Xiang et al. 2011	LR-DDoS	Victim-end	Centralized	src/dst IP protocol	Renyi Entropy Renyi Divergence	Real Datasets	1998 MIT Lincoln CAIDA 2007 attack	Network layer
Karimazad et al. 2011	HR-DDoS attacks	Victim-end	distributed	src/dst IPs no. of packets packets size	RBF Neural network	Simulation	UCLA	Network layer
Das et al. 2011	HR-DDoS	Victim-end	Centralized	no. of requests request pattern	DSB Index Clustering	Simulation	1999 KDD LBNL University campus	Network Layer Application layer

Wang et al. 2012	LR-DDoS	Victim-end	Distributed	src/dst IP, Port protocol packet length,rate	JDR Entropy	Realtime	Synthetic	Network layer Application layer
Tellenbach et al. 2012	HR-DDoS	Victim-end	Centralized	src/dst IPs, ports Correlation	Tsallis entropy	Simulation	Netflow Data Flame attack tool	Network layer Application layer
Franccois et al. 2012	HR-DDoS	Intermediate	Distributed	No. of packets Score	Shannon entropy KL Divergence	Simulation	1999 DARPA Router Adjacency Dataset	Network layer
Bhatia et al. 2012	HR-DDoS	Victim-end	Centralized	src/dst IPs no. of packets CPU Load Memory/CPU Usage	Shannon entropy Correlation	Realtime	CAIDA 2007 1998 MIT Lincoln	Network layer Application layer

(continued)

Table 2 (continued)

Authors/ year	Attack type	Deployment type	Detection mode	Parameters	Detection metric	Validation technique	Datasets used	Detection layer
Beitollahi et al. 2012	LR-DDoS	Victim-end	Centralized	Request/ download rate up/down time page access rate src IP, no. of packets	Shannon entropy	Simulation	Clarknet www server	Application layer
Shiales et al. 2012	LR-DDoS	Victim-end	Centralized	packet inter arrival time	Fuzzy logic	Real Datasets	1999 DARPA Hping, BlackEnergy tools	Application layer
Ni et al. 2013	HR-DDoS	Victim-end	Centralized	No. of requests	Shannon entropy SVM Classifier	Simulation	Changzhov www server logs Mydoom Botnet	Application layer
Ma et al. 2014	HR-DDoS	Victim-end	Centralized	src/dst IPs	Tsallis entropy Lyapunov Exponent	Simulation	1998 MIT Lincoln	Network Layer
Jun et al. 2014	HR-DDoS	Victim-end	Centralized	src/dst IPs, ports protocol	Shannon entropy	Simulation		Network layer

Spognardi et al. 2014	HR-DDoS	Victim-end	Centralized	flow	Renyi's entropy KL divergence	Realtime	Net flows	Application layer
Basicevic et al. 2015	LR-DDoS HR-DDoS	Victim-end	Centralized	src/dst IPs, ports in/out Degree no. of packets	Tsallis Entropy Renyi's entropy Correlation	Realtime		Network layer
Dorbala et al. 2015	HR-DDoS	Victim-end	Centralized	src/dst IPs, ports no. of packets packet size,protocol	Manhattan distance KNN classifier	Real datasets	2000 DARPA 2007 CAIDA	Network layer
Sachdeva et al. 2016	HR-DDoS	Victim-end	Distributed	src/dst IPs protocol	Shannon entropy	Simulation	1998 FIFA 2007 CAIDA	Network layer Application layer
Bhuyan et al. 2016	HR-DDoS	Victim-end	Centralized	src/dst IPs, ports protocol no. of packets	Renyi's entropy Shannon entropy	Real datasets	1998 MIT Lincoln 2007 CAIDA	Network layer
Joldzic et al. 2016	HR-DDoS	Victim-end	Distributed	src/dst IPs	Shannon entropy	SDN technique	–	Network layer

In 2001, Gil et al. [41] proposed a heuristic data-structure called MULTOPS to detect HR-DDoS attacks by analyzing the packet rate in both the directions. MULTOPS is basically a tree of nodes that contains packet rate statistics for subnet prefixes at different aggregation levels. Their idea works on the assumption that the packet rates between two nodes in both the directions are comparative during the normal network conditions i.e. without attack. A significant deviation in the packet rates indicate a bandwidth level DDoS attack. However, their proposed method may fail to detect an attack in the cases where

- malicious packets uses randomized spoofed source IP addresses, and
- a large number of disproportional flows destined towards a specific target.

For example, there is a huge disproportion among the incoming and outgoing packet rates in case of real audio/video streams, on-line movies and news. Such situations would results in increase in false positive rates. Their proposed scheme also require router reconfigurations and new memory management schemes which is again a challenging issue.

Further, Feinstein et al. [42] presented a statistical detection approach based on computing entropy and frequency sorted distributions (chi-square). It had been observed that there were anomalies in the packet header attributes of DDoS attack traffic. After the detection phase, they also proposed some filtering rules for mitigating the impact of DDoS attacks. The drawback of this approach is that there is a minimum interaction between the detection and response module which lead to high false positive and false negative rate.

Akella et al. [43] proposed an ISP level detection mechanism where each router detects traffic anomalies using normal traffic profiles of baseline network behavior. Their proposed method works on the principle that routers usually exchange messages with other neighboring routers to take detection decisions. A router analyze the messages received from other routers and declare the traffic as an attack or legitimate traffic. The main advantage of their scheme is that it produce low FPR and FNR.

Some authors like Jin et al. [44] used the concept of two-variable correlation covariance model to detect different types of DDoS attacks. They compute a covariance matrix distance function to detect traffic anomaly. The attacker nearest router focused on detection of LR-DDoS attacks whereas victim nearest router focused on detecting HR-DDoS attacks. They performed multivariate analysis be considering the six control flags of TCP header to detect SYN flooding DDoS attacks.

To remove the limitations of this work, Jelena et al. [45] proposed an anomaly based distributed model called a D-WARD which continuously monitor the bi-directional traffic flows between the target network and Internet to identify HR-DDoS attacks. Whenever there is a noticeable periodic deviation from the normal flow patterns, attack is declared. They deployed their proposed system at the edge routers of a network and monitor the incoming and outgoing traffic of the network. If there is a significant deviation in the incoming and outgoing packet rates, their proposed system decrease the packet rate. They validated their proposed system in

Emulab, legitimate traffic was taken from UCLA dataset. They generate different types of network layer DDoS attacks using cleo attack tool. False negatives can also occur because of the distributed nature of DDoS traffic and use of a vast number of zombies to launch attacks. Furthermore, some legitimate flows like real time UDP flows do exhibit asymmetry.

Further, Chen et al. [46] extended their idea to propose a distributed change point (DCP) detection architecture to detect HR-DDoS attacks. They used change aggregation trees (CAT) to work in collaboration with edge routers to detect deviations in the network traffic. The computational server construct CATs using the traffic pattern changes at attack-transit routers which represent the attack flow patterns. They observed that in the case a DDoS attack, traffic feature deviation is more. The main feature of change point monitoring method is that it is stateless and requires less computational overhead. The principal objective of this scheme was to determine a point of time when a change happens. It uses CUMSUM approach to detect SYN flooding attack. This approach works effectively if all the networks packets route through the same edge router. However, traffic in autonomous system routed through different edge routers.

Few authors [25, 47, 48] have proposed an ISP level distributed approaches to defend from DDoS attacks. For example, Kumar et al. [25] distribute the computational overhead of computing detection metric at the edge POPs of an ISP level topology. Lu et al. [47] deployed a local analyzer at edge router(s) of an ISP which communicates with a global analyzer. used machine learning algorithm, CUSUM algorithm and spatial correlation of DDoS attack traffic to detect DDoS attacks at ISP level. They also used simulation based experiments to validate their approach. Their proposed approach predicts the next network state using maximum a posteriori (MAP) criteria. They also used a variant of expectation-maximization (EM) algorithm for optimizing searching over large no. of candidate structures. Their framework detect both LR-DDoS and HR-DDoS attacks. Franccois et al. [48] presented an approach named FireCol to detect HR-DDoS attacks. Their proposed system comprised of an intrusion prevention system located at edge routers of an ISP. They form a virtual protection ring around the hosts to defend and collaborate by exchanging selected traffic information.

In 2016, Sachdeva et al. [26] extended the work of [25] to differentiate the attack traffic from behaviorally similar FE traffic. They used an ensemble of cluster entropy and source IP entropy to discriminate the two. They observed that in the case of flash events traffic cluster entropy is small whereas it is more in the case of attack traffic.

Some authors [49, 50] have also used correlation coefficient between different packet header features (source/destination IPs/ports, and the number of distinct destination/source IP pairs) to detect different types of DDoS attacks.

Many authors [14, 15, 51–56] have used information theory based metrics to detect different types of DDoS attacks. Xiang et al. [14] proposed a collaborative detection algorithm using generalized entropy metric to differentiate an LR-DDoS attack from legitimate traffic. Bhuyan et al. [15] extended the idea of [14] to compute extended entropy metric based on packet header features of source IP and incoming packet rate to detect HR-DDoS attacks.

Wang et al. [51] proposed a multistage anomaly detection framework to detect LR-DDoS attacks at an early stage. They deployed their framework at the monitors close to the attack sources i.e. on edge routers and quantitatively analyze the deviations in traffic features. They define a network traffic state (NTS) to represent the state of the network traffic at each monitoring point. Then they compute a joint deviation rate (JDR) which is a combination of the variations of multiple traffic features. Their proposed detection efficiently detects both LR-DDoS and HR-DDoS attacks. The authors claimed that their proposed approach needs only three-time windows to extract malicious IP addresses from the start time of a DDoS attack. They launch a variety of network layer and application layer flooding DDoS attacks using the botnet executables to generate attack datasets in an experimental testbed synthetically. However, their proposed framework did not detect attacks when the attack traffic rate is similar to legitimate traffic.

Bhatia et al. [52, 57] proposed a novel ensemble based detection model which combine the results of network traffic analysis with the server load analysis for detecting HR-DDoS attacks. They compute various packet header features like the number of new source IPs, the total number of source IPs, number of packets per IP from the network traffic in each sampling interval, and a set of server specific parameters of CPU utilization, CPU load and real memory usage for each type of network traffic. They differentiate the different kinds of HR-DDoS attacks on network and application layer using a feature correlation matrix. They found that there is a strong correlation between the different types of network flows. For validating their proposed scheme, the authors performed a set of real experiments to launch the ICMP, HTTP, and SSL attacks by simulating the traffic traces of CAIDA, FIFA and MIT datasets.

Ma et al. [53] analyzed the variation of Lyapunov exponent in combination with Tsallis entropy to detect anomalies in the network traffic. They proposed an exponent separation detection algorithm to verify the feasibility of combining the source and destination entropy variations to detect HR-DDoS attacks. They used the detection system evaluation parameters of true positive rate, false positive rate, and ROC curve to check the efficiency of their proposed detection scheme. They validate their proposed approach by simulating the HR-DDoS attack scenario from MIT Lincoln dataset. Jun et al. [54] proposed a flow entropy and packet sampling based detection scheme to detect HR-DDoS attacks. Their proposed detection system measures the entropy of each flow, the entropy of source port and the number of packets/sec. Spognardi et al. [55] proposed a flexible DDoS defense framework called a fast network analyzer (FAN), which analyze the aggregated network traffic to identify HR-DDoS attacks. They compute a number of information theory metrics such as Shannon entropy, Renyi entropy and KL divergence metrics using traffic features of timestamp, duration, number of packets and transmitted bytes. They found that KL divergence is best for analyzing huge amount of network traffic. Basicevic et al. [56] compute Tsallis detection metric to detect HR-DDoS attacks. They found that Tsallis entropy produce low FPR and high detection accuracy as compared to Shannon entropy in detecting DDoS attacks.

Some authors like Sangkatsanee et al. [58] identified 12 essential features of a network traffic such as source(destination) IPs and port numbers, protocol, packet rate, TCP flags for detecting HR-DDoS attacks. In some recent works, Joldzic et al. [59] proposed a novel software defined networking (SDN) based scalable solution called TIDS (transparent intrusion detection system) for detecting network layer flooding based DDoS attacks. They used Shannon entropy metric for the detection of malicious traffic.

Further, many authors [60–62] have proposed schemes to detect application layer DDoS attacks. Beitollahi et al. [60, 61] proposed a novel ConnectionScore technique to detect and mitigate application layer DDoS attacks. They compared the connection score of malicious connections during the attack with the threshold scores computed during the non-attack period. The connection score is calculated by using various statistical attributes like request/download rate, uptime/downtime, browsing behavior (page classification, page access rate and page popularity), hyperlink fraction click, hyperlink depth, source IP address distribution, arrival distribution rate of users. The connections with low scores are identified as malicious connections; thereby the server retakes bottleneck resources from them. They validate their proposed detection scheme by simulating the real traffic traces of clarknet www server and some benchmark attack tools in Emulab environment. Ni et al. [62] compute entropy of HTTP GET requests per source IP (HRPI) to detect application layer HR-DDoS attacks. They approximate an AAR auto regressive model and a SVM support vector machine classifier to identify DDoS attacks. They observed that HRPI is highest in FEs and least in attack traffic even lesser than the legitimate traffic.

Besides above discussed detection methods, many authors have also proposed efficient DDoS attack detection methods using novel techniques such as:

- Machine learning and neural networks
- Chaos theory
- Fuzzy logic
- and wavelet analysis

Lee et al. [63] performed machine learning based cluster analysis based method for the proactive detection of DDoS attacks. They separate the DDoS attack into different phases and identified various precursors required for the proactive detection of attacks. They proposed a hierarchical type of clustering detection scheme which is often used to classify plants and animals. They proposed detection system compute the Euclidian distance between the entropy values of various precursors and apply WARD's minimum variance method to find the linkage between them. To optimize the number of precursors, they use principal component analysis (PCA) method. They validate their detection scheme by simulating the 2000 DARPA IDS dataset.

Chonka et al. [64] proposed a chaos theory based model to distinguish a HR-DDoS attack based on flow similarity. They developed a neural network based system to detect anomalous traffic. Xia et al. [65] proposed a fuzzy logic based method to identify LR-DDoS and HR-DDoS attacks in real time. Their proposed approach works in two phases. In the first phase, a time series based statistical analysis of network traffic is performed using discrete wavelet transform. A schwarz information criterion (SIC) is used to find the deviations in Hurst parameter. In the second phase, the identification of attack packets and evaluation of the approach is performed by counting the number of dropped packets. The authors validate their proposed method using NS2 simulations, testbed experiments and publically available Internet traffic traces. Karimazad et al. [66] proposed a Radial Basis Function (RBF) neural networks based DDoS detection method. They deployed the proposed scheme to edge routers of the victim network. They defined a network flow consisting of seven traffic features to activate a RBF neural network in each time window. In the case of a DDoS attack, the malicious IPs are forwarded to the filtering module and generate alarm signal for further actions. Otherwise, traffic is forwarded to the downstream routers.

Das et al. [67] proposed a clustering based detection scheme for unsupervised anomaly detection using feature-based analysis of HTTP GET requests traffic. They used three different HTTP flooding attack scenarios of random flooding, shrew flooding, and blast flooding to compute legitimate access pattern and pattern disagreement between request arrivals. Based on these values, they compute a DSB index which then clusters the incoming requests as normal or malicious. They monitor the university campus traffic for making baseline behavior and then, validate their detection scheme using the KDD cup99, and synthetically generated datasets.

Shiaeles et al. [68] proposed a realtime detection and traceback approach for defending against DDoS attacks by constructing a fuzzy estimator using mean packet inter arrival times. They validate their proposed scheme using publically available DARPA dataset and synthetically generated dataset using a real experimentation setup. They used automated botnet attack tools namely Hping and Black Energy for generating encrypted application layer malicious traffic. The authors claimed that their proposed method can detect DDoS attacks and traceback malicious IPs at an early stage before the impact reached at the target server. The reporting results show over 80% success rate of the proposed approach. However, it is vulnerable to more false positives in the case IP spoofing. However, they did not discriminate the legitimate looking FEs from HR-DDoS attacks. Dorbala et al. [69] proposed a scalable implementation of a clustering and classification algorithm for detecting the HR-DDoS attacks. They calculate interval summary based on per second traffic analysis of existing real datasets. An interval summary constitutes the number of packets, average packet length, the number of TCP, UDP and ICMP packets, distinct source and destination IPs and port numbers. They classify different types of network packets using a K- nearest neighbor classification algorithm. They compute information theory based Manhattan distance metric between the various elements of a cluster. They validate their proposed approach using real datasets of DARPA and CAIDA. Firstly, they train the proposed detection system using half of the dataset records and then, apply the detection algorithm on the remaining half of the dataset records. Their proposed detection system detect HR-DDoS attacks with 99.5 precision, and 100% detection accuracy when computed with a tolerance factor k = 5.

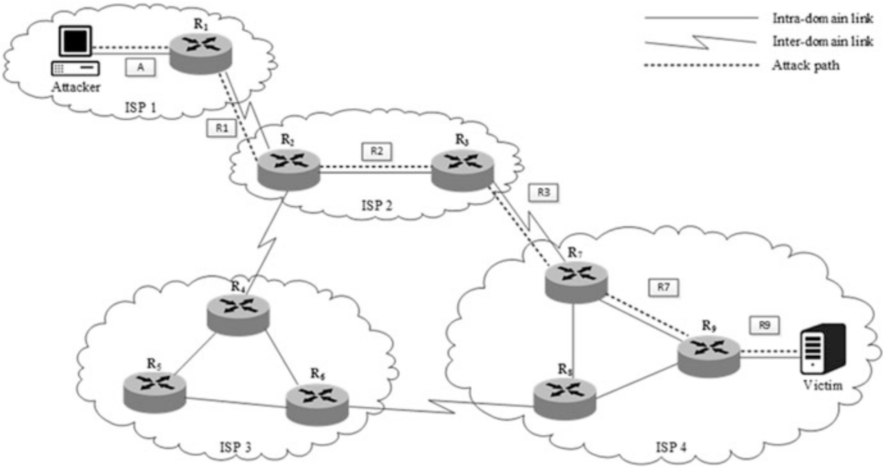


Fig. 6 A typical Traceback mechanism of a DDoS defense

4.3 Traceback Methods

Most of the DDoS attacks are characterized by a high incoming rate of network packets with random and valid source IPs. However, these source IPs are often spoofed. To identify the source of such fake network packets requires tracing the packets back to the source hop by hop. The current traceback approaches necessitate the dreary unrelenting responsiveness and support of each intermediate ISP which is not a trivial task.

Once an attack is detected, the next step is to identify the attack sources and to block the attack traffic. As per [70], traceback is defined as a mechanism of identifying actual sources of a packet sent over the Internet (Fig. 6). Mathematically, let C = $h_1+h_2+h_{n-1}$ . . . ..h_n be a connection chain between the hosts h_n (i = 1 to n). Given a hosts h$_n$ (i.e. IP Address), the traceback problem is to identity recursively the identities of $h_{n-1}, h_{n-2} \dots h_1$ in an automated way. This section summarizes the prominent work done in this area as shown in Table 3.

Burch et al. [71] proposed a generalized traceback scheme without having dependence on the cooperation of intervening ISPs. Their proposed scheme flood the network links with traffic bursts to identify the attack path. However, this scheme is less effective because in the case of a typical DDoS attack, only a small proportion of attack traffic converge from a single link, so there would not be any significant changes in the total attack traffic by flooding a single link. To improve this limitation, Savage et al. [72] proposed a IP traceback scheme based on probabilistic packet marking (PPM). In this scheme, each router is required to embed its IP address in the incoming packets while they travel through that router. Based on this embedded information, the victim can predict the attack transmission path. However, it is very difficult reconfigure the existing well established IPv4

Table 3 Comparison of traceback techniques for a DDoS defense

Authors/year	Parameters	Traceback mechanism
Burch et al. 2000	Packet rate	Flooding of network links to identify attack paths
Savage et al. 2001	src IPs	IP traceback using Probable Packet Marking (PPM) Need to re-configure IPv4 scheme on each router
Dean et al. 2002	src IPs, TOS ID	Used an algebraic approach to insert partial path information low computational comlexity
Al et al. 2006	Path coverage ratio Attack source localization distance ratio Detection % age	Combines packet marking and packet logging techniques
Yu et al. 2011	Entropy variations	Use entropy variations in legitimate and attack traffic
Wu et al. 2011	Misidentified normal edge ratio Misidentified attack edge ratio Entropy, Flow similarity	Proposed an approach based on protection agent and sentinels they apply a C4.5 algorithm to construct a decision tree using TCP SYN and ACK flag rate
Xiang et al. 2011	Information distance	Compute information distance based on variation in entropy values of local and forwarded traffic to its immediate upstream routers
Rajam et al. 2011	Ant density	Deterministic packet marking based on Ant colony optimization Compute ant density of all possible paths Low computational and memory overhead
Saleh et al. 2015	Entropy	Traceback based multi-layer defense framework
Bhuyan et al. 2016	Entropy	Traceback and filtering based on EEM metric compute entropy difference based on in-traffic and out-traffic from a router

protocol as there are no field reserved for the tracking purposes. Their scheme is also independent of any cooperation from intervene ISPs.

Dean et al. [73] proposed an alternative coding scheme to remove the limitations of PPM approach. They applied an algebraic approach to insert the partial path information so as to reduce the number of packets required to reconstruct the attack path. Authors in [74] proposed a hybrid scheme which combines the packet marking and packet logging schemes called a distributed link list traceback (DLLT) and probabilistic pipelined packet marking (PPPM). The first scheme preserves the marking information at the intermediate routers so that it can be collected using a linked list approach when required. The second scheme target to disseminate the source IPs of routers that were involved in marking packets by embedding them into the packets going to the victim. In this way, the scheme avoid the need for long term storage at the intermediate routers.

Yu et al. [75] used the entropy variations of legitimate and attack traffic to propose a new traceback scheme. In comparison to the existing IP traceback methods, their proposed strategy is more efficient in terms of less memory intensive, scalable and independent of any specific attack traffic patterns. Wu et al. [76] designed a system that can detect and traceback the origins of network layer HR-DDoS attacks sources quickly. Their proposed scheme consists of two subsystems namely protection agent and sentinels. The protection agent is located in the Victim (for detection purpose) and sentinels are located in routers (for traceback purpose). Then they apply a decision tree technique using the attributes TCP SYN and ACK flag rate, as the tests to detect abnormal traffic. They adopt the C4.5 algorithm to construct the decision tree which is based on the concept of entropy. Then they use a flow similarity algorithm to isolate the attack flows for trace back purpose. They also used an AI based classifier for detecting DDoS attacks. The authors evaluate their proposed scheme by measuring detection metrics such as false negative rate, false positive rate, false classification ratio, and detection latency.

Further, Rajam et al. [77] proposed an IP traceback mechanism for large scale distributed systems based on deterministic packet marking. Unlike other marking schemes, it reduces the computational and memory overheads. They applied their proposed scheme to secure online voting system, which in turn improves the security processed involved in the distributed systems. Saleh et al. [38] proposed service traceback oriented architecture (STBOA) to trace back the actual attacking IP source. They validate their proposed framework using simulation based experiments. Singh et al. [78] systematically reviewed a number of IP traceback schemes. They concluded that IP traceback does not play a significant role in defending against DDoS attacks. Rather, it only allows to identify the path that the attack flows follows. However, it can be integrated with other defense modules to provide the enhanced mitigation mechanisms.

4.4 Characterization and Mitigation Methods

Mitigation techniques primarily deal with flooding based DDoS attacks. Tolerating DDoS attacks concentrates on controlling the intentional and malicious traffic. Whereas mitigation is defined as the process of minimizing the impact of a DDoS attack. It can be achieved by deploying different filtering and rate limiting methods on the incoming network traffic. The main aim is to dropping out the attack traffic as much as possible whereas keeping the legitimate traffic intact. A mitigation framework requires the communication among different modules of a defense system including detection, characterization and traceback. A considerable amount of research effort has been carried in literature for tolerating and mitigating DDoS attacks as summarized in Table 4.

Floyd et al. [79] stated that flooding DDoS does not observe end to end congestion control. Due to this role of router scheduling and queuing algorithm is very important in tolerating against DDoS attacks. Their proposed mechanism identify and restrict the bandwidth allocation to high-bandwidth flows in the situation of congestion. The proposed scheme utilize the history of dropped packets from queues with RED (Random Early Detection) queue management.

Mahajan et al. [80] propose a mitigation framework called Aggregate Congestion Control (ACC) agent for routers to identify aggregates responsible for the network congestion. ACC agent identify the congestion signature using the history of dropped packets in a time window of k seconds and then filter the useless traffic accordingly. Further, routers cooperate with upstream routers using a pushback scheme to share the filtering information. Peng et al. [34] proposed an integrated framework for mitigation and traceback. They improve the pushback mechanism by introducing selective pushback a router based system to defend against DDoS attacks. DDoS attacks are treated as a congestion control problem. The main issue is to identify the congestions and then pushback a packet filter to the router closed to the source that causes the congestion. Source information is obtained using the probabilistic packet marking (PPM). By filtering the packets using the source information filtering of malicious traffic is achieved while protecting the legitimate traffic.

Zhang et al. [81] proposed a distributed collaborative approach to defend against HR-DDoS attacks. Their proposed system is deployed at an intermediate network. The proposed scheme uses a gossip based communication mechanism to exchange traffic information between independent Internet devices to collect, analyze and predict the network attacks. This compiled information is then shared among these devices so as to use it for detecting and stopping DDoS attacks more effectively and accurately at the local level. The proposed scheme uses an overlay network for the dissemination of attack information. Lu et al. [47] described a perimeter-based anti-DDoS system. Their proposed system is deployed at the edge routers of an ISP level network. Anti-DDoS extracts the relevant traffic features in first phase and then apply a spatial correlation method for the detection. The proposed scheme detect and characterize the attack packets with accuracy and without rendering the embedded logic of routers.

Wang et al. [82] proposed a distributed mitigation and filtering mechanism based on a pushback and resource regulation methods to mitigate the effect of DDoS attacks. They assume that all the routers cooperate with victim to share critical information used in implementing the defense strategy. A Pushback mechanism based on the improved aggregate-based congestion control (IACC) algorithm is applied to routers for defending bandwidth HR-DDoS attacks, whereas resource regulation is applied to victim for defending resource consumption HR-DDoS attacks. Devi et al. [83] used a set of host-network based metrics to detect HR-DDoS attack. They compute various server level statistics like the CPU and memory usage, packet loss, latency, link utilization and throughput in an experimental testbed. They also proposed a DDoS mitigation algorithm based on the interface based rate

Table 4 Comparison of mitigation and characterization techniques for DDoS defense

Authors/year	Deployment location	Detection mode	Parameters	Mitigation/Characterization approach
Floyd et al. 1997	Victim-end	Centralized	No. of dropped packets	Identify, classify and restrict bandwidth allocation to high-bandwidth flows while in congestion using TCP flows
Mahajan et al. 2002	Intermediate	Distributed	Aggregates, flows	Aggregates based congestion control (ACC) using a pushback mechanism. ACC agent identify the congestion signature using the history of dropped packets
Peng et al. 2003	Intermediate	Distributed	src IPs	IP history based dropping of network packets
Zhang et al. 2006	Intermediate	Distributed	No. of dropped packets	Gossip based communication to exchange traffic information between intermediate network nodes using overlay network
Lu et al. 2007	victim-end	distributed	src/dst IP, Port TCP SYN/FIN(RST) pkt rate	Correlation
Wang et al. 2008	Intermediate	Distributed		A distributed mitigation and filtering mechanism based on a pushback and resource regulation methods improved ACC is applied to routers for defending bandwidth HR-DDoS attacks resource regulation is applied to victim for defending resource consumption HR-DDoS attacks

(continued)

Table 4 (continued)

Authors/ year	Deployment location	Detection mode	Parameters	Mitigation/Characterization approach
Devi et al. 2012	Source-end	Distributed	CPU/Memory Usage packet loss, Latency Link utilization, throughput	Interface based Rate Limiting mechanism
Wei et al. 2013	Victim-end	Centralized	Flow, Packet count	Pearson coefficient is used to find relationship relationship between flows using packet count
Zhou et al. 2014	Victim-end	Centralized	src IPs, Packet rate web page frequency	Correlation based detection and characterization
Bedi et al. 2015	Victim-end	Distributed	Packet loss Throughput	Active queue management (AQM) using deterministic weighted fair scheduling (DFS) Dynamically self-adjust buffer usage depending on congestion
Behal et al. 2018	victim-end	Distributed	src IPs, Packet rate	Information distance based characterization and rate limiting mechanism
Wang et al. 2018	victim-end	Distributed	Sketch data structure	Modified Hellinger distance based characterization using whitelists and blacklists of user profiles

limiting (IBRL). Based on the deviations in the observed parameters, their proposed mitigation scheme is activated so as to mitigate the impact of ongoing DDoS attacks.

Gupta et al. [84] proposed dynamic and auto responsive approach for defending against DDoS attack. Various design principles and evaluation results of the proposed framework that autonomously detects and accurately characterizes a wide range of flooding DDoS attacks have been highlighted. Detection of attacks is performed using the low volume based approach that observe abrupt change in the network traffic in the ISP domain. Characterization of attack traffic and normal traffic is performed using total number of the bytes arrival for each flow during monitoring period. The flows that crosses predefined thresholds are classified as either suspicious or attack traffic flows depending on detection from threshold values. Wei et al. [85] proposed a rank correlation-based detection (RCD) approach for detecting LR-DDoS attacks. The simulation results show that RCD can characterize the attack flows from legitimate flows with efficacy.

Zhou et al. [86] observed that the ratio of source IP entropy and click rate entropy of a web page is high in the case of DDoS attacks. Bedi et al. [87] observed that none of the schemes provide an effective solution against the congestion occurred due to flooding DDoS attacks. Under HR-DDoS attack situation, the network resources including routers, links, web server etc. gets overwhelmed and the mitigation systems gets crashed before taking any action to mitigate the situation.

Such kind of problems occur because majority of the DDoS defense methods are deployed primarily at the victim-end. The mammoth network traffic volume generated during DDoS attacks and deficient computational resources at the victim-end, makes defense solution vulnerable to these attacks. Such limitations have lead to the development of many distributed solutions and have shift the trend to more economical Software Defined Technique (SDN) and cloud based DDoS defense solutions [24, 59, 88–90]. All of these novel distributed systems tend to distribute the computational complexity among multiple computational devices with the objective of early detection of malicious traffic.

5 Impact, Sophistication and Future Trends

Usually, the prominent websites are the prime victims of DDoS attacks and suffer interruptions in their services. Such interruptions in the services often have substantial financial implications. The revenue loss has amplified to $209 million in the first quarter of 2016, as compared to $24 million for all of 2015 [91]. According to a recent report by the security firm Imperva Incapsula [16], a single hour of a DDoS attack can cost up to $20,000. A study by the Ponemon Institute [92] also witnessed that the average company's cost for every minute of downtime during a DDoS attack is around $22,000. As majority of DDoS attacks lasts for more than six hours, the incurred losses can reach a high dollar value in a relatively short time. Besides revenue losses, these attacks can also result in financial losses including the cost of investigation and responding to attacks, expenses related to loss in customer support and public relations, and potential financial penalties and lawsuits.

Increased Sophistication, Persistence and Magnitude Global DDoS threat landscape Q4 report [16], indicates that the trend of sophisticated DDoS attacks has shifted from spoofing based network layer DDoS attacks to legitimate TCP connections based application layer DDoS attacks. These attacks sends redundant HTTP GET requests to consume web server's resources such as bandwidth, memory, CPU cycles, file descriptors, and buffers. 2017 also saw an increase in attack duration with an average DDoS attack lasting for 1.2 h with the largest reported attack lasting 5.5 days. The third quarter also showed the number of attacks lasting more than 6 h increased to 7.5% compared to 0.8% in the preceding quarter [16]. Over the years, the conventional DDoS attacks have not only grown in sophistication but have dramatically expanded in their magnitude. As per WISR report [93], the traffic volume of DDoS attacks has touched to 650 Gbps in 2016 as compared to 500 Gbps in 2015 and 350 Gbps in 2014.

DDoS and IoT Devices: The Perfect Match? Apart from using the traditional compromised desktop and workstation systems, the attackers have started making use of less secured Internet of Things (IoT) devices as the launching pad, mainly owing to their astonishing rate of proliferation and their inherent insecurity [94]. Recently Twitter, Spotify, and Amazon suffer interruptions in their services for almost two hours on Oct 21, 2016, because of the large number of unsecured internet-connected digital devices, such as home routers and surveillance cameras. The attackers employed thousands of such devices that had been infected with malicious code to launch a series of DDoS attacks. The Mirai botnet, which harnessed the high CPU capability and high-bandwidth uplinks of hundreds of thousands of IoT devices such as DVRs and CCTV cameras has set new records for DDoS attack size, reaching towards 1 Tbps. With more and more IoT devices coming online every day (Gartner forecasts that there will be 20.4 billion connected devices worldwide by 2020[1]), the threat of DDoS attacks from increasingly sophisticated IoT botnets will only grow.

DDoS and Software Defined Networking – In recent times, dynamic environments such as SDNs (Software Defined Networking) have been used frequently to implement and validate various DDoS defense mechanisms. SDN seems to be promising approach to remove the limitations of existing traditional DDoS defense solutions but still they are susceptible to diversity of attacks that occur in traditional networks, such as the attacks that target control and data plane [95–97]. By exploiting the vulnerabilities in the controller or the communication links between the switch and controller can lead to several attacks such DDoS [88] and Host Location Hijacking Attacks [98]. So, there are possible attack scenarios that make the current architecture of SDN non-secure, which requires more attention to various security aspects of SDNs.

[1] http://www.gartner.com/newsroom/id/3598917

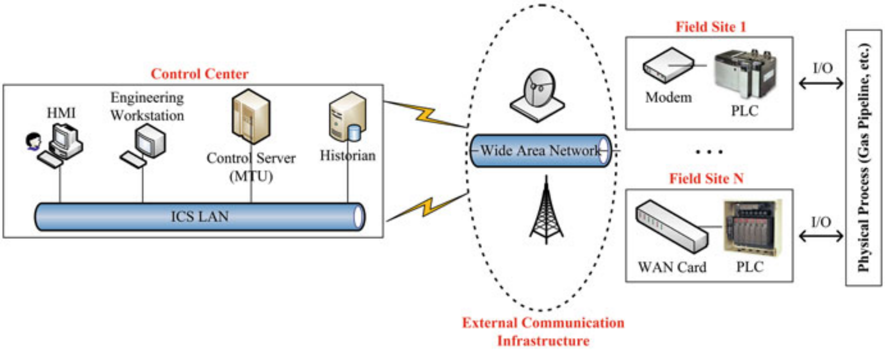


Fig. 7 Overview of an industrial control system environment

DDoS and Blackchain Technology – In some latest works, a company named Gladius has come up with a solution to the DDoS problem by making use of a novel blockchain technology [99]. Gladius provides a decentralized solution to DDoS attacks by allowing participants to rent out their under used network bandwidth in exchange for Gladius tokens. Network participants form "Pools" that monitor requests and traffic to a website, therefore making it harder for any DDoS attacks to occur. Website owners can even switch to larger pools as they grow in return for increased protection. However, currently this technology is in its token sale stage. It would take time before we can have the full-blockchain solution to the crippling effects a DDoS attack.

Industrial Control Systems – a New Target Domain. Industrial control systems (ICS) are classified as a cyber-physical system and are mainly used to control and monitor physical industrial and infrastructure processes such as oil and gas pipeline, power grid, and nuclear plants [100]. Figure 7 provides an overview of a typical ICS environment. It consists of control center and field sites.

The physical processes are located at field sites and are monitored and controlled via sensors, actuators, and programmable logic controllers (PLCs), equipped to communicate with the control center remotely via different proprietary and open ICS protocols such as Modbus, EtherNet/IP, and PROFINET. The control center comprises of several ICS services including human-machine-interface (HMI), Historian and Engineering Workstation. When the data arrives at the control center, the HMI interprets and presents the data in a graphical user interface to a human operator to facilitate in operational decisions. Control engineers use engineering workstation to configure and program PLCs to define how the PLCs should control a physical process.

Industrial control systems run 24/7 for continuous monitoring and controlling of physical processes. These systems run 24/7 and their availability is the main concern in CIA triad. In recent years these systems have been upgraded from the standard serial bus systems to modern TCP/IP based systems, thereby getting connected with larger networks such as corporate network and the Internet, and thus exposing them to cyber-attacks. Attackers target these systems to compromise their availability and sabotage physical processes [101–104]. In particular, they can launch Denial of Service attacks against ICS services, network, and embedded devices such as PLCs at field sites. In particular, they can launch Denial of Service attacks against ICS services, network, and embedded devices such as PLCs at field sites.

- ICS Services – Attacker exploit bugs and vulnerabilities in ICS services to cause denial of service. For instance, ICS-CERT reported that Elipse SCADA application fails when it receives data packets of DNP3 protocol with formatting errors. The vulnerability is found in the DNP Master Driver [105]. Senthivel et al. identify two attack scenarios that crash RSLogix 500 Engineering software when the software attempts to retrieve the control logic from a target PLC [106, 107]. The first scenario involves man-in-the-middle attack between RSLogix and the PLC. It intercepts the control logic traffic and replace a control instruction with noise data such as `0xFFFF`. Apparently, RSLogix cannot handle it and crash. In the second scenario, attacker creates a well-crafted control logic program at the binary level. It involves tempering the metadata related to the size of the program. Attacker installs the program to a target PLC. Apparently, the program runs successfully on the PLC but when RSLogix attempts to retrieve it from the PLC, it crashes the software.
- Programmable Logic Controller – A DoS attack on a PLC device exploits a vulnerability in a PLC component, such as firmware. Recently, ICS-CERT reported a similar vulnerability on Siemens SICAM products. Attacker sends crafted packets to port 2404/TCP to cause a target device to go into defect mode [108]. Similarly, attacker sends crafted packets to Siemens SIPROTEC Compact devices at port 50000/UDP to cause a denial of service [109]. To recover the device, a manual reboot is required.
- Network Connectivity – Control operator monitors the physical processes through HMI that receives data from PLCs periodically. A DoS attack targets the communication link between the PLC and the control center using packet flooding to exhaust the bandwidth of the link [110].

In summary, ICS security is a big concern and timely detection and prevention of DDoS attacks in an ICS environment requires the attention of cybersecurity research community. DDoS attacks are not only increasing in size but are becoming more sophisticated in their makeup. This is largely due to a rapid expansion of the contemporary digital world consisting of ever-increasing number of inherently unsecured and connected devices presenting an ideal platform for the attackers to overwhelm disrupt.

References

1. US Committee on National Security Systems, “National Information Assurance (IA) Glossary,” CNSS, Instruction 4009, 2006.

2. G. Linden, "Make Data Useful," *Presentation, Amazon, November*, 2006.
3. R. Stapleton-Gray and W. Woodcock, "National Internet Defense—Small States on the Skirmish Line," *Communications of the ACM*, vol. 54, no. 3, pp. 50–55, 2011.
4. C. M. R. Dobbins, "Worldwide Infrastructure Security Report," Arbor Networks, Tech. Rep., 2011.
5. D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," *ACM Transactions on Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.
6. "Prolexic Quarterly Global DDoS Attack Report – Q4 2012," Prolexic, Tech. Rep., 2012.
7. "Global ddos threat landscape q3 2017," https://www.incapsula.com/ddos-report/ddos-report-q3-2017.html, 2017.
8. F. Khan, "Botnet Economy," http://dos-attacks.com/2010/10/26/botnet-economy/, [Online; accessed 23-Sep-2012].
9. M. Kenney, "Ping of Death," http://insecure.org/sploits/ping-o-death.html, Jan 1997, [Online; accessed 26-Sep-2012].
10. S. Suriadi, A. Clark, and D. Schmidt, "Validating Denial of Service Vulnerabilities in Web Services," in *IEEE Computer Society Proceedings of the Fourth International Conference on Network and System Security*. IEEE Computer Society, 2010.
11. J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.
12. S. M. Specht and R. B. Lee, "Distributed denial of service: Taxonomies of attacks, tools, and countermeasures." in *ISCA PDCS*, 2004, pp. 543–550.
13. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *Ieee communications surveys & tutorials*, vol. 16, no. 1, pp. 303–336, 2014.
14. Y. Xiang, K. Li, and W. Zhou, "Low-rate ddos attacks detection and traceback by using new information metrics," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 426–437, 2011.
15. M. H. Bhuyan, D. Bhattacharyya, and J. K. Kalita, "E-ldat: a lightweight system for ddos flooding attack detection and ip traceback using extended entropy metric," *Security and Communication Networks*, vol. 9, no. 16, pp. 3251–3270, 2016.
16. Imperva, "Global ddos threat landscape q4 report." https://www.incapsula.com/ddos-report/ddos-report-q4-2016.html, 2017, [Online; accessed 25-Aug-2017].
17. C. Labovitz, "The Internet Goes to War," http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war/, 14 Dec 2010, [Online; accessed 23-Sep-2012].
18. T. Bradley, "Operation Payback: WikiLeaks Avenged by Hacktivists," http://www.pcworld.com/businesscenter/article/212701/operation_payback_wikileaks_avenged_by_hacktivists.html, 7 Dec 2010, [Online; accessed 23-Sep-2012].
19. E. Addley and J. Halliday, "Operation Payback Cripples MasterCard Site in Revenge for WikiLeaks Ban," http://www.guardian.co.uk/media/2010/dec/08/operation-payback-mastercard-website-wikileaks, Dec 2010, [Online; accessed 23-Sep-2012].
20. R. Singel, "Operation Payback Cripples MasterCard Site in Revenge for WikiLeaks Ban," http://www.wired.com/threatlevel/2010/12/web20-attack-anonymous/, Dec 2010, [Online; accessed 24-Sep-2012].
21. V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-service Attacks," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 3, pp. 38–47, 2001.
22. "The DDoS that knocked Spamhaus offline," http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho, 2013, [Online; accessed 2-Apr-2013].
23. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems," *ACM Computing Surveys*, vol. 39, no. 1, p. 3, 2007.
24. V. Gulisano, M. Callau-Zori, Z. Fu, R. Jiménez-Peris, M. Papatriantafilou, and M. Patiño-Martínez, "Stone: A streaming ddos defense framework," *Expert Systems with Applications*, vol. 42, no. 24, pp. 9620–9633, 2015.

25. K. Kumar, R. Joshi, and K. Singh, "An isp level distributed approach to detect ddos attacks," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*. Springer, 2007, pp. 235–240.
26. M. Sachdeva, K. Kumar, and G. Singh, "A comprehensive approach to discriminate ddos attacks from flash events," *Journal of Information Security and Applications*, vol. 26, pp. 8–22, 2016.
27. S. Behal and K. Kumar, "Trends in validation of ddos research," *Procedia Computer Science*, vol. 85, pp. 7–15, 2016.
28. S. Bhatia, "Ensemble-based model for ddos attack detection and flash event separation," in *Future Technologies Conference (FTC)*. IEEE, 2016, pp. 958–967.
29. R. Saravanan, S. Shanmuganathan, and Y. Palanichamy, "Behavior-based detection of application layer distributed denial of service attacks during flash events," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 24, no. 2, pp. 510–523, 2016.
30. A. Bhandari, A. L. Sangal, and K. Kumar, "Characterizing flash events and distributed denial-of-service attacks: an empirical investigation," *Security and Communication Networks*, 2016.
31. D. Senie and P. Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," *Network*, 1998.
32. K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets," in *ACM SIGCOMM computer communication review*, vol. 31, no. 4. ACM, 2001, pp. 15–26.
33. J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, "Save: Source address validity enforcement protocol," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3. IEEE, 2002, pp. 1557–1566.
34. T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from Distributed Denial of Service Attacks Using History-based IP Filtering," in *IEEE International Conference on Communications, 2003. ICC'03*, 2003, pp. 482–486.
35. Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "Packetscore: a statistics-based packet filtering scheme against distributed denial-of-service attacks," *IEEE transactions on dependable and secure computing*, vol. 3, no. 2, pp. 141–155, 2006.
36. X. Liu, X. Yang, and Y. Lu, "Stopit: Mitigating dos flooding attacks from multi-million botnets," Technical Report 08-05, UC Irvine, Tech. Rep., 2008.
37. A. Saifullah, "Defending against distributed denial-of-service attacks with weight-fair router throttling," 2009.
38. M. A. Saleh and A. Abdul Manaf, "A novel protective framework for defeating http-based denial of service and distributed denial of service attacks," *The Scientific World Journal*, vol. 2015, 2015.
39. E. Y. M. Muharish, "Packet filter approach to detect denial of service attacks," 2016.
40. K. Kalkan and F. Alagöz, "A distributed filtering mechanism against ddos attacks: Scoreforcore," *Computer Networks*, vol. 108, pp. 199–209, 2016.
41. T. Gil and M. Poletto, *MULTOPS: a data-structure for bandwidth attack detection*. Defense Technical Information Center, 2001.
42. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical Approaches to DDoS Attack Detection and Response," in *DARPA Information Survivability Conference and Exposition, 2003. Proceedings*, vol. 1. IEEE, 2003, pp. 303–314.
43. A. Akella, A. Bharambe, M. Reiter, and S. Seshan, "Detecting ddos attacks on isp networks," in *Proceedings of the Twenty-Second ACM SIGMOD/PODS Workshop on Management and Processing of Data Streams*. Citeseer, 2003, pp. 1–3.
44. S. Jin and D. S. Yeung, "A covariance analysis model for ddos attack detection," in *Communications, 2004 IEEE International Conference on*, vol. 4. IEEE, 2004, pp. 1882–1886.
45. J. Mirkovic and P. Reiher, "D-ward: a source-end defense against flooding denial-of-service attacks," *IEEE transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 216–232, 2005.

46. Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative detection of ddos attacks over multiple network domains," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 18, no. 12, pp. 1649–1662, 2007.
47. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, "Robust and efficient detection of ddos attacks for large-scale internet," *Computer Networks*, vol. 51, no. 18, pp. 5036–5056, 2007.
48. J. François, I. Aib, and R. Boutaba, "Firecol: a collaborative protection network for the detection of flooding ddos attacks," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no. 6, pp. 1828–1841, 2012.
49. G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*. ACM, 2008, pp. 151–156.
50. B. M. Tellenbach, "Detection, classification and visualization of anomalies using generalized entropy metrics," Ph.D. dissertation, ETH ZURICH, 2012.
51. F. Wang, H. Wang, X. Wang, and J. Su, "A new multistage approach to detect subtle ddos attacks," *Mathematical and Computer Modelling*, vol. 55, no. 1, pp. 198–213, 2012.
52. S. Bhatia, D. Schmidt, and G. Mohay, "Ensemble-based ddos detection and mitigation model," in *Proceedings of the Fifth International Conference on Security of Information and Networks*. ACM, 2012, pp. 79–86.
53. X. Ma and Y. Chen, "Ddos detection method based on chaos analysis of network traffic entropy," *Communications Letters, IEEE*, vol. 18, no. 1, pp. 114–117, 2014.
54. J.-H. Jun, D. Lee, C.-W. Ahn, and S.-H. Kim, "Ddos attack detection using flow entropy and packet sampling on huge networks," *of: ICN*, pp. 185–190, 2014.
55. A. Spognardi, A. Villani, D. Vitali, L. V. Mancini, and R. Battistoni, "Large-scale traffic anomaly detection: Analysis of real netflow datasets," in *E-Business and Telecommunications*. Springer, 2014, pp. 192–208.
56. I. Basicevic, S. Ocovaj, and M. Popovic, "Use of tsallis entropy in detection of syn flood dos attacks," *Security and Communication Networks*, vol. 8, no. 18, pp. 3634–3640, 2015.
57. S. Bhatia, "Detecting distributed denial-of-service attacks and flash events," Ph.D. dissertation, Queensland University of Technology, 2013.
58. P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," *Computer Communications*, vol. 34, no. 18, pp. 2227–2235, 2011.
59. O. Joldzic, Z. Djuric, and P. Vuletic, "A transparent and scalable anomaly-based dos detection method," *Computer Networks*, vol. 104, pp. 27–42, 2016.
60. H. Beitollahi and G. Deconinck, "Tackling application-layer ddos attacks," *Procedia Computer Science*, vol. 10, pp. 432–441, 2012.
61. H. Beitollahi, G. Deconinck, "Connectionscore: a statistical technique to resist application-layer ddos attacks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5, no. 3, pp. 425–442, 2014.
62. T. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection of application-layer ddos attack using time series analysis," *Journal of Control Science and Engineering*, vol. 2013, p. 4, 2013.
63. K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "Ddos attack detection method using cluster analysis," *Expert Systems with Applications*, vol. 34, no. 3, pp. 1659–1665, 2008.
64. A. Chonka, J. Singh, and W. Zhou, "Chaos theory based detection against network mimicking ddos attacks," *IEEE Communications Letters*, vol. 13, no. 9, 2009.
65. Z. Xia, S. Lu, J. Li, and J. Tang, "Enhancing ddos flood attack detection via intelligent fuzzy logic," *Informatica*, vol. 34, no. 4, 2010.
66. R. Karimazad and A. Faraahi, "An anomaly-based method for ddos attacks detection using rbf neural networks," in *Proceedings of the International Conference on Network and Electronics Engineering*, 2011, pp. 16–18.
67. D. Das, U. Sharma, and D. Bhattacharyya, "Detection of http flooding attacks in multiple scenarios," in *Proceedings of the 2011 international conference on communication, computing & security*. ACM, 2011, pp. 517–522.

68. S. N. Shiaeles, V. Katos, A. S. Karakos, and B. K. Papadopoulos, “Real time ddos detection using fuzzy estimators,” *computers & security*, vol. 31, no. 6, pp. 782–790, 2012.
69. S. Y. Dorbala, R. Kishore, and N. Hubballi, “An experience report on scalable implementation of ddos attack detection,” in *International Conference on Advanced Information Systems Engineering*. Springer, 2015, pp. 518–529.
70. R. K. Chang, “Defending against flooding-based distributed denial-of-service attacks: a tutorial,” *IEEE communications magazine*, vol. 40, no. 10, pp. 42–51, 2002.
71. H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” in *LISA*, 2000, pp. 319–327.
72. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Network support for ip traceback,” *IEEE/ACM transactions on networking*, vol. 9, no. 3, pp. 226–237, 2001.
73. D. Dean, M. Franklin, and A. Stubblefield, “An algebraic approach to ip traceback,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 2, pp. 119–137, 2002.
74. B. Al-Duwairi and M. Govindarasu, “Novel hybrid schemes employing packet marking and logging for ip traceback,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 5, pp. 403–418, 2006.
75. S. Yu, W. Zhou, R. Doss, and W. Jia, “Traceback of ddos attacks using entropy variations,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 3, pp. 412–425, 2011.
76. Y.-C. Wu, H.-R. Tseng, W. Yang, and R.-H. Jan, “Ddos detection and traceback with decision tree and grey relational analysis,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 7, no. 2, pp. 121–136, 2011.
77. V. S. Rajam, G. Selvaram, M. PradeepKumar, and S. M. Shalinie, “Autonomous system based traceback mechanism for ddos attack,” in *Advanced Computing (ICoAC), 2013 Fifth International Conference on*. IEEE, 2013, pp. 164–171.
78. K. Singh, P. Singh, and K. Kumar, “A systematic review of ip traceback schemes for denial of service attacks,” *Computers & Security*, vol. 56, pp. 111–139, 2016.
79. S. Floyd and K. Fall, “Router mechanisms to support end-to-end congestion control,” Technical report, February 1997. URL” http://wwwnrg.ee.lbl.gov/floyd/end2end-paper.html, Tech. Rep., 1997.
80. R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, “Controlling High Bandwidth Aggregates in the Network,” *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 3, p. 73, 2002.
81. G. Zhang and M. Parashar, “Cooperative defence against ddos attacks,” *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 69–84, 2006.
82. X. Wang, “Mitigation of ddos attacks through pushback and resource regulation,” in *Multi-Media and Information Technology, 2008. MMIT’08. International Conference on*. IEEE, 2008, pp. 225–228.
83. S. R. Devi and P. Yogesh, “Detection of application layer ddos attacks using information theory based metrics,” *CS & IT-CSCP*, vol. 10, pp. 213–223, 2012.
84. B. Gupta, M. Misra, and R. C. Joshi, “An isp level solution to combat ddos attacks using combined statistical based approach,” *arXiv preprint arXiv:1203.2400*, 2012.
85. W. Wei, F. Chen, Y. Xia, and G. Jin, “A rank correlation based detection against distributed reflection dos attacks,” *IEEE Communications Letters*, vol. 17, no. 1, pp. 173–175, 2013.
86. W. Zhou, W. Jia, S. Wen, Y. Xiang, and W. Zhou, “Detection and defense of application-layer ddos attacks in backbone web traffic,” *Future Generation Computer Systems*, vol. 38, pp. 36–46, 2014.
87. H. Bedi, S. Roy, and S. Shiva, “Mitigating congestion based dos attacks with an enhanced aqm technique,” *Computer Communications*, vol. 56, pp. 60–73, 2015.
88. Y. Cui, L. Yan, S. Li, H. Xing, W. Pan, J. Zhu, and X. Zheng, “Sd-anti-ddos: Fast and efficient ddos defense in software-defined networks,” *Journal of Network and Computer Applications*, vol. 68, pp. 65–79, 2016.
89. S. Behal, K. Kumar, and M. Sachdeva, “D-face: An anomaly based distributed approach for early detection of ddos attacks and flash events,” *Journal of Network and Computer Applications*, 2018.

90. S. Behal, K. Kumar, and M. Sachdeva, "D-fac: A novel ϕ-divergence based distributed ddos defense system," *Journal of King Saud University-Computer and Information Sciences*, 2018.
91. "Twitter, Amazon, other top websites shut in cyber attack," https://ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack/, 2016, [Online; accessed 25-Aug-2017].
92. Poneman, "Evaluating the cost of a ddos attack," http://23.235.200.57/~pcninc5/wp-content/uploads/2014/06/Evaluating-The-Cost-of-A-DDoS-Attack.pdf, Dyn, Tech. Rep., 2016, [Online; accessed 25-Aug-2017].
93. Arbor, "Arbor network wisr report https://www.arbornetworks.com/images/documents/wisr2016enweb.pdf," Arbor Networks, Tech. Rep., 2017. [Online]. Available: https://www.arbornetworks.com/images/documents/WISR2016ENWeb.pdf
94. "Ddos attacks, iot, and the future of it security," https://medium.com/ibm-journal/ddos-attacks-iot-and-the-future-of-it-security-b57975dd1b74, 2016.
95. D. Kreutz, F. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*. ACM, 2013, pp. 55–60.
96. S. Sezer, S. Scott-Hayward, P. K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller, and N. Rao, "Are we ready for sdn? implementation challenges for software-defined networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36–43, 2013.
97. B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.
98. W. Li, W. Meng *et al.*, "A survey on openflow-based software defined networks: Security challenges and countermeasures," *Journal of Network and Computer Applications*, vol. 68, pp. 126–139, 2016.
99. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, vol. 2, pp. 6–10, 2016.
100. I. Ahmed, V. Roussev, W. Johnson, S. Senthivel, and S. Sudhakaran, "A SCADA system testbed for cybersecurity and forensic research and pedagogy," in *Proceedings of the 2nd Annual Industrial Control System Security Workshop*, ser. ICSS '16. New York, NY, USA: ACM, 2016, pp. 1–9. [Online]. Available: http://doi.acm.org/10.1145/3018981.3018984
101. I. Ahmed, S. Obermeier, M. Naedele, and G. G. R. III, "SCADA Systems: Challenges for Forensic Investigators," *Computer*, vol. 45, no. 12, pp. 44–51, Dec 2012.
102. I. Ahmed, S. Obermeier, S. Sudhakaran, and V. Roussev, "Programmable Logic Controller Forensics," *IEEE Security Privacy*, vol. 15, no. 6, pp. 18–24, November 2017.
103. I. Ahmed, "Supervisory Control and Data Acquisition (SCADA) Forensics: Network Traffic Analysis for Extracting a Programmable Logic Controller (PLC) System and Programming Logic Files," in *Proceedings of the 69th Annual Meeting of the American Academy of Forensic Sciences*, ser. AAFS '17. AAFS, 2017.
104. N. Kush, E. Foo, E. Ahmed, I. Ahmed, and A. Clark, "Gap analysis of intrusion detection in smart grids," in *Proceedings of the 2nd International Cyber Resilience Conference*, ser. ICRC '11. Australia: secau-Security Research Centre, 2011, pp. 38–46.
105. "ICS CERT Advisory (ICSA-14-303-02) on Elipse SCADA DNP3 Denial of Service," https://ics-cert.us-cert.gov/advisories/ICSA-14-303-02, 2018.
106. S. Senthivel, I. Ahmed, and V. Roussev, "SCADA Network Forensics of the PCCC Protocol," *Digit. Investig.*, vol. 22, no. S, pp. S57–S65, Aug. 2017.
107. S. Senthivel, S. Dhungana, H. Yoo, I. Ahmed, and V. Roussev, "Denial of Engineering Operations Attacks in Industrial Control Systems," in *Proceedings of the* 8^{th} *ACM Conference on Data and Applications Security and Privacy (CODASPY)*, 2018.
108. "ICS CERT Advisory (ICSA-16-299-01) on Siemens SICAM," https://ics-cert.us-cert.gov/advisories/ICSA-16-299-01, 2018.
109. "ICS CERT Advisory (ICSA-15-202-01) on Siemens SIPROTEC Denial-of-Service Vulnerability," https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01, 2018.
110. S. Bhatia, N. Kush, C. Djamaludin, J. Akande, and E. Foo, "Practical modbus flooding attack and detection," in *Proceedings of the Twelfth Australasian Information Security Conference-Volume 149*. Australian Computer Society, Inc., 2014, pp. 57–65.