

An Intelligent Trust-Based Dissemination Framework for VANETs Using Reinforcement Learning and Edge-Assisted Validation

Anurag Gupta¹, Anil Kumar Sagar²

^{1,2} Department of CSE, School of Engineering and Technology,
Sharda University, Greater Noida, India
03anuraggupta@gmail.com, aksagar22@gmail.com

Abstract. Vehicular ad hoc networks are a key communication component of intelligent transportation systems, where timely and reliable dissemination of critical information is essential for safety and traffic efficiency. Nevertheless, rapid topology changes, intermittent connectivity, and malicious node behavior can degrade dissemination reliability and increase communication delay. This paper presents a trust-based dissemination framework that combines context-aware trust evaluation, reinforcement learning-based dissemination control, and edge-assisted validation to improve secure and efficient data exchange among vehicular nodes. Local trust is computed from forwarding reliability, message consistency, plausibility assessment, historical cooperation, and delay-aware behavior. Based on these trust observations and network conditions, a Q-learning agent adaptively selects forwarding, cautious forwarding, rerouting, holding, or isolation actions. To further enhance decision accuracy and reduce false positives, nearby roadside edge units perform regional corroboration and suspicious-event validation for uncertain or suspicious events. The proposed framework is intended to enhance dissemination reliability, reduce end-to-end delay, and improve resilience against malicious behavior in dynamic vehicular environments. Overall, it offers a scalable and intelligent approach for secure, reliable, and low-latency vehicular communication.

Keywords: VANETs · Trust management · Critical data dissemination · Reinforcement learning · Edge-assisted validation · Malicious node detection · Low-latency communication · Intelligent transportation systems

1 Introduction

VANETs are instrumental in enhancing the communication features of intelligent transportation systems. They enable the exchange of critical information among vehicles as well as between vehicles and roadside infrastructures that improve road safety, provide traffic awareness, and enhance transportation efficiency [10, 13]. Intelligent transport communications are therefore regarded as a key building block for safer, more efficient, and more reliable next-generation transport services [10]. Comparative simulation studies have further shown that

the choice of V2V and routing protocol strongly affects delivery ratio, delay, and coverage in realistic traffic conditions [9, 16].

A message in a VANET can include a time-sensitive braking message, an accident notification, a road hazard message, or a message about an approaching traffic jam. Because these messages carry critical safety information, one must analyze the quality of message dissemination beyond the scope of packet reachability. Factors like accuracy, timeliness, and reliability should all be considered. Unfortunately, in a VANET, the environment is highly dynamic and decentralized. This makes the forwarding decision highly localized and limited; in many instances, the complete state of the forwarding environment is unknown. Beyond these forwarding constraints, unreliable communication can severely affect safety. Malicious or untrustworthy vehicles can cause major harm by sending false or outdated messages, dropping messages, or manipulating the forwarding environment, all of which degrade the routing and forwarding decisions of the network [7, 12]. It has been observed that decentralized trust management is increasingly important in VANETs because conventional security mechanisms do not fully address behavioral misuse after authentication [1, 14].

Trust management therefore complements authentication by evaluating how nodes behave rather than only who they claim to be [11]. Existing trust-based studies in VANETs have increasingly focused on combining node behavior, message plausibility, and historical interaction evidence in order to identify malicious nodes and false-message anomalies more effectively [4, 15, 20]. In particular, hybrid-trust approaches have shown that integrating direct and indirect trust indicators, contextual validation, and behavior-aware assessment can improve the robustness of vehicular communication [15, 20].

At the same time, reinforcement learning has shown strong potential for adaptive dissemination and trust-aware forwarding decisions in vehicular environments. Instead of relying on fixed trust thresholds, reinforcement learning enables a vehicle to learn forwarding behavior from repeated interactions with neighboring nodes and changing network conditions. Sarker et al. demonstrated that reinforcement-learning-based neighbor selection with adaptive trust management can reduce packet dropping and improve response speed in adversarial VANET scenarios, indicating that learning-based forwarding is more suitable than static decision policies in highly dynamic networks [18]. AI-driven VANET architectures for IoT-enabled transportation systems further support this learning-based direction [19].

Another important technological direction is vehicular edge computing. Edge-supported roadside infrastructure can provide real-time assessment of suspicious behavior using local contextual data and corroboration from nearby vehicles, without the delay of remote cloud processing. The survey of vehicular edge computing identifies localized intelligence, low-latency computation, and proximity-based decision support among the characteristics of edge-assisted vehicular systems [13]. These features make edge computing an appropriate means of validating suspicious critical events and supporting trust-aware dissemination, provided that data privacy at the edge is preserved [3, 13].

Building on our earlier trust-based VANET framework [8], this paper introduces a trust-centric dissemination framework that utilizes reinforcement learning and edge-assisted validation within VANETs. The framework is built around three central ideas: (1) streamlining the efficiency of information exchanges; (2) increasing the reliability of crucial data dissemination; and (3) minimizing worst-case communication delay, while preserving resilience against malicious behavior. Through the incorporation of local trust intelligence and expedient edge verification, this framework is envisioned to fill the gap for flexible, practical, and secure intelligent vehicular communication [1, 18, 21].

1.1 Main Contributions

The main contributions of this work are summarized as follows:

1. A trust-based dissemination architecture is proposed for VANETs that integrates local trust computation, Q-learning-based dissemination control, and edge-assisted validation in a unified framework for secure and efficient forwarding.
2. A context-aware trust formulation is developed using forwarding reliability, message consistency, plausibility assessment, historical cooperation, and delay-aware behavior.
3. A reinforcement-learning-based dissemination engine is introduced to adapt forwarding actions dynamically instead of relying on static trust thresholds.
4. An edge-assisted validation layer is incorporated to corroborate suspicious critical events through RSU or MEC support.
5. The proposed framework is designed to jointly improve dissemination efficiency, reliability, and delay performance under dynamic and adversarial vehicular conditions.

2 Related Work and Research Gap

Trust management is vital in VANETs. For example, it is not enough to verify the identity of a transmitting vehicle as the vehicle might still be untrustworthy. Carriers of legitimate credentials might also send false warnings, replay out-of-date messages, drop messages selectively, and manipulate trust feedback. This is why decentralized trust management is seen to be a complement to security mechanisms in vehicular settings [1].

Existing studies on VANET trust management mainly focus on hybrid and context-aware trust models [6]. For malicious-node detection and false-message filtering, Xu et al. have developed a model that combines node behavior, message plausibility, and traces of past interactions. Xu et al. have also shown that behavior-aware trust assessments strengthen the detection of malicious nodes in

dynamically formed vehicular clusters [20]. Byeon et al. developed a distributed trust management scheme to identify and combat malicious nodes and false-message anomalies. The work shows the advantages of using a variety of trust indicators to combat adversary challenges in a VANET [4]. Qi et al. proposed a hybrid trust-based model that integrates entity trust and message consistency. Their model increases the reliability of message dissemination in adverse environments [15]. Machine-learning-based adaptive intrusion detection has also been explored for real-time threat mitigation [2]. Although these methods improve trust evaluation, their main focus is the detection and verification of malicious nodes rather than adaptive dissemination control [4, 15, 20].

Reinforcement learning has also been studied for adaptive trust-aware communication. Sarker et al. introduced a framework for neighbor selection that uses reinforcement learning along with adaptive trust management. They demonstrated that learning-based neighbor selection for message forwarding helps reduce packet dropping and increases the speed of responses even in the presence of attackers within vehicular networks [18]. In other work, the application of deep reinforcement learning in the domain of trust-aware communication among connected vehicles has shown that trust-aware, learning-based communication for connected vehicles is superior to fixed message forwarding in dynamic vehicular networks [21, 22], and deep reinforcement learning has likewise been applied to QoS-aware routing in IoT networks [5]. Nevertheless, these approaches mainly adapt message forwarding and do not incorporate low-latency regional validation of suspicious behavior [18, 21].

Vehicular edge computing stands out as another significant innovation by offering low-latency localized intelligence in proximity to vehicles. Edge-assisted infrastructure can undertake real-time verification, regional confirmation, and faster dissemination decisions without remote cloud processing. Meneguetto et al. highlighted that vehicular edge computing offers localized processing and low-latency service support, making it suitable for time-sensitive vehicular applications [13]. Nevertheless, edge support is often treated separately from trust-aware dissemination control in existing VANET frameworks [13].

Based on the above discussion, the main research gap is the absence of a unified dissemination-oriented framework that jointly integrates context-aware trust computation, reinforcement-learning-based dissemination adaptation, and edge-assisted validation. Existing hybrid-trust methods improve misbehavior detection [4, 15, 20], reinforcement-learning-based approaches improve forwarding adaptability [18, 21], and edge computing improves localized intelligence [13], but these components are rarely combined into a single framework for reliable and low-delay dissemination of critical data in VANETs [1, 13, 18]. This paper addresses that gap by proposing an intelligent trust-based dissemination framework that tightly integrates these three components within one architecture. Table 1 summarizes the related work.

Table 1: Summary of related work and identified research gap

Author & Year	Approach	Main Focus	Strengths	Limitation
M. Al-Marshoud et al., 2024	Decentralized trust management survey	Security, privacy, and decentralized trust in VANETs	Establishes the need for behavior-aware and decentralized trust mechanisms	Does not propose an integrated dissemination framework
R. I. Meneguetto et al., 2021	Vehicular edge computing survey	Edge architecture, localized intelligence, low-latency vehicular services	Highlights the benefit of edge-assisted validation and local decision support	Does not focus specifically on trust-aware dissemination
O. Sarker et al., 2023	RL-based neighbour selection with adaptive trust	Reinforcement-learning-based trust-aware neighbour selection	Improves adaptability, reduces packet dropping, and enhances response speed	Focuses mainly on neighbour selection rather than full dissemination validation
D. Zhang et al., 2018	Deep RL-based trust management	Trust-aware connected-vehicle communication using deep reinforcement learning	Demonstrates the effectiveness of learning-based trust decisions in dynamic environments	Lacks integrated edge-assisted corroboration for suspicious events
X. Xu et al., 2025	Hybrid trust model for node-centric misbehavior detection	Behavior-aware malicious-node detection	Improves node-centric trust assessment in dynamic vehicular clusters	Focuses more on detection than adaptive dissemination control
H. Byeon et al., 2025	Distributed trust management against malicious nodes and false-message anomalies	Detection of malicious nodes and false-message anomalies	Combines multiple trust indicators for improved robustness	Does not fully incorporate learning-based forwarding adaptation
J. Qi et al., 2024	Hybrid-trust-based emergency message dissemination	Trust and consistency analysis for emergency messages	Improves message reliability under adversarial conditions	Does not integrate reinforcement learning or edge-assisted validation

3 Proposed Framework Architecture

The proposed architecture is organized into five functional layers: (i) vehicular communication environment, (ii) critical message classification, (iii) local trust evaluation, (iv) RL-based dissemination decision engine, and (v) edge-assisted validation. A secure response module controls blacklist updates, alerts and trust-table updates after confirmed malicious activity. Most decisions are made locally and with lightweight computation, which suits time-sensitive situations. In ambiguous cases, the design allows verification through nearby infrastructure.

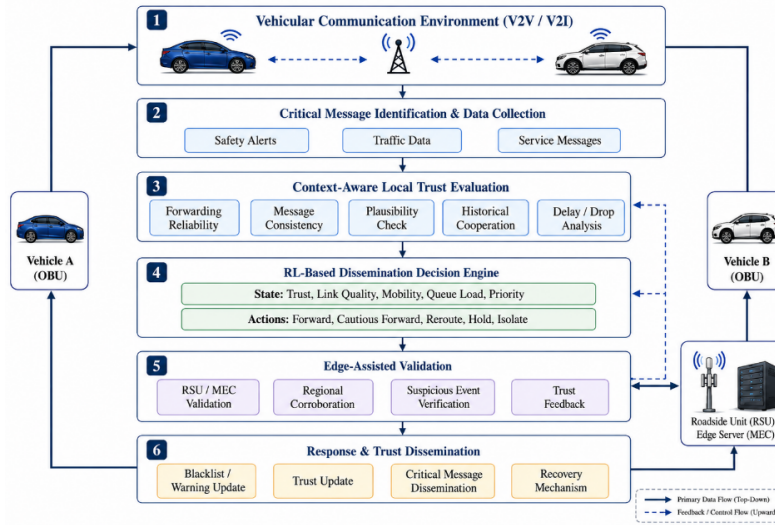


Fig. 1: An intelligent trust-based dissemination framework for VANETs

The step-wise operation of the VANET framework is shown in Fig. 1. In the first step, vehicles communicate by sending and receiving different messages. The trustworthiness of the neighboring vehicles is evaluated by the system based on their forwarding behavior, delay, and accuracy of the messages. Next, the RL-based decision module decides whether the message is forwarded normally, forwarded cautiously, rerouted, held for checking, or blocked. For any suspicious behavior, the RSU or edge server corroborates the incident with data available in its vicinity. In the last step, the system refreshes trust values, issues alerts, and transmits only verified critical messages that bolster secure and trustworthy communication.

4 System Model and Problem Formulation

The VANET is represented as a continuously changing graph $G(t) = (V(t), E(t))$. Here, $V(t)$ is the set of vehicles and roadside units at time t , and $E(t)$ is the set of links established by nodes in the vicinity of one another

that are in the transmission range. Vehicles disseminate safety, traffic, and service messages over V2V and V2I links. The graph changes constantly because of high mobility and shifting neighborhoods.

Consider node i observing the behavior of neighboring node j . The local trust of node j at time t is determined by a set of behavior and context indicators:

$$T_{ij}(t) = w_1 F_{ij}(t) + w_2 C_{ij}(t) + w_3 P_{ij}(t) + w_4 H_{ij}(t) - w_5 D_{ij}(t), \quad (1)$$

where $F_{ij}(t)$ is forwarding reliability, $C_{ij}(t)$ is message consistency, $P_{ij}(t)$ is plausibility, $H_{ij}(t)$ is historical cooperation, and $D_{ij}(t)$ are delay/drop anomalies. The coefficients $w_1, \dots, w_5$ are weight factors with $\sum_k w_k = 1$. This multi-factor trust design is aligned with recent hybrid trust models for malicious-node and false-message detection [4, 20].

To prevent sudden trust fluctuations in rapidly changing vehicular scenarios, the trust value is smoothed with

$$\hat{T}_{ij}(t) = \lambda \hat{T}_{ij}(t-1) + (1-\lambda) T_{ij}(t), \quad (2)$$

where $0 < \lambda < 1$ denotes the forgetting factor. The smoothed trust value is classified into three states of trust: trusted, uncertain, and suspicious. This state of trust is included in the inputs of the dissemination decision engine.

The dissemination decision process is modelled as a reinforcement learning problem. At discrete time step t , the state of the agent is described as

$$s_t = \{\text{trust state, link quality, message priority, mobility stability, queue load}\}. \quad (3)$$

The action set is defined as

$$A = \{a_1, a_2, a_3, a_4, a_5\}, \quad (4)$$

where a_1 = forward, a_2 = cautious forward, a_3 = reroute, a_4 = hold for validation, and a_5 = isolate/report. The Q-learning update rule is defined as

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha \left[r_t + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t) \right], \quad (5)$$

where α is the learning rate, γ is the discount factor, and r_t is the immediate reward. RL-based adaptive trust decisions of this kind have been shown to improve performance in attacker-prone vehicular environments [18].

The reward function is designed to optimize the efficiency, reliability, and security of dissemination:

$$r_t = \beta_1 \text{PDR}_t - \beta_2 \text{Delay}_t - \beta_3 \text{Drop}_t + \beta_4 \Delta T_t + \beta_5 \text{EdgeConfirm}_t - \beta_6 \text{FalseIsolation}_t, \quad (6)$$

where PDR_t rewards successful delivery, Delay_t penalizes latency, Drop_t penalizes packet loss, ΔT_t rewards trust-consistent decisions, EdgeConfirm_t rewards correct edge-confirmed decisions, and FalseIsolation_t penalizes incorrect isolation of benign nodes. This formulation ensures that the framework remains dissemination-oriented while retaining strong malicious-behavior resistance.

4.1 Dissemination Algorithm

Algorithm 1 gives the complete procedure.

Algorithm 1 describes the operational flow of the proposed intelligent trust-based dissemination framework. The first step is the setup of the VANET topology, trust tables, and Q-learning parameters. For each received message, a priority level is assigned first; local trust is then estimated from forwarding reliability, message consistency, message plausibility, historical cooperation, and delay and drop behavior. The resulting trust value is smoothed, and a discrete trust state is assigned. This state is then combined with the state of the link and the network to create the RL state. The Q-learning agent then selects the most appropriate action. An uncertain or suspicious trust state invokes edge-assisted validation, supported by the RSU/MEC, and the final trust value is obtained by fusing local trust with edge verification. The reward is then calculated, the Q-table is updated, and confirmed malicious nodes are added to the blacklist and warning tables. This process repeats throughout the simulation, enabling flexible, trusted, and secure information delivery in disruptive VANET environments.

4.2 Simulation Setup and Evaluation Metrics

The framework can be assessed within a MATLAB simulation environment for various scenarios in VANETs, such as low and high-density traffic, high mobility, false-message injection, selective forwarding, and malicious-node attacks. For example, consider a simulation with a road area of 1000 m by 1000 m, 50 to 200 nodes, a 250 m transmission range, and a 300 s simulation time (Table 2). This configuration will help analyze the proposed framework's dissemination performance and security behavior for varying vehicular dynamics.

Performance should be measured using PDR, End-to-End Delay, Detection Rate, FPR, Throughput, Trust Convergence Time, Routing Overhead, Critical Message Success Ratio, Precision, Recall, and F1-score. Evaluation with these metrics provides a balance between communication efficiency and detection of malicious nodes.

For comparative analysis, the proposed framework can be benchmarked against: (i) static trust-based dissemination, (ii) hybrid trust-based malicious-node detection, (iii) RL-based adaptive neighbor selection, and (iv) edge-free trust dissemination approaches. Such a comparison helps demonstrate the benefit of integrating context-aware trust computation, reinforcement-learning-based dissemination adaptation, and edge-assisted validation within a unified dissemination framework.

5 Comparative Models with Proposed Framework

For comparative evaluation, the proposed framework is benchmarked against three representative models from the literature (Table 3): (i) RL-based adaptive

Algorithm 1 Intelligent trust-based dissemination with edge-assisted validation

Input: Dynamic VANET graph $G(t) = (V(t), E(t))$; message set M ; trust weights $w_1, \dots, w_5$; forgetting factor λ ; trust thresholds $\theta_l, \theta_h, \theta_m$; Q-learning parameters $\alpha, \gamma, \varepsilon$; edge-fusion factor μ .

Output: Adaptive dissemination decision, updated trust values, blacklist/warning updates, and verified critical-message forwarding.

1. Initialize the VANET graph $G(t)$, neighbor sets $N_i(t)$, local trust table $\hat{T}_{ij}(0)$, Q-table $Q(s, a)$, blacklist B , and warning table W .
2. For each received message $m \in M$, classify the message as critical, traffic, or service, and assign priority P_m .
3. For each neighbor $v_j \in N_i(t)$, compute the trust indicators:

$$F_{ij}(t) = \frac{N_{ij}^{\text{fwd}}(t)}{N_{ij}^{\text{recv}}(t) + \varepsilon}, \quad C_{ij}(t) = 1 - \frac{N_{ij}^{\text{inc}}(t)}{N_{ij}^{\text{msg}}(t) + \varepsilon},$$

$$P_{ij}(t) = \frac{1}{K} \sum_{k=1}^K p_k(t), \quad H_{ij}(t) = \frac{N_{ij}^{\text{coop}}(t)}{N_{ij}^{\text{int}}(t) + \varepsilon},$$

$$D_{ij}(t) = \eta_1 \frac{\bar{d}_{ij}(t)}{d_{\max}} + \eta_2 \frac{N_{ij}^{\text{drop}}(t)}{N_{ij}^{\text{recv}}(t) + \varepsilon}.$$

4. Compute the instantaneous trust value $T_{ij}(t)$ using Eq. (1).
5. Update the smoothed trust value $\hat{T}_{ij}(t)$ using Eq. (2).
6. Map the trust value into a trust state:

$$S_{ij}^{\text{trust}}(t) = \begin{cases} \text{Trusted,} & \hat{T}_{ij}(t) \geq \theta_h, \\ \text{Uncertain,} & \theta_l < \hat{T}_{ij}(t) < \theta_h, \\ \text{Suspicious,} & \hat{T}_{ij}(t) \leq \theta_l. \end{cases}$$

7. Form the reinforcement-learning state $s_t = [S_{ij}^{\text{trust}}(t), L_{ij}(t), Q_i(t), M_i(t), P_m]$.
8. Select an action $a_t \in A = \{a_1, \dots, a_5\}$ using the ε -greedy policy

$$\pi(s_t) = \begin{cases} \text{random action,} & \text{with probability } \varepsilon, \\ \arg \max_{a \in A} Q(s_t, a), & \text{with probability } 1 - \varepsilon, \end{cases}$$

where a_1 : forward, a_2 : cautious forward, a_3 : reroute, a_4 : hold for validation, a_5 : isolate/report.

9. If $S_{ij}^{\text{trust}}(t)$ is uncertain or suspicious, invoke edge-assisted validation and compute $E_{ij}(t) = \rho_1 R_{ij}(t) + \rho_2 X_{ij}(t) + \rho_3 U_{ij}(t)$; then update the final trust value as $T_{ij}^{\text{final}}(t) = \mu \hat{T}_{ij}(t) + (1 - \mu) E_{ij}(t)$.
 10. Execute the selected dissemination action according to a_t . If $T_{ij}^{\text{final}}(t) \leq \theta_m$ for τ consecutive observation windows, mark node v_j as malicious.
 11. Compute the immediate reward $r_t = \beta_1 \text{PDR}_t - \beta_2 \text{Delay}_t - \beta_3 \text{Drop}_t + \beta_4 \Delta T_t + \beta_5 E_t - \beta_6 F_t$.
 12. Update the Q-table using Eq. (5).
 13. Update the response tables: $B \leftarrow B \cup \{v_j\}$, $W \leftarrow W \cup \{(v_j, t, \text{warning})\}$.
 14. Repeat Steps 2–13 for all messages and nodes until the simulation ends.
-

Table 2: Representative simulation parameters

Parameter	Value
Simulation area	1000 m $\times$ 1000 m
Number of vehicles	50–200
Transmission range	250 m
Simulation duration	300 s
Mobility scenarios	Sparse, dense, and high-mobility traffic
Attack scenarios	False-message injection, selective forwarding, malicious-node behavior
RL actions	Forward, cautious forward, reroute, hold, isolate/report
Evaluation metrics	PDR, delay, detection rate, FPR, throughput, trust convergence time, CMSR, precision, recall, and F1-score

neighbor selection with trust management, (ii) hybrid trust model for node-centric misbehavior detection, and (iii) trust management scheme against malicious nodes and false-message anomaly. These models are selected because they represent the closest and most relevant research directions to the proposed work, namely adaptive trust-aware forwarding, hybrid behavioral trust evaluation, and secure anomaly-aware trust management.

5.1 Results Analysis

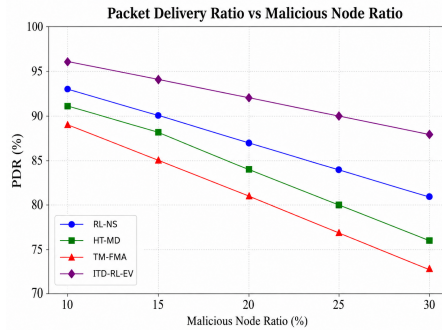


Fig. 2: Packet delivery ratio vs malicious node ratio

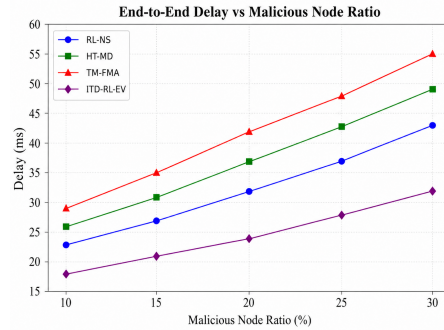


Fig. 3: End-to-end delay vs malicious node ratio

The data in Figs. 2–11 show that ITD-RL-EV outperforms the benchmark models RL-NS, HT-MD, and TM-FMA in almost all metrics. Figs. 2 and 8 show how the proposed model achieves the best Packet Delivery Ratio (PDR) and Critical Message Success Ratio (CMSR) even when the number of malicious nodes increases. This confirms the model's ability to safeguard the reliable

Table 3: Comparative models used for performance evaluation

Model	Citation	Main Focus	Why Compared with Proposed Model
RL-NS: RL-based adaptive neighbor selection with trust management	Sarker et al. (2023)	Adaptive trust-aware forwarding and neighbor selection	Closest RL-based baseline for comparing dissemination adaptation
HT-MD: Hybrid trust model for node-centric misbehavior detection	Xu et al. (2025)	Node-centric malicious-behavior detection using hybrid trust	Strong comparison for multi-factor hybrid trust evaluation
TM-FMA: Trust management scheme against malicious nodes and false-message anomaly	Byeon et al. (2025)	Detection of malicious nodes and false-message anomalies	Suitable secure trust-management baseline for anomaly resistance
ITD-RL-EV: Intelligent trust-based dissemination framework for VANETs using reinforcement learning and edge-assisted validation	This work	Context-aware trust + RL-based dissemination + edge validation	Unified framework combining trust computation, adaptive dissemination, and low-latency validation

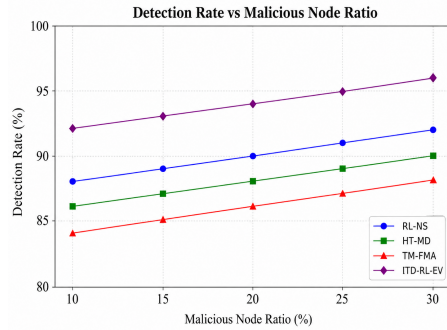


Fig. 4: Detection rate vs malicious node ratio

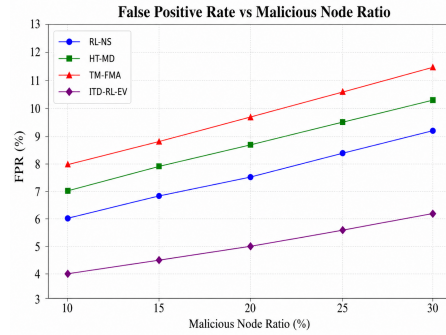


Fig. 5: False positive rate vs malicious node ratio

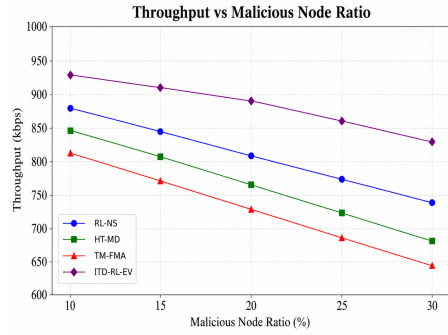


Fig. 6: Throughput vs malicious node ratio

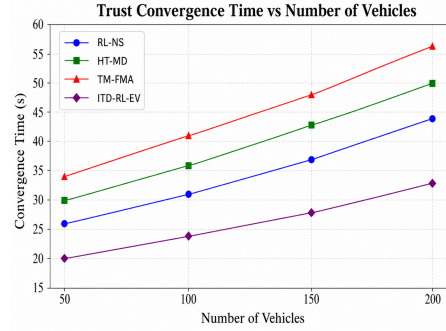


Fig. 7: Trust convergence time vs number of vehicles

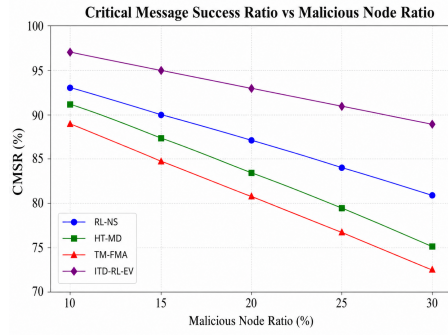


Fig. 8: Critical message success ratio vs malicious node ratio

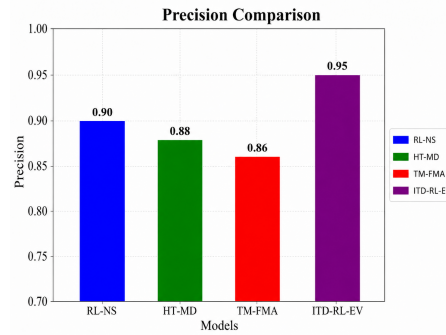


Fig. 9: Precision comparison

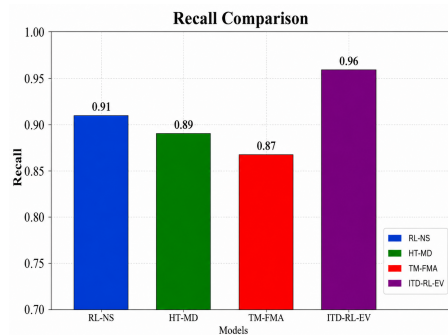


Fig. 10: Recall comparison

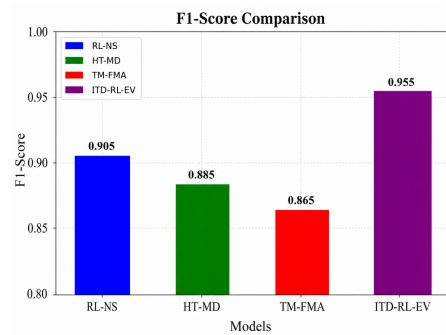


Fig. 11: F1-score comparison

dissemination of normal and safety-critical messages. From Fig. 3, ITD-RL-EV achieves the lowest end-to-end delay, indicating reliable dissemination with minimal latency; this advantage holds as the share of malicious nodes grows. In Fig. 4, we see that the proposed model achieves the highest detection rate, and in Fig. 5, the lowest false positive rate is achieved, which demonstrates more reliable detection of malicious nodes. Again, in Fig. 6, ITD-RL-EV achieves the highest throughput. Fig. 7 shows that the model achieves the fastest trust convergence time. Finally, the classification-oriented comparisons in Figs. 9–11 reveal that the proposed model achieves the best precision, recall, and F1-score, confirming that it provides the most balanced and reliable detection performance among all compared schemes. Overall, the graphical results clearly establish that the integration of context-aware trust computation, reinforcement-learning-based dissemination adaptation, and edge-assisted validation makes ITD-RL-EV a more effective framework for secure, reliable, and efficient information dissemination in VANETs than the existing comparative models.

6 Conclusion

This paper presented ITD-RL-EV, an intelligent trust-based dissemination framework for VANETs that integrates context-aware trust computation, reinforcement-learning-based dissemination adaptation, and edge-assisted validation to improve the reliability, efficiency, and security of critical-message dissemination under dynamic and adversarial vehicular conditions. The comparative evaluation against RL-NS, HT-MD, and TM-FMA demonstrated that the proposed model achieves superior performance in terms of packet delivery ratio, end-to-end delay, detection rate, false positive rate, throughput, trust convergence time, critical message success ratio, precision, recall, and F1-score, thereby confirming that adaptive trust learning with edge corroboration provides a more effective solution for secure and low-latency information dissemination in VANETs. Future work will evaluate the framework in larger and more realistic heterogeneous vehicular scenarios with more variable traffic density and mobility, and will explore deep and multi-agent reinforcement learning. Blockchain-aided trust storage and traceable auditing may further strengthen security [17], and the framework should be tested against more advanced attacks, such as Sybil, replay, collusion, and on/off trust manipulation, to extend it to future IoV and intelligent transportation systems.

References

1. AlMarshoud, M., Kiraz, M.S., Al-Bayatti, A.H.: Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Computing Surveys* **56**(10), 1–39 (2024). <https://doi.org/10.1145/3656166>
2. Ather, D., Kanday, R., Rakhra, M., Kler, R., Aggarwal, G., Jairath, K.: Adaptive intrusion detection systems: Leveraging machine learning for real-time

- threat mitigation. In: 2025 International Conference on Networks and Cryptology (NETCRYPT). pp. 1743–1746. IEEE (2025). <https://doi.org/10.1109/NETCRYPT65877.2025.11102773>
3. Ather, D., Kaur, H., Rakhra, M., Kler, R., Aggarwal, G., Jairath, K.: Data privacy in edge computing: Securing solutions for distributed systems. In: 2025 International Conference on Networks and Cryptology (NETCRYPT). pp. 1747–1752. IEEE (2025). <https://doi.org/10.1109/NETCRYPT65877.2025.11102306>
 4. Byeon, H., Seno, M.E., Srivastava, A.K., AlGhamdi, A., Keshta, I., Soni, M., Prasad, K.D.V., Abdurakhimova, D., Bhatt, M.W.: Trust management scheme for securing vehicular ad hoc networks against malicious nodes and false message anomaly. *Transactions on Emerging Telecommunications Technologies* **36**(4), e70110 (2025). <https://doi.org/10.1002/ett.70110>
 5. Chaudhary, N., Ather, D., Kler, R., Dubey, R., Saxena, U., Singh, G.: Adaptive QoS-aware routing for IoT networks using deep reinforcement learning. In: 2025 International Conference on Intelligent & Innovative Practices in Engineering & Management (IIPEM). pp. 1–5. IEEE (2025). <https://doi.org/10.1109/IIPEM65914.2025.11548315>
 6. Che, H., Duan, Y., Li, C., Yu, L.: On trust management in vehicular ad hoc networks: A comprehensive review. *Frontiers in the Internet of Things* **1**, 995233 (2022). <https://doi.org/10.3389/friot.2022.995233>
 7. Dong, S., Su, H., Xia, Y., Zhu, F., Hu, X., Wang, B.: A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks. *IEEE Transactions on Intelligent Transportation Systems* **24**(12), 13573–13602 (2023). <https://doi.org/10.1109/TITS.2023.3297527>
 8. Gupta, A., Sagar, A.K.: A trust-based framework for enhancing security and reliability in vehicular ad-hoc networks (VANETs). In: 2024 International Conference on Computing, Sciences and Communications (ICCSC). pp. 1–6. IEEE (2024). <https://doi.org/10.1109/ICCSC62048.2024.10830436>
 9. Khan, R.L., Singh, R., Vijay, R., Kumar, R., Singh, A., Ather, D.: Evaluating the impact of different routing protocols on VANET performance. In: 2023 12th International Conference on System Modeling & Advancement in Research Trends (SMART). pp. 308–314. IEEE (2023). <https://doi.org/10.1109/SMART59791.2023.10428409>
 10. Lee, M., Atkison, T.: VANET applications: Past, present, and future. *Vehicular Communications* **28**, 100310 (2021). <https://doi.org/10.1016/j.vehcom.2020.100310>
 11. Li, W., Song, H.: ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems* **17**(4), 960–969 (2016). <https://doi.org/10.1109/TITS.2015.2494017>
 12. Mazhar, S., Rakib, A., Pan, L., Jiang, F., Anwar, A., Doss, R., Bryans, J.: State-of-the-art authentication and verification schemes in VANETs: A survey. *Vehicular Communications* **49**, 100804 (2024). <https://doi.org/10.1016/j.vehcom.2024.100804>
 13. Meneguette, R., De Grande, R., Ueyama, J., Rocha Filho, G.P., Madeira, E.: Vehicular edge computing: Architecture, resource management, security, and challenges. *ACM Computing Surveys* **55**(1), 1–46 (2021). <https://doi.org/10.1145/3485129>
 14. Mundhe, P., Verma, S., Venkatesan, S.: A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Computer Science Review* **41**, 100411 (2021). <https://doi.org/10.1016/j.cosrev.2021.100411>

15. Qi, J., Zheng, N., Xu, M., Chen, P., Li, W.: A hybrid-trust-based emergency message dissemination model for vehicular ad hoc networks. *Journal of Information Security and Applications* **81**, 103699 (2024). <https://doi.org/10.1016/j.jisa.2024.103699>
16. Raj, D., Ather, D., Sagar, A.K.: Advancing vehicular ad-hoc network solutions in emerging economies: A comparative analysis of V2V protocols through simulation studies. *SN Computer Science* **5**(8), 1077 (2024). <https://doi.org/10.1007/s42979-024-03411-1>
17. Rawat, G.S., Singh, K., Shariq, M., Das, A.K., Chaudhry, S.A., Lorenz, P.: BTC2PA: A blockchain-assisted trust computation with conditional privacy-preserving authentication for connected vehicles. *IEEE Transactions on Intelligent Transportation Systems* **26**(1), 1134–1148 (2025). <https://doi.org/10.1109/TITS.2024.3488184>
18. Sarker, O., Shen, H., Babar, M.A.: Reinforcement learning based neighbour selection for VANET with adaptive trust management. In: 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 585–594. IEEE (2023). <https://doi.org/10.1109/TrustCom60117.2023.00091>
19. Singh, R., Kumar, R., Singh, A., Vijay, R., Khan, R.L., Ather, D.: AI-driven VANETs for IoT-enabled transportation systems. In: Artificial Intelligence and Its Applications. Communications in Computer and Information Science, vol. 2308, pp. 178–189. Springer, Cham (2025). https://doi.org/10.1007/978-3-031-84394-5_13
20. Xu, X., Zhu, W., Fu, X., Yang, G., Jin, L., Yu, W., You, L.: Hybrid trust model for node-centric misbehavior detection in dynamic behavior-homogeneous clusters. *Applied Sciences* **15**(4), 2020 (2025). <https://doi.org/10.3390/app15042020>
21. Zhang, D., Yu, F.R., Yang, R., Tang, H.: A deep reinforcement learning-based trust management scheme for software-defined vehicular networks. In: Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '18). pp. 1–7. ACM (2018). <https://doi.org/10.1145/3272036.3272037>
22. Zhang, D., Yu, F.R., Yang, R., Zhu, L.: Software-defined vehicular networks with trust management: A deep reinforcement learning approach. *IEEE Transactions on Intelligent Transportation Systems* **23**(2), 1400–1414 (2022). <https://doi.org/10.1109/TITS.2020.3025684>