جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Defense mechanisms against Distributed Denial of Service attacks: Comparative Review

Fahad Alatawi*
King Fahad Security College, Riyadh, Saudi Arabia.

Received 15 Mar. 2021; Accepted 18 May. 2021; Available Online 01 June. 2021

Abstract

Distributed Denial of Service (DDoS) remains a big concern in Cybersecurity. DDoS attacks are implemented to prevent legitimate users from getting access to services. The attackers make use of multiple hosts that have been compromised (i.e., Botnets) to organize a large-scale attack on targets. Developing an effective defensive mechanism against existing and potential DDoS attacks remains a strong desire in the cybersecurity research community. However, development of effective mechanisms or solutions require adequate evaluation of existing defense mechanism and a critical analysis of how these methods have been implemented in preventing, detecting, and responding to DDoS attacks.

This paper adopted a systematic review method to critically analyze the existing mechanisms. The review of existing literature helped classify the defense mechanism into four categories: source-based, core-router, victim-based, and distributed systems. A qualitative analysis was used to exhaustively evaluate these defense mechanisms and determine their respective effectiveness. The effectiveness of the defense mechanisms was evaluated on six key parameters: coverage, implementation, deployment, detection accuracy, response mechanism, and robustness. The comparative analysis reviewed the shortcomings and benefits of each mechanism.

The evaluation determined that victim-based defense mechanisms have a high detection accuracy but is associated with massive collateral as the detection happens when it is too late to protect the system. On the other hand, whereas stopping an attack from the source-end is ideal, detection accuracy at this point is too low as it is hard to differentiate legitimate and malicious traffic. The effectiveness of the core-based defense systems is not ideal because the routers do not have enough CPU cycles and memory to profile the traffic. Distributed defense mechanisms are effective as components can be spread out across the three locations in a way that takes advantage of each location.

The paper also established that the rate-limiting response mechanism is more effective than packet filtering method because it does not restrict legitimate traffic. The analysis revealed that there is no single defense mechanism that offers complete protection against DDoS attacks but concludes that the best defense mechanism is the use of distributed defense because it ensures that defense components are placed on all locations.

Keywords: Cybersecurity, Cybercrimes, DDoS, DDoS Detection, Source Based, Core Router, Victim-based, Review DDoS.

Production and hosting by NAUSS

* Corresponding Author: Fahad Alatawi
Email: nw4w@hotmail.com

doi: 10.26735/LQEZ4186

I. Introduction

Ever since the invention of computer systems interconnections, Denial-of-Service (DOS) activities have been considered a threat to these computer connections. DoS is a process where an attacker attempts to disrupt the normal traffic flow in a network and eventually brings harm to the service [1]. The attackers normally use many puppet computers or devices to launch a massive request to the target that incapacitates the victim by exhausting the resources through the requests. These requests are not genuine and will overwhelm the host system because of the limited resources available in requests handling. Genuine customers or the users of the victim system are unable to access any information or service as a result of the congestion. These threats are real, and many organizations have fallen victims of this attack. The attacks are performed with different motivations: gaining profit through extortion, hacktivism, political reason, Personal reasons such as disputes, and revenge, and economic reasons [2]. This target host or system could be anything, from machines, ISPs network links to normal network links.

Although, Distributed Denial of Service (DDoS) adopts the same techniques as DOS attacks, DDoS attacks occur on a larger scale because of the use of botnets [1]. Botnets refer to multiple hosts that have been compromised by an intruder, which are manipulated to perform attacks on particular victims. Attackers take control of botnets, which they exploit to send cumulatively large traffic. Depending on the intensity, the attacks can be low rate DDoS attacks (LDDoS), which are hard to expose because the traffic will seem normal, or they can be high rate DDoS (HDDoS). HDDoS can be easily detected because a change in network traffic can be easily identified. DDoS attacks are conducted majorly in the form of link flooding and packet flooding.

Despite the great resources allocated towards mitigating DDoS attacks, there has been an increase in both the frequency and the size of targeted networks [3]. The presence of vulnerabilities in operating systems, internet protocols, and web applications has made it easier to launch these attacks. The data collected by Prolexic Technologies shows that with the increase in the number and size of attacks, it is increasingly getting harder for companies to defend against it.

Hence, there is a need to research and recommend a comprehensively DDoS defense mechanism that can appropriately respond to the attacks before, during, and after the actual attack. This article focuses on DDoS attacks and the defense mechanisms that are effective for attacks that occur over wired network systems. The article aims to compare the effectiveness of the existing defense mechanism measured against six metrics: coverage, implementation, deployment, detection accuracy, response mechanism, and robustness. Many researchers have placed their focus on studying DDoS attacks on the victims alone. A lot of research has been focused on the development of the best methods of defense against DDoS attacks. This should not be the case. A paper leading to the development of a defensive mechanism that is efficient and effective should first have the best method of detecting the DDoS attack.

Therefore, the general objective of this paper is to identify the best practices for defense against DDoS attacks. This was achieved by looking into the different scholarly works done on the existing defensive mechanisms against DDoS attacks. The paper focused on four key defensive mechanisms: Source-based defense, Victim-based defense, core router-based defense, and distributed defense. A comparative analysis was conducted on the four defensive mechanisms with a view of establishing which of the mechanism has superior detection and defensive capabilities. The evaluation of the effectiveness of the defense mechanisms was done against six metrics: coverage, implementation, deployment, detection accuracy, response mechanism, and robustness. More specifically, the objectives of this paper are;

i. To analyze the existing types of DDoS attacks.

ii. ii.To classify the existing defense mechanisms based on the deployment location.

Based on the deployment location classification, the paper will evaluate the best defensive mechanism against DDoS attack. Accordingly, this paper will evaluate the four defensive mechanisms

- source-based defense, victim-based defense, core router-based defense, distributed defense - and answer the following questions:

1. Which defensive mechanism has a greater coverage with relatively limited deployment points?
2. Are there limitations with defensive systems that require local deployment compared to those that are deployed globally?
3. What is the variation in the defensive mechanisms that use packet filtering and those that deploy rate-limiting measures as an attack response?
4. Which defensive mechanisms has a higher degree of sensitivity and resistance to attacks?

As a result, the findings of this paper are beneficial to any individual or organization with systems or networks that could be vulnerable to DDoS attacks. This is because the findings and the recommendations of the paper will guide security experts on the best solution to most of the different types of DDoS attacks.

The findings of the paper not only lead to recommendations on the different strategies of detecting the DDoS attack but also identify the best practice of defense against such an attack. The paper establishes the best way or mechanism to detect and defend against DDoS attacks. DDoS attacks have been on the rise, with many systems and networks becoming victims of these attacks, the findings of this paper will be of great help to any system or network owners who have had problems with network or service outages due to DDoS attacks. The recommendations of the paper on the best method of detection and defense against DDoS attack was as a result of deep research on the different available strategies of detection and defense against the attack.

This research work is motivated by my desire to be a relevant contributor to the field of cyber security. I believe that DOS is an important subject topic in the field and as a member of the academic community, I am deeply encouraged to join other network of researchers in providing useful findings around the subject topic.

The paper focused on existing scholarly works and research. Future work should include experiments on real systems and networks. This is necessary for a deeper analysis of the DDoS attacks that networks and systems face. Experiments, though costly, would help researchers test the effectiveness of the defense systems for different attack levels.

The remainder of this paper is structured as follows: the second section analyszes the key concepts of DDoS, the third section evaluates the qualitative method used in comparing the defense mechanisms, the fourth section discusses the comparative analysis of different DDoS methods and the fifth section is the conclusion.

II. Literature Review

To effectively create solutions against DDoS attacks, it is important to have enough understanding of the types of DDoS attacks. This section critically evaluates the types and classification of DDoS attacks based on layers. In this section, there is also an evaluation of defense mechanisms by classifying them based on location of deployment.

A. DDoS Attacks Based Layers

1) Network Layer Attacks

DDoS attacks usually target the network, transport and application layers respectively. Due to the predominant attacks on theses layers, DDoS attacks can be classified into: network layer attacks and application layer attcks [4].

Under the network layer, attacks are classified into two categories: amplification attacks and flooding attacks. Flooding attacks refer to the attacks where a large volume of traffic is sent to a victim to exhaust the resources of the victims. Flooding attacks include ICMP, UDP, and SYN flooding attacks. SYN flooding is implemented when an attacker sends numerous SYN requests in succession. SYN flooding usually targets the end hosts by consuming server resources to the extent that the system begins to find it difficult to respond to legitimate traffic. SYN flooding can lead to system crash because the OS can be really starved of resources. Since SYN flooding attacks the end hosts, end hosts are advised to implement end-hots defense mechanisms in their OS [5]. Amplification attacks involves manipulating the domain name system (DNS) so that DNS servers that are generating small queries are exploited. These DNS servers are made to send larger payloads that can exhaust resources on the victim's server [4]. The attacker generates large traffic by structuring the requests in a way that the DNS resolvers receive a large response. Therefore, with this method, messages are sent to all the IP addresses that fall within the broadcast address range and this makes the target receive an amplification of the attacker's initial traffic. The common amplification attacks are Fraggle and Smurf attacks.

2) Application Layer Attacks

The second categorization of DDoS attacks is the application layer attacks. Application layer DDoS attacks are designed to imitate communications protocols. They are therefore had to distinguish from legitimate requests in the network layer. Application layer attacks includes: HTTP flood, and SIP flood. HTTP flood is a type of DDoS where an attacker exploits HTTP GET and POST requests to attack a web server [4]. The web server is bombarded by multiple requests that ultimately exhaust the victim server. The second type of application layer attack is the SIP flood, which is mostly executed through the use of Voice over IP (VOIP) mechanism. The novel scheme has been widely adopted by attackers because of its low cost and practicality. Call set-ups are mostly achieved through request packets, and attackers are able to manipulate the SIP proxy server. As more devices are connected to the internet, SIP floods is bound to become more common. The common effect of application layer attack is poor network performance which is usually in the form of difficulty in opening files or accessing websites. Application layer DDoS attacks can also lead to the complete unavailability of a website [5].

B. Classification Based on the Deployment Location

The nature of DDoS attacks is that usually by the time they are detected, there is little that can be done but to disconnect the systems from the network, and manually resolve the issue. DDoS attacks are resource-intensive, and they exhaust resources on the path to the targeted machine. It is because of this reason that the goal of any DDOS defense mechanism is to detect and stop attacks as near as possible to the source. They generate attack traffic flows from multiple sources, and it can be hard to detect them at the upstream network because the traffic flow is isolated. Although attacks should be detected closer to the source, there is a tradeoff between accuracy of detection and how close to the source the defense mechanism can stop or respond to an attack [6]. The packet filtering mechanism from the source end acts to drop legitimate packets from reaching the victim.

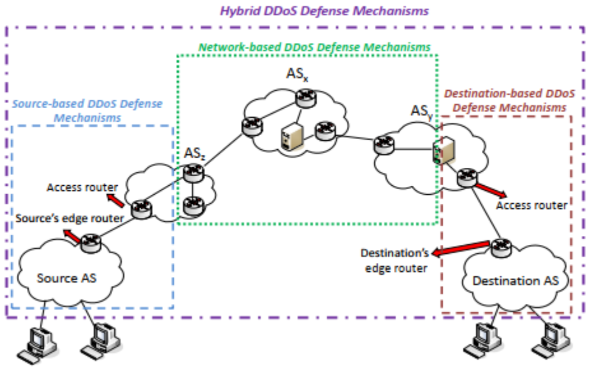
Hybrid DDoS Defense Mechanisms
Network-based DDoS Defense Mechanisms
Source-based DDoS Defense Mechanisms
Destination-based DDoS Defense Mechanisms
AS_x
AS_y
AS_z
Access router
Source's edge router
Source AS
Access router
Destination's edge router
Destination AS

Fig. 1 Classification of the defense mechanisms based on deployment location [3]

The first step in the development of an effective defense mechanism is the classification of the existing defense mechanisms. The first criterion is the classification according to the defense location, which classifies the defense mechanisms into four categories: destination-based, source-based, network-based, and distributed defense as illustrated in Fig. 1.. The classification based on the deployment location was first adopted by Criscuolo, but it has since been used widely [7]. The current analysis adopts the use of this classification criterion to generate a list of defense mechanisms that it can compare.

1) Source-Based Mechanism

Source-based mechanisms: This refers to the source-based mechanisms that are implemented near the end-users to ensure that their devices do not generate DDoS attacks. The defense mechanisms can be deployed either at the access routers of autonomous systems or at the routers of the source local network. Some of the major source-based defense mechanisms include: Egress filtering at the sources' edge routers, D-WARD, MUlti-Level Tree for Online Packet Statistics (MULTOPS), Tabulated Online Packet Statistics, and MANAnet's Reverse Firewall [3].

Egress filtering at the sources' edge routers refers to the defense mechanisms that detect and filter packets that originate from spoofed IP addresses. Spoofed IP addresses are generated based on whether an IP is within the valid IP addresses range. The challenge is that if the spoofed emails are within a valid range, they cannot be detected and spoofed. Given that attackers have adopted the use of botnets, attackers can launch attacks by using botnets that have valid IP addresses [3]. The second source-based defense mechanism is the D-WARD scheme, which works by monitoring both the inbound and outbound traffic of the source network and comparing it to predefined normal traffic information flow models. As such, the defense mechanism tries to block attack traffic that originates from the network, just before they flow into the network. The normal traffic flow model defines the maximum number of traffic that can be allowed to flow to the peer. Although this defense mechanism is essential in filtering data at the source, it consumes great memory space and CPU cycles..

2) *Destination-Based Mechanisms*

With a destination-based defense mechanism, detection and defense are domiciled at the victim's end. Destination based defense mechanism operates by modelling a victim's characteristics so that it can easily detect any anomaly. The defense mechanism can be deployed either at the access router of the destination or at the edge routers. The major destination-based defense mechanisms are captured in the section below.

IP Traceback mechanisms: The process of analyzing IP packets to determine their true source is called traceback. It involves tracing the attack back to the source in order to uncover the identity of the perpetrator. Traceback mechanisms can be classified into two categories: packet marking and link testing. In the Packet marking process, the traceback mechanism operates through the use of routers, which mark packets headed to the victim, so the path followed by packets can be easily identified [4]. However, the stateless state of internet routing is considered a major difficulty in implementing the marking process; for the entire path to be identified, certain coding schemes are needed, and the routers may fail to assign unique identifiers to certain packets thus resulting in false positives [8]. The second category is link testing, which involves the testing of upstream links starting with the one closest to the victim and is repeated recursively until the upstream router is reached. The traceback mechanisms result in heavy management, computational, and network overhead. At the same time, it requires a wide implementation as a sufficient number of routers have to be incorporated for the defense mechanism to be viable. Due to the unavailability of source accountability in TCP/IP protocol, IP traceback is regarded as difficult. The level of accuracy of the process is also questionable because attackers can generate traceback mechanisms that seem to be genuine. Hence, ICMP traceback have been recommended by some other researchers. In the ICMP mechanism, the forwarding packets with reduced probability are sampled by each router and an ICMP traceback message is then sent to the destination. A chain of traceback messages is then constructed and can be used in determining the exact source of traffic. However, when adopting the ICMP mechanism, it can be difficult to validate the tracebook packets and it is very unlikely that a certificate-based scheme can be adopted by all routers [9].

Management information base: the management information base is a data that captures critical information such as the packets and the historical routing statistics. The information can be used to map TCP, ICMP, and UDP packets and generate patterns. The information can be used to identify abnormalities on the network. The data generated from the mapping process can help with providing an effective framework for adjusting the setting of the network to compensate for unwanted traffic [3].

This method holds a lot of promise in controlling traffic loads, but it still needs to be further evaluated in a real network environment [10].

Packet and filtering mechanisms: This detection mechanism involves the marking of the legitimate packets along the path to the destination, creating a basis on which the victim's edge routers can the attack traffic. The marking of legitimate packets makes it possible to block undesirable traffic. The effectiveness of the filters depends on the strength of attackers. Some of the common packet and filtering mechanisms are history-based filtering and Hop-count filtering. The History-based filtering leverages a record keeping mechanism for IP filtering. When the system has not yet experienced a DDoS attack, the History-based filter stores records of the frequently visited IP Addresses [11]. When DDoS attacks occur, the IP addresses in the list will be connected. However, the method requires an offline database to keep track of IP addresses and this has made the cost of storing and sharing information quite expensive [12]. Hop-count filtering involves the storage of IP addresses and the correlated hops from the destination and Packet Identifier which involves the embedding of a path fingerprint to each packet [3]. However, Hop-count can be ineffective due to its limited range. With a range of 1-30, the Hop-count has a limited range and this makes it unable to identify illegitimate source IP addresses with similar hop-count value to a destination as that of a zombie. Therefore, it is advisable that, in order to nullify the negative effect of hop-count limited range, there is adequate examination of hop-count locations in various destinations of the internet [13].

Packet dropping based on the level of congestion: This defense mechanism operates by dropping suspicious packets when the network gets congested. Packet Score mechanism developed by Kim et al. [9] operates by automatically characterizing packets and selectively discarding packets in a bid to manage overload. The idea behind Packest Score is that, it assigns per packet score to packets and this can be used to prioritize packets. The threshold for determining packets to be dropped is determined by the level of overload in the system and the score distribution of the incoming packets. However, the research by Kim et al. [13] does not show enough results to account for when there is a more organized and sophisticated DDoS attack. Hence, in the case of a more sophisticated attack, the research inadequacy makes it unable to know the level of impact on the response time of the time-scale of updates of the score books, dynamic discarding threshold and cumulative distribution function [15].

3) Network-Based Mechanisms

A network-based defense mechanism refers to the defense mechanisms where components are placed on the network's router. The components help in the detection, traceback, and response through filtering and rate-limiting [3]. There are three classifications of network-based mechanisms: perimeter-based defense mechanisms, Controller agent model, and Distributed Change Point Detection. These three classifications of Network-based mechanism are discussed below.

The perimeter-based defense mechanisms: This defense mechanism is mostly used by internet service providers to offer anti-DDoS services to their clients [10]. The edge routers at the ISP's end operate to detect and identify the sources of attack and respond through rate-limit filters to block traffic. The method is effective because it does not require support from the ISP routers, which makes it locally deployable, while not putting a strain on the ISP core routers. It is necessary to know that, it is quite difficult to aggregate and separate attack packets from the illegitimate ones of the same kind. It is usually easier to analyse and detect anomalies in an aggregate that is broader. Hence, this method aggregates traffic attacks instead of packet attacks [17].

Controller Agent Model: The third classification is the controller agent model. This model operates through the edge routers and controller. When an attack is detected, a message is relayed to the agents to mark all the packets destined to the router. Once the packets arrive at the destination, the victim checks the marked fields to establish the entry point of attack traffic. Depending on the identified attack signature, a request will be sent to the controller that requests a particular agent to filter a given set of attack traffic [11]. The major limitation which the defense model is that it employs the use of third party components in the detection and characterization of attack traffic.

Distributed Change-point Detection: The second categorization is the Distributed Change-point Detection. This method actively monitors the propagation patterns and detects any unexpected changes on the network [12]. Once the propagation level exceeds the preset threshold, the system registers that an attack is ongoing. By monitoring the abrupt changes at distributed network points, the mechanism is able to quickly detect if there is a DDoS flooding attack. The system is usually deployed over many AS domains and there is a CAT server in every domain. The CAT servers are actually responsible for the aggregation of distributed alerts while it is the routers that are responsible for detecting the attacks and raising alerts [20].

4) Distributed Defense Mechanisms

For source-based, destination-based, and network-based defense systems, the defense components in the different deployment locations do not cooperate. For the three defense mechanisms, detection and response are either done at a central location in the deployment point or at responsible points within the group of deployment points. It is because of this reason that the three defense mechanisms are referred to as centralized. Unlike the centralized defense system, hybrid (Distributed) defense mechanisms are deployed at multiple points across the entire network [3]. There are different distributed defense combinations that can be adopted, and one could be where detection occurs at the victim's side, and the response mechanism is then distributed to the other nodes. The common distributed defense mechanisms are presented in the section below:

Distributed packet marking and filtering mechanisms: The marking and filtering mechanisms adopts centralized defense mechanisms, attack detection, and packet filtering at the same location. Distributed packet throttling mechanism operates by situating the detection modules nears the victims, whereas packet filtering takes place close to the attack sources [15]. The mechanism takes advantage of the high level of accuracy of detection of attack at the victim's end and filters packets close to the attack sources. Some of the defense mechanisms deploy throttle mechanisms at upstream routers that are hop away, to minimize the packet forwarding rate of packets. The packet filtering mechanism takes advantage of the routers to filter DDoS flows. The mechanisms that can be employed are aggregate-based congestion control (ACC), Attack-Diagnosis and parallel-AD, and TRACK [15].

Aggregate-based Congestion Control (ACC) and Pushback refer to the mechanism that rate limits the aggregate IP sources. ACC uses a sample of packets to determine the aggregates that are overwhelming them. Once the aggregate is identified, a pushback message is sent to the upstream routers to request for rate limit. ACC and Pushback are not effective in acting against distributed sources of attacks since this type of attack is associated with voluminous traffic [15].

Attack Diagnosis adopts the use of packet marking and pushback. Upon the detection of an attack, the victim activates an AD, which is relayed to the upstream routers. The upstream routers act by marking each packet destined to the victim, which the victim will check using a record of router interface information. Once a traceback is complete, the victim issues request to AD-enabled routers to filter identified attack packets. Whereas AD is not effective against large traffic, Parallel AD, which stops traffic from more than one router at the same time. TRACK uses the same mechanism, but it is advantageous because it has a low communication and computation overhead [13]. TRACK is limited since sophisticated attackers can modify the marking fields of packets. At the same time, with the mechanism, it's impossible to find IP addresses of the attacker.

Defensive Cooperative Overlay Mesh (DEFCOM) is a defensive framework that provides a means through which nodes can exchange information and services. The defense mechanism is effective because all the nodes cooperate and collaborate in the detection and defending against an attack. The nodes are specialized for a specific function, and the communication ensures that the defense and response are well-coordinated. Under the DEFCOM each should be able to support at least one of the following: traffic classification nodes which communicate with the downstream nodes to ensure that legitimate traffic is not dropped, attack alerts generated from alert generators and sent to the entire network, resource request that is generated from each node and sent to the neighboring nodes, and rare limit requests that are sent upstream [14]. The design of the defense nodes is that it's possible to discover victim rooted traffic, with the relationship between the upstream and downstream nodes being identified, so that the proper rate limits that can effectively control the traffic can be determined and imposed. The rate limits are imposed as close as possible to the source.

III. Methodology

This paper adopted the use of a systematic literature review in identifying and comparing the defense mechanisms. An effective measurement framework for evaluating all the defense mechanisms does not exist. The use of a monetary base of evaluation is ineffective because it does not consider the effectiveness of the schemes. The overlapping nature of qualities and features of the mechanisms also makes it difficult to give binary differentiations. Therefore, the method used was a qualitative comparison of the effectiveness of the defensive mechanisms against six metrics. The six metrics used were: coverage, implementation, deployment, detection, response, and robustness. The systematic review was instrumental in the identification and selection of the relevant literature material, and it also allowed for exhaustive comparison of the defensive mechanisms. The six metrics selected were used in creating the research questions used in this qualitative analysis. The research questions guided the data inquiry and research endeavours in this paper. The qualitative analysis of the four defense mechanism was therefore controlled by these four research questions:

1. Which defensive mechanism has a greater coverage with relatively limited deployment points?
2. Are there limitations with defensive systems that require local deployment compared to those that are deployed globally?
3. What is the variation in the defensive mechanisms that use packet filtering and those that deploy rate-limiting measures as an attack response?
4. Which defensive mechanisms have a higher degree of sensitivity and resistance to attacks?

The first question was useful in guiding the qualitative analysis of the mechanisms againsts two of the metrics - Coverage and implementation. The question was used in evaluating the existing literature material with a view of determining which defense location has a greater defensive coverage with relatively fewer deployment points. The assessment was done through the review of the number of deployment points of each defense location, and the effectiveness of the defense location in detecting and defending against DDoS attacks. The question also guided a critical evaluation of the mechanisms to deduce their respective requirements for resources and changes during implementation. Each of the defense mechanism was evaluated on how effective they could be without requiring major system architectural changes during implementation.

The second research question was used in guiding the assessment of the mechanisms by considering the variations of requirements for deployment. Based on the existing literature, the defense mechanisms were evaluated based on the limitations that exist for the defensive systems that require local deployment, and those that require global deployment. The existing literature provided adequate information on the requirements for deployment and why each mechanism was more effective if deployed locally or globally.

The third research question used existing literature to evaluate how each respective mechanism responds to attack. The various methods used by each mechanism were analysed for shortcomings and benefits. The research question was however tailored to guide analysis and evaluation around packet filtering or rate-limiting method. These two are the major attack responses and this paper used a comparative analysis to critically examine how each defense mechanism makes use of them. The analysis was also useful in recommending the rate-limiting method over the packet filtering method.

The final question was used to determine which of the mechanism is more effective in detecting and preventing DDoS attacks. The question was used to evaluate the mechanisms on detection and robustness. The qualitative approach also looked at the trade-offs in this mechanisms and how each one might be better in one aspect but be deficient in another aspect.

IV. Comparative Analysis of Different DDoS Defense Methods

The section will focus on the discussion of the selected qualitative metrics that were adopted in the comparative evaluation. The evaluation metrics used in the analysis are coverage, implementation, deployment, detection accuracy, response mechanism, and robustness. The metrics were used to evaluate the defense mechanisms, and the result of the qualitative analysis is summarized in Table II.

The review of the literature has developed different mitigation and defense mechanisms against DDoS attacks and is a case for and against each of the DDoS defense mechanisms. At the different deployment locations and levels, the implementation of the DDoS mechanism is associated with overhead. The different defense mechanisms follow different deployment strategies, as the defense components are deployed in different locations. The deployment of the defense mechanism may require massive changes. The deployment may require a change of the internet protocols, deployment of new software, and altering the behavior of the core router. It can be stressing to realize after implementation that the defense system does not respond to DDoS attacks, especially after resources are spent in making the changes. It is because of this reason that end systems that require local deployment are less costly.

The location of deployment is an important consideration, as it focuses on the ideal place where the defense system should be located. An ideal DDoS defense system should be easy to deploy such that it causes minimal interference on the existing network configuration and protocols. At the same time, the scale of deployment has to be reasonable. Most of the defense mechanisms are designed and deployed at the victim's end, and this can be justified by the fact that maximum impact is felt at the victim’s end. However, the defense mechanism usually does little to contain attack at the victim’s side. The deployment at the source has its limitations, especially given that in a distributed attack, the source is responsible for a fraction of the attack traffic. For the source-based defense system to be effective, global deployment would be required, and this is impossible since the internet has no central control [15]. A bulk of the network traffic passes through core routers, and the deployment of defense mechanisms at these points ensures there is excellent coverage. Unlike the victim-end, which would need the deployment of defense mechanisms at each victim’s end, the deployment at the middle only requires a few components and gives excellent coverage. The challenge with source-based defense is that although the collateral damage may be low, it requires a global implementation, which makes it impractical [15]. DDoS defense that requires global deployment is often implemented through incremental deployment. Although deployment at the middle offers greater defensive coverage, core routers are usually busy, and they cannot allocate substantial resources towards the analysis of individual packets. Because of the limitation in the resources that it can allocate, core routers do not perform serious packet-level analysis. To limit the overhead, simple rules are adopted at the core routers, which affects the accuracy of the core-based defense mechanisms in discriminating DDoS traffic from legitimate traffic as illustrated in Fig. 2.

For the third question, the attack response for the different mechanisms was compared, and a table generated to show the attack response of the different defense mechanisms. As noted, there are two main attack response, rate limiting and packet filtering.

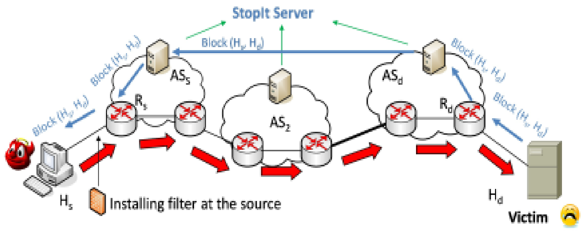

Fig. 2 Core Router Based Defense [3]

For the final research question, the aspect of accuracy focuses on the effectiveness of the defense mechanism on attack detection. Attack detection is usually the first and most important step in DDoS attack mitigation. DDoS detection mechanism operates by monitoring the network in search of an analogous change in traffic volume and IP attributes. Table I categorizes the attack detection schemes employed by the different defense mechanisms. NetBouncer and Preferential filtering, which are victim-based defense mechanisms, use legitimacy tests and Traceback schemes respectively. The traceback scheme involves the use of the upstream routers, which act to mark the packets on their path. The traceback mechanisms result in heavy management, computational, and network overhead. At the same time, it requires a wide implementation as a sufficient number of routers have to be incorporated for the defense mechanism to be viable. Its accuracy is inhibited by the fact that attackers can generate traceback mechanisms that seem to be genuine.

The legitimacy tests adopted by Netbouncer involves the maintaining of a large list of legitimate clients. The legitimacy is usually structured such that it expires after a period of time, and the list is updated. The major advantage of the detection scheme is that it does not require a modification of the server. Unfortunately, sophisticated attackers can use legitimate client identities in DDoS attacks. The accuracy of detection is essential because an attack can be stopped at the initial stages by executing the reaction countermeasure in place [15]. Attack detection mechanisms are essential as they protect legitimate users against an attack. At the same it, it helps in the identification of the source of the attack, making it possible for attacks to be blocked at the source. A detection mechanism is said to be effective if it detects attacks on time, accurately, and with minimal deployment costs. The accuracy of detection at the source is high, but it is not robust, and the defense system is likely to succumb to the high volume of attack traffic. Two source-based defense mechanisms were reviewed: Ingress filtering, a D-ward. The accuracy of ingress-filtering is limited by the fact that it's almost impossible to identify attacks packets based on the source addresses. The method has been proposed as being effective in detecting spoofed packets, but it cannot be achieved if the addresses are within the valid IP address range. Given that most attacks employ internal systems as botnets, the attacks could originate from systems that have genuine IP addresses. D-ward detects abnormality in the network traffic by monitoring the inbound and outbound traffic. The detection scheme consumes more memory space, and an attack can be instituted by attacks that can control traffic with a normal range.

Three distributed defense mechanisms were reviewed to determine their accuracy in detecting DDoS attacks. The three mechanisms are ACC and pushback, StopIt, Defcom, and they use Congestion detection, Passport, and Traffic Tree discovery, respectively, to detect attacks. ACC and Pushback are effective because the detection focuses on the aggregate attack traffic, with detection done at the victim, and pushback messages are sent to the upstream routers with requests. The accuracy of ACC and Pushback is lower when the attack is uniformly distributed because of the volume of traffic. DEFCOM, on the other hand, is ineffective because it requires in-line deployment, and their rate of malfunction deters to the massive deployment of the classifier on the network. The limited deployment of classifier nodes limits the effectiveness of the defense mechanism in verifying traffic and detecting attacks. StopIt is the most effective distributed based defense system which employs Passport to prevent IP address spoofing. Previous studies have shown that Stop-It has a higher detection accuracy compared to filter-based design and can provide continuous and non-interrupted communication in different DDoS attacks [16].

After a DDoS attack is detected, the defense mechanisms usually react by controlling the incom-

TABLE I
DEPLOYMENT BASED COMPARISONS BETWEEN
DIFFERENT DDOS DEFENSE METHODS

Deployment Scheme	SCHEME NAME	Attack Detection	Attack Response
Victim-Based Defense	NetBouncer	Legitimacy tests	Packet filtering based on legitimate lists
	Preferential Filtering	IP Traceback Scheme	Filter packets with infected edges.
Source-Based Defense	Ingress Filtering	IP address validity tests	Rule-based filtering
	D-Ward	Detect Abnormality	Rate limiting of outgoing traffic
Core Router-Based Defense	Collaborative Agent Model	Change Aggregation tree	Packet Filtering
	Collaborative Agent Model	Signature Matching	Packet Filtering
	Perimeter-based defense	Traffic Aggregate	Rate limit filters
Distributed Defense	ACC and pushback	Congestion detection	Rate limiting
	StopIt	Passport	Packet Filtering
	Defcom	Traffic Tree discovery	Distributed rate limiting

ing traffic either through rate-limiting techniques or packet filtering. As already highlighted in the literature review, packet filtering techniques are ineffective because they act to control traffic even from legitimate users. The infectiveness of packet filtering is attributable to the fact that it is hard to distinguish normal traffic from DDoS traffic since attackers tend to employ the use of botnets. The filtering mechanism adopts the use of defined signatures and cannot filter packets that request legitimate services [17]. Additionally, packet filtering requires wide deployment for it to be effective. The rate-limiting approach is effective because a specific limit can be placed on the traffic that is allowed through the network interface. The traffic that exceeds the specified rate is either delayed or dropped. Rate limiting can be set as an automatic response mechanism that automatically kicks and limits incoming traffic. Based on this evaluation, for the core router, the perimeter-based defense is effective because it uses a rate-limiting response. For distributed defense, Defcom, and ACC and pushback are more effective because they employ rate-limiting techniques.

Robustness is a measurement variable that evaluates the degree to which a defense mechanism can protect a system from an attack. When an attacker is aware of the defense system deployed by an organization, they are likely to succeed in compromising the defense system and using it as a botnet in their attacks. The defense system varies on their vulnerability to attacks. Source-based defense systems are effective as they can detect attacks at the early stages and eliminate an attack before it occurs. However, for it to be effective, the defense mechanism has to be deployed across a maximum source network. It is impractical to cover all the possible source networks because the internet does not have a central command. The review of the literature revealed that the best location to deploy detection mechanisms for higher accuracy is the victim network. Generally, the core routers in the intermediate networks offer an ideal place detection and filtration, but it requires an expansive coverage to detect and capture a good number of attacks. Although the four different classifications of defense mechanisms operate well in their respective areas, all of them have a set of drawbacks. An ideal defense and detection system should place the defense components near the victim, near the source, and at the center of the network. At the victim's-end, there is a higher accuracy of detection, and the source offers the best place to differentiate between good and bad packets. The center of the network is an ideal location because a high defensive coverage can be achieved with fewer deployment points.

Distributed defense systems offer a robust defense and mitigate against the shortcomings of source, destination, and intermediate defense systems. With a distributed DDoS defense system, defensive components are distributed across the three locations. The distributed defense is the only mechanism that does not use a centralized deployment structure. This distributed structure of implementation contributes to the robustness and effectiveness of the mechanism against DDoS. However, unlike other easy to implement mechanisms like the Router-Based mechanism, the distributed scheme can be complex because its components are distributed over the internet [15]. The components at the three locations cooperate either passively or actively. Passive defense is ideal because it only kicks in one DDOS attack is detected, which reduces the overhead on the network. The distributed defense systems are highly robust and are less vulnerable compared to the source-based and destination-based defense system. However, distributed internet-based can still fail, especially the information exchange between the multiple defense components are exchanged. The robustness of a defense system depends mostly on how securely the defense components exchange information.

Table II gives a detailed summary of each defense mechanism. The summary table evaluates each mechanism against the six metrics used in this paper.

TABLE II
EVALUATION OF DDOS MECHANISMS AGAINST THE SIX METRICS

Deployment Scheme	Coverage	Implementation	Deployment	Detection Accuracy	Response Mechanism	Robustness
Source-Based Defense	Would have an effective coverage as long as it is deployed globally.	Global deployment is a condition required for its implementation to bring all desired effects. Global deployment is impractical because the internet has no central location.	Centralized. Deployment has its limitations because in a distributed attack, the source is only responsible for a fraction of the attack.	The source is the best place to differentiate between good and bad packets. It Uses IP Address validity tests and can be effective in detecting abnormalities	Uses rate-limiting method. Rate limiting is effective because a specific limit can be placed on a traffic that is allowed through the Network Interface	Very robust because they can detect attacks at the early stages and eliminate an attack before it occurs. However, this depends on it being deployed across maximum source networks
Router-Based Mechanism	Excellent Coverage: This is because a bulk of the network passes through them	Easy to implement: Deployment at middle only requires few components and gives excellent defensive coverage	Centralized. Few components are required for deployment.	Core routers are usually busy and cannot perform serious packet analysis	Only Parameter based defense uses rate limiting. The other schemes under the Router-based Mechanism uses packet Filtering. Packet filtering can be an ineffective response mechanism	Ideally good effective detection and filteration but robustness depends on an expansive coverage in detecting and capturing good number of attacks
Victim-Based Defense	The defense mechanism does little to contain attack at the victim's end	Most defense mechanism are designed at the victim's end	Centralized. It requires wide deployment to be effective	There is higher accuracy of detection at Victim's end	Uses packet filtering based on legitimate lists.	Can be very effective but depends on wide deployment
Distributed Based Defense	Has a relatively higher coverage than others.	Can be complex to implement because for effective communication, distributed components have to be scattered over the internet.	Distributed. Deployed over multiple locations such as source, destination or intermediate networks	Has a relatively good detection accuracy because it has more resources at several levels	Various schemes adopt unique response mechanisms but overall due to the distributed structure, its response mechanism is relatively good.	Very robust against DDoS attacks. Mitigates against the short-comings of the other defense mechanisms

V. Conclusion

The comparative analysis started with the classification of the different defenses based on the deployment location. The analysis adopted four classifications of the defense mechanisms: source-based, core-router, victim-based, and distributed systems. A list of the defense systems that fall in the four categories was selected and evaluated based on five performance metrics: coverage, implementation, deployment, detection accuracy, response mechanism, and robustness. The analysis revealed that there is no single location that offers complete protection against DDoS attacks. The best defense mechanism is the use of distributed systems because it ensures that defense components are placed at all locations. In general, an effective DDoS defense mechanism should have multiple nodes that are involved in detecting and preventing attacks. At the victim's end, the accuracy of detecting DDoS traffic is high, but little can be done to respond to the attack by the time it reaches the victim. Stopping an attack at the source is ideal, but at this stage detection accuracy is low since it is hard to differentiate legitimate and malicious traffic. The core-based defense system is also not ideal because there are not enough CPU cycles and traffic to profile traffic.

References

[1] S. Raghavan and E. Dawson, *An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks*, India: Springer, 2011.

[2] K. M. Prasad, A. R. Mohan and K. V. Rao, "Dos and DDoS attacks: Defense, detection and traceback mechanisms-A survey," in *Glob. J. Comput. Sci. Technol.*, vol. 14, no. 7, 2014.

[3] S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 2046-2069, Mar. 28, 2013, doi: 10.1109/SURV.2013.031413.00127.

[4] M. T. Manavi, " Defense mechanisms against Distributed Denial of Service attacks: A survey," in *Comput. Electr. Eng.*, vol. 72, pp. 26-37, Nov. 2018, doi: 10.1016/j.compeleceng.2018.09.001.

[5] L. Kavisankar, C. Chellappan, and R. Vaishnavi, “Network Layer DDoS Mitigation Model Using Hidden Semi-Markov Model,” in *Int. J. e-Educ. e-Bus. e-Manag. e-Learn.* vol. 4, no. 1, pp. 42-46, Feb. 2014, doi: 10.7763/IJEEEE.2014.V4.299.

[6] B. L. Dalmazo, *et al.* "A systematic review on distributed denial of service attack defence mechanisms in network," *Int. J. Network Mgmt.*, vol. 2021, no. e2163, doi: 10.1002/nem.2163.

[7] S. D. Kotey, E. T. Tchao and D. G. James, "On Distributed Denial of Service Current Defense Schemes," in *Technol.*, vol. 7, no. 1, p. 19, Jan. 30, 2019, doi: 10.3390/technologies7010019.

[8] Y. Wang and R. Sun, "An IP-Traceback-based Packet Filtering Scheme for Eliminating DDoS Attacks," in *J. Netw.*, vol. 9, no. 4, pp. 874-881, Apr. 2014.

[9] I. Sreeram and V. P. Vuppala, “HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm,” in *Appl. Comput. Inform.*, vol. 15, no. 1, pp. 59-66, Jan. 2019, doi: 10.1016/j.aci.2017.10.003.

[10] C. Douligeris and A. Miktrokotsa, “DDoS attacks and defense mechanisms: classification and state-of-the-art,” *Comput. Netw.*, vol. 44, no. 5, pp. 643-666, Apr. 5, 2004, doi: 10.1016/j.comnet.2003.10.003.

[11] T. M. Thang and V. K. Nguyen, “Synflood Spoof Source DDOS Attack Defence Based on Packet ID Anomaly Detection – PIDAD,” *Softw. Netw.*, vol. 2016, no. 1, pp.213-228, Jan. 2018, doi: 10.13052/jsn2445-9739.2016.012.

[12] B. B. Gupta, R. C. Joshi and M. Mishra, "Distributed Denial of Service Prevention Techniques," *Int. J. Comput. Electr. Eng.*, vol. 2, no. 2, Apr. 2010, doi: 10.7763/IJCEE.2010.V2.148.

[13] H. Wang, C. Jin and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," in *IEEE/ACM Trans. Netw.*, vol. 15, no. 1, pp. 40-53, Feb. 2007, doi: 10.1109/TNET.2006.890133.

[14] 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 Trans. Dependable Secure Comput.*, vol. 3, no. 2, pp. 141-155, Apr.-June 2006, doi: 10.1109/TDSC.2006.25.

[15] M. T. Manavi, "Defense Mechanisms Against Distributed Denial of Service attack: A survey," *Comput. Electr. Eng.,* vol. 72, Nov. 2018, pp. 26-38, doi: 10.1016/j.compeleceng.2018.09.001.

[16] R. Yaegashi, D. Hisano and Y. Nakayama, "Light-Weight DDoS Mitigation at Network Edge with Limited Resources," in *2021 IEEE 18th Consum. Commun. Netw. Conf. (CCNC)*, 2021, pp. 1-6, doi: 10.1109/CCNC49032.2021.9369635.

[17] S. Chen and Q. Song, "Perimeter-based defense against high bandwidth DDoS attacks," in *IEEE Trans. Parallel Distrib. Syst.*, vol. 16, no. 6, pp. 526-537, June 2005, doi: 10.1109/TPDS.2005.74.

[18] N. S. Rao, K. Sekharaiah and A. Rao, "A Survey of Distributed Denial-of-Service (DDoS) Defense Techniques in ISP Domains," in *Springer Proceedings in Mathematics & Statistics*, Cham, 2019.

[19] O. Osanaiye, K. R. Choo and M. Dlodlo, "Change-point cloud DDoS detection using packet inter-arrival time," in *2016 8th Comput. Sci. Electr. Eng. (CEEC)*, 2016, pp. 204-209, doi: 10.1109/CEEC.2016.7835914.

[20] Y. Chen, K. Hwang and W. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," in I*EEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 12, pp. 1649-1662, Dec. 2007, doi: 10.1109/TPDS.2007.1111.

[21] R. Chen, J. M. Park and R. Marchany, "TRACK: A novel approach for defending against distributed denial-of-service attacks," Dept. Electr. Comput. Eng., Virginia Tech, Virginia, VA, USA, Tech. Rep. TR-ECE-05-02, 2006.

[22] J. Mirkovic, P. Reiher and M. Robinson, "Alliance Formation for DDoS Defense," in *NSPW03: New Secur. Paradig. Workshop,* Ascona, Aug. 2003, doi: 10.1145/986655.986658.

[23] M. Sachdeva, G. Singh and K. Kumar, "A Comparative Analysis of Various Deployment Based DDoS Defense Schemes," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, Springer, 2013.

[24] F. Angelo, P. Pace, P. Andrea and M. Lorena, "Modelling and Simulation of a Defense Strategy to Face Indirect DDoS Flooding Attacks," Springer International Publishing , Switzerland , 2014.

[25] G. Dayanandam, T. Rao, B. Bujji and N. D. S., "DDoS Attacks—Analysis and Prevention.," in *Innovations in Computer Science and Engineering,* Singapore, Springer, 2019.

[26] "Worldwide Infrastructure Security Report," Ipv6.sa, 2019. [Online]. Available: http://ipv6.sa/wp-content/uploads/2014/05/World_Infrastructure_Security_Report_2011.pdf [Accessed 05 October 2019].

[27] S. Yamaguchi, "Botnet Defense System: Concept, Design, and Basic Strategy," in *Inf.*, vol. 11, no. 11, pp. 516-531, Nov. 4, 2020, doi:10.3390/info11110516.