InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-2 / February - 2026

Original Article

A Study on Flexibility against DDoS Attacks and it's Implications for Mobile Security

Shruti Deepak Thorat[1], Tanuja Ghorpade[2], Prachi Nannavare[3]
[1, 2, 3] Department of Computer Science

Manuscript ID:
IBMIIRJ -2026-030205

Submitted: 06 Jan. 2026

Revised: 10 Jan. 2026

Accepted: 04 Feb. 2026

Published: 28 Feb. 2026

ISSN: 3065-7857

Volume-3

Issue-2

Pp. 26-29

February 2026

Correspondence Address:
Shruti Deepak Thorat, Department of Computer Science
Email: shrutithorat@atsscollege.edu.in

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.21131210

DOI Link:
https://doi.org/10.5281/zenodo.21131210

Abstract

Mobile communication networks have become the backbone of critical services, such as digital payments, online education, healthcare monitoring, and emergency response systems. With the growing dependence on mobile connectivity, distributed denial-of-service (DDoS) attacks have emerged as a serious threat to network availability and reliability. These attacks attempt to overwhelm network resources by generating excessive malicious traffic, preventing legitimate users from accessing essential services. The rapid adoption of advanced technologies, such as 5G, the Internet of Things (IoT), cloud infrastructure, and edge computing, has increased the capability and complexity of mobile networks. Although these technologies improve performance and scalability, they also introduce new security vulnerabilities that are difficult to manage using traditional defence mechanisms. Consequently, the detection and mitigation of DDoS attacks in mobile environments have become increasingly challenging [1], [2]. This study investigates resilience-based strategies for mitigating DDoS attacks in mobile networks. It analyzes common vulnerabilities, reviews existing mitigation techniques, and discusses the role of emerging technologies, such as artificial intelligence, software-defined networking, blockchain, and edge computing. This study emphasizes the importance of adaptive and multilayered defense mechanisms to ensure reliable mobile communication. The findings aim to support telecom operators, network administrators, and researchers in strengthening the security of next-generation mobile networks.

Keywords: *DDoS Attacks, Mobile Network Security, 5G Networks, Network Resilience, AI-Based Detection, SDN, Edge Computing*

Introduction

Mobile networks play a vital role in supporting modern digital services. Activities such as online banking, remote education, healthcare applications, and government services rely heavily on uninterrupted mobile connections. Among the various cybersecurity threats affecting these networks, distributed denial-of-service (DDoS) are considered particularly disruptive because the target service availability rather than data confidentiality [3], [4]. The evolution of mobile communication from 4G to 5G has introduced higher data rates, reduced latency, and massive device connections. However, this evolution has also increased the attack surface. The integration of IoT devices, cloud platforms, and edge computing has significantly expanded the attack surface of modern mobile networks [5], [6]. Detecting DDoS attacks in mobile environments is difficult because of the dynamic traffic behavior, user mobility, and limited resources at edge nodes. Attackers often use large botnets and sophisticated traffic patterns that resemble legitimate traffic patterns. Consequently, traditional rule-based detection techniques are insufficient. Recent studies highlight the use of artificial intelligence and software-defined networking to improve detection accuracy and mitigation response time [7], [8].

Objectives of the Study

The objectives of this study are as follows:

- To identify vulnerabilities in mobile network infrastructure that enable DDoS attacks.
- To study the existing detection and mitigation techniques used in mobile environments.
- To analyze the contribution of emerging technologies, such as AI, SDN, blockchain, and edge computing, in enhancing network resilience.

How to cite this article:
Thorat, S. D., Ghorpade, T., & Nannavare, P. (2026). A Study on Flexibility against DDoS Attacks and it's Implications for Mobile Security. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(2), 26–29. https://doi.org/10.5281/zenodo.21131210

- This study provides insights and future directions for strengthening mobile network security

Research Methodology

This study adopted a qualitative and analytical approach. A detailed review of the existing literature related to DDoS attacks, mobile network security, and resilience mechanisms was conducted. Conceptual models, previously proposed frameworks, and reported case studies were analyzed to understand the strengths and limitations of the current solutions. This study focuses on conceptual evaluation rather than on experimental implementation.

Literature Review

Several studies have explored DDoS mitigation techniques in mobile networks using traffic analysis, anomaly detection, and machine learning-based approaches [9]–[12]. AI-based models have shown promising results in detecting abnormal traffic patterns in 5G and IoT-enabled environments [13], [14]. SDN and NFV technologies enable dynamic traffic control and flexible security policy enforcement [15], [16]. Despite these advancements, many solutions suffer from limitations such as high computational overhead, increased false positives, and limited scalability. Moreover, most existing approaches focus on single-vector attacks, whereas modern DDoS attacks are often multivector and adaptive in nature. These limitations indicate the need for an integrated and resilience-oriented security framework.

Types of DDoS Attacks in Mobile Networks

Table 1: Common Types of DDoS Attacks in Mobile Networks

Attack Type	How the Attack Works	Impact on Mobile Networks
Volumetric Attacks	Large volumes of fake traffic flood network bandwidth	Results in congestion and service unavailability
Protocol-Based Attacks	Exploits weaknesses in TCP, UDP, or signaling protocols	Disrupts session establishment and control
Application-Layer Attacks	Targets specific mobile applications or services	Directly affects user-facing services
Botnet-Based Attacks	Uses compromised devices, often IoT-based	Difficult to trace due to distributed nature

DDoS Mitigation Techniques

Table 2: Comparison of DDoS Mitigation Approaches

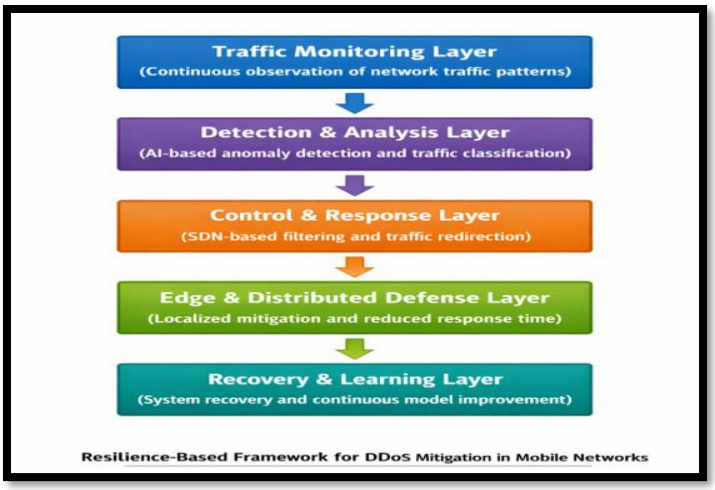
Approach	Key Characteristics	Limitations
Rule-Based Filtering	Blocks traffic based on predefined patterns	Ineffective against unknown attacks
Traffic Rate Limiting	Restricts excessive traffic flow	May affect genuine users
AI-Based Detection	Learns abnormal traffic behavior	Requires training data and resources
SDN-Based Mitigation	Enables programmable traffic control	Central controller may become vulnerable

Emerging Technologies Supporting Network Resilience

Table 3: Technologies Enhancing DDoS Resilience

Technology	Role in Mitigation	Practical Benefit
Artificial Intelligence	Detects anomalies in real-time	Improves detection accuracy
Software-Defined Networking	Enables dynamic traffic management	Flexible and adaptive response
Edge Computing	Processes data closer to users	Reduces latency
Blockchain	Secures coordination among nodes	Enhances trust and transparency

Conceptual Framework for DDoS Resilience



Practical Context and Use Cases

1 SPPU Classroom Perspective

In Computer Networks and Cybersecurity laboratory courses conducted in SPPU-affiliated colleges, students often simulate network traffic scenarios to understand congestion and attack behavior. Practical exercises involving traffic monitoring tools help students observe how sudden traffic spikes affect system performance. Introducing AI-assisted traffic analysis in such laboratories can further improve students' understanding of real-world DDoS detection and mitigation strategies.

2 Indian Telecom Network Scenario

Indian telecom operators manage large-scale mobile networks that experience significant traffic fluctuations during online examinations, digital payment peaks, and other national events. During such periods, DDoS attacks can blend with legitimate traffic, making their detection difficult. AI-driven traffic analysis combined with SDN-based control can help operators distinguish between malicious traffic and genuine demand, ensuring service continuity.

Discussion

Recent surveys emphasize the need for integrated and multi-layered defense architectures to counter adaptive DDoS attacks [17], [18].AI-based detection provides accuracy but requires additional computational resources. Although SDN offer flexibility, they introduce centralized vulnerabilities. Although edge computing reduces latency, it has limited processing power. Therefore, an integrated, multilayered approach is necessary to enhance network resilience.

Future Research Directions

Future research should focus on lightweight AI models suitable for edge devices, decentralized security architectures, and privacy-preserving detection mechanisms, such as federated learning. Large-scale deployment and real-world testing are essential to validate the proposed frameworks.

Conclusion

DDoS attacks continue to pose a significant threat to the availability and reliability of mobile networks. This study reviewed the vulnerabilities, attack types, mitigation techniques, and emerging technologies related to DDoS defense in mobile networks. The proposed resilience-based framework emphasizes adaptive, layered, and intelligent security mechanisms. Strengthening mobile network resilience is critical for supporting future digital services and next-generation communication systems.

Acknowledgment

I would like to express my sincere gratitude to all those who supported and guided us in completing the research study titled "A Study on Flexibility against DDoS Attacks and its Implications for Mobile Security."

I am deeply thankful to the Department of Computer Science and the management of ATSS College for providing the necessary academic support, infrastructure, and encouragement throughout the research process. The institutional environment greatly facilitated the successful completion of this work.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper

Reference

1. Cloudflare, "DDoS Attack Trends for Q3 2023," Cloudflare Report, 2023.
2. Cisco, "Annual Internet Report (2018–2023)," Cisco Systems, 2023.
3. .A. Gupta and B. Singh, "Advanced detection techniques for DDoS attacks in 5G networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 215–230, 2022.
4. R. Jones, M. Patel, and L. Wang, "DDoS attack duration analysis and its impact on network infrastructure," *Journal of Cybersecurity and Privacy*, vol. 12, no. 1, pp. 98–115, 2022.
5. S. Kim, J. Lee, and H. Park, "Mobile network vulnerabilities to cyber threats: A DDoS perspective," *IEEE Access*, vol. 10, pp. 15489–15502, 2022.
6. K. Sharma and P. Patel, "Security challenges in heterogeneous mobile networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 290–305, 2023.
7. L. Chen and T. Nakamura, "AI-driven anomaly detection for network security," *International Journal of Network Security & Its Applications*, vol. 15, no. 3, pp. 55–72, 2023.
8. Y. Meidan et al., "Detection of unauthorized IoT devices using machine learning techniques," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 62–68, 2022.
9. M. Conti, A. Dehghantanha, and K. Franke, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2021.
10. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys*, vol. 39, no. 1, pp. 1–42, 2021.
11. A. Mishra and N. Kaur, "Machine learning approaches for DDoS attack detection: A survey," *Journal of Information Security and Applications*, vol. 58, 2021.

12. S. Behal and K. Kumar, "Detection of DDoS attacks and flash events using information theory," *Computer Networks*, vol. 116, pp. 96–110, 2020.
13. J. Li, Z. Zhao, and R. Li, "Deep learning-based DDoS attack detection in cloud environments," *IEEE Access*, vol. 8, pp. 213123–213134, 2020.
14. M. Roesch, "Snort: Lightweight intrusion detection for networks," in *Proc. USENIX LISA*, 2020, pp. 229–238.
15. N. Feamster, J. Rexford, and E. Zegura, "The road to SDN," *ACM Queue*, vol. 11, no. 12, pp. 20–40, 2019.
16. H. Farhady, H. Lee, and A. Nakao, "Software-defined networking: A survey," *Computer Networks*, vol. 81, pp. 79–95, 2019.
17. R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog and cloud computing: A survey," *Future Generation Computer Systems*, vol. 78, pp. 432–449, 2018.
18. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2018.
19. Z. A. Baig et al., "Future challenges for intrusion detection systems," *IEEE Access*, vol. 5, pp. 20950–20955, 2017.
20. P. Garcia-Teodoro et al., "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & Security*, vol. 28, no. 1–2, pp. 18–28, 2017.