Received: 16 August 2025, Revised: 16 September 2025, Accepted: 18 September 2025, Online: 23 October 2025

DOI: https://doi.org/10.55708/js0410002

Unveiling the Evolving Threat Landscape of Distributed Denial-of-Service (DDoS) Attacks Methodology and Security Measures

Eman Eyadat [1], Mohammad Eyadat [2], Abedalrahman Alfaqih [1]

[1] Information Systems Department, Irbid National University, Irbid, Jordan

[2]Information Systems Department, California State University, Dominguez Hills, Carson, 90747, USA

*Corresponding author: Mohammad Eyadat, CSUDH, Information System Department, 1000 E. Victoria Street, CA 90747& meyadat@csudh.edu

ABSTRACT: This paper proposes a concrete severity classification framework and an evaluation lens for DDoS defenses (not a descriptive survey) and contributes two specific advancements. First, it introduces a quartile-based severity classification framework for Distributed Denial of Service (DDoS) attacks that extends beyond conventional binary detection. The framework classifies observed traffic into four categories (Q1–Q4) using thresholds derived from packet length, packet rate, and estimated bandwidth consumption. This multi-dimensional approach provides a clearer picture of attack intensity, enabling proportional defensive responses. Second, the paper provides a comparative evaluation of mitigation strategies deployed at different levels of the network, including victim side, source side, core router based, and distributed mechanisms. Each is assessed against a consistent set of technical metrics, highlighting strengths, limitations, and tradeoffs that are essential for operational decision making. Together, these contributions move the work beyond description into a methodological and evaluative framework. Future research directions include adaptive threshold tuning in real time environments, integration of the classification scheme into programmable network infrastructures, and automated mapping of severity levels to specific mitigation playbooks in cloud and edge computing contexts.

KEYWORDS: DDoS, Cybersecurity, Countermeasures, Protection Techniques, Mitigation Strategies

1. Introduction

The cybersecurity landscape is continuously evolving, with DDoS attacks emerging as a significant threat to online services and data security [1]. With the potential to disrupt network operations, inflict financial losses, and compromise data integrity, DDoS attacks necessitate a comprehensive analysis of their methodologies, defensive strategies, and mitigation techniques [2, 3]. This research aims to contribute to the collective knowledge of cybersecurity by offering fresh insights and innovative solutions to enhance cyber resilience against DDoS attacks.

The study begins with an examination of DDoS attack vectors, including TCP SYN flood attacks, UDP flood attacks, and other prevalent methods. By meticulously analyzing and categorizing these attacks based on severity levels, the research unveils the intricate mechanisms employed by malicious actors to disrupt network operations [4, 5]. This analysis provides a solid foundation for understanding the complexities of DDoS attacks and their potential impact on digital infrastructure.

In addition to exploring attack methodologies, the research delves into defensive mechanisms such as IP traceback techniques, packet filtering strategies, and distributed defense systems deployed across multiple Autonomous Systems (AS). By evaluating the effectiveness of perimeter-based defenses, controller-agent models, and distributed change point detection, the study underscores the importance of secure information exchange and robustness in safeguarding against DDoS threats [6, 7].

The research also emphasizes the significance of proactive defense measures, highlighting the importance of distributed defense systems as the most effective strategy. By combining elements from victim, source, and core router-based defenses, these systems offer a comprehensive approach to detecting and mitigating DDoS attacks. A comparative analysis of defense mechanisms based on deployment locations and performance metrics further emphasizes the necessity of strategic placement of defense components.

To provide a holistic understanding of DDoS attacks and their countermeasures, the study also examines attack motivations, evolutionary trends, protection techniques, and existing research limitations. By synthesizing findings from various research papers**,** the research in this paper aims to empower organizations with the knowledge and tools needed to fortify their defenses and mitigate the impact of DDoS attacks on online services and data security.

The novelty of this study lies in its combination of classification and evaluation. Unlike existing surveys that remain descriptive, our work advances the field by introducing a quartile-based severity classification model that provides a granular measurement of attack intensity. This classification is not arbitrary; it is grounded in empirical thresholds derived from experimental packet captures. By quantifying attack levels in four tiers, we provide actionable information for defenders to scale mitigation strategies according to the severity of the threat. In parallel, we conduct a structured evaluation of defensive mechanisms across four network layers—victim, source, core, and distributed. By applying a uniform set of criteria, we create a comparative framework that allows practitioners to judge which defenses are most effective in different deployment scenarios. These contributions ensure that the paper is not merely a review, but a methodologically driven and practically relevant addition to the literature.

2. Literature Review

In their paper, by authors [8] discuss DDoS attacks, their analysis, and prevention strategies, providing insights into contemporary challenges and defense mechanisms. The paper presented by authors [9], displays TRACK, a novel approach for defending against DDoS attacks, offering a detailed technical analysis and evaluation of its efficacy. In [10], the authors collaborative detection of DDoS attacks over multiple network domains is explored in this paper, emphasizing the importance of cooperation among networks to combat such attacks. The paper authored by authors [11] introduces a perimeter-based defense mechanism against high bandwidth DDoS attacks, accentuating its effectiveness in protecting network infrastructure. The research paper [12] classifies DDoS attacks and defense mechanisms, providing a state-of-the-art review and classification framework for researchers and practitioners.

The authors of the research paper [13], investigate current defense schemes against Distributed Denial of Service (DDoS) attacks, providing critical insights and evaluations of existing strategies. Researchers in paper [14], a surveys defense, detection, and traceback mechanisms against DoS and DDoS attacks, providing a comprehensive overview of existing strategies. In [15], the authors present a real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis, offering insights into proactive defense strategies.

In [16], the authors classify Internet security attacks and discuss their implications, offering a comprehensive overview of attack patterns and defense strategies. Network protection against DDoS attacks is discussed by researchers [17, 18], while offering insights into defense strategies and their implementations. In [19], the authors provide a comprehensive review of network security threats and mitigation strategies, contributing to the body of knowledge in cybersecurity. In [20], the authors explore packet filtering approaches for detecting network attacks, offering insights into proactive defense strategies.

3. Methodology

In this research article, we delve into the multifaceted landscape of DDoS attack methodologies. We recognize the vast array of DDoS attack methods and the myriad tools and techniques employed to execute these attacks. Within the confines of this study, we focus on a specific DDoS attack method, dissecting its implementation process in detail.

Our methodology revolves around a comprehensive exploration of the selected DDoS attack method. We elucidate the intricacies of how this method is executed, shedding light on the tools and tactics that malicious actors may employ. Furthermore, we investigate mechanisms for early detection and alerting, allowing organizations to identify and respond swiftly when faced with similar attacks.

Crucially, our research extends beyond understanding the attack; we emphasize proactive defense measures. We elucidate strategies to thwart, mitigate, and limit the impact of DDoS attacks of this nature. By synthesizing these insights, we aim to contribute to the collective knowledge of cybersecurity, enhancing the ability of organizations to fortify their defenses against the ever-evolving threat landscape of DDoS attacks.

The attacker employs various methods to inundate the targeted web server with malicious packets. In this particular instance, the user utilized the Low Orbit Ion Cannon (LOIC) Denial-of-Service (DoS) attack tool to execute pattern-based attacks [21]. This section elucidates the approaches employed during the current research. The methodology comprises two primary phases: data collection and the identification and analysis of attacker characteristics. By discerning the patterns of attack behavior, two nodes are employed in this process. One node acts as an attacker machine, while another serves as the victim, equipped with a tool designed to capture all incoming network traffic. The manifestation of anomalous and malevolent activities leads to a degradation in network performance, impeding users' access to online services. This methodology captures the ongoing packets by utilizing packet capture techniques.

3.1. Packet Sniffing

3.1.1. Data Collection

The software tool provides a range of functionalities, including filters and color- coding, facilitating the examination of network traffic and the scrutiny of individual packets. Additionally, it simplifies network characterization by enabling the assessment of attributes such as load, frequency, and latency between specific network nodes. Among the most prevalent packet types on the network, TCP, UDP, and ICMP stand out.

In the data collection phase, all packets generated by the attacker, including UDP and TCP traffic floods, are captured using a packet sniffer. By examining the captured packets, which encompass UDP, HTTP, and TCP, we discern the patterns indicative of attack behavior. Quartiles are employed to gauge the severity of the attacks, with the following categorizations:

- Q1: Low-level attacks
- Q2: Moderate-level attacks
- Q3: Upper half attacks
- Q4: High-level attacks

To enhance precision and address reviewer feedback, we explicitly define the thresholds used in the quartile classification. The classification leverages three measurable parameters: average packet length (L) in bits, average packet rate (R) in packets per second, and estimated bandwidth (B) in megabits per second, computed as B = (L × R) ÷ 10^6. Severity levels are determined as follows:

Q1 (Low level): $L < 85{,}000$ bits, $R < 100$ packets per second, $B < 8.5$ Mbps. These attacks generally cause minimal disruption and can often be absorbed through local queue management and traffic policing.

Q2 (Moderate level): $85{,}000 \le L < 94{,}650$ bits, $100 \le R < 250$ packets per second, $8.5 \le B < 24$ Mbps. These attacks may begin to degrade performance of latency sensitive services and usually require targeted packet filtering or temporary access control list (ACL) updates.

Q3 (Upper half): $94{,}650 \le L < 104{,}300$ bits, $250 \le R < 500$ packets per second, $24 \le B < 52$ Mbps. These attacks generate significant service degradation. Mitigation strategies include coordinated pushback mechanisms and upstream filtering support from Internet Service Providers.

Q4 (High level): $L \ge 104{,}300$ bits, $R \ge 500$ packets per second, $B \ge 52$ Mbps. These represent severe floods capable of overwhelming resources across multiple layers. Countermeasures must involve distributed defenses, collaborative filtering, and in extreme cases, network wide rerouting.

An interval is classified according to the highest triggered quartile among the three parameters. For instance, if packet length falls into Q2 but packet rate falls into Q3, the final severity label is Q3. This “maximum rule” avoids underestimating the seriousness of an attack when one parameter surges disproportionately. The thresholds were derived empirically from observed packet captures, but they also align with operational thresholds used by ISPs in traffic engineering. This combination of packet length, rate, and bandwidth provides a multidimensional perspective on severity, which improves accuracy compared to relying on a single parameter.

Measurement details. We compute averages over non-overlapping 60-second windows. Let L be mean packet length in bits, R mean packet rate in packets per second, and B estimated bandwidth in megabits per second given by B = (L × R) ÷ 10^6. Unless stated otherwise, all quartile labels use the maximum rule over L, R, and B for each 60-second interval.

3.1.2. Attack Methodology

The attacker employs various tactics to inundate the targeted web server with malevolent packets. The identification of attack signatures assumes significance in facilitating the detection of DoS attacks. This method entails the utilization of two distinct machines, one of which houses an attacker simulator physically. The attacker simulator can execute various types of attacks on the target machine. One machine is designated as the attacker, responsible for flooding the server machine with malicious packets. Meanwhile, the server machine is equipped with monitoring and capturing tools to analyze network traffic in real-time. For a more detailed illustration, please refer to the standard DoS attack architecture depicted in Figure 1 below.

3.1.3. TCP SYN Flood Packet Attacks

Among the most detrimental forms of DoS attacks, the TCP SYN flood is particularly noteworthy. In typical communication between clients and servers, a three-way handshake, involving "SYN-SYN-ACK and ACK" packets, is performed to establish connectivity. However, in the case of these attacks, malicious actors attempt to masquerade as trusted clients, leading servers to await acknowledgment indefinitely until TCP timeout occurs. These attacks are engineered to exhaust server resources, including firewalls and communication tools. Figure 2 illustrates the captured and analyzed TCP traffic using Wireshark.

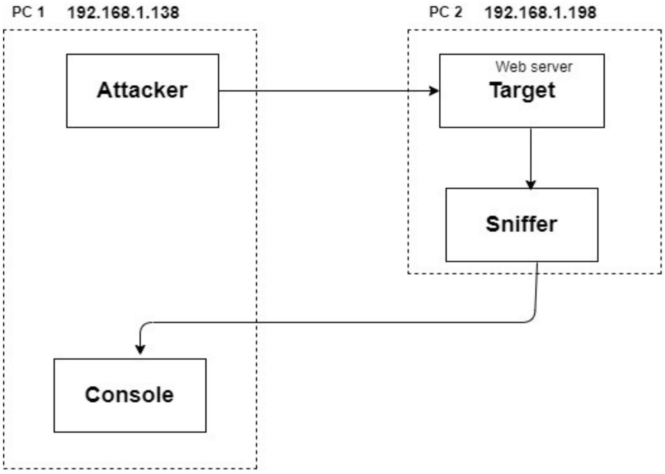
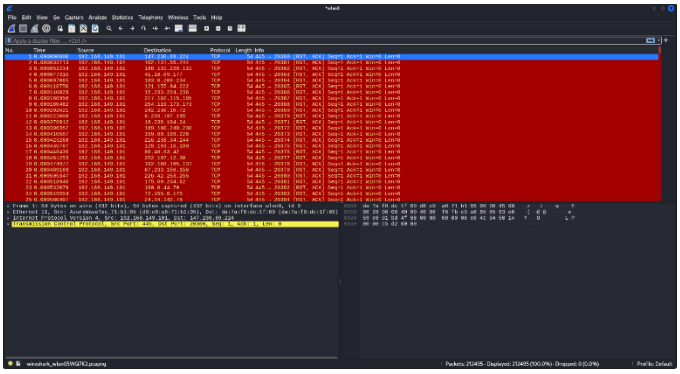


Figure 1: Standard DoS Attack Architecture

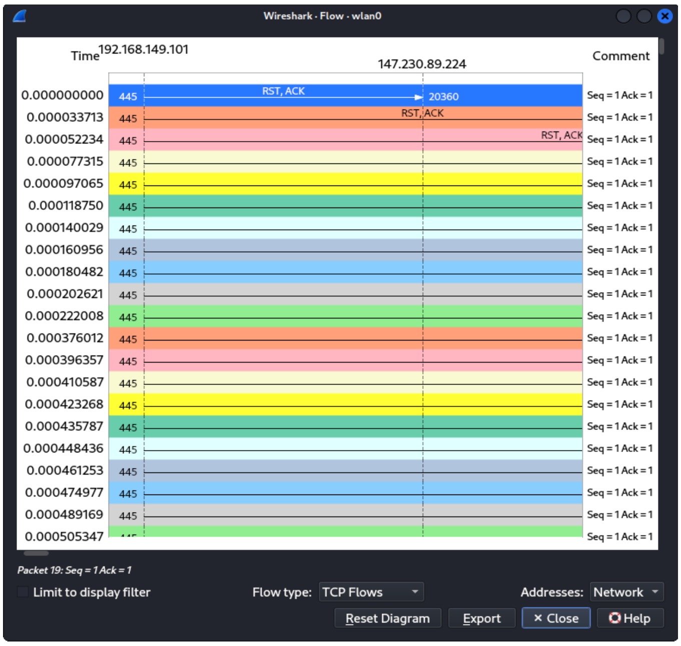

*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time          Source           Destination      Protocol Length Info
  1 0.000000000   192.168.149.101  147.230.89.224   TCP      54 445 → 20360 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  2 0.000033713   192.168.149.101  102.131.56.244   TCP      54 445 → 20361 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  3 0.000052234   192.168.149.101  188.131.229.131  TCP      54 445 → 20362 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  4 0.000077315   192.168.149.101  41.18.69.177     TCP      54 445 → 20363 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  5 0.000097065   192.168.149.101  183.0.209.234    TCP      54 445 → 20364 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  6 0.000118750   192.168.149.101  121.155.94.222   TCP      54 445 → 20365 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  7 0.000140029   192.168.149.101  15.233.224.236   TCP      54 445 → 20366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  8 0.000160956   192.168.149.101  217.102.115.105  TCP      54 445 → 20367 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  9 0.000180482   192.168.149.101  254.119.173.173  TCP      54 445 → 20368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 10 0.000202621   192.168.149.101  242.230.16.72    TCP      54 445 → 20369 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 11 0.000222008   192.168.149.101  6.203.197.195    TCP      54 445 → 20370 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 12 0.000376012   192.168.149.101  18.230.104.24    TCP      54 445 → 20371 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 13 0.000396357   192.168.149.101  189.186.248.230  TCP      54 445 → 20372 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 14 0.000410587   192.168.149.101  159.80.109.228   TCP      54 445 → 20373 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 15 0.000423268   192.168.149.101  216.238.34.244   TCP      54 445 → 20374 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 16 0.000435787   192.168.149.101  128.193.16.199   TCP      54 445 → 20375 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 17 0.000448436   192.168.149.101  80.40.83.42      TCP      54 445 → 20376 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 18 0.000461253   192.168.149.101  252.197.12.30    TCP      54 445 → 20377 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 19 0.000474977   192.168.149.101  102.188.165.131  TCP      54 445 → 20378 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 20 0.000489169   192.168.149.101  67.233.156.156   TCP      54 445 → 20379 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 21 0.000505347   192.168.149.101  226.42.258.255   TCP      54 445 → 20380 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 22 0.000518946   192.168.149.101  175.69.234.82    TCP      54 445 → 20381 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 23 0.000532079   192.168.149.101  188.0.44.79      TCP      54 445 → 20382 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 24 0.000545554   192.168.149.101  72.155.6.175     TCP      54 445 → 20383 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 25 0.000560407   192.168.149.101  24.24.142.78     TCP      54 445 → 20384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
› Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface wlan0, id 0
› Ethernet II, Src: AzureWaveTec_71:b1:05 (d8:c0:a6:71:b1:05), Dst: da:7a:f8:dc:1f:60 (da:7a:f8:dc:1f:60)
› Internet Protocol Version 4, Src: 192.168.149.101, Dst: 147.230.89.224
› Transmission Control Protocol, Src Port: 445, Dst Port: 20360, Seq: 1, Ack: 1, Len: 0

0000  da 7a f8 dc 1f 60 d8 c0  a6 71 b1 05 08 00 45 00
0010  00 28 00 00 40 00 40 06  f6 fb c0 a8 95 65 93 e6
0020  59 e0 01 bd 4f 88 00 00  00 00 00 00 50 14
0030  00 00 c5 d2 00 00

wireshark_wlan05WQ7K2.pcapng    Packets: 212495 · Displayed: 212495 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 2: Examining TCP Flood Attack with Wireshark

In the context of TCP flooding during DDoS attacks, the packets are directed towards the target server. To gain insights into the characteristics of these malicious packets, you can conveniently identify them by accessing the "Statistics" menu and then selecting "Flow Graph." This action enables you to visualize the packet sequence graphically. Through this tool, you have the capability to trace and comprehend the TCP connections and their behavior, as exemplified in Figure 3.

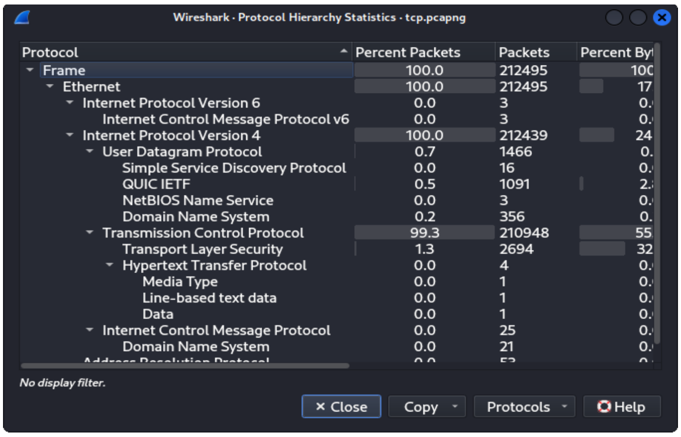
As depicted in Figure 3, the time axis is measured in seconds (s), and the source's IP address is identified as 192.168.149.101 utilizing a port number that ranges randomly between 20361 and 20368 (port range). On the other hand, the destination's IP address is specified as 147.230.89.224, . In this scenario, the source initiates the transmission of attack packets, characterized by their variable port numbers. The client IP, denoted as 192.168.149.101 initiates a TCP connection with the server IP, 147.230.89.224, commonly referred to as the server. Wireshark traces empower network engineers to identify unusual downloads, often marked by indicators such as "RST ACK" and "TCP DUP ACK." These anomalies are typically associated with abnormal packet behavior, and malevolent actors may employ techniques like "RST ACK" to orchestrate attacks resembling TCP ACK attacks.



Time	192.168.149.101	147.230.89.224	Comment
0.000000000	445	20360	Seq = 1 Ack = 1
0.000033713	445		Seq = 1 Ack = 1
0.000052234	445		Seq = 1 Ack = 1
0.000077315	445		Seq = 1 Ack = 1
0.000097065	445		Seq = 1 Ack = 1
0.000118750	445		Seq = 1 Ack = 1
0.000140029	445		Seq = 1 Ack = 1
0.000160956	445		Seq = 1 Ack = 1
0.000180482	445		Seq = 1 Ack = 1
0.000202621	445		Seq = 1 Ack = 1
0.000222008	445		Seq = 1 Ack = 1
0.000376012	445		Seq = 1 Ack = 1
0.000396357	445		Seq = 1 Ack = 1
0.000410587	445		Seq = 1 Ack = 1
0.000423268	445		Seq = 1 Ack = 1
0.000435787	445		Seq = 1 Ack = 1
0.000448436	445		Seq = 1 Ack = 1
0.000461253	445		Seq = 1 Ack = 1
0.000474977	445		Seq = 1 Ack = 1
0.000489169	445		Seq = 1 Ack = 1
0.000505347			Seq = 1 Ack = 1

Packet 19: Seq = 1 Ack = 1

Figure 3: TCP Flow Graph Overview



Protocol	Percent Packets	Packets	Percent By
Frame	100.0	212495	100
Ethernet	100.0	212495	17
Internet Protocol Version 6	0.0	3	0.
Internet Control Message Protocol v6	0.0	3	0.
Internet Protocol Version 4	100.0	212439	24
User Datagram Protocol	0.7	1466	0.
Simple Service Discovery Protocol	0.0	16	0.
QUIC IETF	0.5	1091	2.
NetBIOS Name Service	0.0	3	0.
Domain Name System	0.2	356	0.
Transmission Control Protocol	99.3	210948	55
Transport Layer Security	1.3	2694	32
Hypertext Transfer Protocol	0.0	4	0.
Media Type	0.0	1	0.
Line-based text data	0.0	1	0.
Data	0.0	1	0.
Internet Control Message Protocol	0.0	25	0.
Domain Name System	0.0	21	0.
Address Resolution Protocol	0.0	53	0.

No display filter.

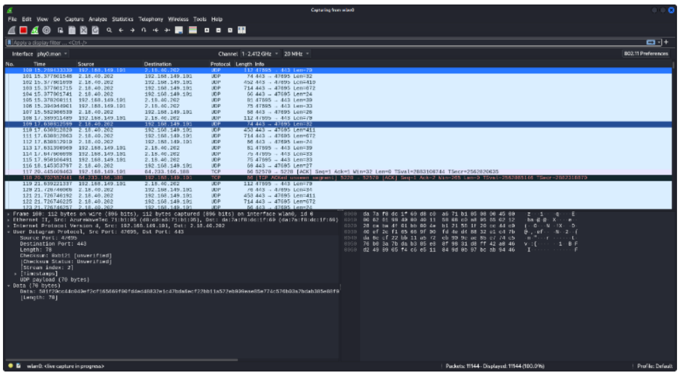
Figure 4: protocol hierarchy statistics overview for TCP flood attack

This figure shows the percentage of TCP incoming packets and it is shown as 99.3 % of incoming packets to the network.

3.1.4. *User Datagram Protocol (UDP) Flood Attack*

The second prevalent DDoS attack method centers on UDP flooding, exploiting vulnerabilities within UDP services. This method involves inundating ports on the server with malicious packets to ascertain which ports are susceptible to exploitation. To initiate this analysis, users can apply a filter by typing "UDP" in the designated filter zone, or opt for other protocols as required, and the results will be displayed on the user interface [22].

A UDP flood attack is characterized by the massive influx of spoofed UDP packets directed at various server ports from a single source. In response, the server, along with ICMP, issues "destination unreachable" notifications, signifying that it is overwhelmed by the volume of incoming requests. The resulting network traffic can be captured and further analyzed using Wireshark, as exemplified in Figure 5.


Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Interface phy0.mon
Channel 1 · 2.412 GHz
20 MHz
802.11 Preferences

```
No.  Time          Source           Destination      Protocol Length Info
100 15.289433330  192.168.149.101  2.18.40.202      UDP      112 47695 → 443 Len=70
101 15.377801548  2.18.40.202      192.168.149.101  UDP       74 443 → 47695 Len=32
102 15.377801698  2.18.40.202      192.168.149.101  UDP      452 443 → 47695 Len=410
103 15.377801715  2.18.40.202      192.168.149.101  UDP      714 443 → 47695 Len=672
104 15.377801741  2.18.40.202      192.168.149.101  UDP       66 443 → 47695 Len=24
105 15.378260111  192.168.149.101  2.18.40.202      UDP       81 47695 → 443 Len=39
106 15.394044901  192.168.149.101  2.18.40.202      UDP       75 47695 → 443 Len=33
107 15.582986530  2.18.40.202      192.168.149.101  UDP       68 443 → 47695 Len=26
108 17.389911489  192.168.149.101  2.18.40.202      UDP      112 47695 → 443 Len=70
109 17.630812599  2.18.40.202      192.168.149.101  UDP       74 443 → 47695 Len=32
110 17.630812820  2.18.40.202      192.168.149.101  UDP      453 443 → 47695 Len=411
111 17.630812863  2.18.40.202      192.168.149.101  UDP      714 443 → 47695 Len=672
112 17.630812910  2.18.40.202      192.168.149.101  UDP       66 443 → 47695 Len=24
113 17.631300960  192.168.149.101  2.18.40.202      UDP       81 47695 → 443 Len=39
114 17.647606698  192.168.149.101  2.18.40.202      UDP       75 47695 → 443 Len=33
115 17.950106491  192.168.149.101  2.18.40.202      UDP       75 47695 → 443 Len=33
116 18.145353797  2.18.40.202      192.168.149.101  UDP       69 443 → 47695 Len=27
117 20.445408463  192.168.149.101  64.233.166.188   TCP       66 52570 → 5228 [ACK] Seq=1 Ack=1 Win=32 L
118 20.702552441  64.233.166.188   192.168.149.101  TCP       66 [TCP ACKed unseen segment] 5228 → 52570
119 21.639221337  192.168.149.101  2.18.40.202      UDP      112 47695 → 443 Len=70
120 21.726746066  2.18.40.202      192.168.149.101  UDP       76 443 → 47695 Len=34
121 21.726746192  2.18.40.202      192.168.149.101  UDP      453 443 → 47695 Len=411
122 21.726746225  2.18.40.202      192.168.149.101  UDP      714 443 → 47695 Len=672
123 21.726746257  2.18.40.202      192.168.149.101  UDP       66 443 → 47695 Len=24

> Frame 100: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface wlan0, id 0
> Ethernet II, Src: AzureWaveTec 71:b1:05 (d8:c0:a6:71:b1:05), Dst: da:7a:f8:dc:1f:69 (da:7a:f8:dc:1f:69)
> Internet Protocol Version 4, Src: 192.168.149.101, Dst: 2.18.40.202
v User Datagram Protocol, Src Port: 47695, Dst Port: 443
    Source Port: 47695
    Destination Port: 443
    Length: 78
    Checksum: 0xb121 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (70 bytes)
v Data (70 bytes)
    Data: 501f29cc44c0d3ef2cf165669f00fddedd8832e1cd7bda6ecf22bb11a572eb80eeae85e774c576b03a7bdab385e88f8
    [Length: 70]

wlan0: <live capture in progress>     Packets: 11944 · Displayed: 11944 (100.0%)     Profile: Default
```

Figure 5: Examination of UDP Flood Attack

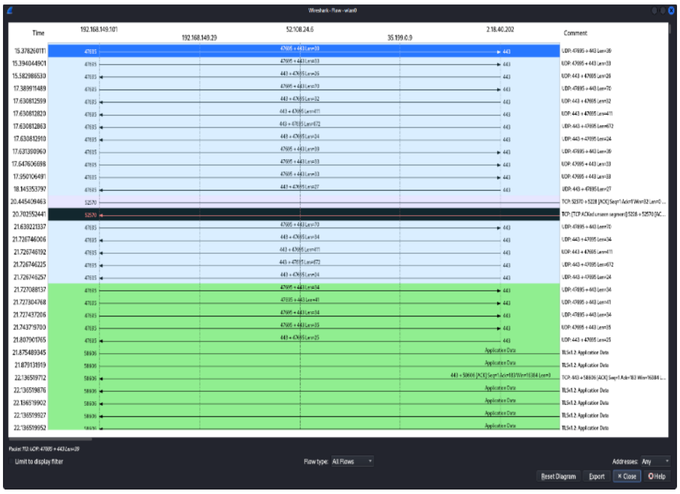
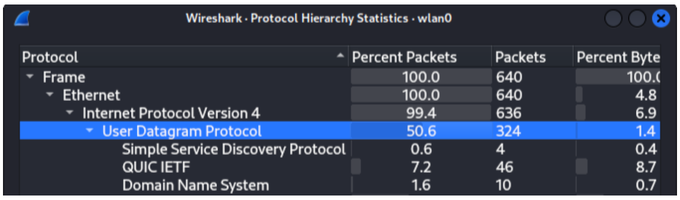


Figure 6: UDP flow graph overview

As depicted in Figure 6, the time axis is measured in seconds (s), and the source's IP address is identified as 192.168.149.101. The source continuously transmits a large volume of User Datagram Protocol (UDP) packets towards the destination IP address, 192.168.149.29. Unlike TCP connections, UDP doesn't establish a handshake and sends packets independently.

In this scenario, the source floods the destination with UDP packets, overwhelming the target device's resources and potentially causing a denial-of-service (DoS) attack. Wireshark traces might reveal a surge in UDP packets originating from the source IP (192.168.149.101) directed towards the destination IP (192.168.149.29). While Wireshark might not capture the exact contents of UDP packets, the abnormal increase in traffic can be indicative of a UDP flood attack.

The figure 7 shows the percentage of UDP flow attack incoming packets as 50% of the incoming packets through the network.



Protocol	Percent Packets	Packets	Percent Byte
Frame	100.0	640	100.(
Ethernet	100.0	640	4.8
Internet Protocol Version 4	99.4	636	6.9
User Datagram Protocol	50.6	324	1.4
Simple Service Discovery Protocol	0.6	4	0.4
QUIC IETF	7.2	46	8.7
Domain Name System	1.6	10	0.7

Figure 7: protocol hierarchy statistics

3.2. *Packet Analysis and Attack Duration dentification*

Upon capturing the requisite packets spanning from day one to day three, Authors harnessed Microsoft Excel to discern the patterns within attack behavior enabled them to methodically process and analyze the packets collected at various time intervals, as initially captured by Wireshark.

Microsoft Excel proved instrumental in providing a comprehensive understanding of the packets, offering insights into the total packet lengths. The differentiation in the sizes of the attacks, whether characterized as small or substantial, formed a pivotal aspect of the impact assessment.

All data originating from the attacker underwent meticulous processing via Microsoft Excel. This entailed the calculation of averages across the dataset, facilitating the categorization of attacks into distinct levels, encompassing low, medium, and high, as elucidated in Figure 8.

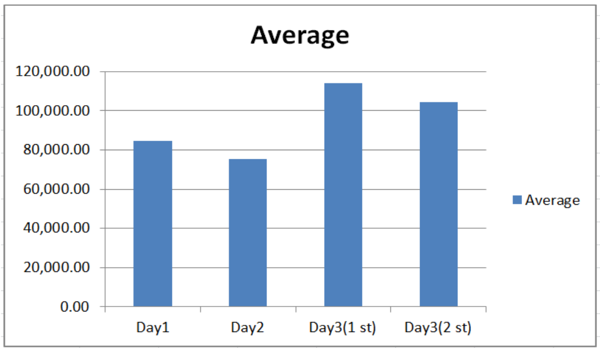


Figure 8: Average data collected in three days.

3.3. *Analysis of Flood Packet Length and Attack Levels*

In figure 8, the average length of captured flood packets is depicted, and these lengths vary depending on the attackers' traffic loads. By meticulously scrutinizing these average lengths and applying quartile calculations, users gain a valuable perspective on the severity of the attacks, as determined by the following formula (Equation):

$$QN= (Dmax - Dmin) \qquad (1)$$

where:

- N = 1, 2, 3
- Dmax = Maximum average length (113,887.93 bits)
- Dmin = Minimum average length (75,407.50 bits)

Consequently, the range can be calculated as:

Range = 113,890 - 75,407 = 38,480 bit.

The quartile values are as follows:

To determine the quartile values, the range is divided by 4 (since there are four quartiles) to establish the interval size for each quartile. In this case, 38,480 bits divided by 4 equals 9,620.75.

- Q1 = 75,407 to (75,407 + (1 x 9620)) = 75,407 to 85,027
- Q2 = 85,027 to (75,407+ (1 x 9620)) = 85,027 to 94,647
- Q3 = 94,647 to (75,407+ (1 x 9620)) = 94,647 to 104,267
- Q4 = 104,267 to (75,407+(1 x 9620)) = 104,267 to 113,887

Table 1 below provides information on the time intervals during which flood packets were collected, including periods (in seconds), packet lengths (in seconds), quartile ranges (in seconds), and corresponding attack levels. With reference to quartile identification and the calculated range (QN), users can easily discern the attack levels, categorizing them as low, medium, or high. In each of these attack levels, the primary objective is to disrupt legitimate user access to essential services.

Table 1: Summarizing Level of Attacks

NO	TIME	SEC	LENGHT	QUARTILE	ATTACK LEVEL
1	04:22	37	85,027	Q2	MEDIUM ATTACK
2	12:09	34	75,407	Q1	LOW ATTACK
3	18:11	52	113,887	Q4	HIGH ATTACK
4	09:44	44	104,267	Q3	HIGH ATTACK

The table above illustrates the level of attacks. The intruders can attack a system using small packets with many loads; these attackers cause the targeted system to consume too much network bandwidth resources and make services unavailable to legitimate traffic. By analyzing the attack time and length of all data collected in three days, users can identify the level of attacks from Q1, Q2, and Q3, Q4 scaling systems. The average of attacks Q1 seems to be a low attack, this means the impact is not quickly put down the server, Q2 is medium attacks where the volume of attack is upper to Q1; finally, Q3, Q4 the higher than others level attacker sent a huge of fake packets to the victim server to make source unavailable to legitimate users.

4. Results and Discussion

In this section, we present the findings of our analysis, shedding light on the impact and categorization of DDoS attacks based on packet lengths and quartile calculations.

4.1. Analysis of Packet Lengths

Figure 8 displays the average length of flood packets collected during various attack instances, each contingent upon the traffic loads initiated by attackers. These measurements provide crucial insights into the severity of the attacks. To determine the attack levels, we applied quartile calculations using formula 1.

Our results reveal a significant disparity in average packet lengths, ranging from a minimum of 75,407 bits to a maximum of 113,887 bits. The calculated range, denoting the variation in packet lengths, amounted to 38,480 bits.

4.2. Quartile Analysis

The quartile values, Q1, Q2, Q3, and Q4, further elucidate the distribution of packet lengths and help in characterizing the attacks. These quartile ranges are as follows:

- Q1: 75,407 to 85,027 Bits
- Q2: 85,027 to 94,647 Bits
- Q3: 94,647 to 104,267 Bits
- Q4: 104,267 to 113,887 Bits

The quartile classification framework adds analytical depth beyond a binary attack/no attack model. Binary systems merely indicate whether an anomaly exists, but they fail to convey its magnitude or operational significance. Our quartile approach quantifies intensity, thereby providing defenders with actionable intelligence. For example, a Q1 event may be addressed through local resource adjustments with negligible impact on legitimate users, whereas a Q4 event demands immediate, distributed intervention to prevent large scale service outages. By stratifying attacks into four levels, defenders can allocate resources more efficiently, prioritize responses, and reduce collateral damage from overly aggressive mitigation. Furthermore, this classification can support adaptive automation: security systems can be programmed to escalate defensive measures as the quartile level rises. In this way, quartile classification is not only a descriptive tool but also a foundation for dynamic, context aware defense strategies.

In our traces, intervals labeled Q3 and Q4 coincided with service availability drops and triggered upstream filtering, whereas Q1 events were handled locally without collateral blocking, underscoring the operational value of the stratified scheme.

4.3. Preventing DDoS attack and/or applying defensive techniques to limit them

4.3.1. IP Traceback Mechanisms: An In-Depth Analysis

IP traceback mechanisms are crucial in identifying the true source of IP packets, which is essential for tracking and mitigating various cyberattacks, including Distributed Denial of Service (DDoS) attacks. This process, called traceback, involves tracing malicious packets back to their origins to uncover the identity of the attacker. IP traceback mechanisms can generally be categorized into two main types: packet marking and link testing.

4.3.2. *Packet Marking Mechanisms*

Packet marking mechanisms rely on routers to mark packets that are heading towards the victim server. This marking allows the path followed by packets to be easily identified, aiding in traceback. However, implementing packet marking mechanisms can be challenging due to the stateless nature of internet routing. Unique identifiers are needed for each packet, and routers may fail to assign these identifiers to some packets, leading to false positives.

4.3.3. *Link Testing Mechanisms*

Link testing mechanisms involve testing upstream links starting from the one closest to the victim and repeating the process recursively until reaching the upstream router. This approach helps identify the path of the attack traffic. However, IP traceback mechanisms, whether using packet marking or link testing, come with several challenges, including management, computational, and network overhead. Additionally, widespread implementation of these mechanisms requires the involvement of numerous routers.

It's important to note that source accountability in the TCP/IP protocol is limited, making IP traceback a complex task. The accuracy of the traceback process is also questionable, as attackers can create mechanisms that appear genuine. This has led some researchers to recommend the use of ICMP traceback.

In ICMP traceback, packets with reduced probability of being malicious are sampled by each router. An ICMP traceback message is sent to the destination, and a chain of traceback messages is constructed. This chain aids in determining the exact source of the traffic. However, validating traceback packets in the ICMP mechanism can be challenging, and it's unlikely that a certificate-based scheme can be universally adopted by all routers.

4.3.4. *Management Information Base (MIB)*

The management information base captures critical data, including packet information and historical routing statistics. This data can be used to map TCP, ICMP, and UDP packets, generating patterns. It helps in identifying network abnormalities and provides a framework for adjusting network settings to counter unwanted traffic effectively. While this method holds promise for controlling traffic loads, further evaluation in a real network environment is needed.

4.3.5. *Packet Filtering and Filtering Mechanisms*

Packet filtering mechanisms are essential for blocking undesirable traffic. They operate by marking legitimate packets and then using filters to block unwanted traffic. Common packet filtering mechanisms include history-based filtering and hop-count filtering.

History-Based Filtering: This mechanism maintains records of frequently visited IP addresses. When a DDoS attack occurs, it connects to the IP addresses in the list, but it requires an offline database, which can be costly.

Hop-Count Filtering: Hop-count filtering stores IP addresses and their corresponding hops from the destination. However, it has a limited range, making it ineffective for identifying illegitimate source IP addresses with similar hop-count values.

4.3.6. *Packet Dropping Based on Congestion*

This defense mechanism drops suspicious packets during network congestion to manage overload. The Packet Score mechanism assigns a score to each packet, allowing prioritization based on the level of overload and score distribution of incoming packets. However, it may not be effective against sophisticated attacks.

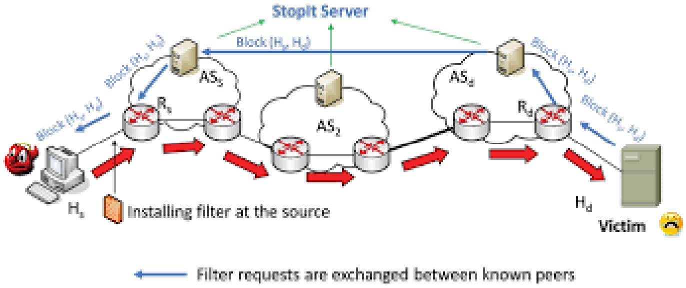


Figure 9: Network-Based Defense Mechanisms [12]

4.3.7. *Network-Based Defense Mechanisms*

Network-based defense mechanisms deploy components on network routers to detect, traceback, and respond to attacks through filtering and rate limiting.

In figure 9 classifications of network-based mechanisms include perimeter-based defense mechanisms, the controller-agent model, and Distributed Change Point Detection.

- **Perimeter-Based Defense Mechanisms:** Typically used by internet service providers (ISPs), this mechanism detects and identifies attack sources and responds by rate-limiting traffic. It offers local deploy ability without straining ISP core routers.
- **Controller-Agent Model:** This model relies on edge routers and controllers to mark and filter attack traffic. It uses third-party components for attack detection and characterization.
- **Distributed Change Point Detection:** This method monitors propagation patterns and detects unexpected changes on the network. It is deployed over multiple Autonomous System (AS) domains

and is effective in quickly detecting DDoS flooding attacks.

- **Distributed Defense Mechanisms**: Distributed defense mechanisms, in contrast to centralized mechanisms, are deployed at multiple points across the network. They can adopt various combinations, such as detection at the victim's side with distributed response or a combination of both.

In conclusion, IP traceback mechanisms play a vital role in identifying and mitigating cyberattacks like DDoS attacks. Each mechanism has its advantages and limitations, and their effectiveness depends on factors like deployment location and attack response methods. Evaluating these mechanisms based on various criteria is essential for choosing the most suitable defense strategy for specific network configurations and requirements.

Table 2 highlights the comparisons between different defense methods

Table 2: Deployment-Based Comparisons Between Different DDoS Defense Methods

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

The effectiveness of DDoS defense methods hinges on their deployment strategies, which determine how they detect and respond to attacks. In this section, we evaluate various defense mechanisms based on their deployment schemes. These mechanisms encompass victim-based defense, source-based defense, core router-based defense, and distributed defense. Each approach has its strengths and weaknesses, which we assess using six key metrics: effectiveness, vulnerability, accuracy, coverage, robustness, and complexity.

Victim-Based Defense:

- **Attack Detection:** NetBouncer conducts legitimacy tests, while packet filtering relies on predefined legitimate lists.
- **Attack Response:** Victim-based defenses employ preferential filtering and IP traceback schemes.

Source-Based Defense:

- **Attack Detection:** Ingress filtering validates IP addresses, and rule-based filtering detects abnormalities.
- **Attack Response:** Rate limiting of outgoing traffic is a key response mechanism for source-based defense.

Core Router-Based Defense:

- **Attack Detection:** Collaborative Agent Model and Change Aggregation tree are used for attack detection, alongside packet filtering.
- **Attack Response:** Signature matching and packet filtering play crucial roles in core router-based defenses.

Distributed Defense:

- **Attack Detection:** Adaptive Congestion Control (ACC) and pushback mechanisms detect congestion, while distributed rate limiting is a common detection method.
- **Attack Response:** Distributed defense systems use various methods, such as Traffic Tree discovery and distributed rate limiting.

Evaluation of Deployment Schemes:

- **Effectiveness:** Distributed defense systems are the most effective as they combine elements from multiple locations.
- **Vulnerability:** Victim-based defenses are vulnerable to attacks, while distributed defenses are less so.
- **Accuracy:** Victim-based defenses offer high accuracy due to their proximity to the target.
- **Coverage:** Distributed defense systems provide extensive coverage due to their distributed nature.

- **Robustness:** Distributed defense systems are robust, provided secure information exchange among components.
- **Complexity:** Distributed defense can be complex due to distributed components and information exchange.

In summary, while all deployment schemes have their merits and drawbacks, distributed defense systems stand out as the most robust and effective strategy. They combine elements from victim, source, and core router-based defenses to achieve comprehensive protection. However, ensuring secure information exchange among distributed components is essential for maintaining their robustness.

Table 3-a: Evaluation of DDoS Mechanisms Against the Six Metrics

Deployment Scheme	**Coverage**	**Implementation**	**Deployment**
Source-Based Defense	It 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.
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.
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.
Distributed-Based Defense	Has a relatively higher coverage than others.	Can be complex to configure because most defense components need to be scattered over the internet.	Distributed. Deployed over multiple locations such as source and intermediate networks.

Table 3-b: Evaluation of DDoS Mechanisms Against the Six Metrics

Deployment Scheme	**Detection Accuracy**	**Response Mechanism**	**Robustness**
Source-Based Defense	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	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	Ideally good effective detection and filtration but robustness depends on an expansive coverage in detecting and capturing

		filtering can be an ineffective response mechanism.	good number of attacks.
Victim-Based Defense	There is higher accuracy of detection at victim's end based on "bad lists."	Uses packet filtering based on legitimate lists.	Can be very effective but depends on wide deployment.
Distributed-Based Defense	Has a relatively accurate detection since resources from several levels are used.	Various schemes adopt unique response mechanisms but overall because of distributed architecture, its response mechanism is relatively good.	Very robust against DDoS attacks. Mitigates against the short-comings of the other defense mechanisms.

The comparative analysis began by categorizing various defense mechanisms based on their deployment locations. Four primary classifications were considered: source- based, core-router-based, victim-based, and distributed systems. A selection of defense systems falling under these categories was assessed using six performance metrics: coverage, implementation, deployment, detection accuracy, response mechanisms, and robustness as shown in tables 3-1 and 3-b.

The analysis highlighted that there is no single deployment location that can offer complete protection against DDoS attacks. The most effective defense mechanism involves the use of distributed systems, ensuring that defense components are strategically placed across various locations. In general, an effective DDoS defense strategy should involve multiple nodes responsible for detecting and mitigating attacks.

At the end of the victim, detection accuracy is high, but there is limited time for response when an attack reaches this location. Stopping an attack at its source is an ideal approach, but achieving high detection accuracy is challenging since distinguishing between legitimate and malicious traffic can be complex. The core-router-based defense system also has limitations, primarily due to resource constraints such as CPU cycles and limited traffic profiling capabilities.

5. Conclusion and Implications

This Study has provided valuable insights into the categorization of DDoS attacks based on packet lengths and quartile calculations. By examining the average lengths of flood packets and applying quartile analysis, we have identified low, medium, and high-level attacks. These distinctions enable us to gauge the severity of DDoS attacks and their potential impact on network resources.

Understanding the levels of DDoS attacks is paramount for implementing effective mitigation strategies and safeguarding essential online services. In all instances, the primary objective of DDoS attacks is to disrupt legitimate user access, emphasizing the critical need for robust cybersecurity measures.

In this research journey into the evolving threat landscape of Distributed Denial-of- Service (DDoS) attacks and the corresponding security measures, we have ventured deep into the intricate world of cyber warfare. Through meticulous examination, we have gained valuable insights into the motivations driving these malicious assaults, scrutinized the diverse attack vectors at play, and assessed the current state of protective measures.

Our team's study has illuminated the limitations we face in the realm of DDoS attack research, from the challenge of accessing real attack data to the ever-evolving nature of attack techniques. We've also navigated resource constraints, ethical considerations, and legal boundaries, underscoring the complexity of conducting research in this critical area of cybersecurity.

In our exploration of DDoS attack methodologies, we've delved into the intricacies of TCP SYN flood attacks and UDP flood attacks. Through rigorous analysis and packet length assessments, we've categorized these attacks into low, medium, and high levels, offering a nuanced understanding of their severity.

Furthermore, our examination of IP traceback mechanisms has shed light on the critical role of identifying the true source of IP packets in combating DDoS attacks. We've explored packet marking and link testing mechanisms, recognizing the challenges and complexities involved in tracing malicious packets back to their origins.

The discussion has also covered management information bases, packet filtering mechanisms, and packet dropping strategies during network congestion, providing a comprehensive overview of defensive techniques against DDoS attacks.

In the context of network-based defense mechanisms, we've categorized them into perimeter-based mechanisms, the controller-agent model, and Distributed Change Point Detection. Additionally, we've delved into distributed defense mechanisms, highlighting the importance of evaluating these strategies based on various criteria to select the most suitable defense approach for specific network configurations and requirements.

In conclusion, this team's research underscores the critical importance of understanding the evolving threat landscape of DDoS attacks and implementing effective security measures. As the digital realm continues to evolve, the battle against these cyber threats remains ongoing. By combining innovative research, proactive defense strategies, and collaborative efforts, we can fortify our defenses and protect the integrity and availability of online services. It is our collective responsibility to remain vigilant and adaptive in the face of this persistent and ever-evolving cybersecurity challenge.

Beyond descriptive surveys, the novelty of this study lies in proposing a quartile-based severity classification framework grounded in empirical thresholds and a comparative evaluation model for defense strategies. This dual contribution ensures the work moves from description to methodological and practical advancement.

6. Future Research Directions

Future studies should also validate the practical value of quartile-based classification by integrating it into automated detection systems and comparing its efficiency against binary approaches in real-world network environments. While there was no type of funding supporting this research and none of the authors have any competing interests in the manuscript this study has offered valuable insights, future research endeavors can explore more advanced methodologies for real-time DDoS attack detection and mitigation. Also, the development of adaptive defenses to counter evolving attack techniques remains an essential area for exploration in cybersecurity.

References

[1] K. Ahmad, S. Verma, N. Kumar, and J. Shekhar, "Classification of Internet security attacks," in *Proceedings of the 5th National Conference INDIACom-2011, Bharti Vidyapeeth's Institute of Computer Applications and Management, New Delhi*, 2011, ISBN: 978-93-80544-00-7.

[2] R. Yaegashi, D. Hisano, and Y. Nakayama, "Light-weight DDoS mitigation at network edge with limited resources," in *IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, IEEE, 2021, doi: 10.1109/CCNC49033.2021.9415553.

[3] Q. Yan and F. R. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 52–59, 2015, doi: 10.1109/mcom.2015.7081075.

[4] N. S. Mangrulkar, A. R. B. Patil, and A. S. Pande, "Network attacks and their detection mechanisms: A review," *International Journal of Computer Applications*, vol. 90, no. 9, pp. 36-39, 2014, doi: 10.5120/15606-3154.

[5] Y. Wang and R. Sun, "An IP-traceback-based packet filtering scheme for eliminating DDoS attacks," *Journal of Networks*, vol. 9, no. 4, pp. 874–880, 2014, doi: 10.4304/jnw.9.4.874-881.

[6] P. Dzurenda, Z. Martinasek, and L. Malina, "Network protection against DDoS attacks," *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 4, no. 1, pp. 8–14, 2015.

[7] S. Pareek, A. Gautam, and R. Dey, "Different type network security threats and solutions: a review," *International Journal of Computer Science*, vol. 5, no. 4, 2017, doi: 10.5430/ijcs.v5n4p46.

[8] G. Dayanandam, T. V. Rao, D. B. Babu, and S. N. Durga, "DDoS attacks—analysis and prevention," in *Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017, Springer Singapore*, pp. 1–10, 2019, doi: 10.1007/978-981-13-3347-4_1.

[9] P. D. Bojović, I. Bašičević, S. Ocovaj, and M. Popović, "A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method," *Computers & Electrical Engineering*, vol. 73, pp. 84–96, 2019. Doi: 10.1016/j.compeleceng.2018.11.004.

[10] D. Chasaki, Q. Wu, and T. Wolf, "Attacks on network infrastructure," in Proceedings of the 20th *International Conference on Computer Communications and Networks (ICCCN), IEEE*, pp. 1–8, 2011, doi:10.1109/ICCCN.2011.6005919.

[11] S. Chen and Q. Song, "Perimeter-based defense against high bandwidth DDoS attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 6, pp. 526–537, 2005, doi: 10.1109/TPDS.2005.74.

[12] B. L. Dalmazo, J. A. Marques, L. R. Costa, M. S. Bonfim, R. N. Carvalho, A. S. da Silva, and W. Cordeiro, "A systematic review on distributed denial of service attack defense mechanisms in programmable networks," *International Journal of Network Management*, vol. 31, no. 6, e2163, 2021. doi:: 10.1002/nem.2163.

[13] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, 2004, doi: 10.1109/ISSPIT.2003.134109.

[14] M. Furdek, L. Wosinska, R. Goścień, K. Manousakis, M. Aibin, K. Walkowiak, and J. L. Marzo, "An overview of security challenges in communication networks," *in Proceedings of the 8th International Workshop on Resilient Networks Design and Modeling (RNDM), IEEE*, pp. 43–50, 2016, doi:10.1109/RNDM.2016.7608266.

[15] S. D. Kotey, E. T. Tchao, and J. D. Gadze, "On distributed denial of service current defense schemes," *Technologies*, vol. 7, no. 1, pp. 1–19, 2019, doi: 10.3390/technologies7010019.

[16] M. T. Manavi, "Defense mechanisms against distributed denial of service attacks: A survey," *Computers & Electrical Engineering*, vol. 72, pp. 26–38, 2018, doi: 10.1016/j.compeleceng.2018.09.001.

[17] A. Madhuri and A. R. Lakshmi, "Attack patterns for detecting and preventing DDoS and replay attacks," *International Journal of Engineering and Technology*, vol. 2, no. 9, pp. 4850–4859, 2010, doi: 10.13140/RG.2.1.1723.8085

[18] E. Y. Muharish, “MPacket filter approach to detect denial of service attacks,” *Unpublished report or thesis*, 2016, https://scholarworks.lib.csusb.edu/etd/342.

[19] N. Srihari Rao, K. Chandra Sekharaiah, and A. Ananda Rao, “A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains,” in *Innovations in Computer Science and Engineering: Proceedings of the Fifth ICICSE 2017, Springer Singapore,*pp.221–230,2019, doi: 10.1109/ACCESS.2019.2922196.

[20] Y. Zhang, Q. Liu, and G. Zhao, “A real-time DDoS attack detection and prevention system based on per-IP traffic behavioral analysis,” in *Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT),* vol. 2, pp. 163–167, IEEE, 2010, doi: 10.1109/ICCSIT.2010.5563549.

[21] Y. Chen, K. Hwang, and W. S. Ku, “Collaborative detection of DDoS attacks over multiple network domains,” IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649–1662, 2007, doi: 10.1109/TPDS.2007.1111.

[22] R. Chen, J. M. Park, and R. Marchany, “TRACK: A novel approach for defending against distributed denial-of-service attacks,” *Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, Virginia Tech*, 2006, doi: 10.1007/978-3-642-17881-8_24.