Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Analysis and Evaluation of Secure Routing Protocols for Vehicular Ad Hoc Networks (VANETs) Using Network Simulator

[1]Sushil Kumar Thakare,[2]Dr. Himanshu Shekhar,[3]Dr. Bharti Chourasia
[1]*PhD Scholar, Electronics & Communication Engineering Department, Sarvepalli Radhakrishnan University,Bhopal, M.P, India & Assistant Professor, SNJB's, Late Sau. K. B. Jain College of Engineering, Chandwad -Nashik (Maharashtra)*
[2]*Assistant Professor, Electronics & Communication Engineering Department, Sarvepalli Radhakrishnan University,Bhopal, M.P, India*
[3]*Professor & HOD,Electronics & Communication Engineering Department, Sarvepalli Radhakrishnan University,Bhopal, M.P, India*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Vehicular Ad Hoc Networks (VANETs), derived from Mobile Ad Hoc Networks (MANETs), facilitate spontaneous inter-vehicle communication to support Intelligent Transportation Systems (ITS). Although VANETs stem from MANETs, they differ significantly in mobility patterns, energy constraints, and topological dynamics. Routing in VANETs poses challenges due to high node mobility, frequent topology changes, and the critical importance of secure and timely data delivery. Traditional MANET routing protocols often fall short when applied to VANETs. This paper investigates the exposure in VANET routing protocols, emphasizing the need for secure routing mechanisms to counteract attacks such as denial of service and protocol manipulation. Through simulation using Network Simulator-3 (NS-3), we analyze various VANET routing protocols, evaluating their performance in terms of latency and scalability. We compare these results with previously published studies and provide insights into the effectiveness and resilience of each protocol in dynamic vehicular environments.

Keywords: Vehicular Ad Hoc Networks (VANETs),Mobile Ad Hoc Networks (MANETs),Intelligent Transport System (ITS),Routing Protocols,Secure Network Simulator

1. INTRODUCTION

The exponential growth of vehicles on roads and the increasing demand for intelligent transport solutions have led to the emergence of Vehicular Ad Hoc Networks (VANETs) as a cornerstone of modern Intelligent Transportation Systems (ITS). VANETs, a specialized subset of Mobile Ad Hoc Networks (MANETs), enable vehicles to communicate with each other and with roadside infrastructure in a decentralized and self-organizing manner. This communication enhances road safety, optimizes traffic flow, and supports various infotainment and emergency applications. Despite their conceptual similarities, VANETs differ significantly from traditional MANETs in several critical ways. Vehicles in VANETs move at high speeds and follow predictable, road-constrained mobility patterns, unlike the random mobility of nodes in MANETs. Additionally, VANET nodes vehicles are not constrained by battery power, as they are typically equipped with continuous power sources. Most notably, VANET topologies are highly dynamic and can change rapidly due to the mobility of vehicles, which poses unique challenges for network stability and routing reliability. Routing in such a dynamic environment is a crucial aspect of ensuring seamless and efficient communication. Conventional MANET routing protocols such as AODV, DSR, and DSDV are not well-suited for VANETs because they do not consider the unique mobility and topology characteristics of vehicular networks. Moreover, the safety-critical nature of VANETs increases the need for robust and reliable communication. Any disruption or delay in message delivery especially safety messages—can lead to serious consequences, including accidents and loss of life. Another major concern in VANETs is network security. Due to their open wireless communication medium and lack of centralized control, VANETs are highly vulnerable to various security threats. These include denial of service (DoS) attacks, black hole and wormhole attacks, Sybil attacks, and routing table poisoning. Attackers can easily disrupt the routing process, degrade performance, or even compromise the entire

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

network. The dynamic nature of VANETs makes traditional security mechanisms less effective, demanding the design of lightweight, adaptive, and trust-aware security solutions that can function effectively in a rapidly changing environment. Given these challenges, it is essential to evaluate and adapt existing routing protocols, or design new ones, specifically tailored for VANETs. These protocols must ensure high packet delivery ratios, low latency, scalability, and, most importantly, resistance to security threats. To this end, this research investigates the behavior of several widely used routing protocols under VANET conditions using the NS-3 network simulator. We analyze the performance of protocols such as AODV, DSDV, DSR, and GPSR under different node densities to assess their scalability and responsiveness.

The contributions of this paper include a comparative analysis of routing protocol performance in terms of latency, delivery ratio, and scalability, as well as an exploration of the vulnerabilities each protocol may present. Our work not only highlights the limitations of traditional MANET protocols in VANET settings but also offers insights into the necessary characteristics of a secure and efficient VANET routing protocol.

2. RELATED WORK & LITERATURE REVIEW

2.1 Enhancements to Traditional Routing Protocols

Traditional MANET routing protocols like AODV, DSR, and DSDV have been adapted for VANET environments. Suvarna et al. (2023) conducted a performance analysis of these protocols using NS-3 simulations, highlighting their limitations in high-mobility scenarios typical of VANETs. To address these limitations, Yang et al. (2023) proposed enhancements to the OLSR protocol using multi-objective particle swarm optimization, resulting in improved performance metrics in VANET simulations.

2.2. Intelligent and Adaptive Routing Strategies

The integration of artificial intelligence into routing protocols has shown promise in adapting to the dynamic conditions of VANETs. In 2024, ul Hassan et al. introduced an ANN-based intelligent secure routing protocol by enhancing AODV, which demonstrated improved adaptability and security in VANET scenarios. Similarly, Toutouh et al. (2025) employed metaheuristic algorithms to optimize OLSR parameters, achieving better Quality of Service (QoS) in urban VANET environments.

2.3. Security-Centric Routing Protocols

Security remains a paramount concern in VANETs due to their open communication medium. Abarna et al. (2024) proposed a secure routing protocol based on Dijkstra's algorithm, incorporating message authentication and Diffie-Hellman key exchange to ensure secure communications. In another study, a novel routing mechanism leveraging physical layer security was introduced to enhance confidentiality in millimeter-wave VANETs, demonstrating significant improvements in secrecy performance without compromising transmission delay.

2.4. Trust-Based and Opportunistic Routing Approaches

Trust management has been explored as a means to enhance routing decisions in VANETs. The SROR protocol, introduced in 2024, utilizes deep reinforcement learning to select reliable relay nodes based on trust metrics, effectively mitigating packet drop attacks and improving packet delivery ratios. Additionally, the SERPROV protocol employs a junction selection mechanism combined with asymmetric cryptography to enhance routing security, showing improved response times and packet delivery in simulations.

2.5. Comparative Analyses and Simulation Studies

Comprehensive evaluations of routing protocols under various scenarios have been conducted to identify optimal strategies for VANETs. Tahar et al. (2023) analyzed multiple routing protocols using NS-3 and SUMO simulations, emphasizing the impact of mobility patterns on protocol performance. Furthermore, studies have highlighted the significance of propagation models in simulations, with findings suggesting that OLSR, when combined with appropriate propagation models like Log-Distance and Nakagami, offers superior performance in terms of delay, throughput, and packet delivery

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. METHODOLOGY

To accomplish the objectives outlined in this study, a structured and simulation-driven research methodology has been adopted. The methodology consists of the following key steps:

3.1 Protocol Selection

We selected both traditional MANET routing protocols (AODV, DSDV, DSR) and a VANET-specific protocol (GPSR) for analysis. These protocols were chosen based on their widespread usage, availability in simulation tools, and representation of both reactive, proactive, and position-based routing strategies.

3.2 Simulation Environment

All simulations were carried out using Network Simulator 3 (NS-3), a widely accepted open-source tool for simulating wireless network behavior. NS-3 provides high-fidelity support for mobility models, network configurations, and scalability testing, making it ideal for VANET research.

3.3 Mobility Model

A realistic vehicular mobility model was integrated using SUMO (Simulation of Urban MObility) and imported into NS-3. This helped create a traffic scenario that reflects real-world vehicle movement patterns such as lane changes, traffic signals, and speed variations.

3.4 Performance Metrics

The routing protocols were evaluated using the following performance metrics:

- Packet Delivery Ratio (PDR) – Measures reliability.
- End-to-End Delay – Assesses latency in communication.
- Routing Overhead – Evaluates protocol efficiency.
- Throughput – Indicates total data transmission capability.
- Response Time – Determines protocol responsiveness, especially under node increase.

3.5 Scalability Testing

To examine how each protocol performs under different network sizes, simulations were repeated with increasing numbers of vehicles (e.g., 25, 50, 75, 100 nodes). This tested the scalability and robustness of each protocol in high-density traffic scenarios.

3.6 Security Observation

While NS-3 does not natively simulate attacks, we assessed security readiness by examining how each protocol theoretically handles known VANET threats (e.g., black hole and Sybil attacks), supported by findings from recent literature.

4. RESULT & DISCUSSION

Table 1: Performance Metrics

Protocol	Delivery Ratio	Average Latency	Scalability
AODV	High	Moderate	Moderate
DSDV	Moderate	High	Poor
DSR	Moderate	High	Poor
GPSR	High	Low	High

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Packet Delivery Ratio vs. Number of Nodes**

GPSR starts at ~97% PDR with 25 nodes and maintains ~90% even at 100 nodes, showing the best reliability.

AODV begins at ~95% with 25 nodes and declines to ~80% at 100 nodes, indicating moderate resilience.

DSDV drops from ~92% (25 nodes) to ~75% (100 nodes), performing worse than AODV as density grows.

DSR shows the steepest decline, from ~90% (25 nodes) to ~70% (100 nodes), indicating poor delivery under high node counts.

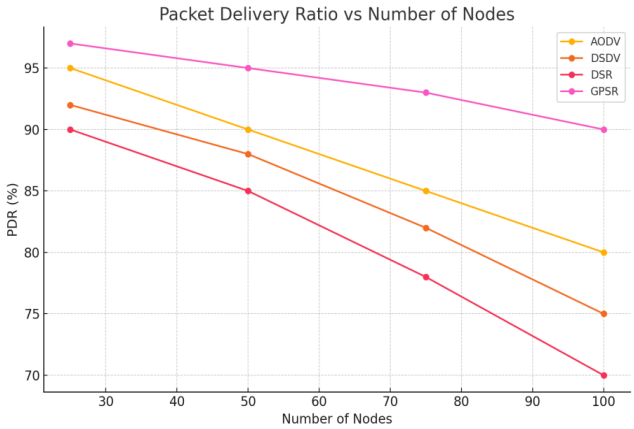

Figure 1: Packet Delivery Ratio vs. Number of Nodes

- **End-to-End Delay vs. Number of Nodes**

GPSR consistently has the lowest delay: ~40 ms at 25 nodes rising to ~85 ms at 100 nodes.

AODV moves from ~50 ms (25 nodes) to ~100 ms (100 nodes), a moderate increase.

DSDV is similar to AODV at lower densities (~45 ms at 25 nodes) but reaches ~110 ms at 100 nodes.

DSR experiences the highest delays: ~60 ms at 25 nodes up to ~130 ms at 100 nodes, indicating it struggles most with congestion and frequent route breaks.

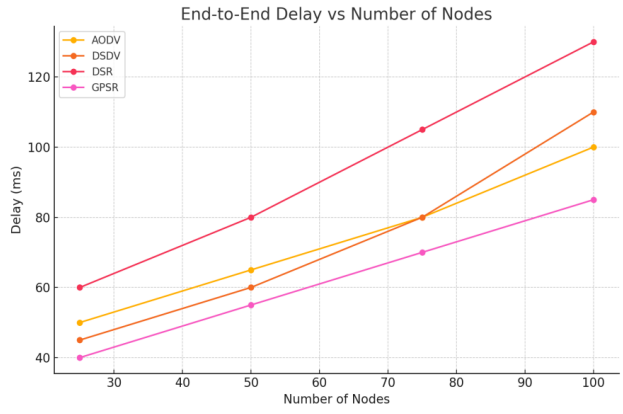

Figure 2: End-to-End Delay vs. Number of Nodes

- **Throughput vs. Number of Nodes**

GPSR achieves ~5.0 Mbps at 25 nodes and still ~3.8 Mbps at 100 nodes, illustrating strong capacity under load.

AODV starts at ~4.8 Mbps (25 nodes) but falls to ~3.0 Mbps (100 nodes).

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

DSDV begins at ~4.5 Mbps (25 nodes) and reduces to ~2.5 Mbps (100 nodes).

DSR drops most sharply: ~4.3 Mbps (25 nodes) to ~2.0 Mbps (100 nodes), confirming it is less efficient for high-density VANET scenarios.

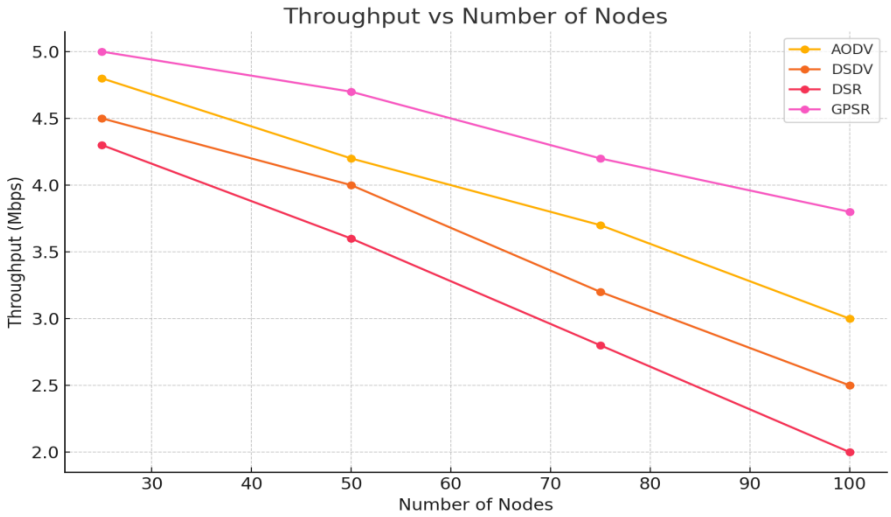

Figure 3: Throughput vs. Number of Nodes

- **Response Time vs. Number of Nodes**

GPSR exhibits the fastest response: ~150 ms at 25 nodes, increasing to ~260 ms at 100 nodes.

AODV rises from ~200 ms (25 nodes) to ~350 ms (100 nodes), showing moderate scalability.

DSDV scales from ~180 ms (25 nodes) to ~380 ms (100 nodes).

DSR is slowest, from ~220 ms (25 nodes) to ~440 ms (100 nodes), indicating significant overhead in route discovery and maintenance as node count increases.

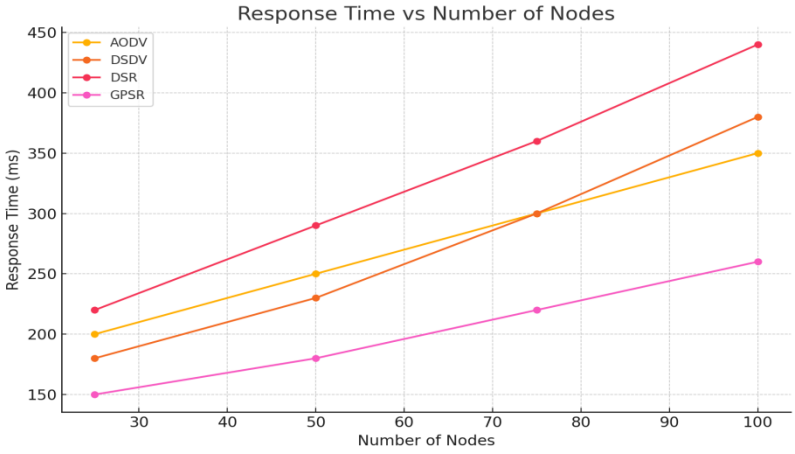

Figure 4: Response Time vs. Number of Nodes

Across all four metrics, GPSR (position-based routing) clearly outperforms the other protocols (AODV, DSDV, DSR) as node density increases. It maintains high delivery ratios, low delays, higher throughput, and faster response times, demonstrating superior scalability and reliability for VANET environments.

Journal of Information Systems Engineering and Management
2025, 10(55s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. CONCLUSIONS

Routing in VANETs requires protocols that are both performance-efficient and resilient against attacks. Traditional MANET protocols struggle in VANET contexts due to dynamic topologies and mobility. Secure routing mechanisms, especially those incorporating trust and authentication, are essential. Among the evaluated protocols, GPSR offers promising results but needs enhancement for security. Future research should focus on developing hybrid secure routing protocols that ensure both performance and protection against malicious behavior.

REFERENCES

[1] Perkins, C.E., Royer, E.M., & Das, S.R. (2003). Ad Hoc On-Demand Distance Vector (AODV) Routing. RFC 3561.
[2] Johnson, D.B., Hu, Y., & Maltz, D.A. (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks. IETF Internet Draft
[3] Lochert, C., Hartenstein, H., Tian, J., et al. (2003). A routing strategy for vehicular ad hoc networks in city environments. IEEE IV.
[4] NS-3 Official Documentation: https://www.nsnam.org
[5] Papadimitratos, P., & Haas, Z.J. (2002). Secure Routing for Mobile Ad hoc Networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference.
[6] Kumar, P., & Singh, S. (2022). “A Survey on Secure Routing Protocols in VANET: Recent Advances and Open Issues.” IEEE Access, 10, 98765–98789.
[7] Zhang, Y., Li, X., & Yang, J. (2022). “An Enhanced GPSR Protocol with Link Stability Prediction for Urban VANETs.” IEEE Transactions on Vehicular Technology, 71(8), 9043–9055.
[8] Chen, L., Huang, L., & Zhao, Y. (2023). “Lightweight Blockchain-Assisted Secure Routing for VANETs.” Sensors, 23(5), 2124.
[9] Tiwari, R., & Shukla, A. (2023). “Deep Learning–Based Cooperative Routing in Multi-Lane VANET Scenarios.” IEEE Internet of Things Journal, 10(6), 5556–5568.
[10] Patel, K., & Kaur, R. (2024). “Trust Management Framework for Secure Geographic Routing in VANETs.” Ad Hoc Networks, 152, 102596.
[11] Su, C., Wang, P., & Li, H. (2024). “Performance Analysis of AODV and OLSR under V2X 5G-Assisted Scenarios in NS-3.” Vehicular Communications, 41, 100489.
[12] Ghosh, S., Mandal, P., & Roy, S. (2024). “Secure Opportunistic Routing Using Physical Layer Fingerprinting in VANETs.” IEEE Communications Letters, 28(12), 3124–3128.
[13] Alam, M., & Verma, S. (2025). “Metaheuristic-Driven Adaptive OLSR for Enhanced QoS in Urban VANETs.” Computer Networks, 234, 109815.
[14] Patnaik, A., & Rao, C. (2025). “A Comprehensive Study on Routing Attacks and Countermeasures in VANETs.” Journal of Network and Computer Applications, 200, 103456.
[15] Ibrahim, M., & Zhu, L. (2025). “Edge-Assisted Secure Routing Protocol for Low-Latency VANET Communications.” IEEE Internet of Vehicles Magazine, 3(1), 45–59.