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 8, May 2025
Impact Factor: 7.67

A Review on Various Security Attacks in Vehicular Ad hoc Networks

Simran Mansuri[1], Dr. Harsh Lohiya[2], Mr. Jitendra Tiwari[3]
Research Scholar, Department of CSE[1]
Assistant professor, Department of CSE[2,3]
Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India

Abstract: *Vehicular Ad Hoc Networks (VANETs) have emerged as a crucial subclass of Mobile Ad Hoc Networks (MANETs), playing a vital role in delivering various safety and communication services to vehicle occupants. The widespread adoption of VANETs can be attributed to their ability to integrate seamlessly with numerous backend services, often invisible to users. Ensuring the security of VANETs is essential, as any vulnerabilities could compromise the safety and privacy of drivers and passengers. As the technology rapidly evolves, the need for robust and reliable security frameworks has become increasingly significant. This survey explores the current challenges associated with VANETs, focusing on the efficiency of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Key security issues such as data confidentiality, user authentication, message integrity, availability, and non-repudiation are addressed. We also examine potential threats that target these security aspects. Based on various performance evaluations and analytical studies, the paper demonstrates that the ACPN (Access Control Protocol for Networks) offers a practical and effective solution for authenticating entities within VANETs. Ultimately, the findings highlight the importance of implementing strong encryption and authentication mechanisms to maintain secure and trustworthy vehicular networks.*

Keywords: Vehicular Ad Hoc Networks

DOI: 10.48175/568