Distributed denial of service attack in HTTP/2: review on security issues and future challenges

ABSTRACT

This article offers a comprehensive overview of recent literature on the HTTP/2 protocol and conducts an analysis of the security threats and DDoS attack typologies associated with HTTP/2. The investigation revealed that the introduction of new features in HTTP/2 has significantly improved the network transmission speed and utilization. However, these advancements have also brought forth a series of emerging network security risks. This study examines the current state of the art in DDoS attacks tailored for HTTP/2 and their detection methods, proposing future research directions in the field of attack detection. By analyzing the distinctive features of HTTP/2 protocol, the study suggests extending DDoS attack detection techniques established for HTTP/1 to the realm of HTTP/2. Furthermore, the research underscores the ease with which adversaries can exploit the intrinsic multiplexing in HTTP/2 to launch a large number of malicious requests, leading to severe depletion of network bandwidth and exhaustion of valuable server resources. Additionally, it highlights the potential applicability of deep learning algorithms in the context of the HTTP/2 protocol. Additionally, the article proposes strategies to address challenges associated with DDoS attacks and the scarcity of adequate datasets for HTTP/2. This research contributes to a comprehensive understanding of the security implications surrounding the HTTP/2 protocol and provides valuable insights for advancing DDoS attack detection technologies.