

**Securing the VANET through a Hybrid Approach by Mitigating
DoS Attacks and its types with Self-healing
and Immunization**

By

Ms. S. Rama Mercy
(17PHCSP011)

Supervisor

Dr. G. Padmavathi
Professor
Department of Computer Science

Thesis Submitted to
Avinashilingam Institute for Home Science and Higher Education
for Women, Coimbatore – 641 043

In Partial fulfilment of the requirements for the Degree of
Doctor of Philosophy in Computer Science

January 2025

80_RECOMMENDATION

The proposed research presents a three-phase methodology that successfully secures VANETs by detecting and preventing DoS attacks with integrated self-healing and immunization, laying a strong foundation for future advancements. Potential directions include:

The three-phase methodology enforces TRHE with Hex-Tuple matched mapping for secured transmission. However, future research could focus on developing stronger privacy measures to further enhance VANET performance.

Optimization techniques adopted for the immunization based on MFO rely on high PDR for efficient data delivery. The current approach optimizes single attributes like stable clusters and reliable relay nodes. Future research into a multi-attribute optimization approach would balance scalability, communication efficiency, and reliability, leading to more robust VANET performance.

Emerging technologies like edge computing, AI-based anomaly detection, and 5G/6G connectivity can be explored to improve real-time attack detection, reduce response times, and enhance the overall resilience of VANET infrastructures.