Detection of management-Frames-Based Denial-of-Service Attack in Wireless LAN network using artificial neural network

ABSTRACT

Wireless Local Area Networks (WLANs) have become an increasingly popular mode of communication and networking, with a wide range of applications in various fields. However, the increasing popularity of WLANs has also led to an increase in security threats, including denial of service (DoS) attacks. In this study, management-frames-based DoS attacks, in which the attacker floods the network with management frames, are particularly concerning as they can cause widespread disruptions in the network. Attacks known as denial of service (DoS) can target wireless LANs. None of the wireless security mechanisms in use today contemplate defence against them. At the MAC layer, there are multiple vulnerabilities that can be exploited to launch DoS attacks. This paper focuses on designing and developing an artificial neural network (NN) scheme for detecting management-frames-based DoS attacks. The proposed scheme aims to effectively detect fake de-authentication/disassociation frames and improve network performance by avoiding communication interruption caused by such attacks. The proposed NN scheme leverages machine learning techniques to analyse patterns and features in the management frames exchanged between wireless devices. By training the NN, the system can learn to accurately detect potential DoS attacks. This approach offers a more sophisticated and effective solution to the problem of DoS attacks in wireless LANs and has the potential to significantly enhance the security and reliability of these networks. According to the experimental results, the proposed technique exhibits higher effectiveness in detection compared to existing methods, as evidenced by a significantly increased true positive rate and a decreased false positive rate.