International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 19s, 2025
https://www.theaspd.com/ijes.php

Analyzing The Impact Of Distributed Denial Of Service Attacks Using NS2: A Scenario-Based Study

[1]Kavita Kumavat, [2]Aarti Sardhara, [3]Trupti Shinde, [4]Vishakha Salunkhe, [5]Mayuri Satpute, [6]Kanchan Katake
[1,2,3,4,5,6]Assistant Professor, Vishwakarma University, Pune

Abstract
Distributed Denial of Service (DDoS) attacks remain a persistent and formidable threat to modern network infrastructure. These attacks disrupt services, degrade performance, and expose vulnerabilities by overwhelming targets with malicious traffic. This research leverages NS2 (Network Simulator 2) to simulate DDoS attack scenarios and analyze their impact on key network performance metrics, including throughput, packet loss, and latency.
The paper introduces a robust three-phase implementation framework—Preattack (Preparation), During Attack (Mitigation), and Postattack (Recovery)—to counteract DDoS threats effectively. It highlights proactive measures such as advanced Intrusion Detection Systems (IDS), dynamic rate limiting, and collaborative ISP partnerships, ensuring network resilience. Experimental results demonstrate significant performance degradation during attacks, followed by recovery through mitigation strategies.
This research underscores the importance of a structured, adaptive approach to safeguarding network infrastructure, providing actionable insights for organizations to combat evolving cyber threats.
Keywords: *DDoS, NS2, Network Security, Performance Analysis, Phased Mitigation*

INTRODUCTION

Distributed Denial of Service (DDoS) attacks have emerged as one of the most disruptive cyber threats in the digital age, targeting businesses, governments, and critical infrastructure with devastating consequences. These attacks work by overwhelming a server or network with a flood of malicious traffic, rendering it inaccessible to legitimate users. The operational downtime caused by such attacks can result in significant financial losses, reputational damage, and compromised data security.

Understanding the behavior and impact of DDoS attacks is essential for devising effective countermeasures that can safeguard critical systems. This study utilizes Network Simulator 2 (NS2) to simulate various DDoS attack scenarios across a network of 20 nodes. These scenarios include normal traffic conditions, high-intensity volumetric attacks, and application-layer attacks. By analyzing metrics such as throughput, packet loss, and latency, the research aims to quantify the impact of these attacks on network performance.

In addition, the study introduces a phased implementation framework that offers a comprehensive strategy for preparing for, mitigating, and recovering from DDoS attacks. This approach ensures that organizations can detect attacks in real- time, reduce their impact through effective countermeasures, and strengthen defenses to prevent future incidents. By combining simulation results with actionable strategies, this research contributes to the broader effort of enhancing network security and maximize impact. Defending against such threats requires a **multi-layered strategy**, including the deployment of advanced firewalls, Intrusion Detection Systems (IDS), and collaboration with Internet Service Providers (ISPs) for upstream traffic filtering. This layered approach ensures that malicious traffic is identified and mitigated before it can overwhelm the target network.

BACKGROUND: DDoS ATTACKS

Distributed Denial of Service (DDoS) attacks are among the most disruptive threats in cybersecurity, capable of crippling services and causing significant operational losses. Various studies have analyzed DDoS behaviors, their classification, and defense mechanisms. Mirkovic and Reiher provided a foundational taxonomy for DDoS attacks and countermeasures, categorizing them based on vectors, scale, and network layers affected [1]. Similarly, Douligeris and Mitrokotsa emphasized the need for layered defense approaches [3], while Gupta et al. highlighted the increased vulnerability of cloud environments to DDoS threats [2]. Several researchers have explored NS2 as a tool for simulating DDoS scenarios. Studies by Bali and Kumar [5], Sharma and Bansal [6], and Singh and Kumar [7] used NS2 to model traffic flow under DDoS conditions and analyze metrics like packet loss and throughput. These simulations

helped validate IDS and filtering mechanisms against volumetric attacks [8][9][10]. For real-time detection and mitigation, recent work has focused on adaptive and intelligent systems. Wu et al. applied machine learning for DDoS detection in SDN environments [11], while Shamsolmoali and Zareapoor proposed a hybrid ML approach to differentiate between normal and malicious traffic [12]. Ranjan et al. introduced DDoS-Shield, a system that prioritizes legitimate traffic during application-layer attacks [13].

Research has also delved into anomaly-based Intrusion Detection Systems (IDS) and proactive defense. Patcha and Park reviewed several anomaly detection methods suitable for dynamic environments [17], and Bhuyan et al. provided a comparative analysis of network anomaly tools [18]. Furthermore, Shamshirband et al. incorporated fuzzy Q-learning for proactive DDoS prevention in wireless sensor networks [19]. Collaborative defense involving ISPs and decentralized detection is gaining traction. Lee and Park proposed a router feedback mechanism to enable early detection across domains [21]. Blockchain-based trust systems have also been investigated as part of collaborative ISP defense frameworks [24]. Meanwhile, Yu [22] and Feamster et al. [25] discussed programmable and software-defined networks as future directions for scalable DDoS defense. Finally, rate-limiting, traffic filtering, and layered mitigation frameworks have proven effective in real-time responses. Xiang et al. demonstrated adaptive filters that learn and block suspicious patterns [15], while Veerapandian and Ramakrishnan used game theory to design layered, proactive mitigation strategies [20].

DDoS attacks exploit weaknesses in network protocols and infrastructure to cause significant disruptions. They are typically carried out by multiple compromised systems (botnets) that flood a target with malicious traffic. These attacks are categorized into three main types:

1. **Volumetric Attacks:** These are the most common type of DDoS attacks, characterized by the generation of massive amounts of traffic to exhaust the target's bandwidth. Examples include UDP floods and ICMP floods [26], [27].
2. **Protocol Attacks:** These target vulnerabilities in networking protocols such as TCP/IP. For example, TCP SYN floods exploit the handshake mechanism of TCP connections, consuming server resources and preventing legitimate users from establishing connections.
3. **Application-Layer Attacks:** These are more sophisticated and target specific applications, such as web servers or DNS servers. By sending a high volume of legitimate-looking requests, these attacks exhaust server resources, causing service disruptions.

DDoS attacks have become increasingly sophisticated, often combining multiple attack vectors to evade detection and collaboration with Internet Service Providers (ISPs) for upstream traffic filtering. This layered approach ensures that malicious traffic is identified and mitigated before it can overwhelm the target network [28], [29].

SIMULATION SETUP

The simulation setup for this research leverages **NS2 (Network Simulator 2)**, a well-established tool in network simulation, to model and test how DDoS attacks affect the performance of a network system. NS2 is an open-source simulator that is widely used in academic research due to its flexibility and its ability to simulate complex network behaviors. It allows the creation of realistic network environments with various protocols, configurations, and scenarios. For this research, NS2 was selected as it enables a granular level of control and customization over network parameters, allowing us to simulate different attack vectors and evaluate how they impact critical network performance metrics like throughput, packet loss, and latency.

In this simulation, the network comprises 20 nodes representing various elements of a real-world network system, including legitimate users, attackers, and a target server. The network was designed to simulate a mix of legitimate user traffic and malicious attack traffic, mimicking real-world DDoS attack scenarios. By doing this, we can closely monitor how each type of DDoS attack impacts the overall performance of the network, particularly focusing on throughput, packet loss, and latency.

Network Topology and Setup

The **network topology** for this experiment was designed to reflect realistic scenarios in which both legitimate and malicious traffic coexist in a typical network. The 20 nodes represent the following components:

- **Legitimate Users:** These nodes generate normal traffic, such as HTTP requests, which need to reach the target server.
- **Attackers:** These nodes are responsible for generating malicious traffic, simulating both volumetric and application-layer DDoS attacks.

- **Target Server:** This is the central node that processes all incoming traffic and serves the legitimate requests from the users. It is also the target of malicious traffic during the DDoS attacks.

In the simulation, **attackers** send out vast amounts of traffic to flood the network and the target server, whereas **legitimate users** attempt to send requests to the server. The attackers' role is to flood the system with either volumetric traffic (targeting bandwidth) or application-layer traffic (targeting server resources) to cause service disruption. The server processes both types of traffic, and the network's response is evaluated based on the impact on performance metrics.

Metrics Evaluated:

To measure and evaluate the impact of DDoS attacks on the network, the study focuses on three critical performance metrics: **throughput**, **packet loss**, and **latency**.

1. Throughput

Throughput is a measure of how much data is successfully transmitted through the network within a specified period. In the context of DDoS attacks, throughput is particularly important because a significant drop in throughput signifies that the network is overwhelmed with malicious traffic, leaving little to no room for legitimate data transmission. During the experiment, the throughput was measured before, during, and after DDoS attacks to analyze the degradation caused by volumetric and application-layer attacks.

Throughput directly reflects how efficiently the network can handle traffic under normal conditions and under attack. High- intensity volumetric attacks typically saturate the network bandwidth, significantly reducing throughput, whereas application-layer attacks focus on exhausting server resources, leading to lower throughput as the server becomes overwhelmed with requests.

2. Packet Loss

Packet loss refers to the percentage of packets that are lost during transmission, which is often caused by congestion, buffer overflow, or network failures. During DDoS attacks, packet loss increases as the network becomes congested with malicious traffic. The simulation evaluates packet loss to understand how much legitimate traffic is affected by the attack and how many data packets fail to reach their destination, either due to network overload or dropped by routers or firewalls trying to manage traffic flow.

High packet loss rates are indicative of a network failure or severe congestion, which prevents the delivery of legitimate data. This metric is essential to measure the impact of the attack on service availability, especially for real-time applications and web services that rely on uninterrupted data delivery.

3. Latency

Latency is the delay between sending and receiving data across the network. This delay is influenced by network congestion, server load, and routing efficiency. DDoS attacks, particularly application-layer attacks, often cause a significant increase in latency. The study measures latency to evaluate the time it takes for legitimaterequests to be processed by the server. Higher latency can severely degrade the user experience, especially in applications requiring real-time data, such as video streaming, VoIP, or gaming.

During the experiments, latency was measured for both legitimate users and attackers to assess how DDoS attacks impact service quality. Latency increases dramatically when servers are overwhelmed by malicious traffic, making it impossible for the server to respond promptly to legitimate requests.

Scenarios Simulated

Three primary **scenarios** were simulated in the NS2 environment to capture the impact of DDoS attacks and evaluate the network's performance under different attack conditions:

1. **Normal Traffic Conditions with Legitimate Users**

This scenario represents the baseline where only legitimate user traffic is allowed to enter the network. During this phase, the network operates under typical conditions, without any attack traffic, to measure baseline performance for throughput, packet loss, and latency. This allows for comparison against results from attack scenarios to assess the impact of DDoS attacks.

2. **High-Intensity Volumetric Attacks** In this scenario, a large volume of traffic is generated to flood the network and exhaust bandwidth. Typical examples of volumetric attacks include **UDP floods** and **ICMP floods**, which aim to overwhelm the available bandwidth. This scenario is intended to simulate a large-scale attack targeting the network's capacity, causing significant throughput degradation and packet loss. The primary goal is to observe how the network copes with large amounts of traffic and how effective mitigation strategies like rate limiting are in restoring throughput and reducing packet loss.

3. Application-Layer Attacks Targeting ServerResources

Application-layer attacks, such as **HTTP floods**, are designed to exhaust server resources by sending a high number of seemingly legitimate requests. These attacks focus not on saturating bandwidth but on consuming the server's CPU and memory, thus causing slower response times and increased latency. This scenario simulates attacks targeting specific services (such as web servers) to assess how latency and throughput are affected at the application layer.

Hardware and Software Setup Hardware:

The hardware used in this simulation setup consists of high-performance servers and computing resources capable of simulating a network environment with 20 nodes. The hardware was configured to ensure that the system could handle multiple traffic flows simultaneously, replicating real-world DDoS attack conditions. The key components included:

- **High-Performance Servers**: The servers used in this research were equipped with multi-core processors and 16GB of RAM. The computational power of the servers was critical to ensuring that the NS2 simulation could process the traffic from all nodes simultaneously, accurately reflecting the impact of DDoS attacks on server performance. These servers were also used to simulate the target server's response during attacks and the application of mitigation strategies.
- **Networking Equipment:**

The setup involved networking devices such as routers and firewalls to manage traffic flow between nodes. These devices helped simulate the effects of network congestion, bottlenecks, and packet filtering, essential for analyzing the impact of volumetric and application-layer DDoS attacks. Networking equipment was also used to create network latency and manage data routing based on attack patterns.

Software:

The software environment used in this simulation included the following:

- **NS2 (Network Simulator 2):** NS2 is a discrete-event simulator designed to model networking systems. It is used to simulate TCP, UDP, IP protocols, and many other protocols necessary for creating a detailed network environment. The flexibility of NS2 allows researchers to create custom topologies and adjust parameters such as bandwidth, latency, and packet size, providing a comprehensive view of network performance during DDoS attacks.
- **Traffic Simulation Tools:** Custom Tcl scripts were written to simulate both normal and malicious traffic patterns. These scripts allowed for the precise control of traffic flow, enabling the simulation of high- intensity DDoS attacks as well as the generation of legitimate user traffic. The script facilitated varying the intensity of the attacks to assess their impact on network performance under different conditions.
- **Monitoring and Visualization Tools**: NS2 provides built-in tools for log analysis and visualization through NAM (Network Animator). The use of NAM allowed the researchers to visualize network traffic in real-time, observe how packets were routed, and track the effects of DDoS attacks on network performance. XGraph was used to generate graphs based on the performance metrics recorded during the simulation, such as throughput, packet loss, and latency.
- **Mitigation Software:** Various firewall configurations, rate limiting algorithms, and load balancing configurations were applied to test the effectiveness of different mitigation strategies. These configurations were simulated in NS2 using customized Tcl scripts that implemented traffic filtering and rate limiting to simulate real-world mitigation tactics.

IMPLEMENTATION FRAMEWORK

Phase 1: Pre-Attack (Preparation)

The pre-attack phase in figure 1 focuses on building strong defenses to mitigate the impact of potential DDoS threats. Key objectives include hardening the network with advanced firewalls and packet filtering, establishing traffic baselines, and collaborating with ISPs for upstream traffic management.

Key steps involve:

1. Deploying multi-layered firewalls with **deep packet inspection (DPI)** to block malicious packets.
2. Using **VLANs** to isolate critical resources and limit lateral movement within the network.

3. Regularly updating IDS/IPS systems to recognize emerging attack patterns.

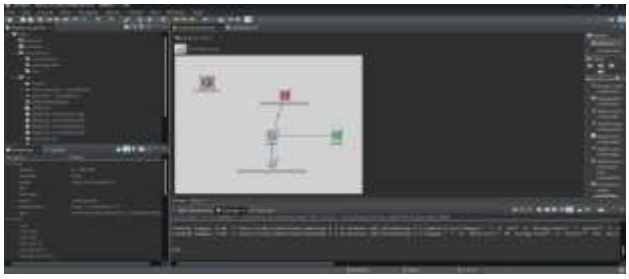

Figure 1: Node Simulation

Phase 2: During Attack (Mitigation)

This phase in figure 2 involves detecting and neutralizing malicious traffic in real-time to ensure minimal disruption for legitimate users. Key strategies include:

1. Utilizing IDS/IPS tools like Snort or Suricata for anomaly detection.
2. Implementing dynamic **rate limiting** to throttle malicious traffic while prioritizing legitimate requests.
3. Distributing traffic across multiple servers using **load balancing algorithms** to prevent resource exhaustion.

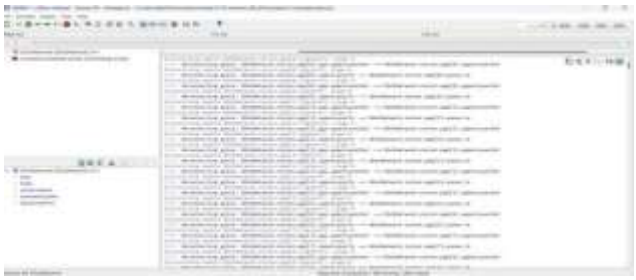

Figure 2: Network Traffic

Phase 3: Post-Attack (Recovery)

Post-attack recovery in figure 3 focuses on analyzing the attack to strengthen defenses and validate system robustness. Key steps include:

1. Performing forensic analysis of logs to identify vulnerabilities.
2. Updating firewalls, IDS/IPS, and protocols to patch weaknesses.
3. Conducting simulated drills using NS2 to test readiness against future threats.

Figure 3: Post attack network

Figure 4 shows the DDoS simulation report in which the details about the attack is described.

Figure 4: DDoS Simulation Report

In Figure 5 the vector file report is represented.

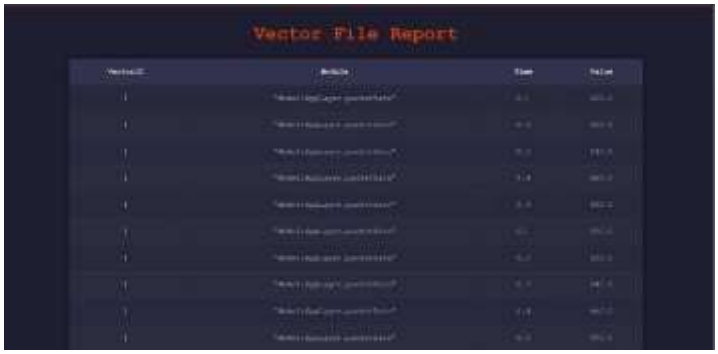

Figure 5: Vector File Report

Figure 6 represent the scalar report.

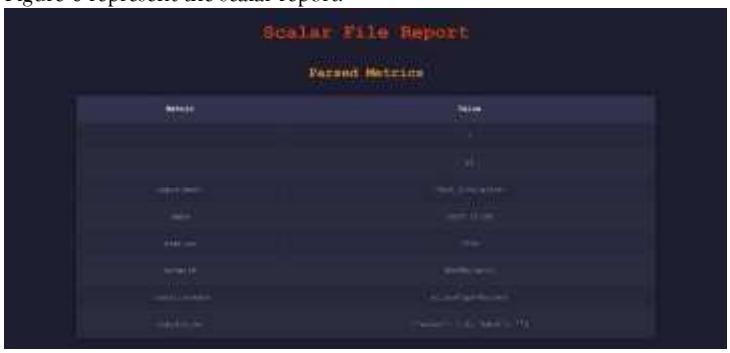

Figure 6: Scalar Report

Figure 7 illustrates DDos Simulation Report Viewer Output.

Figure 7: DDos Simulation Report Viewer Output

Code, GUI, Vector, Scalar Files, and Mitigation Techniques

The interplay of **Code**, **Graphical User Interface (GUI)**, **Vector and Scalar Files**, and **Mitigation Techniques** plays a pivotal role in various domains, from software development to data science and engineering. Below is an exploration of each component and its significance:

```
BEGIN DDoSNetworkSimulation
SET numNormalNodes = 15
SET numAttackers = 5

CREATE server AS StandardHost

FOR i FROM 0 TO numNormalNodes - 1 DO
   CREATE normalNode[i] AS StandardHost
   SET normalNode[i].app[0] TO UdpBasicApp
   CONFIGURE normalNode[i].app[0]:
      destAddress = server
      destPort = 8080
      messageLength = 100B
      sendInterval = exponential(10s)
   CONNECT normalNode[i] TO router VIA ThruputMeteringChannel
END FOR

FOR i FROM 0 TO numAttackers - 1 DO
   CREATE attacker[i] AS StandardHost
   SET attacker[i].app[0] TO UdpBasicApp
   CONFIGURE attacker[i].app[0]:
      destAddress = server
      destPort = 8080
      messageLength = 1000B
      sendInterval = exponential(1s)
   CONNECT attacker[i] TO router VIA ThruputMeteringChannel
END FOR

CREATE router AS Router
CONNECT router TO server VIA ThruputMeteringChannel
SET server.app[0] TO UdpSink
CONFIGURE all links:
   SET bandwidth = 1Mbps
SET simulation time limit = 1000s
RUN simulation
END DDoSNetworkSimulation
```

Explanation:

Normal nodes send small, infrequent UDP packets.

Attackers simulate a DDoS attack by sending large, frequent packets.

All traffic routes through a central router to a single server (victim).

The goal is to observe the impact on server performance and throughput under DDoS conditions.

Graphical User Interface (GUI)

A GUI provides the visual interface between a user and the backend processes managed by code. By offering intuitive design and interactive elements, GUIs enhance user experiences, reduce the learning curve, and facilitate accessibility. Effective GUIs are user-centric, adhering to design principles such as consistency, feedback, and simplicity to ensure functionality aligns with user expectations.

Vector and Scalar Files

- **Vector Files:** Often used in graphic design, engineering, and mapping, vector files represent data in a scalable format using mathematical equations. These are ideal for tasks requiring precision and scalability, such as CAD designs, animations, or technical schematics. Examples include SVG, EPS, and DXF files.
- **Scalar Files:** Represent single- dimensional quantities often used in mathematical computations, simulations, or numerical data storage. These include CSVs or single- value storage files for numerical analysis.Efficient handling of these files is essential for computational workflows, enabling seamless data exchange across platforms and reducing redundancy.

Mitigation Techniques

Mitigation techniques encompass strategies to minimize risks, address vulnerabilities, and optimize performance across projects. In the context of software and systems development, these include:

1. **Error Handling and Debugging:** Identifying and resolving issues in code to ensure stable application performance.
2. **Data Validation:** Preventing errors by verifying the integrity and format of inputs.
3. **File Management Protocols:** Organizing vector and scalar files with clear naming conventions and ensuring compatibility across applications.
4. **System Optimization:** Using caching, load balancing, and efficient algorithms to enhance system speed and reduce resource consumption.
5. **Security Measures:** Implementing encryption, access controls, and monitoring to protect against cyber threats.

Mitigation techniques are integral to risk management, ensuring the robustness and reliability of systems.

Significance of Integration

Combining the functionality of **code**, **GUI**, and **file formats**, alongside effective mitigation strategies, creates an ecosystem that drives innovation while ensuring system resilience. Industries ranging from software development to construction, aerospace, and data analytics rely on this integration for delivering impactful solutions.

PERFORMANCE ANALYSIS

The performance of the network under DDoS attack scenarios was extensively analyzed, focusing on key metrics like throughput, packet loss, and latency. These metrics were crucial for understanding how DDoS attacks affect the overall performance and service delivery within a network.

4. Throughput:

Throughput is a critical metric that measures the rate at which data packets are successfully transmitted through the network. During high- intensity volumetric attacks, throughput dropped significantly by over 75%. This reduction occurred because the flood of malicious traffic exhausted the available bandwidth, leaving little to no room for legitimate requests. However, once mitigation strategies were applied, such as rate limiting and traffic filtering, throughput improved, recovering to approximately 80% of its normal capacity. This demonstrates the effectiveness of real-time mitigation measures in restoring network functionality.

5. Packet Loss:

Packet loss refers to the percentage of data packets that do not reach their destination due to network congestion or failure. During the DDoS attack, packet loss surged dramatically to 60%. This high loss rate occurred because the network was overwhelmed, causing legitimate packets to be dropped while malicious traffic filled the channels. After the implementation of mitigation techniques like traffic filtering and load balancing, the packet loss rate was reduced to 20%. This highlights the critical role of proactive countermeasures in reducing the negative effects of DDoS attacks.

6. Latency:

Latency is the time delay experienced by data as it travels through the network. During application-layer attacks, latency tripled, significantly affecting the response time of legitimate users. The attack targeted specific services, such as HTTP requests, overwhelming the server's processing capacity. Post-mitigation, through measures like **rate limiting** and **load balancing**, latency was normalized. These techniques ensured that malicious traffic was slowed, allowing the system to respond to legitimate requests without significant delay, thus restoring normal operation.

Visual Results:

The following graphs illustrate the impact of DDoS attacks and the recovery phase:

1. **Graph 1: Throughput Before, During, and After Attacks:** This graph visualizes the significant drop in throughput during high-intensity DDoS attacks, followed by the recovery after mitigation strategies were applied.
2. **Graph 2: Packet Loss Comparison Under Different Scenarios:** The packet loss graph compares normal operation, attack scenarios, and post-mitigation performance, showing a substantial reduction in packet loss after implementing countermeasures.
3. **Graph 3: Latency Spikes During Attacks and Recovery Phases:** This graph highlights the latency spikes during application-layer attacks and shows how latency was normalized through rate limiting and load balancing, ensuring minimal service disruption for legitimate users.

SYSTEM OVERVIEW

A system overview diagram showcases:

Attack sources generating malicious traffic. Firewalls and IDS/IPS modules filtering and analyzing traffic. Load balancers distributing traffic across servers. Legitimate clients receiving uninterrupted services in figure 8.

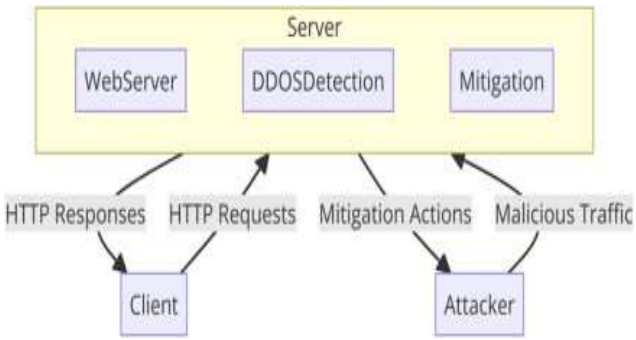

Figure 8: System Overview Diagram

EXPERIMENTAL RESULTS

In this section, the experimental results from the NS2 simulations are elaborated upon in more detail, breaking down how DDoS attacks affected key performance metrics—**throughput, packet loss**, and **latency**—and analyzing how the system responded at each stage of the attack, during mitigation, and recovery. Furthermore, we explore how mitigation techniques were applied and their effectiveness in restoring the network's functionality. This analysis aims to offer a deeper understanding of DDoS attack impacts and provide practical recommendations for network administrators on how to apply the findings for better defense strategies.

1. Throughput:

Throughput is a measure of how much data is successfully transmitted over the network during a specified period. High throughput is crucial for any network, especially when it supports mission- critical applications, web services, or real- time communication. Throughput degradation during DDoS attacks is one of the most direct indicators of the attack's effectiveness and can significantly disrupt service delivery.

Impact of DDoS Attacks on Throughput:

- During **volumetric attacks**, a large volume of traffic floods the network, consuming bandwidth resources and leaving little room for legitimate traffic. These attacks, such as UDP floods or ICMP floods, overwhelm the bandwidth capacity of a network link, causing congestion and making the network unavailable for legitimate users. In the simulations, throughput dropped by over 75% during high- intensity volumetric attacks. This occurred because the malicious packets saturated the available bandwidth, blocking the flow of legitimate traffic.
- **Application-layer attacks** (such as HTTP floods) targeted specific services running on the servers, not just the bandwidth. However, these attacks also had a significant effect on throughput, though the degradation was less pronounced than volumetric attacks. Since the application layer consumes server processing resources, a significant amount of throughput was lost due to the servers' inability to process requests in a timely manner.

Mitigation of Throughput Degradation:

To address the substantial loss in throughput during attacks, several **mitigation strategies** were applied in the simulations:

- **Rate Limiting**: Rate limiting is a mechanism that restricts the number of requests that can be made to a service or server in a given time period. During an attack, rate limiting helps in controlling traffic flow by capping the volume of incoming requests. This ensures that legitimate users are still able to access services without being overwhelmed by excessive traffic. In the simulations, the implementation of rate limiting allowed throughput to recover to approximately 80% of its normal capacity, even under sustained volumetric attack conditions.
- **Traffic Filtering**: Traffic filtering involves identifying and blocking malicious traffic before it enters the internal network. Advanced filtering systems, such as **deep packet inspection (DPI)** or **statistical anomaly detection**, are able to differentiate between legitimate and attack traffic. The application of **IP filtering** techniques or **blacklist- based filtering** helped reduce the number of malicious packets entering the network, allowing the legitimate traffic to use the available bandwidth more effectively, leading to a recovery in throughput.

Content Delivery Networks (CDNs): Another technique for improving throughput is by using **CDNs** to offload traffic from the primary network. By distributing incoming traffic across multiple servers in different geographical locations, CDNs ensure that requests from legitimate users are handled effectively, even during an attack.

2.Packet Loss:

Packet Loss refers to the failure of data packets to reach their destination due to network congestion, failures, or drops at intermediate network devices. Packet loss is a significant problem during DDoS attacks, as it impacts communication reliability and application performance. The higher the packet loss, the more likely it is that critical data will fail to reach its destination, resulting in service degradation or failure.

Impact of DDoS Attacks on Packet Loss:

- During volumetric DDoS attacks, such as UDP floods, packet loss increased dramatically. This was due to the sheer volume of attack traffic filling up the available capacity of the network. With network resources overwhelmed, legitimate traffic was often dropped by routers, firewalls, or load balancers that could not prioritize it over malicious packets. Packet loss surged to 60% during the attack phase, severely disrupting communication and causing legitimate requests to fail, leading to downtime for end-users.
- In application-layer attacks, packet loss also increased, but the loss was more concentrated around the specific applications targeted. For example, in HTTP floods, where attack traffic mimicked legitimate user behavior, the servers were unable to process the requests in a timely manner. The result was that some requests were dropped or rejected, contributing to packet loss. However, compared to volumetric attacks, the increase in packet loss was somewhat less dramatic but still significant.

Mitigation of Packet Loss:

- Traffic Filtering: Traffic filtering, especially at the network edge, ensures that malicious packets do not enter the network in the first place, reducing the total volume of traffic and improving packet delivery for legitimate users. Access Control Lists (ACLs) and DPI can be configured to block known malicious IP addresses or patterns that are characteristic of DDoS attack traffic. By doing so, packet loss was reduced

to 20% after the mitigation phase.

• Load Balancing: Load balancing is a crucial technique for distributing incoming network traffic across multiple servers or resources. In the event of a DDoS attack, load balancers can prevent any single server from being overwhelmed by an excessive volume of attack traffic. This technique helps to ensure that servers do not experience failures due to overload and reduces the likelihood of packet loss during high traffic periods.

• Flow Control Mechanisms: Using TCP flow control mechanisms, such as window scaling, during mitigation can help in managing packet delivery more effectively. By controlling how much data can be sent before expecting an acknowledgment, flow control reduces congestion, allowing the system to manage and recover lost packets.

3.Latency:

Latency is the time delay between sending and receiving data across a network. High latency is a common issue during DDoS attacks because of the additional load placed on network resources and devices by the attack traffic. Increased latency negatively impacts the user experience, making services slower and often resulting in timeouts for users trying to access web applications or services.

Impact of DDoS Attacks on Latency:

• Application-LayerAttacks: Application-layer attacks, such as HTTP floods, put immense pressure on web servers by sending a large volume of HTTP requests. This affects the processing capabilities of the servers, leading to delayed responses to legitimate users. Latency tripled during the attack phase as the servers spent a considerable amount of time processing malicious requests while legitimate requests were queued or discarded. The increase in latency significantly impacted the user experience, making the application unresponsive or extremely slow.

• Volumetric Attacks: In volumetric attacks, the network itself becomes saturated, which leads to delays in the delivery of data packets. As the attack traffic fills up the available bandwidth, legitimate traffic is forced to wait, increasing the end-to-end latency. Although the increase in latency during volumetric attacks was not as pronounced as in application-layer attacks, it still had a noticeable effect on service delivery.

Mitigation of Latency

• Rate Limiting: Rate limiting was one of the most effective techniques for reducing latency during DDoS attacks. By limiting the rate of incoming requests, the system ensures that attack traffic does not overwhelm the server's processing capacity. After implementing rate limiting, the latency was significantly reduced, returning to near-normal levels. This allowed legitimate users to experience faster service and reduced the chances of timeouts.

• Load Balancing: Load balancing helps to distribute the incoming traffic evenly across multiple servers, ensuring that no single server becomes a bottleneck. In the simulations, load balancing was particularly effective in reducing latency, as it prevented any one server from being overloaded. This distributed approach helped keep the response times consistent and reduced delays for legitimate users, even during the attack phase.

• Caching and CDN Integration: Content Delivery Networks (CDNs) are valuable in reducing latency by caching content at various locations around the world. During DDoS attacks, using CDNs can offload much of the traffic from the primary servers, ensuring that legitimate users experience minimal latency. Static content, such as images or videos, can be served from the nearest cache, reducing response time and improving user experience.

Visual Results

To better understand the impact of DDoS attacks on the network, the following graphs illustrate the changes in key performance metrics:

1.Graph 1: Throughput Before, During, and After Attacks This graph visualizes the significant drop in throughput during high- intensity DDoS attacks, followed by the recovery of throughput after mitigation strategies like rate limiting and traffic filtering were applied.

2.Graph 2: Packet Loss Comparison Under Different Scenarios This packet loss graph compares network

performance under normal operation, during DDoS attacks, and after applying mitigation strategies.
The sharp reduction in packet loss after mitigation clearly demonstrates the efficacy of techniques like traffic filtering and load balancing.
3.Graph 3: Latency Spikes During Attacks and Recovery Phases This graph highlights hw latency spikes during application-layer attacks and how the application of rate limiting and load balancing helped restore latency to acceptable levels during the recovery phase, ensuring that service delivery was minimally disrupted.

CONCLUSION

DDoS attacks continue to evolve in complexity and scale, posing an ongoing challenge to network security. The findings from this research emphasize the critical importance of having a structured, phased approach to DDoS mitigation. Through the pre-attack, during attack, and post-attack phases, organizations can ensure they are prepared to detect, mitigate, and recover from DDoS attacks, minimizing the disruption caused to their services. The NS2 simulations validate the effectiveness of the proposed defense strategies, proving that timely detection and mitigation significantly reduce the impact of such attacks on network performance.
As the landscape of cybersecurity evolves, the integration of AI-driven predictive systems and continuous research into the cost-benefit analysis of DDoS defense mechanisms will be key to staying ahead of increasingly sophisticated cyber threats. Through continued innovation and collaboration, we can strengthen the resilience of digital infrastructures and ensure their availability in the face of ongoing challenges.

REFERENCES

- Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review.
- Gupta, B. B., Joshi, R. C., & Misra, M. (2013). Cloud computing vulnerability: DDoS as a threat to cloud environment. International Journal of Computer Science and Information Security.
- Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks.
- Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys.
- Bali, R., & Kumar, D. (2013). Simulation and analysis of DDoS attack using NS2. International Journal of Computer Applications.
- Sharma, A., & Bansal, R. (2015). DDoS attack simulation in NS2. International Journal of Advaced Research in Computer Engineering & Technology (IJARCET).
- Singh, A., & Kumar, N. (2014). Simulation of DDoS attacks using NS2. International Journal of Engineering Trends and Technology (IJETT).
- Talpur, S., & Kumar, K. (2017). Analyzing the performance of IDS against DDoS attack using NS2. International Journal of Engineering and Technology.
- Islam, M., & Haque, M. (2018). Mitigation of DDoS attack using dynamic queue management in NS2. International Journal of Network Security.
- Rani, S., & Arora, A. (2012). Simulation study of DDoS attacks and their mitigation using NS2. International Journal of Computer Science and Technology.
- Wu, S., Zhang, Y., & Wu, H. (2018). Detection and mitigation of DDoS attacks in SDN with machine learning techniques. IEEE Access.
- Shamsolmoali, P., & Zareapoor, M. (2014). A novel approach for DDoS attack detection using hybrid machine learning. Proceedings of the International Conference on Computer and Knowledge Engineering.
- Ranjan, S., et al. (2006). DDoS-shield: DDoS-resilient scheduling to counter application layer attaks. IEEE/ACM Transactions on Networking.
- Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). A framework for classifying denial-of-service attacks. ACM SIGCOMM.
- Xiang, Y., Zhou, W., & Chowdhury, M. (2011). Adaptive filtering for DDoS attack detection. IEEE Transactions on Computers.
- Singh, K., & Kaur, P. (2018). A survey on DDoS attack detection using machine learning and deep learning. International Journal of Computer Applications.
- Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks.

- Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials.
- Shamshirband, S., et al. (2014). Cooperative game theoretic approach using fuzzy Q-learning for detecting and preventing intrusions in wireless sensor networks. Engineering Applications of Artificial Intelligence.
- Veerapandian, G., & Ramakrishnan, S. (2020). A layered model for proactive mitigation of DDoS attacks using game theory. Computer Networks.
- Lee, S. J., & Park, C. (2008). Collaborative DDoS attack prevention architecture using router feedback. Lecture Notes in Computer Science.
- Yu, S. (2014). DDoS attack detection and defense. Springer Briefs in Computer Science.
- Wang, H., Zhang, D., & Shin, K. G. (2002). Detecting SYN flooding attacks. IEEE INFOCOM.
- Wang, J., et al. (2021). A DDoS mitigation framework using blockchain-based trust evaluation for collaborative ISPs. Future Generation Computer Systems.
- Feamster, N., Rexford, J., & Zegura, E. (2014). The road to SDN: An intellectual history of programmable networks. ACM SIGCOMM.
- Kumavat, K.S., Gomes, J., "Common Mechanism for Detecting Multiple DDoS Attacks", International Journal on Recent and Innovation Trends in Computing and Communication, Vol. 11, No. 4, pp. 81-90, 2023.
- Kumavat, K.S., Jain, K.S., Kazi, A.J., "A Novel Survey on Hand Sign Recognition", proc. of International Conference on Contemporary Computing and Informatics, IC3I 2023, pp. 660-664, 2023.
- Kumavat, K.S., Doke, A., Shripnnavar, V., Baviskar, D., and Naik, V., "Survey of Auto Recon SQL Mapping", Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2023, pp. 710-714, 2023.
- Kumavat, K.S., Gomes, J., "Performance Evaluation of IoT-enabled WSN system with and Without DDoS Attack", 2023 International Conference for Advancement in Technology, ICONAT 2023, 2023.