IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 2, December 2025

Impact Factor: 7.67

Mitigating DoS Attacks in VANETs Using an Innovative Security Method

Ajit Kumar[1], Dr. Harsh Lohiya[2], Mr. Ankit Navgeet Joshi[3]

[1]Research Scholar, Department of CSE

[2]Associate Professor, Department of CSE

[3]Assistant Professor, Department of CSE

Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India

Abstract: *The high mobility of Vehicular Ad Hoc Networks (VANETs) makes secure routing a critical challenge. Their highly dynamic topology leads to frequent changes and susceptibility to network disruptions caused by obstacles such as buildings, tunnels, and bridges. These intermittent connections often result in packet loss, degrading overall network performance. Identifying the root cause of packet loss is difficult, as it may stem from both network instability and various security threats. As a subset of Mobile Ad Hoc Networks (MANETs), VANETs are vulnerable to attacks including denial of service (DoS), black hole, gray hole, and ghost attacks. Although numerous security mechanisms have been proposed for MANET routing, VANETs require more robust solutions due to their unique communication modes—vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V). There is a growing need to secure the interaction between these communication types. This paper presents a security approach designed to detect, analyze, and mitigate existing threats to ensure reliable and secure routing in VANET environments.*

Keywords*:* Authentication, Confidentiality, Attack,VANET, Replay.

DOI: 10.48175/568