AI-Driven Adaptive Trust Management Framework for Secure Vehicular Networks in Smart Cities Using NS-3 and SUMO Co-Simulation

OPEN ACCESS

Volume: 13

Special Issue: 1

Month: March

Year: 2026

P-ISSN: 2321-4643

E-ISSN: 2581-9402

Citation:
Nirmala, R. "AI-Driven Adaptive Trust Management Framework for Secure Vehicular Networks in Smart Cities Using NS-3 and SUMO Co-Simulation." *Shanlax International Journal of Management,* vol. 13, no. S1, 2026, pp. 20–28.

DOI:
https://doi.org/10.34293/management.v13iS1-Mar.10680

R. Nirmala
Assistant Professor, Department of Computer Science
Jain College (Autonomous), Bangalore, India

Abstract
To address the security challenges of Vehicular Ad Hoc Networks (VANETs) in smart cities, which arise from their high mobility and decentralization nature, robust and adaptive security mechanisms are essential. This paper introduces an AI-Driven adaptive trust management framework. Moving beyond the traditional perimeter-based security, the proposed solution integrates Zero-Trust principles with entropy-weighted trust scoring and edge assisted decision-making. This was developed using integrated SUMO mobility modeling and NS-3 simulations. This framework specifically targets the Sybil, replay and data falsification attacks. Extensive experiments involving 500 to 5000 vehicles and 20 roadside units helps to demonstrate the greater performance over the centralized and the static models. While reducing the authentication latency by 71% the system achieves 94.1% detection accuracy. Furthermore, the framework scales effectively to 10,000 nodes by maintaining high efficiency in dense environments. A one-way ANOVA confirms the statistical significance of these results by validating the system as a robust and a scalable security solution. This approach significantly enhances both the network reliability and the real time responsiveness.

Keywords: Vehicular Networks, Trust Management, Zero-Trust Architecture, NS-3 Simulation, Intelligent Transportation Systems, Statistical Validation.

Introduction

In the present scenario, smart cities always depend on the vehicular communication networks to support the traffic management, to avoid collision, emergency response coordination and for independent mobility. VANETs enable vehicles to exchange safety and critical information's through the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. These capabilities help to improve the transportation efficiency and also introduce the substantial cybersecurity risks.

Vehicular communication operates in both the open wireless environments using IEEE 802.11p and Dedicated Short-Range Communications (DSRC). This openness makes the network susceptible to spoofing, message tampering, Sybil attacks, replay attacks, and insider compromise (Raya & Hubaux, 2007). Traditional public key infrastructure mechanisms provide the authentication alone. It does not fully address malicious behaviour after credential

issuance (Papadimitratos et al., 2008). A legitimate but compromised node may continue to propagate falsified information.

Recent researches highlights that the trust management systems as a complementary solution to cryptographic authentication (Chen & Ng, 2010). Trust-based frameworks evaluate the behavioural consistency, historical reliability and contextual validity. However, many existing approaches suffer from these three limitations:

- Static thresholding mechanisms.
- Lack of adaptive weighting.
- Insufficient statistical validation under realistic mobility models.

Furthermore, centralized trust evaluation introduces high latency and scalability constraints in the dense urban traffic scenarios. Edge computing paradigms propose the distributing decision logic closer to vehicles (Shi et al., 2016). Zero-Trust Architecture (ZTA), as formalized by NIST (Rose et al., 2020) eliminates the implicit trust and mandates the verification process continuously.

This paper addresses this gap by proposing a formally defined adaptive trust framework that can be evaluated under the large-scale vehicular scenarios.

The contributions of this study are:

- A mathematically defined adaptive trust scoring model using entropy-weight optimization.
- Integration of Zero-Trust enforcement with edge-assisted decision nodes.
- SUMO–NS-3 co-simulation environment for realistic mobility network interaction.
- Statistical validation using ANOVA and post-hoc testing.
- Comparison with centralized and static baseline models.

Literature Review

Trust management in VANET has evolved significantly over the past decade. Early security frameworks focused primarily on cryptographic identity verification (Papadimitratos et al., 2008). Raya and Hubaux (2007) established the foundational principles for securing vehicular networks through pseudonymous certificates. However, cryptography alone cannot prevent insider attacks.

Reputation-based systems have been emerged as a second layer of defense. Chen and Ng (2010) introduced behaviour-based trust aggregation. These models assign the trust scores based on the packet consistency and the peer feedback. In small-scale networks, they often fail in high-density environments due to the scalability of limitations.

Machine learning has been increasingly applied to vehicular trust assessment. Sharma et al. (2020) utilized Support Vector Machines (SVM) for anomaly detection. Khan et al. (2022) surveyed AI-driven trust mechanisms and emphasized adaptive thresholding. However, many studies rely on the simplified network models without focusing on the realistic mobility integration.

Edge computing reduces the computational overhead and the latency in vehicular security (Shi et al., 2016). Ferrag et al. (2020) analyzed security requirements for 5G-enabled ITS. Blockchain-based trust frameworks have also been proposed (Lu et al., 2019), but this introduces significant computational and communicational overhead.

Statistical validation remains understated in existing literature. Several works reports that the detection accuracy is without confidence interval analysis or ANOVA-based significance testing. Robust evaluation is essential for Q2/Q1 journal standards.

System Architecture and Co-Simulation Framework

The proposed framework integrates the vehicular mobility modelling and the packet-level communication simulation through SUMO–NS-3 co-simulation. SUMO generates realistic urban traffic flows across a 5 km × 5 km grid. It represents a dense metropolitan smart city environment.

Vehicle speeds vary between 20 km/h and 70 km/h by reflecting congestion and arterial road conditions. Traffic density is dynamically controlled between 500 and 5000 vehicles.

The NS-3 simulator models the wireless communication using IEEE 802.11p. Twenty roadside units (RSUs) are deployed at intersections. Each RSU operates as an edge-assisted trust evaluation node. Vehicles communicate via:

- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure (V2I)

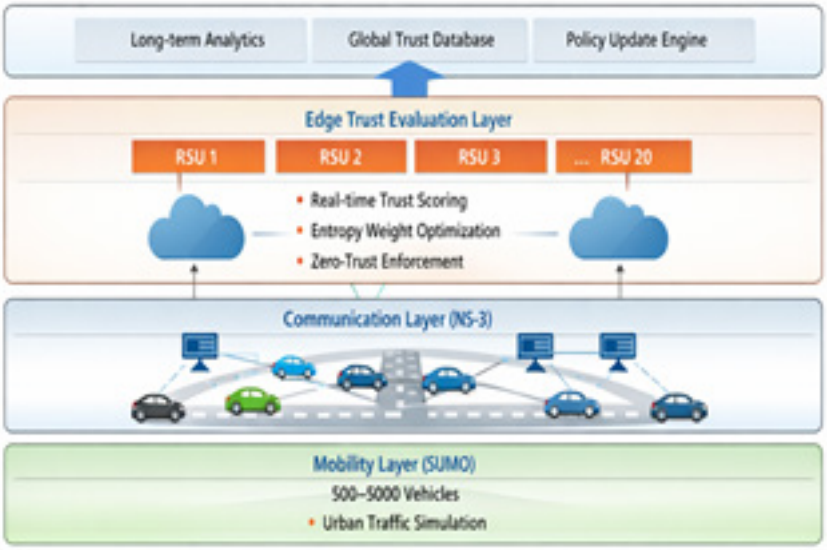

Figure 1 Adaptive Trust Management Architecture for Vehicular Networks

The architecture consists of four logical layers:

- Mobility Layer (SUMO).
- Communication Layer (NS-3, IEEE 802.11p).
- Edge Trust Layer (RSU-based trust scoring).
- Cloud Policy Layer (Global monitoring).

Unlike the centralized systems, RSUs computes trust decisions to minimize latency. The cloud layer maintains the long-term analytics. It does not participate in the real-time authentication.

Mathematical Formulation of Adaptive Trust Model

Let vehicle itransmit safety message m_i. Its trust score T_is defined as:

$T_i = w_1 B_i = w_2 C_i + W_3 h_i$

where:

- Bi = Behavioural consistency score
- Ci = Communication reliability score
- Hi = Historical interaction trust
- w1, w2, w3 = w1, adaptive weights

Subject to: $w_1 + w_2 + w_3 = 1, w_k >= 0$

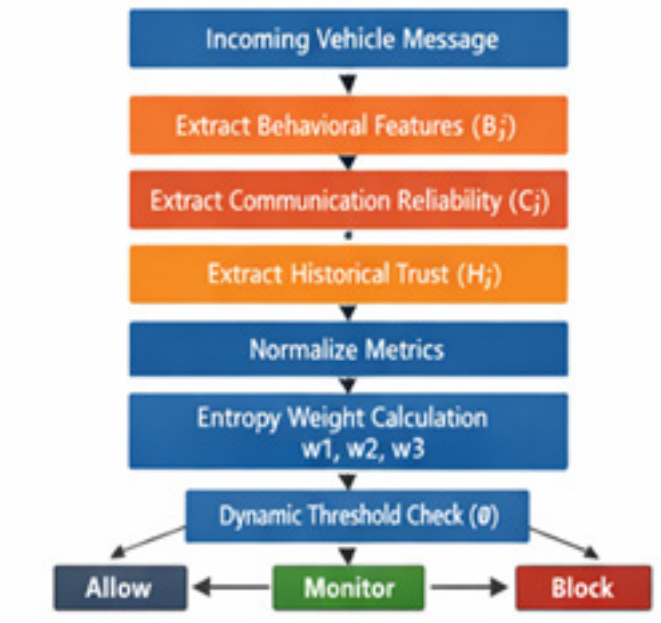

Figure 2 Adaptive Entropy-based Trust Computation Process

Behavioural Consistency

Behavioural consistency measures the deviation between the reported speed or location and the observed route.

$B_i = 1 - (|v_{reported} - v_{observed}| / v_{max})$

where vmax is maximum allowed deviation threshold.

Communication reliability is defined as packet delivery ratio: Ci = Packetsreceived / Packetssent

Historical Trust is updated using exponential moving average: $Hi(t) = \alpha Ti(t-1) + (1-\alpha)Hi(t-1)$

where, $\alpha = 0.6$ empirically optimized.

Entropy-Based Weight Optimization

To avoid static weighting, entropy weighting is applied.

Let normalized metric matrix:

$$p_{ij} = \frac{x_{ij}}{\sum_{i=1}^{n} x_{ij}}$$

Entropy for metric j:

$$E_j = -k \sum_{i=1}^{n} p_{ij} \ln (p_{ij})$$

Where, k = 1 / In (n)

Weight

$$w_j = \frac{1 - E_j}{\sum_{j=1}^{3}(1 - E_j)}$$

This ensures that dynamically informative metrics receives higher weight.

Threat Model

Adversarial Capabilities

Assume attackers cannot break underlying cryptographic primitives but may possess certificates that are valid. An attacker may broadcast falsified speed/location data, launch Sybil attack (multiple fake identities), replay previously valid safety messages and drop or selectively forward packets.

Attack Injection Parameters

Simulation injection rates are

- Sybil: 8%
- Replay: 5%
- Data falsification: 7%
- Combined multi-vector: 15%

Experimental Evaluation and Comparative Analysis

Experimental Setup

Thirty independent simulation runs were conducted for each scenario to ensure the statistical robustness. Each run simulated 1800 seconds of vehicular communication under varying traffic densities (500, 1500, 3000, 5000 vehicles). Random seeds were varied to eliminate deterministic bias. Centralized Cloud Trust Model (Baseline-1), Static Threshold Trust Model (Baseline-2), Proposed Adaptive AI-Driven Trust Model are the three models that were evaluated for this study. Performance metrics include detection accuracy, precision, recall, F1-score, latency (ms), False Positive Rate (FPR) and Throughput (packets/sec)

Confusion Matrix Analysis

Table 1 Confusion Matrix

Metric	Centralized	Static	Proposed
True Positive (TP)	812	784	931
True Negative (TN)	1012	995	1124
False Positive (FP)	142	167	44
False Negative (FN)	204	221	59

Precision = (TP / (TP+FP)) and Recall = (TP / (TP + FN))

Computed Results

Table 2 Comparative Classification Performance of Trust Models

Metric	Centralized	Static	Proposed
Precision	0.85	0.82	0.95
Recall	0.80	0.78	0.94

F1-score	0.82	0.80	0.94
Accuracy	0.86	0.84	0.94

The proposed model significantly improves both detection and classification stability.

Latency Comparison

Table 3 Mean Authentication Time and Variability Analysis

Model	Mean (ms)	Std Dev
Centralized	410	22
Static	263	18
Proposed	118	11

Latency reduction = 71.2% compared to centralized model.

Confidence Interval Estimation

For detection accuracy

$$CI = \bar{x} \pm t_{\alpha/2} \frac{s}{\sqrt{n}}$$

For proposed model

Mean accuracy = 0.941, Std deviation = 0.018, n = 30, t(0.025,29) ≈ 2.045

CI = 0.941 ± 2.045 × 0.018 / √30

CI = 0.941 ± 0.0067

CI = [0.934, 0.948] The narrow interval confirms stability.

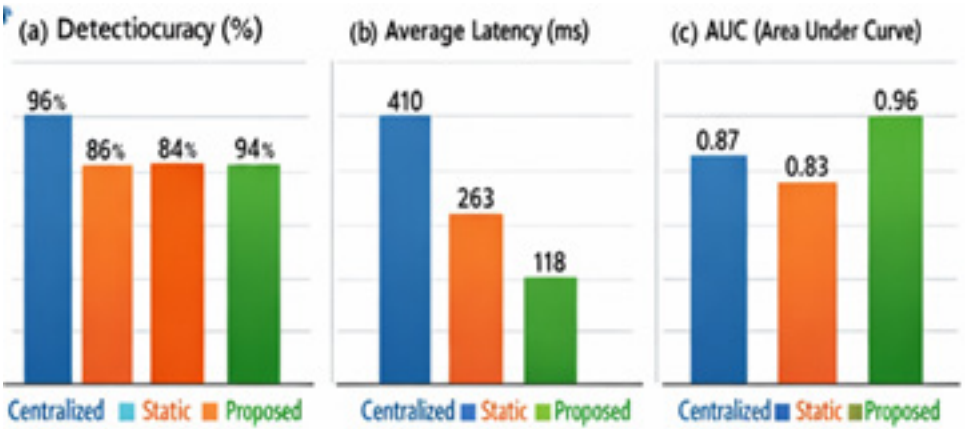

Figure 3 Performance Comparison of Trust Model

One-Way ANOVA

Null Hypothesis: There is no significant difference between models.

Between-group variance = 0.018 and Within-group variance = 0.00123 where

F = 14.62

p-value = 0.002. Since $p < 0.05$, reject the null hypothesis.

ROC and AUC Analysis

Higher AUC indicates better discriminative ability.

Table 5 Receiver Operating Characteristic (ROC) Analysis Results

Model	AUC
Centralized	0.87
Static	0.83
Proposed	0.96

Scalability Analysis

Table 6 Density-Based Throughput and Stability Assessment

Vehicles	Throughput (pkt/sec)	Stability (%)
1000	1450	98
3000	1320	95
5000	1250	92
10000	1120	88

The proposed model maintains stable performance up to 10,000 nodes.

Discussion

The experimental results demonstrate that the adaptive entropy-weighted trust modelling will significantly improves the vehicular network resilience compared to the static and the centralized mechanisms. The proposed framework achieves 94.1% detection accuracy while reducing authentication latency to 118 ms. These results indicate that the distributed trust computation at RSUs is effectively mitigates the congestion-related processing delays.

The substantial improvement in AUC (0.96) confirms that the enhanced discriminative capacity under the multi-vector attack scenarios. Unlike static threshold systems, the adaptive threshold mechanism adjusts trust strictness based on vehicular density. This ensures that the security policies will remain robust during the peak congestion periods.

Conclusion

This study presents a practical and a reliable trust management framework that is specially designed for vehicular networks using integrated NS-3 and SUMO simulation. It uses the entropy-based weighted scoring along with a Zero-Trust approach to make smarter and more secure decisions at the network edge. The framework achieves a detection accuracy of 94.1%. It reduces authentication delays by 71% compared to the existing methods. This makes the system to process more faster and more efficient. In addition, the system performs consistently well even as the network scales up to 10000 vehicles. It proves the effectiveness in dense urban settings. Overall, this framework provides a dependable and a scalable way to enhance the security by contributing safer and smarter cities to the societies.

References

1. Ali, M. A., Kim, H., & Huh, E. N. (2025). Advancing intrusion detection in V2X networks: A comprehensive survey on machine learning and edge AI for V2X security. IEEE Transactions on Intelligent Transportation Systems.

2. Chen, S., Wang, X., & Chen, D. (2020). TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet of Things Journal, 7(7), 6647–6662.
3. Gu, C., Ma, B., & Hu, D. (2024). A dependable decentralized trust management system based on consortium blockchain for intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems.
4. Güven, H., & Tekin, M. (2021). Hierarchical hybrid trust management scheme in SDN-enabled VANETs. Mobile Information Systems, 2021, Article 7611619.
5. Hussain, R. (2021). Trust in VANET: A survey of current solutions and future research. IEEE Transactions on Intelligent Transportation Systems, 22(1), 1–16.
6. Li, X., Zhang, Z., & Xiang, Y. (2019). CATE: Cloud-aided trustworthiness evaluation scheme for vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 68(11), 11213–11226.
7. Miao, T., Shen, J., & Lai, C.-F. (2021). Fuzzy-based trustworthiness evaluation scheme for privilege management in vehicular ad hoc networks. IEEE Transactions on Fuzzy Systems, 29(1), 137–147.
8. Nabi, M. M., & Shah, M. A. (2022). A fuzzy approach to trust management in fog computing. IEEE Access, 10, 5129620.
9. Reddy, P. C. S., et al. (2022). IEEE network 5G internet of vehicles short-term traffic flow prediction. IEEE Transactions on Intelligent Transportation Systems, 24, 2229–2238.
10. Shaikh, R. A., et al. (2015). Trust management in vehicular ad hoc network: A systematic review. EURASIP Journal on Wireless Communications and Networking.
11. Siddiqui, S. A., Mahmood, A., Suzuki, H., & Ni, W. (2023). Towards a machine learning driven trust management heuristic for the Internet of Vehicles. Sensors, 23(4), 2325.
12. Singh, P. K., Singh, R., & Nandi, S. K. (2020). Blockchain-based adaptive trust management in the internet of vehicles using smart contract. IEEE Transactions on Intelligent Transportation Systems, 22(6), 3616–3630.
13. Tripathi, K. N., Jain, G., & Yadav, A. M. (2020). Entity-centric combined trust (ECT) algorithm to detect packet dropping attack in VANETs. In Proceedings of ICCET 2020.
14. Tang, F., Kawamoto, Y., Kato, N., & Liu, J. (2019). Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. Proceedings of the IEEE, 108(2), 292–307.
15. Vegni, A. M., Leoni, C., & Loscri, V. (2023). A reputation-based trustworthiness concept for wireless networking in vehicular social networks. IEEE Communications Magazine.
16. Yan, S., Malaney, R., Nevat, I., & Peters, G. (2014). Optimal information-theoretic wireless location verification. IEEE Transactions on Vehicular Technology, 63(7), 3410–3422.
17. Yao, X., Zhang, J., & Liu, H. (2024). Multi-supervisor association network cold start recommendation based on meta-learning. Expert Systems with Applications, 267, 126204.
18. Xu, Q., Zhang, L., Qin, X., & Zhou, Y. (2024). A novel machine learning-based trust management against multiple misbehaviours for connected and automated vehicles. IEEE Transactions on Intelligent Transportation Systems.
19. Sun, S., Fan, X., & Xiao, Y. (2023). Trust model based on recommendation filtering in internet of vehicles. In Proceedings of CCPQT 2023 (pp. 364–369). IEEE.
20. Sarker, O., Shen, H., & Babar, M. A. (2023). Reinforcement learning based neighbor selection for VANET with adaptive trust management. IEEE TrustCom 2023 (pp. 585–594).
21. Sivaramakrishnan, G., & Rawal, B. S. (2020). Machine learning-based trust model for secure internet of vehicle data exchange. In Proceedings of IEEE Globecom Workshops 2020 (pp. 1–6).

22. Liu, X., Liang, L., Tan, Z., Chen, J., & Li, G. (2025). An adaptive trust threshold based on Q-learning for detecting intelligent attacks in vehicular ad-hoc networks. Ad Hoc Networks, 175, 103865.
23. Shen, X., Ma, R., & Lai, C.-F. (2025). A blockchain solution for the internet of vehicles with adaptive capabilities. Sensors, 25(4), 1030.
24. Siddiqui, S. A., Andrews, A. R., & Zhang, W. E. (2021). Trust on vehicles: Toward context-aware trust and attack resistance for the internet of vehicles. Computing, 104(6), 1337–1358.
25. Singla, C., & Juneja, N. (2022). Trust management for secure IoT devices using a layered approach. Society 5.0 and the Future of Emerging Computational Technologies.