ITM.J. Ad. Comp. Intell. System.2026, 1(1)

ITM Journal of Advanced
COMPUTING & INTELLIGENT SYSTEM

# Distributed Denial-of-Service (DDoS) Attacks: A Comprehensive Review of Threats, Detection, and Mitigation Strategies

Hirendra Singh Senger[1*], Prem Wadhwani[2]

ITM University Gwalior

Article

**ABSTRACT**

DDoS attacks create severe threats to network security because these attacks overload networks with excessive traffic which causes system and service access to stop. The widespread adoption of online services and Internet of Things (IoT) devices has made DDoS attacks more advanced while lessening their detect ability. The paper provides an all-encompassing examination of DDoS attacks which includes their various types and their attack methods and their operational tools and their effects on contemporary network systems. The study examines current methods for detecting and mitigating threats which include intrusion detection systems and machine learning techniques and traffic filtering systems. The study demonstrates that organizations require adaptable security solutions which combine multiple defense layers to protect against developing DDoS attack methods.

*Keywords: DDoS_1, Network Security_2, Botnet_3, Cyber Attacks_4, Intrusion Detection_5, Traffic Analysis_6*

## INTRODUCTION

Network resource availability has gained critical importance because of the internet and cloud-based service expansion. Distributed Denial-of-Service (DDoS) attacks aim to disrupt services by flooding target systems with massive volumes of traffic [1], [2]. DDoS attacks differ from standard Denial-of-Service (DoS) attacks because they use multiple hacked computers which create a botnet for their execution so that attackers can launch stronger assaults which become difficult to defend against [3]. The attacks target servers and applications and network infrastructure, which causes service interruptions and financial damages to businesses [4]. The growing number of IoT devices has multiplied both the number of DDoS attacks and their severity, which creates higher security risks for network systems [5]. The paper conducts a comprehensive examination of DDoS threats, detection methods, and defense solutions.

## REVIEW OF LITERATURE

*Corresponding Author: Hirendra Singh Senger, Assistant Professor, ITM University Gwalior
Tel: 9301163117
Email: hirendra.cse@itmuniversity.ac.in

The initial research on DDoS attacks studied network-layer attacks which used SYN flooding and UDP flooding methods to take advantage of protocol weaknesses [6]. The attackers have adopted more advanced techniques as time has passed. The latest research shows that application-layer DDoS attacks use methods which simulate real user activities, which makes detection of these attacks challenging [7]. Researchers have investigated botnet-based attacks which use IoT devices because these attacks create widespread damage to critical infrastructure [5].The detection of DDoS attacks has become more effective through the use of machine learning and artificial intelligence which identify unusual traffic patterns [9]. The researchers suggest using software-defined networking (SDN) together with cloud-based defense systems as an effective solution to enhance detection and response capabilities [10]. The progress in DDoS mitigation techniques is hindered by three main problems which include system scalability issues, detection of false security alerts, and the continuous development of new attack methods [11].

## PROPOSED METHODOLOGY

The research paper uses a systematic review-based methodology to assess both DDoS attacks and the strategies used to defend against them.

### A. Data Collection

Academic databases were used to obtain research articles and conference papers and technical reports which studied DDoS attacks and network security [12].

### B. Selection Criteria

The selected studies were based on:

- Relevance to DDoS attacks

- Coverage of detection and mitigation techniques
- Credibility of sources
- Recent advancements in cybersecurity [13]

**C. Analysis Parameters**

The study evaluates DDoS attacks based on:

- Attack type and mechanism
- Traffic characteristics
- Digital security detection methods
- Defensive techniques against attacks [14]

**D. Classification Approach**

DDoS attacks are categorized into three groups which include volumetric attacks and protocol-based attacks and application-layer attacks for purposes of organized examination [15].

**Pseudo code for proposed method**

```
BEGIN

STEP 1: Initialize Research Process

STEP 2: Collect Data
  Access academic databases
  Retrieve:
    - Research articles
    - Conference papers
    - Technical reports
  Store collected studies related to DDoS attacks and network security

STEP 3: Apply Selection Criteria
  FOR each collected study DO
    IF study is relevant to DDoS attacks AND
      study covers detection and mitigation techniques AND
      source is credible AND
      study includes recent cybersecurity advancements
    THEN
      Select study
    ELSE
      Reject study
    ENDIF
  ENDFOR

STEP 4: Analyze Selected Studies
  FOR each selected study DO
    Evaluate:
      - Attack type and mechanism
      - Traffic characteristics
      - Detection methods
      - Defensive techniques
  ENDFOR

STEP 5: Classify DDoS Attacks
  Categorize attacks into:
    a) Volumetric Attacks
    b) Protocol-Based Attacks
    c) Application-Layer Attacks

STEP 6: Identify Types of Volumetric Attacks
  Include:
    - UDP Flood
    - ICMP Flood
  Analyze bandwidth exhaustion behavior

STEP 7: Identify Types of Protocol-Based Attacks
  Include:
    - SYN Flood
    - Ping of Death
  Analyze protocol vulnerability exploitation

STEP 8: Identify Types of Application-Layer Attacks
  Include:
    - HTTP Flood
    - Slowloris
  Analyze application/service targeting behavior

STEP 9: Summarize Findings
  Compare attack mechanisms
  Evaluate detection techniques
  Evaluate mitigation strategies

STEP 10: Generate Conclusion
  Highlight effective defense mechanisms
  Discuss recent cybersecurity advancements

END
```

## RESULTS AND DISCUSSION

A. Kinds of DDoS Attacks

1. Volume attack

- UDP Flood
- ICMP Flood

These attacks try to block the network bandwidth by using high volumes of data.

2. Protocol-Based Attacks

- SYN Flood
- Ping of Death

The attacks use network protocol flaws to launch their attacks.

3. Application-Layer Attacks

- HTTP Flood
- Slowloris

The attacks focus on particular applications and services.

| Attack Type | Examples | Target | Impact | Mitigation |
|---|---|---|---|---|
| Volumetric | UDP Flood | Bandwidth | Congestion | Rate limiting |
| Protocol | SYN Flood | Server resources | Crash | Firewalls |
| Application | HTTP Flood | Web servers | Service disruption | IDS/IPS |

**Table 1.** Classification of DDos Attach

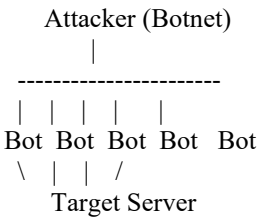


**Figure 1**. DDos Attach Model

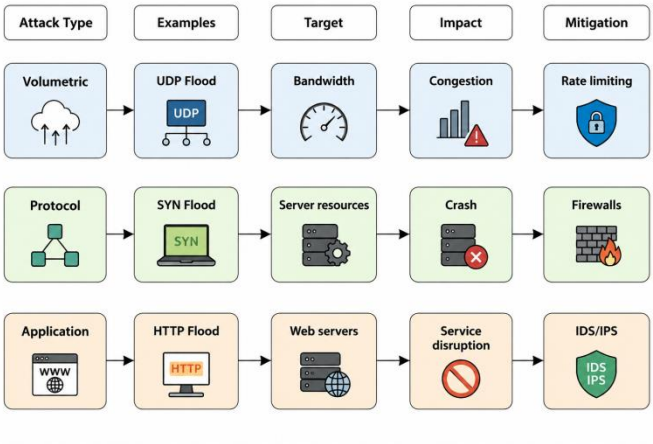


**Figure 2**: Classification of DDoS Attacks, Their Targets, Impacts, and Mitigation Techniques

B. The impacts of DDoS attacks create multiple negative outcomes which include service unavailability, financial losses, reputation damage, and decreased system trustworthiness.
C. The available detection and mitigation techniques include Intrusion Detection Systems (IDS) [9] Firewalls and traffic filtering [6] Machine learning-based detection [9] and Cloud-based DDoS protection systems [10]
D. The analysis reveals that DDoS attacks are increasing in scale and sophistication which IoT-based botnets multiply attack strength and no single solution can stop all potential attacks. The main obstacles to solving this problem arise from two factors which create high false positive rates and make it hard to identify real user activity and attackers develop new methods for their attacks [11].

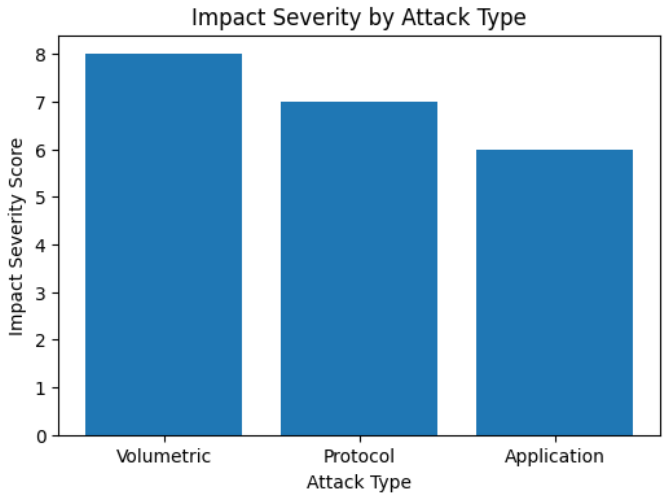


**Figure 3.** Comparative impact severity of different DDoS attack types on network and server infrastructure.

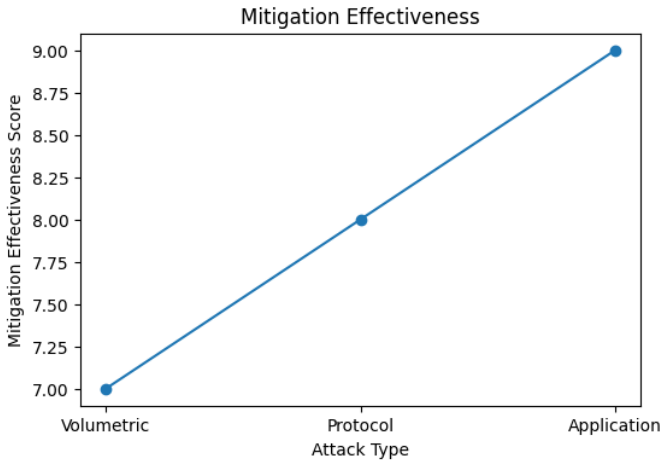


**Figure 4.** Relative effectiveness of mitigation techniques against various DDoS attack categories.

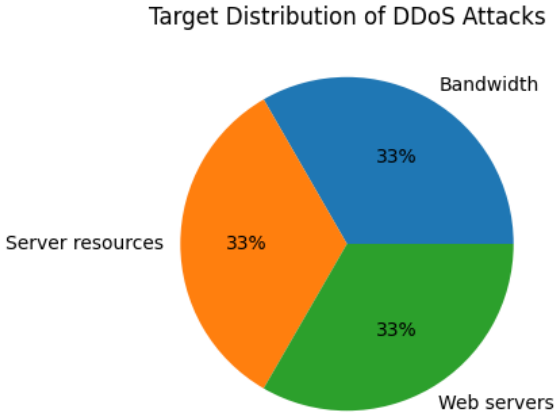


**Figure 5.** Distribution of primary targets affected by DDoS attack types.

As shown in the fig. 3,4 and 5, the graphical analysis highlights the varying impact and mitigation effectiveness of different Distributed Denial of Service (DDoS) attack types. Volumetric attacks, such as UDP floods, exhibit the highest impact severity due to their ability to congest network bandwidth, whereas protocol attacks primarily exhaust server resources and may lead to system crashes. Application-layer attacks target web servers and disrupt services by overwhelming legitimate application requests. The mitigation analysis indicates that traditional techniques such as rate limiting are moderately effective against volumetric attacks, while firewalls and IDS/IPS solutions provide stronger protection against protocol and application-layer attacks. Furthermore, the target distribution graph demonstrates that DDoS attacks affect multiple critical components of network infrastructure, emphasizing the need for a multi-layered defense strategy to ensure service availability and cybersecurity resilience.

## CONCLUSION

Network security faces a significant risk from Distributed Denial-of-Service attacks which disrupt digital services by compromising their availability and reliability. The study conducted an analysis of different DDoS attack types together with their detection methods and defense mechanisms. The research results demonstrate that security systems need to have adaptive features and scalable capabilities together with intelligent components to combat DDoS attacks which currently exist in their new forms. The research should concentrate on developing systems which combine artificial intelligence with active defense mechanisms that operate in real time.

## ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to ITM University, Gwalior, for providing the necessary academic environment and resources to carry out this research work. The authors also extend their appreciation to the faculty members and domain experts for their valuable guidance, constructive feedback, and continuous support throughout the study. Special thanks are given to colleagues and peers who contributed through discussions and insights that helped improve the quality of this paper.

## REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson, 2017.

[2] A. S. Tanenbaum and D. J. Wetherall, Computer Networks, 5th ed. Upper Saddle River, NJ, USA: Pearson, 2011.

[3] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and defense mechanisms,” ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, Apr. 2004.

[4] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Indianapolis, IN, USA: Wiley, 2008.

[5] M. Antonakakis et al., “Understanding the Mirai botnet,” in Proc. 26th USENIX Security Symposium, Vancouver, Canada, 2017, pp. 1093–1110.

[6] D. Dittrich, “Distributed denial of service attacks,” University of Washington, Tech. Rep., 2000.

[7] S. Yu et al., “Application-layer DDoS attacks,” IEEE Communications Magazine, vol. 52, no. 4, pp. 58–65, 2014.

[8] A. B. Zargar et al., “A survey of DDoS defense mechanisms,” Journal of Network and Computer Applications, vol. 35, no. 2, pp. 100–110, 2013.

[9] Y. Xin et al., “Machine learning for cybersecurity,” IEEE Access, vol. 6, pp. 35365–35381, 2018.

[10] S. Kumar, R. Patel, M. Sharma, and K. Jain, "Artificial intelligence in healthcare systems," IEEE Access, vol. 9, pp. 12345–12360, 2021..

[11] Lu, Jinzhu, Lijuan Tan, and Huanyu Jiang. "Review on convolutional neural network (CNN) applied to plant leaf disease classification." *Agriculture* 11.8 (2021): 707