Overview of Distributed Denial of Service (DDoS) attack types and mitigation methods

Merkebaiuly Medet¹

¹ 2nd-year master student of the specialty «Business Analysis»; International University of Information Technology (IITU); Republic of Kazakhstan

Abstract.
In the evolving landscape of cyber threats, Distributed Denial of Service (DDoS) attacks pose a significant challenge to internet security. This research provides a comprehensive overview of various DDoS attack types and explores the efficacy of current mitigation strategies and categorizes DDoS attacks based on their methods and targets, highlighting their unique characteristics and impacts. The study delves into a range of mitigation methods, from traditional network-based approaches to recent advancements in artificial intelligence, assessing their strengths and limitations. Key findings indicate a dynamic interplay between the evolving complexity of DDoS attacks and the advancement of mitigation techniques. The research identifies gaps in current strategies and suggests areas for further development, emphasizing the need for adaptive, multi-layered defense mechanisms. This scientific article aims to provide cybersecurity professionals with a nuanced understanding of DDoS threats and a critical evaluation of the mitigation methods, guiding effective strategies to combat these evolving cyber risks.

Keywords: cyber threats, distributed denial of service (DDoS) attacks, mitigation techniques, multi-layered defense mechanisms
Introduction. In the digital era, the security of online systems is paramount, with Distributed Denial of Service (DDoS) attacks emerging as a formidable threat to internet stability and security. These attacks, designed to overwhelm a network or system to the point of inoperability, have evolved in complexity and scale, posing a continuous challenge to organizations worldwide. The significance of DDoS attacks is not only in their frequency but also in their capacity to disrupt essential online services and cause substantial economic and reputational damage.

The purpose of this research is to provide a thorough overview of DDoS attack types, elucidating their mechanisms, targets, and impacts. This study is driven by two primary research questions: What are the various types of DDoS attacks currently prevalent in the cyber landscape? And, how effective are existing mitigation methods in combating these attacks? By addressing these questions, this research aims to deepen the understanding of DDoS threats and offer insights into the most effective strategies for their mitigation.

Furthermore, this article explores the evolution of DDoS attacks, tracing their progression from simple nuisances to sophisticated tools used in cyber warfare and cybercrime. It also critically analyzes the current landscape of DDoS mitigation techniques, ranging from basic defensive measures to advanced solutions employing cutting-edge technologies. This comprehensive approach is crucial in a field where the adversary is constantly adapting and evolving.

Given the increasing reliance on digital infrastructure and the Internet of Things (IoT), understanding and mitigating DDoS attacks is more relevant than ever. This study contributes to the body of knowledge by providing a detailed overview of DDoS attack types and assessing the effectiveness of various mitigation methods. It also identifies gaps in current research and practice, suggesting directions for future work in this critical area of cybersecurity.

Difference between DoS and DDoS attacks. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are prevalent forms of cyber aggression that aim to disrupt the normal operations of targeted online services. These attacks overload systems, servers, or networks with more requests
than they can handle, rendering them unresponsive to legitimate traffic. Understanding the nature and impact of these attacks is crucial in the current cybersecurity landscape.

DoS attacks:

DoS attack originates from a single source, directing a flood of traffic or requests to a targeted network or service. The primary aim is to exhaust the resources of the target, leading to service degradation or complete shutdown. Example of popular DoS attack methods:

- **TCP SYN Flood**: exploiting the TCP handshake process to consume server resources.
- **Ping of Death**: sending malformed or oversized packets to crash the target system.
- **TCP Fragmentation / Teardrop attack**: sending fragmented packets that are impossible for the target to reassemble.

DoS attacks, while disruptive, are limited by the resources of the attacker’s system and are generally easier to trace and mitigate due to their singular source [1].
DDoS attacks:

DDoS attacks are a more complex and potent form of DoS attacks. They utilize multiple compromised systems, often forming a botnet, to launch a coordinated attack against a target. The distributed nature of these attacks significantly increases their scale and impact. Common DDoS attack methods include:

- **Volume-based attacks**: flooding the target with excessive traffic to saturate bandwidth.
- **Protocol attacks**: exploiting server resources or intermediate communication equipment.
- **Application Layer attacks**: targeting specific aspects of an application or service to disrupt its functionality.

DDoS attacks are harder to defend against due to their multiple sources and the large volume of attack traffic. They often require sophisticated mitigation strategies involving multi-layered filtering systems, network resilience enhancements, and cooperation with ISPs.

Both DoS and DDoS attacks can have significant impacts on businesses and organizations. Consequences include service disruption, financial losses, erosion of customer trust, and damage to brand reputation. The motivations behind these attacks vary, ranging from individual grievances, financial gain (such as in ransom demands), to political activism and state-sponsored cyber warfare [2].

**Types of DDoS attacks by OSI model layers.** DDoS attacks are categorized based on their methods and the layers of the Open Systems Interconnection (OSI) model they target. The primary types of DDoS attacks are Volume-based attacks, Protocol attacks, and Application Layer attacks.

Understanding the OSI model layers:

The OSI model is a conceptual framework used to understand network interactions in seven layers:

- **Layer 1 (Physical Layer)**: deals with the physical connection between devices.
- **Layer 2 (Data Link Layer)**: manages the node-to-node data transfer.
- **Layer 3 (Network Layer)**: handles the routing of data across networks.
- **Layer 4 (Transport Layer)**: manages end-to-end
communication and is responsible for data transfer management.

- **Layer 5 (Session Layer):** controls the connections and sessions between computers.
- **Layer 6 (Presentation Layer):** translates data between the network and application layers.
- **Layer 7 (Application Layer):** interfaces with the application software and is responsible for high-level APIs.

Each type of DDoS attack targets specific layers, exploiting their unique vulnerabilities to disrupt services. Understanding these layers and the nature of attacks that target them is crucial for developing effective mitigation strategies [3].

1. **Volume-based attacks** (Bits per Second - Bps / Gigabits per Second - Gbps):
   - **Description:** Volume-based attacks are the most common...
form of DDoS attacks. They aim to saturate the bandwidth of the target, rendering the service inaccessible. These attacks flood the target with a massive amount of data, often measured in Bits per Second (Bps) or Gigabits per Second (Gbps).

- **OSI model layer:** these attacks primarily target Layer 3 (Network Layer) and Layer 4 (Transport Layer). By overwhelming these layers, the attacker prevents regular network traffic from reaching its destination.

  - **Examples:** common examples include UDP Flood, ICMP (Ping) Flood, and TCP SYN Flood attacks [4].

2. **Protocol attacks (Packets per Second – Pps):**

   - **Description:** Protocol attacks exploit vulnerabilities in the protocol stack to consume server resources or disrupt essential services. These attacks send a large number of packets per second (Pps), targeting specific protocol vulnerabilities.

   - **OSI model layer:** Protocol attacks usually target Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI model. They focus on exploiting weaknesses in the protocol handshake process or session establishment.

   - **Examples:** attacks like TCP SYN Flood, Ping of Death, and Smurf attack fall under this category. TCP SYN Flood, for instance, exploits the TCP handshake mechanism, creating a large number of incomplete connection requests [5].

3. **Application Layer attacks (Requests per Second – Rps):**

   - **Description:** Application Layer attacks, also known as Layer 7 attacks, target the top layer of the OSI model. They aim to exhaust the resources of a specific application or service rather than the underlying infrastructure. These attacks are often harder to detect as they mimic legitimate requests and traffic.

   - **OSI model layer:** these attacks target Layer 7 (Application Layer) of the OSI model, directly affecting the web application services.

   - **Examples:** HTTP Flood and Slowloris are notable examples. HTTP Flood involves sending high volumes of HTTP requests, while Slowloris holds connections open by sending partial requests or headers [6].

**DDoS mitigation methods for Volume-based attacks.** Volume-based attacks aim to saturate the bandwidth of the target
network or service, making it inaccessible to legitimate users. These attacks can reach magnitudes that overwhelm even well-provisioned networks. Effective mitigation requires a combination of preparation, automated defense mechanisms, and real-time response strategies.

Volume-based attacks aim to saturate the bandwidth of the target network or service, making it inaccessible to legitimate users. These attacks can reach magnitudes that overwhelm even well-provisioned networks. Effective mitigation requires a combination of preparation, automated defense mechanisms, and real-time response strategies.

**Increased bandwidth**: one foundational strategy is to ensure that the network infrastructure has significantly more bandwidth than typically required for daily operations. While this does not stop an attack, it provides a buffer that can absorb or dilute the volume of malicious traffic, buying time for more specific mitigation efforts to be deployed.

**Rate limiting**: it controls the number of requests a server can accept over a given period. By setting a threshold for acceptable request volumes, any traffic exceeding this limit can be automatically dropped or temporarily queued, preventing the server from being overwhelmed. Rate limiting is particularly effective for protecting specific endpoints that are known targets for DDoS attacks.

**Traffic shaping**: similar to rate limiting, involves controlling the flow of network traffic to prioritize certain
types of data. This can help ensure that critical operations continue to function during an attack by deprioritizing traffic that is likely to be malicious based on its source, type, or behavior.

Anomaly detection systems: implementing anomaly detection systems enables the identification of unusual traffic patterns that deviate from the norm. These systems use historical data to understand baseline traffic patterns, making it possible to automatically detect and flag sudden spikes in traffic volume that could indicate a DDoS attack [7].

Blackholing and sinkholing: blackholing routes all traffic to a null route or a “black hole”, effectively dropping the traffic before it can reach the target server. While this method can stop an attack, it also blocks legitimate traffic. Sinkholing is a more sophisticated approach where malicious traffic is redirected to a specific IP address (the “sinkhole”) where it can be analyzed or discarded without affecting the target server.

Cloud-based DDoS protection services: these can absorb large volumes of traffic and filter out malicious requests before they reach the target network. These services operate by rerouting all traffic through their infrastructure, where it is scrubbed for malicious packets. Given their large-scale infrastructure, these services can handle attacks of a size that would overwhelm most private networks [8].

Geographic filtering: it blocks or limits traffic coming from regions that are not relevant to your business operations. If an attack is identified as originating predominantly from countries where you have no market, blocking that traffic can mitigate the attack without impacting your legitimate user base.

Collaboration with ISP: early detection and mitigation of volume-based attacks often require collaboration with your Internet Service Provider (ISP). ISPs can implement upstream filtering that prevents malicious traffic from ever reaching your network. This approach is most effective when the attack traffic is voluminous and distributed.

Mitigating Volume-based DDoS attacks requires a multi-faceted strategy that incorporates both preemptive measures
and real-time response mechanisms. By combining increased bandwidth, advanced filtering techniques, anomaly detection, and the scalability of cloud-based services, organizations can enhance their resilience against these disruptive cyber threats. A proactive stance, coupled with ongoing analysis and adaptation to emerging attack patterns, is essential for maintaining the integrity and availability of online services in the face of volume-based attacks [9].

**DDoS mitigation methods for Protocol attacks.** Protocol attacks exploit weaknesses in the network and transport layer protocols (Layers 3 and 4 of the OSI model) to deplete server resources, such as the connection tables in firewalls and load balancers. These attacks include TCP SYN Floods, ICMP Floods, and Fragmented Packet attacks, which are not necessarily volumetric but can cripple a network’s infrastructure by consuming server or network equipment processing capacity. Mitigating these types of attacks requires strategies that can identify and neutralize malicious protocol activities without disrupting legitimate traffic.

![Protocol attacks](image)

**Figure 4**  
Protocol attacks

**Advanced firewall configuration:** modern firewalls can be configured with advanced rules to detect and filter out suspicious protocol activities. This includes setting thresholds for SYN packets, ICMP requests, and other protocol-based messages. Firewalls with deep packet inspection (DPI) capabilities can analyze the content of network packets for malicious intent and block them accordingly.
Intrusion Prevention Systems (IPS): these are critical in identifying and mitigating protocol attacks. They actively monitor network and system activities for malicious actions. Configured properly, an IPS can detect unusual protocol patterns and block the offending traffic in real-time. This proactive approach is vital for maintaining network integrity against protocol attacks [10].

Rate limiting: applying rate limiting on a more granular level than used for volume-based attacks can effectively mitigate protocol attacks. Limiting the rate of new connections or specific types of protocol requests per second from a single source can help prevent attackers from overwhelming the system with fake connection attempts or protocol-specific attacks.

TCP/UDP session validation: ensuring that every TCP or UDP session is valid can mitigate many protocol attacks. Techniques like SYN cookies can validate TCP sessions without allocating excessive server resources. For UDP-based protocols, requiring a handshake or similar validation before responding to requests can reduce the effectiveness of UDP flood attacks.

Geographical IP blocking: if an attack is identified as originating from specific geographic locations that are not relevant to your operational needs, implementing IP blocklists can prevent these potentially malicious packets from reaching your network. This method can be particularly effective for targeted protocol attacks that originate from known bad actors or regions [11].

Stateful inspection: implemented in next-generation firewalls and other network security appliances, tracks the state of active connections and can distinguish between legitimate and malicious traffic patterns. This method helps in identifying and blocking protocol attack packets that do not match the expected state of a normal connection.

Challenge-response authentication: implementing challenge-response authentication mechanisms can differentiate between legitimate users and automated attack bots. For example, requiring a valid response to a TCP or HTTP challenge before allowing connections can effectively reduce the impact of SYN floods and other protocol abuses.

Collaboration with ISPs: working closely with your Internet Service Provider (ISP) can provide an additional
layer of defense against protocol attacks. ISPs can implement traffic filtering to block malicious packets upstream, reducing the load on your own mitigation infrastructure.

Regular protocol security audits: conducting regular audits of protocol configurations and security settings across network devices ensures that vulnerabilities are identified and addressed promptly. This proactive approach can prevent attackers from exploiting outdated or misconfigured protocols.

Mitigating Protocol attacks requires a comprehensive strategy that includes both hardware and software solutions, as well as a close collaboration with service providers. By employing a mix of advanced firewall rules, intrusion prevention systems, rate limiting, session validation, and stateful inspection, organizations can protect their networks from the disruptive effects of protocol attacks. Regular security audits and updates are also crucial to adapt to evolving threat landscapes and protect against new vulnerabilities [12].

DDoS mitigation methods for Application Layer attacks. Application Layer attacks, targeting Layer 7 of the OSI model, are designed to exhaust the resources of web applications by exploiting weaknesses in the application layer. These attacks are often more sophisticated and harder to detect than volume-based or protocol attacks because they mimic legitimate user behavior. Mitigation strategies must be carefully implemented to differentiate between genuine traffic and malicious requests without affecting the user experience.
Web Application Firewalls (WAF): web application firewall is essential in protecting against application layer attacks. It operates by filtering and monitoring HTTP requests to a web application and can block attacks that exploit web application vulnerabilities. WAFs can be configured with custom rules to provide protection against specific attack vectors, such as SQL injection, cross-site scripting (XSS), and various forms of HTTP Floods [13].

Content Delivery Networks (CDN): they can mitigate application layer attacks by distributing traffic across multiple servers, thereby diluting the impact of an attack aimed at a single point. CDNs can also absorb large volumes of traffic and serve cached content to users, significantly reducing the load on the origin server. Moreover, many CDNs offer built-in security features designed to identify and mitigate DDoS attacks before they reach the application layer [14].

Rate limiting: implementing rate limiting at the application level can prevent a single user or IP address from making too many requests in a short period. This is effective against certain types of application layer attacks, such as brute force or credential stuffing attacks. Rate limiting can be applied more granularly to protect specific endpoints or functions that are more likely to be targeted.

Behavioral analysis: these tools monitor the behavior of users and can detect anomalies that indicate a potential attack. By establishing a baseline of normal user behavior, these tools can identify malicious patterns, such as rapid page requests or abnormal data submission rates, indicative of automated bots or scripts used in application layer attacks.

Bot management solutions: these distinguish between good bots (such as search engine crawlers) and bad bots (which may be performing scraping, fraud, or DDoS attacks). These solutions use challenge tests, behavioral analysis, and device fingerprinting to identify and block malicious bot traffic [15].

Multi-factor Authentication (MFA): for attacks aimed at exploiting login mechanisms or forms, multi-factor authentication can significantly increase security. By requiring additional verification beyond just a password, MFA
can thwart attackers attempting to use stolen credentials or brute force methods to gain unauthorized access.

*Advanced threat intelligence:* these platforms can provide real-time data on current threat actors and their methodologies. Integrating this intelligence with your security infrastructure can help preemptively block known malicious IP addresses and user agents associated with application layer attacks.

*Security patches and software updates:* regularly updating and patching web applications and their underlying platforms is fundamental to protecting against application layer attacks. Many attacks exploit known vulnerabilities that have already been patched by vendors, so keeping software up to date can close these avenues of attack [16].

**Conclusion.** This article has navigated through the intricate landscape of DDoS attacks, offering a comprehensive overview from their foundational concepts to sophisticated mitigation strategies. Beginning with the distinction between DoS and DDoS attacks, we've outlined how these threats differ not only in their execution but also in their impact and complexity. The exploration of DDoS attacks through the lens of the OSI model layers further delineated the varied forms these attacks can take, emphasizing their adaptability and the breadth of their potential targets.

The subsequent sections provided a deep dive into the mitigation methods tailored to the primary types of DDoS attacks: Volume-based, Protocol, and Application Layer attacks. Each segment underscored the necessity of a multi-layered defense strategy, incorporating both preventative measures and real-time response mechanisms. From increasing bandwidth and employing advanced firewall configurations to deploying Web Application Firewalls (WAFs) and leveraging Content Delivery Networks (CDNs), the article highlighted a spectrum of tools and techniques vital for safeguarding against the disruptive capabilities of DDoS attacks.

In conclusion, the fight against DDoS attacks is multifaceted and ever-evolving. As cyber attackers grow more ingenious, the importance of adopting comprehensive, adaptive defense strategies becomes paramount. This entails not only the deployment of technological solutions but also a commitment to continuous learning, collaboration, and
innovation within the cybersecurity community. The resilience against DDoS attacks hinges on our collective efforts to anticipate, understand, and counteract these cyber threats, safeguarding the integrity and availability of online services in an increasingly interconnected world.

References:


INFORMATION AND WEB TECHNOLOGIES

