




# Reputation Consensus-Based Scheme for Information Sharing in Internet of Vehicles

Kun Yan , Ping Zeng, Kan Wang , Wenping Ma   
Geng Zhao, and Yingjie Ma

**Abstract**—Low latency and low energy consumption are prerequisites for Internet of Vehicles (IoV) research; nevertheless, consensus mechanisms of legacy blockchain applied to IoV typically incur high delay and serious energy consumption due to the computational puzzle. In this paper, Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is used to implement a novel reputation consensus mechanism for IoV based on vehicle reputation values and traffic environment, which can not only reduce the computational pressure but also ensure the fairness of consensus. Firstly, the information transmission vehicles (ITVs) would be picked following the reputation value and its associated environmental data that makes the choice more comprehensive and objective than other mechanisms. Secondly, the authenticity of sharing information is determined with the help of Bayesian inference, aided by the reputation value of message reporting vehicles (MRVs). Finally, simulation results show that the proposed scheme can improve consensus efficiency by picking ITVs in a short time and avoid the spreading of false information effectively in the IoV system.

**Index Terms**—Reputation consensus, blockchain, internet of vehicles, TOPSIS, bayesian inference.

## I. INTRODUCTION

The development of communication and the prevalence of Internet of Things (IoT) technology allow vehicles in the networked environment to use sensors and on-board units (OBU), thereby realizing information interaction and sharing between vehicle-to-everything (V2X). Such state-of-the-art technology iterations can effectively boost vehicle collaboration, improve traffic efficiency, and optimize the traffic environment [1]. However, due to the networking of vehicles and traffic devices, some issues have been brought in, such as communication security, privacy protection, and system reliability, many current

researches introduce blockchain to address these security issues. Blockchain integrates cryptography, P2P networks, smart contracts, consensus mechanisms, etc., and the combination of these technologies creates its decentralization, distributed storage, immutability, and high security, coinciding with the security needs of IoV [2]. Yet, in the case of blockchain, its performance is largely influenced by the performance of its consensus mechanism [3]. Proof of Work (PoW), for example, is a consensus mechanism traditionally designed for digital currencies, where hashing problems are used as a selective transaction validator [4], resulting in huge resource consumption. This can lead to high energy consumption and high waiting time during information transmission in PoW-based IoV systems, which affects the timeliness of information sharing, even if it can provide reliable sufficient and security.

To solve the incurring timeliness issue, two representative solutions have emerged recently. On one hand, it is desired that the computing is offloaded to cloud servers or edge devices from vehicles through cloud computing [5] or edge computing [6]. Despite the alleviation of computing loads on vehicles, the resources and energy devoted to computing are only transferred but not eliminated. Therefore, It can not completely solve the problem of useless waste of resources caused by PoW. On the other hand, PoW is replaced with the non-compute-intensive consensus mechanism that leverages lightweight blockchains to meet the needs of IoV [7]. Li *et al.* [8] protected the user privacy in IoV with a Proof of Stake (PoS) based blockchain, and the authors in [9] designed a hybrid blockchain based on Delegated Proof of Stake (DPoS) to solve the edge data sharing among vehicles by combining federated learning. Both types of solutions mitigate the latency and computing power to a certain extent. However, the terms of their consensus remain in blockchain data such as tokens and holding times and do not effectively use the data in IoV.

Blockchain-based IoV information sharing can only guarantee the attribution and tamper-proof of information, but not the authenticity of it. Focusing on the authenticity of information in IoV, there exist two solutions: identity-based and data-based judgment. In the former, the blockchain is leveraged to identify and manage vehicles. In particular, there exists a threat initiated by successfully authenticated vehicles, since a successfully authenticated vehicle could communicate with each other [10]. In the latter, the location [11] and reputation [12] data are leveraged to justify the information authenticity and circumvent the selfish behavior of vehicles in the traffic environment. Although the latter does not focus on the identification of vehicles, it could measure the information credibility concerning the traffic environment and vehicle characteristics, thus exhibiting higher accuracy in determining information authenticity.

In this paper, we propose a TOPSIS based Proof of Reputation (tPoR) consensus mechanism for information sharing in IoV. When a traffic event occurs, its associated message would be reported by surrounding vehicles, and the system would evaluate the traffic conditions and reputation values of surrounding vehicles to pick ITVs. After that, the ITVs send the collected messages to neighboring Roadside Units (RSU), then determining the information authenticity to judge

This work was supported in part by the National Nature Science Foundation of China under Grant 61772047, in part by the First class discipline construction project of Beijing Electronic Science and Technology Institute under Grant 3201017, in part by the Foundation of the State Key Laboratory of Integrated Services Networks of Xidian University, China under Grant ISN21-08, and in part by the Key Industry Innovation Chain Project of Shaanxi Provincial Science and the Technology Department, China under Grant 2022ZDLGY03-08. (Corresponding author: Ping Zeng.)

Kun Yan and Wenping Ma are with the School of Telecommunications Engineering, Xidian University, Xi'an 710071, China. Yan Kun is also with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China. (e-mail: kyan@stu.xidian.edu.cn; wp\_ma@mail.xidian.edu.cn)

Kan Wang is with the School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China, and is also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: wangkan@xaut.edu.cn).

Ping Zeng, Geng Zhao, and Yingjie Ma are with the Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China (e-mail: zp@besti.edu.cn; zg@besti.edu.cn; myj@besti.edu.cn).

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

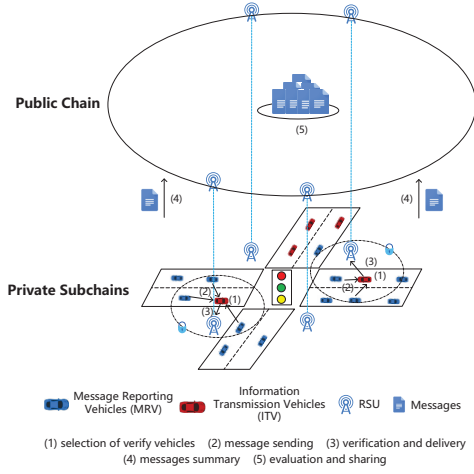


Fig. 1. Scheme model.

whether or not to share the event information. Next, TOPSIS is introduced in the consensus mechanism of IoV for multi-objective-decision-making to identify ITVs and reach consensus. Finally, the reputation value is incorporated into the Bayesian inference as the main factor to improve the accuracy of information authenticity discrimination.

In the rest, we present the architecture and formula model in Section II, evaluate the effectiveness of our scheme through simulation in Section III, and finally concludes the work with future research in Section IV.

## II. SYSTEM MODEL AND SCHEME DESCRIPTION

### A. Overview of System Model

Inspired by [13], we implement tPoR with a hybrid blockchain, consisting of the public blockchain in RSUs and private subchains in vehicles, as shown in Fig. 1. Such a scheme, compared with public chain, private chain, and consortium chain, ensures the integrity of system information while providing better privacy protection for users [14]. As one of consensus mechanism to ensure the integrity of a distributed network, Practical Byzantine Fault Tolerance (PBFT) is applied to public chain, while tPoR is adopted for private subchains. At the same time, subchains are dynamically created and released depending on the traffic information sharing requirements. Since cross-chain communication in this scheme focuses on the request, response, transmission and sharing of messages, there is no need to build a bridge module for it. In particular, the vehicles are divided into two categories: MRVs and ITVs, and the scheme is implemented through two parts: preliminary consensus and information verification. On one hand, the preliminary consensus is implemented in the private subchains, involving the computing capability of OBU, while tPoR is leveraged to reduce the computational pressure. Besides, the reputation values are updated and stored in the vehicle itself, and thus the ITVs could be figured out quickly in combination with the traffic environment. On the other hand, the information verification is inclined to be executed in RSUs, since the message sets of same event can be synchronized instantly, and the true information can be

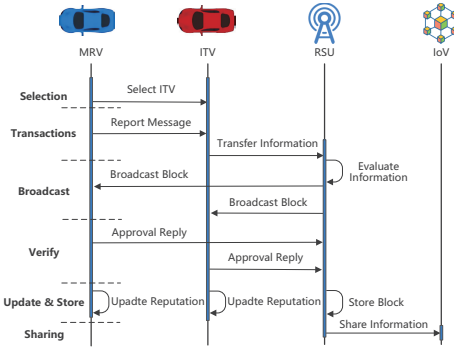


Fig. 2. Consensus process of tPoR.

broadcast and shared after judgment with a public blockchain deployed among RSUs.

### B. tPoR for IoV

In the initial state, the system would calculate the initial values of the vehicles' reputation using the weighted evaluation from the driver's driving age (the longer the driving age, the better the driving behavior), the vehicle's age (the smaller vehicle's age represents the better condition), and the vehicle's violations within one year (the more violations represent the poorer driving behavior). Meanwhile, each vehicle would get a blockchain wallet involving a public key, a private key, and a wallet address.

When a traffic event occurs, the vehicles and RSU within its radius of  $r$  form a subchain. The process of information sharing based on tPoR is illustrated in Fig. 2, and Algorithm 1 briefly describes the workflow of tPoR.

---

#### Algorithm 1 tPoR Consensus

---

**Input:**  $R_i, S_i, DE_i, DR_i$

**Output:** new Block

---

- 1: Assessment of input parameters with TOPSIS, while the results are sorted from largest to smallest to obtain the series  $C[i]$
  - 2:  $ITV = C[0]$
  - 3: **while** RSU received  $TX$  from ITV **do**
  - 4:   ITV collects messages from MRVs
  - 5: **end while**
  - 6: **if** RSU received  $TX$  from ITV **then**
  - 7:   RSU evaluates the information and broadcasts the block, which is packed by the evaluation result and  $TX$
  - 8: **end if**
  - 9: **return** new Block
- 

The detailed steps of the proposed scheme are as follows:

*Step 1 (ITVs Selection):* Since RSUs are not necessarily present near traffic events, this results in vehicles not being able to communicate directly with them, and therefore ITVs are needed for information transfer. tPoR could pick the best ITVs based on four metrics, including reputation and traffic environment data, more specifically:

- 1)  $R_i$ : The reputation value of vehicles in current status, proportional to the message credibility.

- 2)  $S_i$ : The success rate of vehicles' message transmission in current status, proportional to the efficiency of message transmission.
- 3)  $DE_i$ : The distance between the location of vehicles and the one of event occurred; the smaller distance, the more accurate judgment can be made about the event.
- 4)  $DR_i$ : The distance between the vehicle and nearest RSU, proportional to the message exchange time.

For traffic event  $e_i$ , assume there are  $n$  vehicles of MRV  $v_i$  in its region with radius  $r$ , and then we get the following original evaluation matrix as

$$X = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ \vdots & \vdots & \vdots & \vdots \\ x_{i1} & x_{i2} & x_{i3} & x_{i4} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & x_{n3} & x_{n4} \end{bmatrix}, \quad (1)$$

where  $x_{ij}$  is the  $j$ -th evaluation criterion of the  $i$ -th vehicle.

For fairness, the entropy of  $j$ -th attribute of vehicle could be calculated as

$$e_j = -\frac{1}{\ln n} \sum_{i=1}^n \frac{x_{ij}}{\sum_{i=1}^n x_{ij}} \ln \frac{x_{ij}}{\sum_{i=1}^n x_{ij}} \in [0, 1]. \quad (2)$$

Then, the entropy weight of the  $j$ -th vehicle's evaluation criterion can be calculated as

$$\omega_j = \frac{1 - e_j}{\sum_{j=1}^4 (1 - e_j)}. \quad (3)$$

After that, the evaluation weighting matrix of candidate vehicles turns out to be:

$$Q = \begin{bmatrix} q_{11} & q_{12} & q_{13} & q_{14} \\ \vdots & \vdots & \vdots & \vdots \\ q_{i1} & q_{i2} & q_{i3} & q_{i4} \\ \vdots & \vdots & \vdots & \vdots \\ q_{n1} & q_{n2} & q_{n3} & q_{n4} \end{bmatrix}, \quad (4)$$

where

$$q_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^n x_{ij}^2}} \omega_j.$$

Next, following TOPSIS, the positive-ideal solution  $Q^+$  and negative-ideal solution  $Q^-$  of the alternatives could be acquired as:

$$Q^+ = (q_1^+, q_2^+, q_3^+, q_4^+) = \left\{ \max_i q_{ij} \mid j \in [1, 4] \right\}, \quad (5)$$

and

$$Q^- = (q_1^-, q_2^-, q_3^-, q_4^-) = \left\{ \min_i q_{ij} \mid j \in [1, 4] \right\}. \quad (6)$$

Finally, the synthetic value of each candidate vehicle becomes evaluated as follows:

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-}, \quad (7)$$

where

$$D_i^+ = \sqrt{\sum_{j=1}^4 (q_{ij} - q_i^+)^2}, \quad D_i^- = \sqrt{\sum_{j=1}^4 (q_{ij} - q_i^-)^2}.$$

The candidate vehicles are ranked following the size of  $C_i$ , and the one with the largest value is indexed as ITV  $v_j$ .

*Step 2 (Information Transmission)*: In particular,  $v_i$  sends the report message (encapsulated as the transaction  $TX_{rm}$ ) to  $v_j$ . After receiving  $TX_{rm}$ ,  $v_j$  would process the transaction and then send the delivery message (encapsulated as the transaction  $TX_{dm}$ ) to the RSU. More precisely,  $TX_{rm}$  and  $TX_{dm}$  are defined as follows:

$$\begin{aligned} TX_{rm} &: \{ID_i, Event_i, R_i, \text{Sig}_{sk_i}[H(Event_i)]\} \\ TX_{dm} &: \{ID_i, ID_j, R_i, R_j, Event_i, Tab, \text{Sig}_{sk_j}[H(TX_{rm})]\}, \end{aligned} \quad (8)$$

where  $ID_i$ ,  $R_i$ , and  $sk_i$  are the blockchain wallet address, reputation value, and private key of  $v_i$ , respectively. In particular,  $Tab$  is the opinion of  $v_j$  on this event, which would be marked when the message reported by  $v_i$  is judged to be false,  $\text{Sig}_a(B)$  is a digital signature function utilizing  $a$  to sign  $B$ , and  $H$  is a hash function.

*Step 3 (Information Evaluation)*: If RSU collects sufficient messages regarding an event within a predefined time, then Bayesian inference is used to verify the event authenticity. For the message set  $M^j = \{m_1^j, m_2^j, \dots, m_i^j, \dots\}$  regarding event  $e^j$ , (9) is used to calculate the credibility  $f_i$  of message  $m_i$  (that is uploaded by the vehicle  $v_i$  with the reputation value of  $R_i$ ). The credibility set of all messages for  $e^j$  can be obtained as

$$F^j = \{f_1^j, f_2^j, \dots, f_i^j, \dots\}, \quad (9)$$

with

$$f_i^j = \alpha \cdot e^{-\gamma d_i^j - \eta t_i^j} + \beta R_i, \quad (10)$$

where  $f_i \in [0, 1]$ ,  $d$  is the distance between MRV  $v_i$  and the place where  $e^j$  occurs,  $t$  is the time difference between the  $i$ -th message and the first message received regarding  $e^j$ , and  $\alpha$ ,  $\beta$ ,  $\gamma$ ,  $\eta$  are preset parameters, for the adjustment of  $f_i$ , respectively.

Following  $F_j$ , (11) could be leveraged to infer the credibility of information regarding  $e^j$  based on Bayesian inference [15]. It can be judged that the information regarding  $e^j$  is true only when  $P(\frac{e^j}{F^j})$  reaches the preset threshold, as follows:

$$P\left(\frac{e^j}{F^j}\right) = \frac{P(e^j) \cdot \prod_{i=1}^n P\left(\frac{f_i^j}{e^j}\right)}{P(e^j) \cdot \prod_{i=1}^n P\left(\frac{f_i^j}{e^j}\right) + P(\bar{e}^j) \cdot \prod_{i=1}^n P\left(\frac{f_i^j}{\bar{e}^j}\right)}, \quad (11)$$

where  $\bar{e}$  is the opposing event of  $e$ ,  $P(\frac{f_i^j}{e^j}) = f_i^j$ ,  $P(\frac{f_i^j}{\bar{e}^j}) = 1 - f_i^j$ ,  $P(\frac{e^j}{F^j}) \in [0, 1]$ , and  $P(e^j)$  is the prior probability of the event  $e^j$ , respectively.

*Step 4 (Bonus-penalty):* After evaluating the authenticity of the information, RSU calculates and updates the reputation values of all participants of the event. The reputation value of vehicles sending correct messages is increased, and vice versa. The MRVs' reputation values associated with each message in  $M_j$  can be computed as

$$R_{\text{new}} = \left( 1 \pm \frac{f_i^j}{\sum_{k=1}^n f_k^j} \right) R_{\text{old}} \quad (12)$$

Meanwhile, (13) is utilized to incentivize the reputation value of the ITVs as follows:

$$R_{\text{new}} = \left( 1 + \frac{\min F^j}{\sum_{k=1}^n f_k^j} \right) R_{\text{old}}. \quad (13)$$

*Step 5 (Block Generation):* After the preceding procedures, the subchain is released. The master RSU, which receives the information packet, broadcasts the verified block as a prepare packet to the public chain. The other consensus nodes will broadcast the commit packet after receiving the prepare packet with correct verification result, and the prepare packet number is greater than  $2f+1$  ( $f$  is the maximum number of fault tolerant nodes). Similarly, if a consensus node receives  $2f+1$  commit packets with correct verification, then it will submit the confirmation message. Eventually, the new block, with format in Fig. 3, will be recorded in the public chain.

Header	Prehash	Block Height	Timestamp	Signature
Body	Judgment Result			
	Message Set: $TX_{dm}^1, TX_{dm}^2, \dots, TX_{dm}^f, \dots$			
	Reputation Values			

Fig. 3. The block format of public chain.

### III. EXPERIMENTAL AND DISCUSSION

In order to validate the effectiveness and feasibility of the proposed scheme, Golang language is used for performance testing as well as OMNeT++ 6.0, SUMO 1.11.0, and Veins 5.2 co-simulation platforms are used to generate traffic scenarios. The configurations of critical parameters are listed in Table I. This section is divided into four main parts. The

first part investigates the performance comparison of different consensus algorithms and the effect of prior probability on information accuracy judgment. The second section provides the evaluation of tPoR in IoV. The third section studies the computational complexity and communication complexity of the scheme. Finally, the security analysis of the scheme is discussed.

TABLE I  
KEY PARAMETERS

Parameters	Values
Simulation Area	3 km * 3.1 km
RSU Transmission Range	150 m
Vehicles Transmission Range	100 m
Simulation Time	500 s
Data Packet Size	138 bytes
$\alpha, \beta, \gamma, \eta$	0.4, 0.006, 0.001, 0.001

#### A. Simulation of tPoR algorithm

In this part, to validate the superiority of tPoR, we test the effectiveness of tPoR, PoS [8], and DPoS [9] consensus algorithms by Golang language. The physical machine is equipped with Intel i7-10710U@1.1GHz with 16 GB RAM Windows 10 system. We simulate the consensus process by treating vehicles as nodes in the blockchain, and the number of nodes in the experiment ranges from 20 to 200; different numbers of nodes reach consensus, and the program outputs the correct transaction information, implying that a consensus is reached among similar numbers of vehicles in the IoV.

First, we test the consensus time of three consensus algorithms, 600 experimental tests are conducted and the average value of every twenty data is used as the experimental data, thus guaranteeing the reliability of the experimental data. As shown in Fig. 4, the result shows that the consensus time of tPoR is significantly lower than others, and its time consumption can be reduced by up to 53.38% and 61.99% compared with DPoS and PoS, respectively; also, as the number of nodes grows, tPoR rises less significantly than the other two, thus ensuring low latency and high efficiency of information transfer in the IoV environment. The main reason for the above results is that tPoS utilizes a multi-objective decision technique, TOPSIS, that completely replaces the hash computation in PoS and DPoS, and thus the consensus time has been drastically reduced.

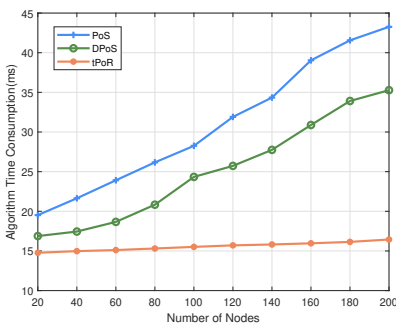


Fig. 4. Consensus time comparison.

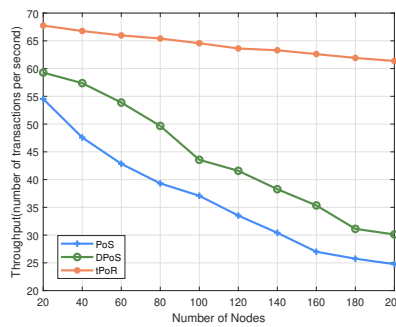


Fig. 5. Throughput comparison.

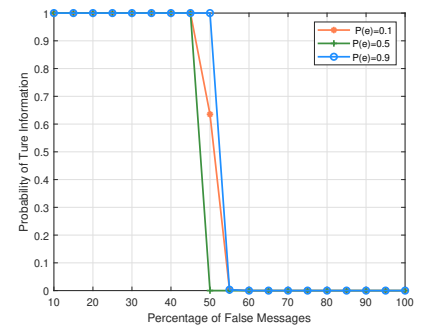


Fig. 6. Authenticity detection vs. prior probabilities.



Next, we compare the throughput of transaction, and test the Transaction Per Second (TPS) as illustrated in Fig. 5. The TPS decreases as the number of nodes increases, whereas the advantage of tPoR is still obvious, with throughput improvements of up to 50.93% and 59.65% over the other two algorithms, respectively. The main reason is that the consensus time of each transaction in tPoR is much lower than the other two, and thus tPoR can complete more transactions per unit of time.

### B. Simulation of information evaluation

In this part, we test the ability of Bayesian inference-based information detection under reputation endorsement. The prior probability in Bayesian inference is usually an uncertain value that can be derived from previous experience, or judged and selected based on practical applications when lacking necessary information [16]. To achieve more accurate information detection, three prior probability values are picked and tested separately, with results shown in Fig. 6. As the percentage of false messages increases, the probability of true information under the three a priori probabilities show the same trend. All three curves almost overlap, with the difference only at the 50% false information, where, the inferred results with a priori probabilities of 0.5 and 0.9 are approximately 0 and 1, respectively, and the pre-determined probability of 0.5 would misinterpret in some cases, thus a priori probability of 0.1 is more favorable. More information is reported by vehicles with large reputation values leading to a probability of 0.635 of true information at this time, and the proposed reputation-based evaluation mechanism identifies this information as true. Benefiting from the influence of prior knowledge on decision-making, in the real traffic scenario, the prior probability can be calculated by counting the frequency of traffic events (e.g. traffic jams, tailgating.) occurring at a certain place during a certain period, contributing to the subsequent information evaluation with Bayesian inference.

### C. Simulation of proposed scheme in traffic communication

In this part, to verify the impact of tPoR-based blockchain on traffic communication, the proposed scheme is evaluated using the IoV simulation platform mentioned before. The physical machine is equipped with Intel i5-8500@3GHz with 8 GB RAM Ubuntu 20.04 system. A real map of the city of Erlangen, Germany is used to simulating road traffic, which was shipped by Veins, as shown in Fig. 7. We test the variation of Average Packet Loss Rate (APLR) and Average Communication Delay (ACD) for 20, 40, and 60 vehicles at different speeds with proposed scheme, respectively.

In this experiment, APLR is the average of the ratio of the difference between the total number of packets sent by MRVs and the total number of packets received by ITVs to the total number of packets received by ITVs during the simulation time. Fig. 8 depicts the impact of vehicle speed and number on APLR. The APLR decreases progressively with vehicle speed for a constant number of vehicles. The transmission of packets is higher during lower vehicle speed levels since the duration of MRVs and ITVs within the communication range is longer, and packet queuing time exceeds the threshold value leading



Fig. 7. Traffic network and IoV scenario in simulations.

to packet loss, so the packet loss rate is higher. In the case of higher speed levels, the transmission of packets is lower, and the communicating parties stay within the communication range of each other for less time, so the packet loss rate is also lower. With constant vehicle speed, APLR is also in lockstep with the number of vehicles. As the number of vehicles rises, more packets are generated in the communication range, causing the message collision and queuing delay increases, which results in more packets being dropped, and the packet loss rate becoming larger.

We define ACD as the average of the difference between the time to report messages from MRVs and the time for the set of messages to reach the RSU after the consensus process. Fig. 9 depicts the impact of vehicle speed and number on ACD. Under a certain number of vehicles, the decrease in ACD is accompanied by an increase in vehicle speed. The change of vehicles within the communication range of ITVs and RSUs accelerates due to the acceleration of vehicle speed, which leads to the decrease in the number of packets received by both and the decrease in packet queuing delay. Meanwhile, the reduction of ACD slows down during the change of vehicle speed from 80 km/h to 120 km/h. This is because as the vehicle speed increases, the distance between communication parties increases, and the communication time delay increases. The reason for the increase of ACD with the number of vehicles at constant speed is the increase in packet queuing delay due to the increase in packets.

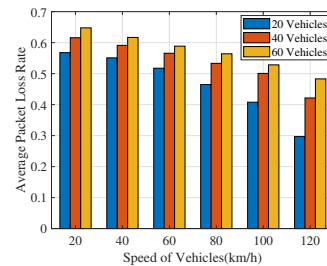


Fig. 8. APLR comparison.

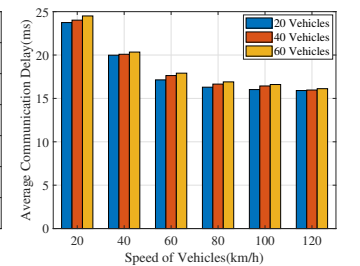


Fig. 9. ACD comparison.

### D. Communication and computational complexity

The communication and computational complexity of tPoR are shown in Table II, where  $n$  represents the number of

vehicles participating in the consensus. First, the communication complexity indicates the number of communications between the transmitter and the receiver [3]. In particular, in the Information transmission, from the ITV's perspective, it first receives messages from the remaining  $n - 1$  vehicles, and then sends the packaged messages to the RSU, thus with the communication complexity of  $\mathcal{O}(n)$ . In the Bonus-penalty, from the RSU's perspective, it needs to synchronize the updated values of reputation to each vehicle involved in the information sharing and consensus, and thus the communication complexity is  $\mathcal{O}(n)$ . More precisely, ITVs selection and Information evaluation do not involve the communication process. Second, the computational complexity mainly arises during the ITVs' selection, the computation on the 4-column evaluation matrix leads to the complexity of  $\mathcal{O}(4n)$ . More precisely, the complexity of both Information evaluation and Bonus-penalty is  $\mathcal{O}(n)$ , since each vehicle has to be traversed. There exists no computation involved in the information transmission, so the complexity is 0.

TABLE II  
COMMUNICATION AND COMPUTATIONAL COMPLEXITY

	Communication complexity	computational complexity
ITVs selection	–	$\mathcal{O}(4n)$
Information transmission	$\mathcal{O}(n)$	–
Information evaluation	–	$\mathcal{O}(n)$
Bonus-penalty	$\mathcal{O}(n)$	$\mathcal{O}(n)$

### E. Security Analysis

In this part, we analyze the proposed scheme under several common malicious attacks.

1) *Double-spending attack*: In the proposed scheme, the transaction validators would be picked by tPoR integrating with the traffic environment and the reputation value of vehicles, and thus it is almost impossible for two blocks to have the same attributes simultaneously, thereby resolving the double-spending attack.

2) *Sybil attack*: In the proposed scheme, each vehicle has to be authenticated when entering the system, and a blockchain wallet is issued for it, with the wallet address as its unique communication id. In the consensus process, vehicles with higher reputation values are more likely to become transaction validators, and IoV has high mobility, ensuring the randomness of consensus process, and thus eliminating Sybil attack.

3) *Collusion attack*: Firstly, most ITVs have high reputation values, and collusion with MRVs can be avoided significantly. Secondly, if a group wants to launch a collusion attack successfully, then it has to ensure that all vehicles in the group have high reputation value and appear in the same place simultaneously. Also, it needs to ensure that no other vehicles with high reputation values could report messages, which is very challenging to implement in the IoV with heavy traffic.

4) *Bad-mouthing attack or False-praise attack*: In the proposed scheme, the management of all nodes' reputation values is realized by the system through the judgment feedback of information, and there is no malicious comment among nodes. Therefore, tPoR can resist such attacks.

5) *Self-promoting attack*: In the proposed scheme, the reputation of message set would be considered in the information verification phase, thus hardly posing a threat to this scheme.

## IV. CONCLUSION

In this paper, a novel consensus mechanism tPoR is proposed for the information sharing in IoV, which could improve the consensus efficiency and randomness by integrating TOPSIS (to pick transaction validators) with various traffic environment factors. Meanwhile, the authenticity of the sharing information is judged based on the vehicles' reputation value. This paper also provides an idea for the application of blockchain in other fields, which uses TOPSIS to combine data from scenarios to achieve lightweight consensus. In the future, more realistic and complex traffic scenarios will be studied to verify the applicability of tPoR, and the privacy protection of the vehicle will be considered more comprehensively.

## REFERENCES

- [1] J. Wang, C. Jiang, Z. Han, Y. Ren, and L. Hanzo, "Internet of vehicles: Sensing-aided transportation information collection and diffusion," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, p. 13, 2018.
- [2] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, 2021.
- [3] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, "How much communication resource is needed to run a wireless blockchain network?" *IEEE Network*, vol. 36, no. 1, pp. 128–135, 2022.
- [4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," [Online]. Available: <https://bitcoin.org/bitcoin.pdf>, 2008.
- [5] W. Junfei, J. Li, Z. Gao, Z. Han, C. Qiu, and X. Wang, "Resource management and pricing for cloud computing based mobile blockchain with pooling," *IEEE Trans. Cloud Comput.*, 2021.
- [6] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5549–5561, 2020.
- [7] Z. Zheng, J. Pan, and L. Cai, "Lightweight blockchain consensus protocols for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5736–5748, 2020.
- [8] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, 2019.
- [9] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, 2020.
- [10] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–11, 2021.
- [11] Y. Song, Y. Fu, F. R. Yu, and L. Zhou, "Blockchain-enabled internet of vehicles with cooperative positioning: A deep neural network approach," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3485–3498, 2020.
- [12] C. Jiang, H. Zhang, Z. Han, Y. Ren, V. C. M. Leung, and L. Hanzo, "Information-sharing outage-probability analysis of vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9479–9492, 2016.
- [13] S. Zhu, Z. Cai, H. Hu, Y. Li, and W. Li, "zkcrowd: A hybrid blockchain-based crowdsourcing platform," *IEEE Trans. Ind. Inf.*, vol. 16, no. 6, pp. 4196–4205, 2020.
- [14] H. Desai, M. Kantarcioglu, and L. Kagal, "A hybrid blockchain architecture for privacy-enabled and accountable auctions," in *Proc. IEEE Int. Conf. Blockchain*, Jul. 2019, pp. 34–43.
- [15] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1238–1246.
- [16] B. P. Carlin and T. A. Louis, *Bayesian methods for data analysis*. CRC Press, 2008.