Game Theoretic Detection of RSU Collusion in Vehicular Blockchain Networks

YOUSIF ABDULWAHAB KHEERALLAH[1], GHAZWH G. JUMAA[2], ATHEER R. MUHSEN[2], SAIMA ANWAR LASHARI[3], MAHMOOD A. AL-SHAREEDA[4,5,6,*], MOHAMMED ALMAAYAH[7], RAMI SHEHAB[8]

[1]Department of Mechatronics Engineering, University of Basrah, Basrah, State, IRAQ

[2]College of Computer Science, University of Technology, Baghdad, IRAQ

[3]College of Computing and Informatics, Saudi Electronic University, Riyadh, 11673, SAUDI ARABIA

[4]Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, IRAQ

[5]College of Engineering, Al-Ayen University, Thi-Qar, IRAQ

[6]Department of Communications Engineering, Iraq University College, Basrah, IRAQ

[7]King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, JORDAN

[8]Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, SAUDI ARABIA

Corresponding Author

Abstract: Dynamic environments and coordinated malicious behavior remain major challenges in virtually any Internet of Vehicle system, making trust a challenging proposition. This paper devises a novel approach to achieve blockchain consensus through collective computation and dynamic Work evaluation to detect/evade Roadside station collusion. It creates Trust evaluation based on historical reviews, behavior significance, and scoring - variation and plugs into adaptive difficulty adjustment. This leads to differences in Shapley value, and similarity-based metrics, allowing the system to identify colluding RSUs and influence their mining probability. Nash stability and compatible desires are guaranteed by game-theory analysis. Planned framework is seen to enhance packet delivery ratio up to 17.4%, lessen end-to-end delay up to 21.6% and increase throughput by 13.9% when compared with basic planned frameworks as shown in reproduction results. This framework provides a scalable and reliable solution to secure and fair data sharing in blockchain-based Internet of Vehicles.

Key-Words: Internet of Vehicles (IoV), Blockchain, Trust Management, Coalition Game Theory, Roadside Units (RSUs), Proof-of-Work (PoW), Collusion Detection, Dynamic Consensus, Shapley Value, Incentive Mechanism.

Received: June 27, 2025. Revised: November 19, 2025. Accepted: March 5, 2026. Published: June 2, 2026.

1 Introduction

The relentless progression of the Internet of Vehicles has enabled perceptive transportation infrastructures to offer unfolding amenities such as autonomous driving, traffic tracking, and reactive routing in real-time,[1],[2]. In this architecture, Roadside Units (RSUs) play a key role as they gather information from vehicles

and communicate it with server or fog based systems,[3]. Nevertheless, due to their static deployment and permanence in the surrounding, Roadside Units are very attractive for adversaries in order to perform manipulation, collusion or Sybil attacks,[**?**],[4].

Recently, the applications of blockchain in the Internet of Vehicles(IoV) have become more for ensuring data integrity and transparency,[5],[6]. More specifically, consensus techniques such as Proof-of-Work enable Roadside Units to cooperatively verify data before adding it into the distributed ledger,[7],[8]. Although such techniques work in fine on traditional blockchain networks, they bring about the problems of scalability, energy-efficiency, and security when applied to the vehicular scenarios,[9],[10],[11]. Furthermore, most trust models base their decisions on the trustworthiness of the RSUs individually which may lead to group-wise attacks where a set of RSUs collude towards modifying consensus results-an attack vector mostly overlooked in current designs,[12],[13].

Work has been done on dynamic trust management,[14], and adaptive consensus schemes, but few attackers take into account the coordinated behavior of RSUs and not many lay emphasis on incorporating game-theoretic thinking into protocol design,[15],[16]. These collusive RSUs can increase the value of mutual trust, delay block propagation or hijack consensus to suppress honest nodes. Meanwhile, without sensing coalitions like that and rational RSU behavior model under reward-schooling mechanism, consensus is long-term manipulable.

Thus, in this paper, we focus on the urgent topic of building a robust game-theoretic model with dynamic trust management and mining difficulty adjustment to defend RSU collusion in blockchain-based IoV. Our approach consisted of coalition identification through Shapley value, diversity exam for feedbacks authenticity and a behaviour-weighted punishment mechanism to minimize the trust ination. This paper makes the following primary contributions:

- We introduce a dynamic trust assessment model for RSUs to discourage collusion by feedback diversity metrics, history weighting and behavioural dissimilarity.
- We propose a game-theoretical approach for coalition detection, which uses the deviation from Shapley value in order to identify a distribution of payoff as being unfair.
- Updated trust values are taken into consideration within an implemented PoW consensus model and the mining difficulty of RSUs is adjusted on-the-fly according to their levels of trustworthiness and incentive.
- We provide theoretical game-theoretic analysis for Nash stability and incentive compatibility under honest and malicious RSU strategies.
- We conduct extensive simulations using Veins (OMNeT++ and SUMO) to evaluate the proposed models performance in terms of security, latency, packet delivery ratio, and throughput.

The remainder of the paper is structured as follows: Section 2 reviews related work. Section 3 defines the system and threat models. Section 4 introduces the coalition game-based detection framework. Section 5 presents the dynamic trust mechanism. Section 6 provides game-theoretic analysis. Section 7 evaluates the security and performance, and Section 8 concludes with future directions.

2 Related Work

2.1 Management of Trust in Vehicular Networks

Systems for evaluating trust have long played a crucial role in ensuring secure communication across Vehicle-to-Everything environments,[17]. Conventional approaches frequently depend on direct or indirect feedback, historical patterns of action, or fuzzy logic to compute node reliability. In previous research,[14] designed a blockchain-based model that uses vehicle-submitted scores to review Roadside Unit performance. Separately,[18] developed a method to detect Sybil attacks based on location proof and time stamps. Moreover,[19], utilized deep learning to rate trust dynamically for vehicular cloud platforms. These approaches, however, have mostly been limited to examining individual nodes, and so are unlikely to reveal coordinated efforts in trust distortion or collusion involving components of the infrastructure.

2.2 Blockchain-Driven Consensus Mechanisms for IoV

Several consensus protocols have been adapted for dynamic vehicular scenarios,[20],[21],[22]. In their work,[15], authors proposed a credit-based Proof-of-Work that adjust mining difficulty based on Roadside Unit reputation to achieve scalability and fairness. In addition,[16] proposed Enhanced

Proof-of-Work, a new high-mobility protocol that incorporates both trust management and flexible difficulty. Though more efficient, these approaches are susceptible to group manipulation and ignore diversity in trust and behavior changes.

2.3 Game Theory in Vehicular Security

In this context, game theory has attracted attention to consider the strategic interactions among users and service providers in vehicle networks. Previously,[23] used coalition formation games to approach distributed task allocation and,[24] applied evolutionary games to analyse trust dynamics in vehicles. Separately,[25] developed a game-based model of Roadside Unit trust evaluation and Proof-of-Work difficulty adjustment but did not offer explicit collusion detection or diversity metrics. However, current models assume independent behavior of nodes and are blind to correlated feedback patterns that indicate collusion.

Notably, despite advancements in trust and consensus mechanisms, existing solutions do not provide an integrated framework with a capacity for dynamic identification of Roadside Unit collusion (as well as the game theory modeling necessary to ensure incentive compatibility) or that can embed trust management directly into consensus protocols. This reinforces the need for a dynamic, trust-aware Proof-of-Work scheme with coalition game-theoretic evaluation and filtering of feedback diversity as proposed herein.

3 System Model

In this section, we introduce the framework, introducing our assumptions and providing a formalization of the threat model that is useful for detecting and prevent collusion between RSUs in an IoV platform enabled by blockchain.

3.1 Network Entities

- **Vehicles:** They are portable hubs with sensors and correspondence modules. Vehicles routinely provide traffic data nearby RSUs and input on the idea of administrations got.
- **Roadside Units (RSUs):** Stationary ground stage establishments responsible for harvesting vehicle information, drafting transactions into blocks and engaging in blockchain consensus. RSUs are treated as potentially dubious things.
- **Blockchain Network:** A distributed ledger maintained jointly by RSUs. It logs the approved trades and information source, ensuring data changeless-ness, effortlessness, and following.
- **Trust Investigator:** A hypothetical module iterated inside the blockchain custom, in charge of refreshing and computing RSU trust esteems based on vehicle contributions, conduct investigation and assortment checks.

3.2 Assumptions

The framework works on the accompanying suppositions: All correspondence between vehicles and RSUs is confirmed by standard cryptographic conventions, guaranteeing information honesty and unwavering quality. Each vehicle can utilize this to estimate the quality of service offered by an RSU, and provide corresponding feedback which is verifiable and tamper-resistant. Vehicles are accepted to be by and large straightforward, while RSUs may act perilously or shape conniving affiliations to alter the framework. A worldwide time synchronization system exists to part the framework task into discrete time pieces for periodic trust refreshes.

3.3 Threat Model

The framework principally addresses the accompanying risks: Collusion Attacks: Different RSUs coordinate to alter input and trust measurements to acquire accord prevalence. Feedback Manipulation: RSUs fabricated or urge one-sided input to synthetically surge their trust scores. Trust Inertia Exploitation: RSUs act straightforwardly for extended periods to collect high trust, then misbehave abruptly (swing assaults). Selfish Mining and Data Tampering: RSUs defer square distribution or inject false information to acquire unjust rewards or disturb traffic knowledge.

4 Coalition Game-Based Collusion Detection Framework

This section designs a coalition game framework to identify the collusion of Roadside Units (RSUs) in blockchain-based Internet of Vehicles (IoV). Such trust evaluation methods are inadequate to IPCAS problem that have key assumption of independence among malicious nodes and our proposed method was successfully devised based on the strategic collaboration of RSUs for their collective manipulation of system in a smarter way.

4.1 Overview of Coalition Game Theory

Coalition game theory is a use of cooperative game theory using concepts from the alternative,

or non-cooperative, uml games branch. A coalition game is formally characterized by a tuple denoted as $(\mathcal{N}, v)$, where $\mathcal{N}$ represents the set of RSU nodes and $v : 2^{\mathcal{N}} \rightarrow \mathbb{R}$ is seen as a characteristic function providing payoff to each possible coalition formed by combining RSUs based on their decisions.

As an example in vehicular networks, RSUs can collaborate to subvert the integrity of trust assessments and increase mining chances. Solution concepts, such as the *core*, *Shapley value*, and *Nash stability*, are used to evaluate the stability and fairness of coalition. Such concepts are used to examine if RSUs have incentives to stay in the coalition or to deviate from it (Eq. 1). The total utility of a coalition $\mathcal{C} \subseteq \mathcal{N}$ is beneficial if:

$$v(\mathcal{C}) > \sum_{i \in \mathcal{C}} v(\{i\}), \tag{1}$$

4.2 Formation of RSU Coalitions

In a vehicular blockchain system, multiple Roadside Units (RSUs) may collude to behave together in order to gain from the trust evaluation mechanism as much as possible. This behavior results in the formation of collusive coalition, in which $\mathcal{C} \subseteq \mathcal{N}$ RSUs exchange trust scores to each other or hiding itself.

In prioritizing strategies, each of the RSU aims at maximizing its own payoff: mining rewards, lowered computational loads and enhanced control over block building. RSUs, upon realizing that cooperation can achieve more overall benefits (i.e., Sum-Utility), will coordinate their efforts in a distributed manner to form a coalition $\mathcal{C}$ (Eq 2) where:

$$v(\mathcal{C}) > \sum_{i \in \mathcal{C}} v(\{i\}), \tag{2}$$

where $v(\cdot)$ is the utility function of the coalition, and $\mathcal{N}$ is the complete set of RSUs. Behavioural alignment (e. g. trust trajectories or feedback manipulation patterns) usually drives coalition formation.

4.3 Collusion Indicator Metric

To generically detect colluded behavior among RSUs, we provide a collusion indicator metric that measures behavioral similarity property of an coalition. Intuitively, RSUs that collude are expected to have significantly correlated trust value patterns over time (in contrast with the case of non-colluding nodes).

Now, $\mathbf{T}_i(t)$ be the trust history vector of RSU i over a previous window of observation time t, and let sim(i,j) is how much cosine similarity between the trust vectors more than two RSUs i,J Pairwise similarity is calculated as:

Let $\mathbf{T}_i(t)$ represent the trust history vector of RSU i over a defined observation window t, and let $\text{sim}(i, j)$ denote the cosine similarity between the trust vectors of RSUs i and j (Eq. 3). The pairwise similarity is computed as:

$$\text{sim}(i, j) = \frac{\mathbf{T}_i(t) \cdot \mathbf{T}_j(t)}{\|\mathbf{T}_i(t)\| \, \|\mathbf{T}_j(t)\|}, \tag{3}$$

where $\| \cdot \|$ denotes the Euclidean norm. We can then define the aggregate collusion score between all the candidates in coalition $\mathcal{C}$ of size $|\mathcal{C}| \geq 2$ (Eq. 4) as follows:

$$\text{CollusionScore}(\mathcal{C}) = \frac{2}{|\mathcal{C}|(|\mathcal{C}| - 1)} \sum_{i \neq j \in \mathcal{C}} \text{sim}(i, j). \tag{4}$$

A high collusion score implies that RSUs in $\mathcal{C}$ have similar trust trajectories and hence may act in a potentially coordinated manner. The suspicion is detected by a pre-defined threshold θ_c. Then if $\text{CollusionScore}(\mathcal{C}) \geq \theta_c$, the coalition is deemed to be contentious and sent for review. This allows the system to distinguish trust that is eponymous of nature puts up with similar patterns and a mischief coordination where users directly follow each other in order to trick trust.

4.4 Decision Rules

The system needs to determine whether a coalition $\mathcal{C}$ with high collusion score acts maliciously. For this, we take recourse to game-theoretic fairness metrics, specifically the Shapley value, to evaluate individual contributions within a coalition.

The Shapley value ϕ_i of RSU i in coalition C (Eq. 5) is given by:

$$\phi_i = \sum_{\mathcal{S} \subseteq \mathcal{C} \setminus \{i\}} \frac{|\mathcal{S}|!(|\mathcal{C}| - |\mathcal{S}| - 1)!}{|\mathcal{C}|!} \left[v(\mathcal{S} \cup \{i\}) - v(\mathcal{S}) \right], \tag{5}$$

where $v(\cdot)$ is the utility function of the coalition or subcoalition. The Shapley value averages, over all models and configurations of the data, how much RSU i contributes to different coalitions. The system also computes and checks the deviation of actual utility (gain) per RSU against its Shapley value to detect any type of fairness violation and to prevent excess gain. If the deviation is more than a certain threshold ϵ_ϕ, then

it is considered as that RSU might be malicious (Eq. 6):

$$|\text{ActualUtility}_i - \phi_i| > \epsilon_\phi. \tag{6}$$

These decision rules allow the system to enforce accountability and discourage long-term strategic collusion among RSUs in blockchain-enabled vehicular networks.

5 Dynamic Trust Management with Anti-Collusion Strategy

To address this in the paper, we improve trust management process by adding dynamic anti-collusion mechanisms depending on RSU behavior change. We extend the classical beta-based trust model with three main features: groupware trust adaptation, temporal behavior importance and feedback diversity assessment. This process guarantees that RSUs with reduce altered trust scores encounter higher mining challenge, so blocking cooperation and supporting safe consensus contribution.

5.1 Modified Trust Evaluation Algorithm

But the traditional trust evaluation methods regard RSUs as isolated agent entities and ignore its dependence in a group and any cooperation behaviors of this group. To overcome this, we further model collusion emerged in test execution as a version of trust model with additional penalty. Where $\tilde{T}_i$ is the adjusted trust of RSU i (Eq. 7).

$$\tilde{T}_i = T_i \cdot (1 - \delta_i), \quad \text{where} \quad 0 \leq \delta_i \leq 1, \tag{7}$$

where T_i is the extreme trust value, and δ_i is a penalty rating calculated using RSU i participation in any flagged coalition.

5.2 Behavior History Weighting

The RSU behavior is time-varying so it could evolve over time by changes in environment, node mobility or adaptive adversary. Therefore, static synthesis of feedback may not reflect trustworthiness at the current time. Thus, we improve this and suggest a temporal weighting approach with a forgetting factor to provide higher weight-ages to the latest feedback and lesser orders/decreases in the older observations.

Where n is the number of last time slices to consider $g \in (0, 1]$ is a forgetting factor. Weighted average of positive and negative feedback over the time slices $t_{k-n+1}, \ldots, t_k$ for RSU i (Eq. 8).

$$s = \sum_{j=k-n+1}^{k} s_j \cdot g^{k-j}, \quad f = \sum_{j=k-n+1}^{k} f_j \cdot g^{k-j}, \tag{8}$$

is the number of positive feedback and the number of negative feedbacks received by RSU i at time slice t_j respectively. Finally, this weighted feedback is fused into the trust model in Beta calculus, rendering an adaptive and responsive evaluation of RSU behavior while vehicular network dynamics.

5.3 Feedback Diversity Measure

When rogue RSUs cooperate, they may receive inflated or coordinated ratings from a limited set of vehicles artificially. To find such abnormalities, we introduce a *feedback diversity measure* that assesses the differences in feedback an RSU gets from different vehicle sources within a recent time frame. Let $\mathcal{V}i$ represent the group of vehicles that rated RSU i in the recent window. Let fv, i symbolize the normalized feedback value (positive or negative) given by vehicle $v \in \mathcal{V}_i$ to RSU i (Eq. 9). The diversity score D_i is calculated as:

$$D_i = \text{Var}\left(\{f_{v,i} \mid v \in \mathcal{V}_i\}\right), \tag{9}$$

where $\text{Var}(\cdot)$ denotes the statistical variance. A small value of diversity score D_i indicates that RSU i is being feedbacked about by a set of uniform RSUs that are potentially deceiving in the form of information gain or reputation gaming.

For the purpose of robustness, the system introduces a diversity threshold θ_d. If $D_i < \theta_d$, RSU i is marked for added scrutiny, or action. Trust computing by considering feedback variety can increase the systems robustness against tampering and uncovering hidden collusion attempts.

5.4 Integration with Dynamic PoW Consensus

This trust model will impact the process of consensus through a method by means of which makes miners difficulty, distributed to each RSU of Vehicle, dynamically adjusted. To do so, the corrected trust value $\tilde{T}_i$ added of penalty and diversity factors is used in Proof-of-Work (PoW) difficulty computation. Let $D_i^{(t)}$ be the difficulty level of RSU i at time t, and $\tilde{T}_i$ be the basic system-wide difficulty related to incentive intensity $\beta(t)$. The difficulty of mine, hereafter called simply the difficulty (Eq. 10), is thereby calculated as:

$$D_i^{(t)} = D_0^{\beta(t)} \cdot \frac{T_0}{\tilde{T}_i}, \qquad \text{for } \tilde{T}_i \geq T', \tag{10}$$

where T_0 is initial trust of all RSUs and T' in what eligible RSU cannot take part in consensus. The integration of trust management with consensus mechanism forms a strong and decentralized security defense can enhance effectivenessfairness and efficiency of blockchain-based vehicular network.

6 Game-Theoretic Analysis

In this section, we conduct the game theoretic analysis of trust-aware consensus framework with incentives and punishments. We employ utility based rationality to model the behaviors of RSUs and analyze collusion conditions, equilibrium stability, and deviation risks.

- RSU Utility in Case of Collusion: Let U_i denote the utility gotten by RSU i for contributing to the blockchain consensus. U_i consists of expected mining reward R_i, effort cost $C_i(a_i)$, and risk or penalty P_i in case of collusion. The general form is (Eq. 11):

$$U_i = R_i - C_i(a_i) - P_i, \tag{11}$$

where a_i is the effort level (e.g., computational resources) and P_i increases if RSU i is detected as part of a colluding group.

In a coalition $\mathcal{C}$, the total utility is distributed among members. Using the Shapley value ϕ_i, we evaluate the fair share of RSU i (Eq. 12):

$$\phi_i = \sum_{\mathcal{S}\subseteq\mathcal{C}\setminus\{i\}} \frac{|\mathcal{S}|!(|\mathcal{C}| - |\mathcal{S}| - 1)!}{|\mathcal{C}|!} [v(\mathcal{S}\cup\{i\}) - v(\mathcal{S})]. \tag{12}$$

If the true reward deviates far from ϕ_i, such means unfair payoff of benefits might cause coalition to instability.

- Stability of the RSU Behavior: We investigate which extent of cooperation among RSUs is pursued in a game-theoretical sense. A coalition $\mathcal{C}$ is Nash-stable if no RSU $i \in \mathcal{C}$ has a strictly increasing unilateral deviation. The condition is(Eq. 13):

$$U_i(\mathcal{C}) \geq U_i(\mathcal{C} \setminus \{i\}). \tag{13}$$

Our trust-penalty mechanism decreases $U_i(\mathcal{C})$ as δ_i grows in case of detecting collusion, thereby destroying stability and discouraging the prolonged form of group manipulation.

- Strategic Level Incentive-alignment: Principals vs. Agent Model In this approach, we extend the Principal-Agent structure where vehicles act as principals and RSUs are agents. So, the reward β motivates RSUs to exert their maximum's degree of true effort a_i, conditioned upon a given contract design14, to maximize expected utility.

$$a_i^* = \arg\max_{a_i} \left(\alpha + \beta(a_i + rT_i) - \frac{b}{2}a_i^2\right), \tag{14}$$

with risk aversion ρ, and contract coefficients α, β and r. Through trust-related reward and penalty mechanisms, we coordinate the RSU strategies for cooperation such that incentive compatibility is achieved in dynamic environments.

- Mixed-Strategy Resistance: In order to capture adaptive attackers, we study the game under mixed-strategy equilibria where RSUs stochastically (i.e., with a probability) decide between being honest and colluding. Let p_i represent the probability that RSU_i is honest. The expected utility becomes 15:

$$\mathbb{E}[U_i] = p_i \cdot U_i^{\text{honest}} + (1 - p_i) \cdot U_i^{\text{collude}}. \tag{15}$$

In this situation (when penalties and trust cost are stronger than the short-term benefit of collusion), system resilience is more robust when the honest strategies ($p_i \to 1$) collectively become a Nash equilibrium.

In summary, the proposed scheme incentivizes RSUs to act honestly for maximizing their utility and discourages collusive behaviors through adaptive penalties,trust decay, and fair incentive penetration based on game-theoretic foundations.

6.1 Security Comparison

As listed in Table 1 (Appendix), compared to [15], [16], and [25], the proposed scheme achieves broader and deeper security coverage by integrating a feedback-diversified, penalty-enforced trust evaluation model with coalition game-theoretic detection. Where prior works emphasize adjusting difficulty based on solitary behavior, they regularly fail to anticipate plotted manipulation between participants and lack strong game-theoretic modeling. Our solution can identify Sybil, swing, and selfish mining attacks while dynamically sanctioning RSUs utilizing Shapley value analysis of fairness and a study of feedback irregularities, thus confirming individual liability and assemblage reliability simultaneously.

7 Performance Evaluation

In this section, the performance of the proposed scheme is evaluated from both security assurance and operation aspects.

7.1 Performance Metrics

To evaluate system performance, we model several key performance indicators by considering various vehicular densities, message generation rates and the PoW difficulty. More specifically, the system performance is considered in terms of throughput (i.e., blocks appended to the blockchain per unit time), latency (i.e., average time from when a data is generated by an OBU until it is confirmed within a block of chain) and scalability measures how responsive our system keeps up with growing amount of vehicles and RSUs.

7.2 Simulation Setup

We conduct simulation experiments in a realistic vehicular scenario covering an area of 2700 m × 3000 m using the Veins framework that enables OMNeT++ to connect with and interface with SUMO. There are two basic components in every simulation run, which lasts 300 seconds each: six RSUs and vehicles communicating over IEEE 802.11p wireless standard. For RSUs, we invoke an initial trust value $T_0 = 0.5$ and also define the threshold trust value as $T' = 0.3$, so that RSUs whose trust level is below this value are deemed untrustworthy. A forgetting factor $g = 0.5$ is applied to emphasize recent interactions, and a penalty factor $\lambda = 0.98$ is used to accelerate trust decay in the presence of malicious or collusive behavior. Trust evaluation is performed over $n = 10$ effective time slices to capture temporal trust variations. For the blockchain consensus process, adaptive Proof-of-Work difficulty levels are selected from $\{10, 12, 14\}$ and implemented using the SHA-256 hash algorithm. Vehicles periodically broadcast messages at an interval of 5 seconds, and the communication bandwidth is set to 6 Mbps. These parameter settings are chosen to reflect realistic vehicular communication conditions and to enable a fair evaluation of the proposed trust-aware adaptive consensus mechanis

7.3 Results and Analysis

In this regard, we evaluate the trust robustness and consensus adaptability of the proposed trust-aware adaptive PoW scheme and also demonstrate how we can gains with network-level performance metrics under different vehicular densities. As shown in Table 2 (Appendix), the results confirm the reactivity of trust management to malicious attempts, where RSUs receiving low or negative diversity feedback would make the system induces a rapid decay depending on penalty factor and isolates manipulated or collusion entities. In addition, PoW difficulty is dynamically tuned based on RSU trust values and known system rewards allowing for a finer-grain tradeoff between security and efficiency than that offered by neither the static nor the credit-based approaches. In terms of network performance, due to the trust-weighted consensus priority and diversified feedback filtering, our proposed scheme can always obtain a larger packet delivery ratio (PDR) as the number of vehicle grows with congestion and redundant transmission being mitigated in dense scenarios.

8 Conclusion and Future work

In this paper, we propose a trust-enabled consensus framework through coalition game theory and dynamic trust management to detect and mitigate collusion in the environment of blockchain-based vehicular networks between Roadside Units (RSUs). Improved long-term rate model trust incorporates penalty adjustment and calculation of feedback diversity and behavior history for precise, adaptive assessment. By employing coalition game theory techniques such as Shapley value and Nash stability, the system is able to identify and penalize coordinated RPGs while not losing fairness and incentive compatibility. This serves as a kind of level balance mechanism, so that the colluding RSUs won't dominate over consensus power. By bringing and incorporating the corrected trust scores into an effective dynamic PoW (Proof-of-Work), we can adjust the mining proof difficulty dynamically to settle on how often they are able to mine blocks efficiently. Based on security analysis and simulation-based performance evaluation, we demonstrate that the resilience of this scheme against Sybil attack, selfish mining and swing behavior is better than existing state-of-the-art solutions. Furthermore, the system has also obtains better packet delivery ratio, less latency and throughput in other network environments.

Further extensions to the framework shall include sensor fused federated learning models that enable distributed behavioral analysis as well as trust decay functions that optimize long term stability and further evaluation in multi-domain vehicular forests with cross-border trust delegation capabilities. In future works, we will take also into account real deployment issues such as privacy preservation and extendability to thousands of RSUs.

References:

[1] X. Wang, H. Zhu, Z. Ning, L. Guo, and Y. Zhang, "Blockchain intelligence for internet of vehicles: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, pp. 2325–2355, 2023. [Online]. Available: https://doi.org/10.1109/COMST.2023.3305312

[2] P. Agbaje, A. Anjum, A. Mitra, E. Oseghale, G. Bloom, and H. Olufowobi, "Survey of interoperability challenges in the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, pp. 22 838–22 861, 2022. [Online]. Available: https://doi.org/10.1109/TITS.2022.3194413

[3] E. R. Magsino and I. W. H. Ho, "An enhanced information sharing roadside unit allocation scheme for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, pp. 15 462–15 475, 2022. [Online]. Available: https://doi.org/10.1109/TITS.2022.3140801

[4] Y. Zhu, J. Zeng, F. Weng, D. Han, Y. Yang, X. Li, and Y. Zhang, "Sybil attacks detection and traceability mechanism based on beacon packets in connected automobile vehicles," *Sensors (Basel, Switzerland)*, vol. 24, 2024. [Online]. Available: https://doi.org/10.3390/s24072153

[5] A. Hussain, M. A. Saare, O. M. Jasim, and A. A. Mahdi, "A heuristic evaluation of iraq e-portal," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, pp. 103–107, 2018, [Accessed Date: 28/04/2026]. [Online]. Available: https://jtec.utem.edu.my/jtec/article/view/3799

[6] I. A. Abed, M. S. M. Ali, and A. A. A. Kadhim, "Using particle swarm optimization to solve test functions problems," *Bulletin of Electrical Engineering and Informatics*, vol. 10, 2021, [Accessed Date: 28/04/2026]. [Online]. Available: https://doi.org/10.11591/eei.v10i6.3244

[7] A. A. A. Kadhim, M. S. Kadhim, H. A. Khamis, M. A. Al-Shareeda, M. Amin, and R. Shehab, "Sustainable green unmanned aerial vehicles (uav) systems for smart and environmental applications: A review," *International Journal of Robotics and Control Systems*, vol. 6, no. 1, pp. 718–740, 2026. [Online]. Available: https://doi.org/10.31763/ijrcs.v6i1.2455

[8] A. A. A. Kadhim, A. F. Abdulhasan, and F. F. Jaber, "Improvement of extracted photovoltaic power using artificial neural networks mppt with enhanced flyback controller," *Iraqi Journal for Electrical and Electronic Engineering*, pp. 237–250, 2025. [Online]. Available: https://doi.org/10.37917/ijeee.21.2.22

[9] "Durable-rl: A dynamic uncertainty-aware hybrid reinforcement learning framework with adaptive buffer and ensemble modelling," *International Journal of Intelligent Engineering and Systems*, pp. 494–509, 2025. [Online]. Available: https://doi.org/10.22266/ijies2025.1031.32

[10] A. Seddighi, S. Asghari, M. Romoozi, and H. Babaei, "A review of game theory-based trust modeling approaches in infrastructure-free social networks," *Management Strategies and Engineering Sciences*, vol. 7, pp. 81–95, 2025. [Online]. Available: https://doi.org/10.61838/msesj.7.4.9

[11] I. A. Abed, S. Koh, K. S. M. Sahari, S. Tiong, M. M. Ali, and A. A. A. Kadhim, "A new proposed pendulum-like with attraction-repulsion mechanism algorithm for solving optimization problems," *IOP Conference Series: Materials Science and Engineering*, vol. 881, 2020. [Online]. Available: https://doi.org/10.1088/1757-899X/881/1/012132

[12] S. H. A. Alwaeli, A. A. Abdulsaeed, S. J. Fayyadh, M. I. Khan, A. Yousif, T. Saba, and S. A. O. Bahaj, "A unified spectral-persistent homology framework for stable and generalizable topological deep learning," *Discover Computing*, vol. 28, 2025, [Accessed Date: 28/04/2026]. [Online]. Available: https://api.semanticscholar.org/CorpusID:282751773

[13] S. H. Abbood, H. N. A. Hamed, and M. S. M. Rahim, "Automatic classification of diabetic retinopathy through segmentation using cnn," in *International Conference on Internet of Things Technologies for HealthCare*, 2021, [Accessed Date: 28/04/2026]. [Online]. Available: https://api.semanticscholar.org/CorpusID:256504952

[14] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, pp. 1495–1505, 2019. [Online]. Available: https://doi.org/10.1109/JIOT.2018.2836144

[15] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 3680–3689, 2019. [Online]. Available: https://doi.org/10.1109/TII.2019.2903342

[16] G. Du, Y. Cao, J. Li, Z. Yan, X. Chen, Y. Li, and J. Chen, "A blockchain-based trust-value management approach for secure information sharing in internet of vehicles," *IEEE Internet of Things Journal*, vol. 11, pp. 333–344, 2024. [Online]. Available: https://doi.org/10.1109/JIOT.2023.3277691

[17] M. Ho, S. Ang, S. Huy, and M. Janarthanan, "Mumspi: A model for usability measurement of single-platform interface for multi-tasking in big data tools," *Jordanian Journal of Informatics and Computing*, vol. 2026, no. 1, p. 114, 2026. [Online]. Available: http://dx.doi.org/10.63180/jjic.thestap.2026.1.1

[18] S. Benadla, O. R. Merad-Boudia, S.-M. Senouci, and M. Lehsaini, "Detecting sybil attacks in vehicular fog networks using rssi and blockchain," *IEEE Transactions on Network and Service Management*, vol. 19, pp. 3919–3935, 2022. [Online]. Available: https://doi.org/10.1109/TNSM.2022.3216073

[19] V. Chourasia, S. Pandey, and S. Kumar, "Reliable data exchange in vehicular delay tolerant networks using aibased hybrid trust management," *International Journal of Communication Systems*, vol. 35, p. e5197, 2022. [Online]. Available: https://doi.org/10.1002/dac.5197

[20] D. Alalisalem and H. Rahman, "Securing healthcare digital twin with blockchain: A systematic review of architecture, threats and evaluation," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, p. 4666, 2026. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2026.1.3

[21] A. Ali, "Adaptive and context-aware authentication framework using edge ai and blockchain in future vehicular networks," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, p. 4556, 2024. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2024.1.3

[22] A. Alotaibi, H. Aldawghan, and M. M. H. Rahman, "Iot security concerns with non-fungible tokens: A review," *STAP Journal of Security Risk Management*, vol. 2026, no. 1, p. 130, 2026. [Online]. Available: http://dx.doi.org/10.63180/jsrm.thestap.2026.1.1

[23] W. Saad, Z. Han, T. Baar, M. Debbah, and A. Hjørungnes, "Hedonic coalition formation for distributed task allocation among wireless agents," *IEEE Transactions on Mobile Computing*, vol. 10, pp. 1327–1344, 2010. [Online]. Available: https://doi.org/10.1109/TMC.2010.242

[24] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory," *IEEE Transactions on Vehicular Technology*, vol. 68, pp. 5971–5980, 2019. [Online]. Available: https://doi.org/10.1109/TVT.2019.2910217

[25] L. Wei, Y. Cao, J. Cui, H. Zhong, I. P. Bolodurina, and D. He, "Game theory and trust management driven dynamic proof-of-work blockchain consensus algorithm for securing internet of vehicles," *IEEE Transactions on Mobile Computing*, vol. 25, pp. 434–450, 2026, [Accessed Date: 28/04/2026]. [Online]. Available: https://api.semanticscholar.org/CorpusID:280356255

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors contributed to this work as follows: Conceptualization was carried out by Mahmood A. Al-Shareeda and Yousif Abdulwahab Kheerallah. Methodology and formal analysis were developed by Ghazwh G. Jumaa and Atheer R. Muhsen. Software implementation and simulation were performed by Saima Anwar Lashari and Mohammed Almaayah. Validation and investigation were conducted by Rami Shehab. Writingoriginal draft preparation was completed by Mahmood A. Al-Shareeda, while all authors contributed to writingreview and editing. Supervision and project administration were handled by Mahmood A. Al-Shareeda. All authors have read and approved the final version of the manuscript.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Appendix

Table 1: Security Comparison with Existing Schemes

Security Feature	**Proposed Scheme**	[25]	[15]	[16]
Sybil Attack Resistance	✓	✓	∼	∼
Collusion Detection	✓	✓	×	×
Selfish Mining Mitigation	✓	✓	∼	∼
Swing Attack Defense	✓	✓	×	×
Feedback Diversity Evaluation	✓	✓	×	×
RSU Blacklisting Mechanism	✓	✓	∼	∼
Game-Theoretic Incentive Modeling	✓	✓	×	×
Support for Dynamic Environments	✓	✓	∼	✓

Source: Created by the authors.

✓: Fully Supported, ∼: Partially Supported, ×: Not Supported

Table 2: Summary of performance comparison between the proposed scheme and existing approaches

Metric	**Proposed Scheme**	[25]	[15]
Trust robustness	High (rapid decay, diversity-aware)	Medium	Low
PoW difficulty control	Dynamic, trust-aware	Semi-adaptive	Static / credit-based
Packet Delivery Ratio (PDR)	Highest under dense networks	Moderate	Lower
End-to-end latency	Lowest	Higher	Highest
Throughput	High and stable	Moderate	Low
Scalability	Strong under increasing nodes	Limited	Limited

Source: Created by the authors.