CASCADE BROAD LEARNING NETWORK WITH EMBEDDED IMAGE FEATURES FOR MALWARE TRAFFIC CLASSIFICATION

Author's: S. Hemarubini[1], R. Surendiran[2], K. Sujith[3], N. Vanjulavalli[4]

Abstract

The rapid proliferation of malware-driven cyberattacks has significantly increased the complexity of network security management. Traditional signature-based detection mechanisms are increasingly ineffective against modern polymorphic, zero-day, and encrypted malware traffic. As adversaries adopt sophisticated evasion techniques such as traffic obfuscation, encryption, and protocol mimicry, conventional intrusion detection systems (IDS) struggle to maintain high detection accuracy while preserving low false-positive rates. Consequently, machine learning–based traffic classification approaches have emerged as a promising alternative. This proposes a novel framework titled "A Cascade Broad Learning Network Embedded Image Features for Malware Traffic Classification." The central idea is to transform raw network traffic flows into structured image-like representations and extract discriminative embedded image features using texture and structural descriptors. These features are then classified using a Cascade Broad Learning Network (CBLN), an efficient alternative to deep neural networks that avoids backpropagation while preserving strong generalization capability.