$\mathcal{R}$-Tracing: Consortium Blockchain-Based Vehicle Reputation Management for Resistance to Malicious Attacks and Selfish Behaviors

Yuwei Xu, *Member, IEEE*, Enze Yu, *Student Member, IEEE*, Yuxing Song, Fei Tong, *Member, IEEE*, Qiao Xiang, *Member, IEEE*, and Liang He, *Senior Member, IEEE*

***Abstract*—Empowered by 5G communication technology, high-speed information exchange can be realized on the Internet of Vehicles (IoV) for intelligent transportation applications. Since most applications require vehicles to report perceived information to nearby base stations, how to defend against malicious attacks and selfish behaviors of vehicles in reporting activities has become an essential security issue. Some researchers have attempted to encourage vehicles to actively report information by establishing reputations for them, but these efforts have some shortcomings. In model design, they neither verify the basis and process of reputation evaluation nor pay attention to the diversity and intelligence of vehicle behaviors. In system construction, they fail to meet the management needs of multi-party participation and provide verifiable reputation management services. In this paper, we propose $\mathcal{R}$-tracing, a consortium blockchain-based vehicle reputation management scheme. The main contribution of our work lies in three points. First, a vehicle reputation model is designed with a reward and punishment mechanism and a regular tax mechanism. Second, a vehicle reputation management system is constructed by multiple organizations, in which all tasks of reputation update are abstracted into three types of transactions. Finally, the effectiveness of $\mathcal{R}$-tracing is verified by extensive simulations running on a large-scale traffic scenario and performance evaluation on a prototype system. Compared with the typical linear reputation model, our model not only resists the usual malicious attack and selfish behavior but also effectively deals with the on-off attack and rational selfish behavior. In the throughput test, $\mathcal{R}$-tracing achieves 600*tps*, outperforming two state-of-the-art schemes.**

***Index Terms*—Vehicle reputation management, consortium blockchain, 5G Internet of Vehicles, malicious attacks, selfish behaviors.**

I. Introduction

With the rapid development of 5G communication technology, the Internet of Vehicles (IoV) has become the cornerstone of the intelligent transportation system (ITS). It supports a variety of future applications, such as road traffic status detection [1], anti-collision warning for autonomous driving [2], and vehicle service information sharing [3]. For intelligent transportation applications, there is a typical information exchange mode in which a vehicle first reports its perceived information to the nearby base station, and the base station shares the processed results with other vehicles on the road. Therefore, the stable operation of applications in this mode largely depends on vehicles actively reporting a large amount of truthful information. Since the vehicle is manned, it may launch malicious attacks [4] and demonstrate selfish behaviors [5] when reporting information. On the one hand, malicious attackers can make vehicles send fake information to interfere with applications. On the other hand, selfish users can refuse vehicles to undertake the task of information reporting from the perspective of reducing overhead. To ensure the availability of intelligent transportation applications, how to resist malicious attacks and suppress selfish behaviors has become an important security issue.

The schemes based on cryptography [6], [7] can guarantee the confidentiality, integrity, and availability of the reported information but cannot identify the authenticity of the information content. To encourage vehicles actively report truthful information, it is a promising idea to assign them reputation values and build a reputation model for management [8]. To resist malicious attacks and suppress selfish behaviors, vehicle reputation models have been proposed by leveraging many methods such as machine learning [9] and Dempster-Shafer theory [10]. Although they have been used to evaluate the reputation of vehicles and the authenticity of reported information, there are still some challenges to resolve. First, the traceability of the calculation basis and the verifiability of the calculation process have not been considered in reputation evaluation. The methods [11], [12] of establishing trust relationships through reviews from neighbor vehicles cannot meet those requirements. Attackers can exploit

Manuscript received 1 May 2022; revised 27 August 2022 and 6 November 2022; accepted 10 January 2023. Date of publication 20 January 2023; date of current version 20 June 2023. This work was supported in part by the National Key R&D Program of China under Grant 2020YFB1005500, in part by the National Natural Science Foundation of China under Grant 61702288, and in part by the Fundamental Research Funds for the Central Universities, Southeast university. The review of this article was coordinated by Prof. Zibin Zheng. *(Corresponding author: Yuwei Xu.)*

Yuwei Xu and Fei Tong are with the School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China, also with the Purple Mountain Laboratories, Nanjing 211111, China, and also with the Engineering Research Center of Blockchain Application Supervision, Ministry of Education, Nanjing 211189, China (e-mail: xuyw@seu.edu.cn; ftong@seu.edu.cn).

Enze Yu and Yuxing Song are with the School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China (e-mail: enzeyftong@seu.edu.cn; yuxingftong@seu.edu.cn).

Qiao Xiang is with the School of informatics, Xiamen University, Xiamen 361000, China (e-mail: qiaoxiang@xmu.edu.cn).

Liang He is with the Department of Computer Science and Engineering, University of Colorado, Denver 80204 USA (e-mail: liang.he@ucdenver.edu).

Digital Object Identifier 10.1109/TVT.2023.3238507

their vulnerabilities to forge a vehicle's reputation value. Second, little attention has been paid to the adversarial capabilities improved by intelligent vehicles. Malicious vehicles can avoid being kicked out of the system by switching states, while selfish vehicles can also selectively report information to maintain a minimum overhead. Third, the circulation of reputation value in the whole system has not been considered for long-term management. After many nodes obtain high reputation values, the problem of reputation depreciation may occur, which breeds malicious attacks and selfish behaviors of vehicles.

In addition to the work of model design, the construction of a vehicle reputation management system is another important issue attracting attention from academia and industry. In the 5G-enabled intelligent transportation scenario, the department of motor vehicle (DMV), police department (PD), and multiple mobile operators (MO) have the willingness and responsibility to participate in the reputation management of vehicles. The centralized solutions [13], [14] cannot meet the needs of multi-party management and suffer from some inherent shortcomings such as performance bottleneck and single-point vulnerability. Distributed deployment schemes [15], [16] can overcome the above shortcomings, but still face the problem of how to provide publicly verifiable reputation management services. In recent years, some scholars have tried to use blockchain technology to build a vehicle reputation management system. So far, most previous attempts have only utilized the properties of blockchain, such as distributed storage and data immutability. They have failed to meet the management needs of multi-party participation in future intelligent transportation scenarios. Besides, most previous works have focused on the scheme design but ignored the construction and testing of a prototype system. Although a few studies [17], [18] have built experimental systems through Ethereum technology, their performance does not meet the requirements for implementation in real scenarios.

To address the limitations of previous works, we propose $\mathcal{R}$-tracing, a consortium blockchain-based scheme to manage the reputation value $\mathcal{R}$ of vehicles. The main contributions of our work are summarized as follows.

- A complete vehicle reputation model is proposed with three innovations. First, our model takes the confirmed information as the calculation basis to ensure the update process of reputation value is credible. Second, a reward and punishment mechanism based on the signaling model is proposed, which effectively resists malicious attacks and derived on-off attacks. Finally, a regular tax mechanism is designed for vehicles' reputation, which not only suppresses various selfish behaviors but also maintains the dynamic balance of reputation value in the management system.
- A vehicle reputation management system based on consortium blockchain is designed for 5G-enabled intelligent transportation scenarios. First, a distributed architecture is adopted by leveraging Hyperledger Fabric to meet the management needs of multi-party participation. Second, management tasks are abstracted into three types of transactions and recorded on the chain to realize the traceability of the reputation update process. Finally, three smart contacts are designed for different types of transactions. Besides, an organization-based endorsement strategy is proposed to ensure that each update of reputation value is verifiable by executing a smart contract.
- $\mathcal{R}$-tracing is fully verified to be an effective scheme for vehicle reputation management in future intelligent transportation scenarios. First, through theoretical analysis and software simulation, we prove that our model not only resists malicious attacks and selfish behaviors but also copes with challenges posed by vehicle intelligence. Second, by building and testing a prototype system, we show the feasibility of the system design and its performance advantages compared with previous works.

The remainder of this paper is organized as follows. The related work is summarized in Section II. The overview of $\mathcal{R}$-tracing is described in Section III by introducing the system components, management tasks, and design goals. We present our vehicle reputation model in Section IV and the system scheme in Section V. An in-depth analysis is given in Section VI to demonstrate that $\mathcal{R}$-tracing achieves the design goals. In Section VII, $\mathcal{R}$-tracing is verified by software simulations and system experiments. Finally, our work is concluded in Section VIII.

II. Related Work

In this section, we analyze the previous studies from different concerns and summarize their contributions to model design and system construction in Table I.

A. Vehicle Reputation Model

Early studies focused on assessing the authenticity of the information reported by vehicles. In [19], the authenticity of information content is calculated by detecting contextual associations using information entropy theory. On this basis, the reporter's certificate is also introduced into the scheme of [20]. The generation time and signature times of the certificate are used as two important evaluation indicators. In [21] the authors argue that the closer the reporting vehicle is to the accident site, the higher the credibility of the information. Therefore, a method is proposed to assign different weights to different reporters of the same event by distance calculation and then evaluate the authenticity of the information through a voting algorithm. Although the factors considered by the above methods are related to the authenticity of the information, they are unreliable for evaluation, so the results may have serious deviations. In [22], the reporter's reputation is used as an important basis for evaluating whether a piece of information is truthful. Information sent by vehicles with high reputations is considered more credible than that sent by vehicles with low reputations. Therefore, vehicle reputation evaluation has gradually become the focus of research on building trust in IoV.

Some researchers try to solve the malicious behaviors of reporting forged information by establishing a vehicle reputation model. In [11], a model is proposed by combining subjective trust and recommendation trust. Subjective trust is the local

TABLE I
COMPARISON OF STUDIES ON VEHICLE TRUST MANAGEMENT

No.	Paper	Vehicle Trust Model					Vehicle Trust Management System					
		Basic idea	Malicious attack	Selfish behavior	Intelligent vehicle	Long-term balance	Deployment mode	Leverage blockchain	Multiple managers	Verifiable data	Verifiable calculation	System implementation
1	[10]	▽	✔	✗	✗	✗	▽	✗	✗	✗	✗	✗
2	[11]	△	✔	✗	✔	✗	▽	✗	✗	✗	✗	✗
3	[12]	△	✔	✗	✗	✗	▽	✗	✗	✗	✗	✗
4	[13]	▽	✔	✗	✗	✗	△	✗	✗	✗	✗	✗
5	[15]	△	✔	✗	✗	✗	▽	✗	✗	✗	✗	✗
6	[16]	▽	✔	✔	✔	✗	▽	✗	✗	✗	✗	✗
7	[17]	-	✔	✗	✗	✗	▽	✔	✔	✗	✔	✔
8	[18]	-	✔	✔	✗	✗	▽	✔	✗	✗	✔	✗
9	[19]	▽	✔	✗	✗	✗	△	✗	✗	✗	✗	✗
10	[20]	▽	✔	✗	✗	✗	▽	✗	✗	✗	✗	✗
11	[21]	▽	✔	✔	✗	✗	▽	✗	✗	✗	✗	✗
12	[22]	▽	✔	✗	✗	✗	▽	✔	✗	✗	✔	✗
13	[23]	△	✔	✗	✗	✗	▽	✔	✗	✗	✔	✗
14	[24]	▽	✔	✗	✔	✗	▽	✗	✗	✗	✗	✗
15	[25]	△	✔	✗	✗	✗	▽	✗	✗	✗	✗	✗
16	[26]	△	✔	✔	✗	✗	▽	✗	✗	✔	✔	✗
17	[28]	△	✔	✗	✔	✗	▽	✗	✗	✗	✗	✗
18	[29]	△	✔	✔	✔	✗	▽	✗	✗	✗	✗	✗
19	[30]	▽	✔	✔	✗	✗	△	✗	✗	✗	✗	✗
20	[31]	△	✔	✗	✗	✗	▽	✗	✗	✗	✗	✗
21	[32]	△	✔	✔	✗	✗	▽	✔	✗	✗	✔	✗
22	[33]	△	✔	✗	✗	✗	▽	✔	✔	✗	✔	✗
23	$\mathcal{R}$-tracing	△	✔	✔	✔	✔	▽	✔	✔	✔	✔	✔

In the basic idea column, △ represents the data-centric trust model, ▽ represents the entity-centric trust model.
In the column of deployment mode, △ represents the centralized solution while ▽ represents the distributed solution.

node's evaluation of the target vehicle based on historical communication records, while recommendation trust comes from the results obtained by asking other vehicles. The above idea is followed in [10]. The direct trust and recommendation trust are calculated respectively through the reputation matrix, and then the global trust value for the target vehicle is generated through a weight-based method. Similarly, a model named E-R is built in [12], in which the reputation value is evaluated according to knowledge, experience, and review. Experience and review respectively correspond to objective trust and recommendation trust in [11], while knowledge is calculated based on the trajectory of the target vehicle. Besides, the roadside unit (RSU) is set as the evaluator of vehicles' reputation values in [23]. After collecting neighbors' comments on the target vehicle, RSU calculates a global reputation value by using a deep learning algorithm. All the above methods utilize the reviews of other vehicles for reputation evaluation, but they cannot guarantee that every review is correct. Some studies attempt to design evaluation methods from other perspectives. In [24], the authors propose a vehicle trust management model named NOTRINO. This model calculates the reputation value based on two measurements, the distance between the evaluator and the target vehicle and the heights of their antennas. In [25], a vehicle's reputation value is calculated based on the forwarding ratios of data packets and control packets during a period. The calculation basis used in both schemes is reliable, but whether the vehicles' reputation can be accurately measured by these data or not is still a problem. To deal with selfish behaviors, the model in [26] requires that the reputation value should be deducted as the cost of reporting information. The more times a vehicle reports, the stronger its willingness to cooperate, therefore the lower the cost per report should be. The authors in [27] introduce an incentive mechanism to encourage vehicle cooperation. The vehicles are rewarded for successfully reporting information, thereby reducing the occurrence of selfish behaviors.

As the degree of intelligence increases, vehicles can adopt on-off attacks to evade the penalty of the reputation model. In [28], a reputation framework is proposed to distinguish normal behaviors from on-off attack behaviors. Since the local trust, recommendation trust, and event trust are comprehensively considered in reputation evaluation, the model obtains good results. A reputation model that combines vehicle-vehicle trust and vehicle-RSU trust is proposed in [16]. It can not only detect malicious attacks at an early stage but also defend against malicious on-off attacks. The method proposed in [29] not only calculates the current reputation value according to the neighbors' reviews but also predicts the change of reputation value by using the Dirichlet distribution function. Due to the increased punishment for malicious reporting, this method can effectively resist on-off attacks.

To deal with malicious attacks and selfish behaviors of vehicles, the reputation models are constructed by using different methods in the above studies. However, there are still three shortcomings. (1) When updating vehicles' reputation values, the calculation basis and process are not verified, which leads to the unreliability of the model. (2) There is not enough consideration for the confrontation ability exhibited by the intelligent vehicle. Not only malicious vehicles can switch states to evade detection, but also selfish vehicles can selectively report to maintain a minimum overhead. (3) Reputation management is not considered from the perspective of long-term operation, and reputation devaluation is a potential problem faced by a management system.

B. *Vehicle Reputation Management System*

In addition to model design, the construction of a reputation management system is another important issue that attracts academics and industries. In [13], a central server is deployed to store vehicles' reputation value, which is responsible for daily

updates and query requirements. The system implementation is vulnerable to various performance bottlenecks and single-point failure. Some scholars have tried to use cloud services to build a hierarchical reputation management system. A three-layer system architecture is proposed in [14]. According to its plan, vehicles at the bottom layer are responsible for reporting the perceived information, RSUs at the middle layer provides data transmission services, and cloud servers at the top layer are used to calculate and store the reputation values. In [30], the authors propose a similar hierarchical implementation. It differs from the scheme of [14] in that the vehicles at the bottom layer complete the initial evaluation of the reputation value through fog computing, while the cloud host at the top calculates a global result. Although the hierarchical scheme has made progress in performance than the server-based scheme, it does not meet the requirements of multi-party management in the 5G-enabled intelligent transportation scenarios.

Some scholars have proposed several distributed system schemes to manage the reputation of vehicles. In [15], each vehicle independently completes the reputation management by updating a local matrix according to the information received from neighbors. The authors of [31] follow this idea and propose to maintain a reputation table on each vehicle. A similar scheme is also adopted in [16], the difference is that the way of storing reputation values is upgraded to a lightweight database. Although these schemes achieve distributed reputation management, they bring a lot of overhead to vehicles. Furthermore, since they cannot verify the authenticity of information, the reputation values are unreliable.

In recent years, blockchain has become an important means of value transfer on the Internet due to its decentralization and immutability. In [34], the authors believe that blockchain technology can meet the needs of distributed management and publicly verifiable service in future intelligent transportation scenarios. A system implementation is proposed in [32], which builds a blockchain on the RSUs to store the vehicles' reputation values. To improve operation efficiency, it adopts a consensus mechanism combining proof-of-work (PoW) and proof-of-stack (PoS). The authors of [22] follow this architecture and build a trust management system on the Ethereum platform. In [33], a consortium blockchain is deployed on the edge base stations for data storage and management. To achieve secure and efficient data sharing, a smart contract requires the on-chain nodes to return the provider's reputation to the requester, so that the requester can choose the best data acquisition path. In [18], a dynamic proof-of-work (dPoW) consensus algorithm is proposed to scale the system operation according to the incoming traffic flow of vehicles. A reputation management system is built in [17] by using Ethereum, which adopts the idea of sharding to reduce the workload from the main chain, thereby improving the overall throughput. However, the above studies have not fully utilized the advantages of blockchain to meet the requirements of vehicle reputation management in future intelligent transportation scenarios. (1) Since most schemes adopt public chain technology, they cannot meet the requirements of distributed management involving multiple organizations such as DMV, PD, and MOs. (2) Since the public blockchain runs complicated consensus algorithms like PoW among all nodes, a transaction consumes a lot of computing and communication resources. As a result, the low system performance cannot meet the requirements for these schemes implemented in real scenarios.

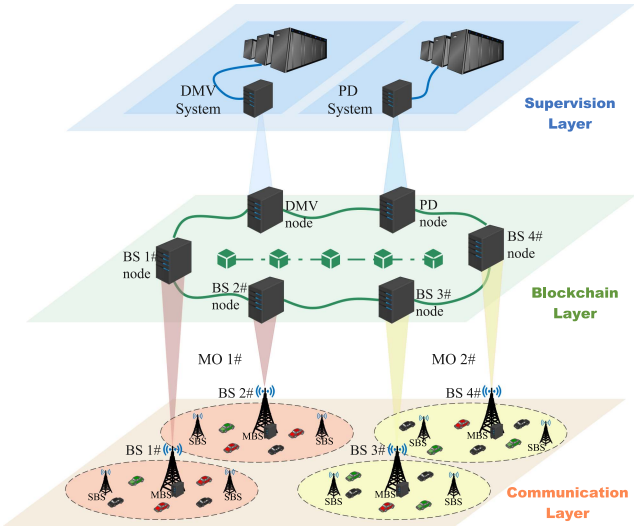


Fig. 1. Three-layer system for vehicle reputation management.

III. $\mathcal{R}$-Tracing in a Nutshell

To address the shortcomings of previous works, we propose $\mathcal{R}$-tracing, a vehicle reputation management scheme. It not only resists malicious attacks and suppresses selfish behaviors by establishing a reputation model but also meets the requirements of multi-party management and public verifiability by building a distributed ledger on a consortium blockchain. Next, we will introduce $\mathcal{R}$-tracing from three aspects: system components, reputation management tasks, and design goals.

A. System Components

As shown in Fig. 1, our system involves four roles: mobile operator (MO), department of motor vehicles (DMV), police department (PD), and vehicle. In cities, it is general that multiple MOs build and operate 5G networks. Besides, DMV and PD also have corresponding official bodies in different jurisdictions. Therefore, we introduce the concept of organization to represent DMV, PD, and each MO. According to $\mathcal{R}$-tracing, those organizations can deploy multiple nodes on the consortium chain for vehicle reputation management. All nodes within an organization trust each other, but organizations do not fully trust each other.

MOs are responsible for deploying base stations and building 5G networks to ensure that wireless signals can reach every block in urban areas. It is worth noting that the scenario in Fig. 1 includes two types of base stations: macro base station (MBS) and small-cell base station (SBS). In addition to transmitting wireless signals, MBS also has excellent computing and storage capabilities and is directly connected to the Internet. In Fig. 1, several SBSs are deployed around each MBS to make up the limited coverage of 5G signals. These SBSs can interact with

vehicles as an extension of the MBS, but do not own other resources. Therefore, the base station (BS) described below includes one MBS and its extended SBSs. In $\mathcal{R}$-tracing, each BS needs to deploy a node on the consortium blockchain to participate in reputation management and belong to the organization of the corresponding MO. Besides, BSs in cities are typically deployed by multiple MOs. As shown in Fig. 1, since two MOs have deployed four BSs in the scenario, they respectively manage two nodes on the consortium blockchain.

DMV is a government department responsible for registering vehicle information, issuing and revoking driving licenses, etc. According to $\mathcal{R}$-tracing, a vehicle should apply to the DMV before joining the intelligent transportation application. After receiving a request from a vehicle, the DMV needs to establish a reputation account on the consortium blockchain, assign an initial value, and issue a digital certificate for it. Besides, after a vehicle permanently exits the application, the DMV should withdraw its certificate, clear its reputation value, and cancel its account.

PD is a government department responsible for dealing with daily road congestion and traffic accidents to maintain good traffic order. In $\mathcal{R}$-tracing, PD takes the task of investigating the information reported by vehicles. As the content of any information may be forged, only the information confirmed by PD can be used as the reliable basis for the reputation calculation. In addition, since different neighborhoods have their own PDs, $\mathcal{R}$-tracing not only allows deploying a node on the consortium blockchain for each PD but also supports setting up only one node connecting to the internal system of PDs. Once a piece of new information is recorded on the chain, PD should immediately prove its authenticity. On the one hand, PD can confirm on the spot by dispatching the police, such as dealing with vehicle collisions. On the other hand, it can use the existing road traffic monitoring system for direct confirmation, such as observing congestion on a road segment.

Vehicles are both users of intelligent transportation services and probes reporting a large amount of sensing data. In our scheme, vehicles can accumulate their reputation by reporting information to BSs. However, vehicles are manned, so they inevitably exhibit malicious and selfish behaviors in the reporting activities. Besides, some vehicles also show certain intelligence to avoid detection. To deal with these problems, the distributed management of vehicle reputation needs to be achieved by DMV, PD, and MOs. It is worth noting that vehicles are the objects managed by those organizations, so they are not the nodes that constitute the consortium blockchain. In addition to reporting information, vehicles can also access the query service as users to check the reputation values of other vehicles. The whole process contains three steps. (1) A vehicle sends a request to an on-chain node providing the reputation value query service. (2) The node parses the request and obtains the reputation value from the consortium chain. (3) The result is encapsulated in a response and sent back to the user.

As shown in Fig. 1, the system of $\mathcal{R}$-tracing consists of three layers: the communication layer, the blockchain layer, and the supervision layer. At the communication layer, MOs deploy many BSs to achieve 5G signal coverage on all road sections. Vehicles report their perceived information to the nearest BS anytime and anywhere through the 5G wireless connections. At the blockchain layer, DMV, PD, and MOs jointly maintain a distributed ledger on the consortium blockchain. As $\mathcal{R}$-tracing records all the update operations in the form of transactions, it can obtain the current reputation value of each vehicle at any time. It is worth noting that the entire chain is composed of nodes deployed by DMV, PD, and MOs. Since the BSs have sufficient computing, storage, and communication resources, MOs should add their BSs as nodes to the consortium blockchain. Besides, DMV and PD also need to deploy multiple nodes on the chain according to their organization settings. At the supervision layer, DMV and PD need to provide off-chain support for the system operation of $\mathcal{R}$-tracing. DMV undertakes the vehicle registration and identity verification services. Once a vehicle's reputation value reaches 0, DMV should immediately log off its account and kick it out of the intelligent transportation applications. For every piece of reported information, PD should verify its authenticity. In this way, each update of the reputation value is based on objective facts rather than subjective evaluations.

B. Reputation Management Tasks

In $\mathcal{R}$-tracing, DMV, PD, and MOs jointly set up an official account on the consortium blockchain and manage the reputation values of all vehicles in the form of transactions. Based on the scenario analysis in Section III-A, we set two types of reputation management tasks: reputation management for reported information and periodic reputation management for vehicles.

The reputation management for reported information aims to reward and punish vehicle's reputation values according to the authenticity of their reported information. In Fig. 1, vehicles report the perceived information to the nearest BS during the driving process. After verifying the identity of reporting vehicle, BS submits a transaction request to the chain. In this transaction, a portion of the reputation value in the vehicle account is deducted as the cost of reporting the information. After receiving the request, other nodes on the chain should endorse this transaction. Only when the number of endorsements reaches the specified threshold, this transaction is successfully recorded on the chain. At the same time, PD knows this transaction on the chain and tries to investigate the authenticity of the reported information. After obtaining the result, PD submits another transaction on the chain to update the reputation value of the reporter. If the investigation result is true, the reputation value is increased as a reward. Otherwise, a part of the reputation value is deducted as a penalty. Similarly, the transaction is recorded on the chain after being endorsed by enough nodes.

The periodic reputation management for vehicles focuses on preventing vehicles from selfish behaviors. When a vehicle exhibits selfish behavior, it will not actively report information to the BS. Therefore, the method of rewarding and punishing vehicles based on the reported information cannot be used to suppress selfish behaviors. To deal with vehicles that only want to enjoy the convenience and not fulfill the responsibility, $\mathcal{R}$-tracing requires the system to periodically collect the reputation value from the vehicle as a tax. At the end of each management

period, the system first counts the income and expenditure of the official account and all vehicle accounts, then calculates the total amount of tax that needs to be collected from vehicles, and finally calculates the tax for each vehicle based on its performance in the last period.

C. Design Goals of $\mathcal{R}$-Tracing

To achieve the reputation management of vehicles in 5G-enabled intelligent transportation scenarios, we summarize the design goals of our $\mathcal{R}$-tracing in the following aspects.

1) Resistance to Malicious Attacks: The **Malicious Attack (MA)** is carried out by the vehicle sending false information to the roadside base station to disrupt intelligent transportation applications. For example, a malicious vehicle reports a traffic accident that did not occur to obstruct the traffic order. For reputation management, once a vehicle with MA is detected, it should be severely punished or even excluded from the system.

2) Resistance to Selfish Behaviors: The **Selfish Behaviors (SB)** is displayed by the vehicle not reporting any perceived information to the roadside BS. In this way, it can avoid the overhead in computing, communication, and energy during its driving progress. In reputation management, the vehicles that actively report information should be rewarded, while those with SB should pay for their silence.

3) Resistance to Intelligent MA and SB: With the improvement of computing power and the application of AI technology, vehicles are becoming more intelligent to implement MA and SB. The **Malicious On-off Attack (MOA)** is an upgraded variant of MA. The vehicle that has accumulated a good reputation by actively reporting for a long time may launch a MA under certain circumstances and switch back to the normal mode as soon as the attack is over. In addition, the **Rational Selfish Behaviors (RSB)** becomes a more reasonable choice for the vehicle to survive in the system. The vehicle participates in intelligent transportation activities with the premise of minimizing its overhead. In general, it does not report any information. Only when it finds itself unsustainable will the vehicle switch back to the normal mode. For MOA, it is necessary to record the attacks carried out by each vehicle and increase the punishment according to the number of attacks. For RSB, the reputation value needs to be reduced continuously to force the vehicle back to the normal reporting mode.

4) Distributed Management of Reputation: From the view of system design, $\mathcal{R}$-tracing must meet the requirements of distributed reputation management in 5G-enabled intelligent transportation scenarios. First, different mobile operators and government departments ally to manage the reputation values of all vehicles in the system. Second, each update of the vehicles' reputation value requires the participation of multiple managers to calculate authoritative results based on the consensus protocol.

5) Reputation Calculation is Publicly Verifiable: In the scenario shown in Fig. 1, although MO, PD, and DMV ally to manage the reputation of vehicles, they do not fully trust each other. In addition, system users hope to verify the reputation value of any vehicle at any time. Therefore, publicly verifiable reputation calculation is another design goal of our system. First, the calculation basis in each update operation should be the confirmed objective facts rather than the subjective evaluations derived from others. Second, the calculation basis must be recorded and not tampered with to ensure the reliability of raw data. Finally, the calculation progress must be agreed upon by managers to establish standard methods for public verification.

6) Avoidance of Reputation Devaluation: Reputation devaluation refers to the phenomenon that after the long-term operation of the reputation management system, the reputation values of most vehicles are close to or even reach the upper bound due to the active reporting of real information. In this case, any trust relationship established based on the vehicle's reputation values will become unreliable. Therefore, it is necessary to manage reputation from the perspective of the whole system to realize the circulation of reputation value among different entities.

IV. Vehicle Reputation Model

In this section, we propose a vehicle reputation model as the cornerstone of $\mathcal{R}$-tracing. Compared with previous works, our model makes three improvements. First, to ensure the reliability of the reputation evaluation, only the confirmed information is used as the calculation basis. Both the information reported by vehicles and the investigation results returned by PD are recorded as transactions on a consortium blockchain to ensure that the update of reputation value is traceable. Second, a reward and punishment mechanism based on a signaling model is presented to defend against malicious attacks and derived on-off attacks. Finally, a regular tax mechanism is proposed to suppress various selfish behaviors and achieve a dynamic balance of reputation value for long-term management.

A. Reward and Punishment Mechanism

To resist malicious attacks in the reporting activities of vehicles, we propose a reward and punishment mechanism based on the signaling model in economics. Vehicles are required to add a signal value e to each reported information. e indicates the degree to which the vehicle confirms its current reported information. If the value of e is high, it means that the vehicle is very sure of the information it reports. After a BS receives the information, even if the authenticity of the information has not been verified, it can make a preliminary judgment through a high e value. In addition, the vehicle needs to deduct a part of the reputation value from its account as the cost c of reporting a piece of information. In our model, the function $C(e, \mathcal{R})$ is designed for the calculation of c. There are three properties that $C(e, \mathcal{R})$ needs to satisfy. First, the vehicle should be able to pay the cost for each reported information. Second, the vehicle that set a higher e when sending information should pay more. Third, the vehicle with a higher value of reputation $\mathcal{R}$ should pay less in the same situation. Based on the above analysis, these properties are described as follows.

- $\forall e, \mathcal{R}, C(e, \mathcal{R}) \in [e, \mathcal{R}]$
- $\forall \mathcal{R}, C(0, \mathcal{R}) = 0$
- $\frac{\partial C(e,\mathcal{R})}{\partial e} > 0$

- $\frac{\partial C(e,\mathcal{R})}{\partial \mathcal{R}} < 0$

To satisfy three properties, $C(e,\mathcal{R})$ is defined formula (1), where α is the tuning parameter set for different applications. Since the vehicle should be kicked out of the system after its $\mathcal{R}$ becomes 0, the value of $\mathcal{R}$ in our model is always greater than 0. According to formula (1), when e takes the value of $\mathcal{R}/\sqrt{\alpha}$, $C(e,\mathcal{R})$ reaches the maximum value $\mathcal{R}$.

$$C(e,\mathcal{R}) = \frac{e^2}{\alpha \mathcal{R}} \tag{1}$$

After the information is verified, the model needs to reward or punish the reputation value of the reported vehicle. The function $W(e)$ is designed for the calculation of the reward w. On the one hand, the value of w should be higher than the cost of c paid by the vehicle before. On the other hand, the vehicle that set a higher e when sending information should obtain more reward. Besides, the function $P(f)$ is designed for the calculation of the penalty. After the information is verified as false, the model proportionally deducts a portion of the vehicle's current reputation value. Since all reporting activities are recorded on the chain, the model can count the number of malicious attacks f the vehicle has performed, and make the penalty become severe as f increases. According to the above analysis, properties that $W(e)$ and $P(f)$ need to satisfy are summarized as follows:

- $\forall e, \mathcal{R}, W(e) > C(e,\mathcal{R})$
- $\frac{\partial W(e)}{\partial e} > 0$
- $\frac{\partial P(f)}{\partial f} > 0$

To achieve the above properties, we respectively define $W(e)$ and $P(f)$ in formula (2) and (3). Like α, β in formula (2) is also a tuning parameter set for different applications. Due to equipment failures and programming errors, the model should tolerate the vehicle reporting incorrect information several times. The vehicle should only be removed from the system if it is found to have carried out multiple malicious attacks. Therefore, $P(f)$ is designed as a piecewise function. The reputation value of the vehicle is reduced to 0 only when f is greater than the threshold thr_1.

$$W(e) = \begin{cases} 0 & r = false \\ \beta e & r = true \end{cases} \tag{2}$$

$$p(f,\mathcal{R}) = \begin{cases} \mathcal{R} & f > thr_1 \\ \left(1 - \left(\frac{1}{2}\right)^f\right) * \mathcal{R} & f \le thr_1 \end{cases} \tag{3}$$

B. Tax Mechanism

For long-term management of vehicle reputation, we propose a regular tax mechanism. $\mathcal{R}$-tracing sets up an official account for multiple managers. In daily management, the reputation value circulates between the official account and the private accounts of vehicles. When a management period ends, the reputation value S paid from the official account is counted according to formula (4). W is the total number of reputation values awarded to the honestly reporting vehicles, P is the total number of reputation values deducted from vehicles performing malicious attacks, and C is the sum of the costs paid by vehicles for reporting information. Besides, l is the total number of times that all vehicles report information in one period, where m represents the number of times PD's investigation result is true, and n represents the number of times the result is false.

$$S = W - P - C = \sum_{i}^{m} w_i - \sum_{i}^{n} p_i - \sum_{i}^{l} c_i \tag{4}$$

If S is greater than 0, the official will charge reputation value to all vehicles as tax. The function T($\mathcal{R}, \delta, d$) is designed to calculate the tax paid by each vehicle, and it should satisfy three properties. First, the vehicle is classified into a subset for processing according to its reputation value change δ in the last management period. Three subsets are set up in the model, which correspond to the increase, decrease and unchanged situation of the reputation value respectively. Second, no matter whether the reputation value increases or decreases, the tax paid by the vehicle increases with the increment in the absolute value of δ. If the reputation value remains unchanged, the tax paid by the vehicle is positively related to the value of $\mathcal{R}$. Finally, the mileage d in the last period is also used as an evaluation factor. The larger the d, the longer the vehicle has been active in the system, and the more tax it needs to pay. The vehicle with a higher d enjoys more service, so it should pay more tax. According to the above analysis, $T(\mathcal{R}, \delta, d)$ is defined in formula (5), where n_1, n_2 and n_3 are the number of vehicles in the three subsets. T_1, T_2 and T_3 are the taxes that the vehicles in the three subsets should pay respectively. When the model is applied, $T_i, i \in \{1,2,3\}$ can be calculated by presetting the ratio γ_i of each subset in total tax S.

$$T(\mathcal{R},\delta,d) = \begin{cases} \frac{1}{2}\left(\frac{\delta}{\sum_{i=1}^{n_1}\delta_i} + \frac{d}{\sum_{i=1}^{n_1} d_i}\right) T_1 & \delta > 0 \\ \frac{1}{2}\left(\frac{|\delta|}{\sum_{i=1}^{n_2}|\delta_i|} + \frac{d}{\sum_{i=1}^{n_2} d_i}\right) T_2 & \delta < 0 \\ \frac{1}{2}\left(\frac{\mathcal{R}}{\sum_{i=1}^{n_3}\mathcal{R}_i} + \frac{d}{\sum_{i=1}^{n_3} d_i}\right) T_3 & \delta = 0 \end{cases} \tag{5}$$

V. Vehicle Reputation Management System

In $\mathcal{R}$-tracing, we build a vehicle reputation management system based on a consortium blockchain, which meets the needs of multi-party management in the 5G-enabled intelligent transportation scenarios and achieves the public traceability of the reputation update process. In the following paragraphs, we define the vehicle reputation management activities as three types of transactions, show the system component and workflow, and introduce three smart contracts and related endorsement strategies.

A. Transactions on Consortium Blockchain

According to the vehicle reputation management activities described in Section III-B, three different types of transactions are defined on the chain. Type 1 transaction is designed for the reporting activities of vehicles. In such transactions, the information is recorded on the chain and a certain amount of reputation value is deducted from the reporting vehicle's account. Type 2 transaction is designed to reward and punish a vehicle by updating its reputation value after its reporting information is verified. The reward or punishment is calculated according to the investigation result provided by PD. All the details are kept in a

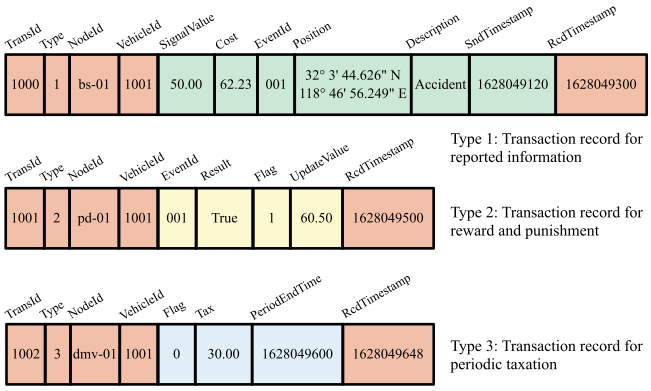


Fig. 2. Three types of transaction records.

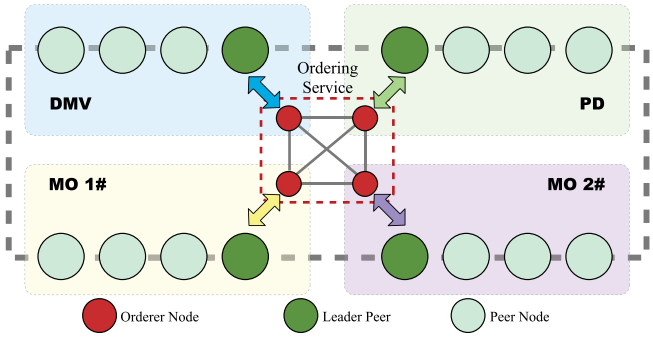


Fig. 3. System construction by consortium blockchain.

transaction record and submitted to the chain. Type 3 transaction is designed to tax vehicles periodically. In such transactions, a portion of the reputation value is deducted from the vehicle's account and transferred to the official account.

Fig. 2 shows the structure of the three types of transactions. In our system, *TransId* is the identifier assigned to each transaction, *Type* is the field marking the transaction type, *NodeId* records the node who submits this transaction, and *RcdTimestamp* is the time when the transaction is submitted to the chain. In the record of Type 1 transaction, *VehicleId* indicates the identity of the reporter, *SndTimestamp* saves the time when the information is sent, and the fields of *EventId*, *Position*, and *Description* record the event details contained in the information. According to our vehicle reputation model, a vehicle should select a signal value before reporting information to BS. On basis of it, the cost of reporting this information is calculated and deducted from the vehicle's reputation account. In Fig. 2, the fields of *SignalValue* and *Cost* are set to record these two important values. In the record of Type 2 transaction, *EventId* specifies the event described in the information, and *Result* is the feedback provided by PD after investigating the event. If the event is confirmed, the vehicle's reputation value is increased as a reward. Otherwise, a part of the reputation value is deducted as a penalty. In the record of Type 2 transaction, *Flag* marks whether the current transaction is a reward or punishment, and *UpdateValue* records the specific value of this operation. In the record of Type 3 transaction, *Tax* indicates the reputation value that needs to be deducted from the vehicle marked by *VehicleId*. Since all vehicles are divided into three categories to calculate taxes separately, *Flag* records the category of the current vehicle. Besides, *PeriodEndTime* records the end moment of the last management period.

B. System Architecture

As shown in Fig. 3, our vehicle reputation management system is built on a consortium blockchain. Different organizations, such as DMV, PD, and MOs, are responsible for constructing this chain. Each organization should deploy multiple hosts as peer nodes and elect a leader peer to communicate with other organizations. As mentioned in Section III-A, MOs can determine the number of peer nodes by referring to the number of their base stations, while DMV and PD need to set the number of peer nodes according to their demands. In Fig. 3, all the peer nodes jointly maintain a distributed ledger. Each transaction that updates a vehicle's reputation value is recorded on the chain for publicly verifiable reputation management. Besides, each organization should deploy an orderer node in the system. Those orderer nodes form a network that provides an ordering service for every transaction.

In $\mathcal{R}$-tracing, we achieve vehicle reputation management by executing three types of transactions. Every transaction must pass through the following three steps before being recorded on the chain. First, a peer node submits a transaction on the chain. Different types of transactions are submitted by the peer nodes of different organizations. For Type 1 transactions, BS is the local receiver of the information, so its peer node is responsible for the submission. For Type 2 transactions, as PD is the authoritative provider of the investigation result, its peer nodes should complete this task. For Type 3 transactions, since DMV is the official manager of vehicles, its peer nodes are responsible for the submission. Second, the transaction is confirmed according to an endorsement strategy. It is essentially a process of repeated execution of the same smart contract by other peer nodes. Only after the endorsement strategy is satisfied is the transaction confirmed officially and granted the qualification to record on the chain. Finally, the peer node submitting the transaction sends it to the orderer nodes. After reaching a consensus on the sequence of recent transactions, the orderer nodes pack the transaction records into a block and notifies all on-chain nodes to update the distributed ledger.

C. Smart Contracts

In our system, the update process of reputation value is guaranteed to be publicly verifiable by using smart contracts. For three types of transactions, different smart contracts are designed and deployed on the chain in the form of chaincodes. When a peer node submits a transaction, other nodes endorse it by executing the corresponding smart contract. If the execution result is correct, the transaction is successfully endorsed once. For a consortium blockchain, a unified endorsement strategy needs to be formulated for three types of transactions. In our system, we adopt two different endorsement strategies. The first is the basic N-time endorsement strategy (N-strategy), while the second is an organization-based endorsement strategy

Algorithm 1: O-strategy.

Input: *trd*: transaction record; $\mathbb{O}$: organization set; $\mathbb{E}$: endorsing node set;
Output: *rlt*: endorsement result;
for o_i *in* $\mathbb{O}$ **do**
  $e_i \leftarrow o_i$.***get_random_node***();
  $\mathbb{E}$.***add_node***(e_i);
$cnt \leftarrow 0$;
for e_i *in* $\mathbb{E}$ **do**
  switch (*trd.type*) **do**
    case *1* **do**
      $f \leftarrow e_i$.***call_smart_contract_1***(*trd*);
      break;
    case *2* **do**
      $f \leftarrow e_i$.***call_smart_contract_2***(*trd*);
      break;
    case *3* **do**
      $f \leftarrow e_i$.***call_smart_contract_3***(*trd*);
      break;
  if f **then**
    $cnt \leftarrow cnt + 1$;
if (cnt = $\mathbb{E}$.***get_size***()) **then**
  rlt $\leftarrow$ true;
else
  rlt $\leftarrow$ false;
return *rlt*;

Algorithm 2: Smart Contract for Type 1 Transactions.

Input: *trd*: transaction record;
Output: *rlt*: execution result;
$r \leftarrow$ ***get_report_from_node***(*trd.nodeId,trd.transId*);
$\mathcal{R} \leftarrow$ ***get_reputation_from_chain***(*trd.vehicleId*);
if (*trd.signalValue* = *r.signalValue*) **then**
  $c \leftarrow$ ***cal_cost***(*trd.signalValue*,$\mathcal{R}$);
  if ($c > \mathcal{R}$ OR $c < 0$) **then**
    rlt $\leftarrow$ false;
  else if (c = $trd.cost$) **then**
    rlt $\leftarrow$ true;
  else
    rlt $\leftarrow$ false;
else
  rlt $\leftarrow$ false;
return *rlt*;

Algorithm 3: Smart Contract for Type 2 Transactions.

Input: *trd*: transaction record;
Output: *rlt*: execution result;
$r \leftarrow$ ***get_report_from_node***(*trd.nodeId,trd.transId*);
$\mathcal{R} \leftarrow$ ***get_reputation_from_chain***(*trd.vehicleId*);
if (*trd.result* = *r.result*) **then**
  if (*trd.result*) **then**
    $e \leftarrow$ ***get_signal_from_chain***(*trd.eventId*);
    $w \leftarrow$ ***cal_reward***(e);
    if (w = *trd.updateValue*) **then**
      $\mathcal{R}' \leftarrow \mathcal{R} + w$
    else
      rlt $\leftarrow$ false;
  else
    $f \leftarrow$ ***get_punish_num_from_chain***(*trd.vehicleId*);
    $p \leftarrow$ ***cal_punish***(f,$\mathcal{R}$);
    if (p= *trd.updateValue*) **then**
      $\mathcal{R}' \leftarrow \mathcal{R}$ - p
    else
      rlt $\leftarrow$ false;
  if ($\mathcal{R}' > \mathcal{R}_{max}$ OR $\mathcal{R}' < 0$) **then**
    rlt $\leftarrow$ false;
  else
    rlt $\leftarrow$ true;
else
  rlt $\leftarrow$ false;
return *rlt*;

(O-strategy) proposed by us. In N-strategy, if the endorsement times of a transaction reach the threshold n, it will be delivered to the orderer node. O-strategy requires that any transaction is allowed to be delivered to the orderer node only after at least one node of each organization completes the endorsement. As shown in Algorithm 1, O-strategy consists of two main steps: (1) An endorsing node is randomly selected from each organization and added to the specified set constructed for the current transaction. (2) Each endorsing node executes the corresponding smart contract to confirm the transaction. Only after all the selected nodes have confirmed the transaction is the entire endorsement process completed.

In $\mathcal{R}$-tracing, we design three smart contracts for different types of transactions. The first one is for Type 1 transactions. As shown in Algorithm 2, it takes a transaction as input and the execution result as output. According to the contract, the endorsing node first gets the report from the submitting node and queries the current reputation value of the specified vehicle. Then, it verifies the signal value in the transaction and calculates the cost that the reporting vehicle should pay for the information. Finally, the endorsing node checks whether the result of cost is correct. If all condition is satisfied, it returns true. Otherwise, it returns false. The second smart contract is for Type 2 transactions. It also takes a transaction as input and the execution result as output. According to Algorithm 3, the endorsing node first gets the report from a PD's node and queries the current reputation value of the specified vehicle. Then, it calculates the reward or punishment for the reporting vehicle according to the investigation result. Finally, it checks whether the updated value is reasonable. If the new reputation value is confirmed correct, it returns true. Otherwise, it returns false. The third smart contract is designed for Type 3 transactions. Its input is a transaction, and the output is the execution result. According to Algorithm 4, the endorsing node first calculates the changes of the official account and vehicles' accounts in the latest management period, then calculates the tax of the specified vehicle according to its category, and finally checks the reputation value after deducting the tax. It returns true if the updated reputation value is correct. Otherwise, it returns false.

VI. Analysis of $\mathcal{R}$-Tracing

In this section, we conduct an in-depth analysis of $\mathcal{R}$-tracing to demonstrate that it can meet the design goals presented in Section III-C.

Algorithm 4: Smart Contract for Type 3 Transactions.

Input: *trd*: transaction record;
Output: *rlt*: execution result;
$S \leftarrow$ ***get_official_account_change***(*trd.periodEndTime*);
$T_1 \leftarrow \mathrm{a} \cdot S$;
$T_2 \leftarrow \mathrm{b} \cdot S$;
$T_3 \leftarrow \mathrm{c} \cdot S$;
$\mathcal{R} \leftarrow$ ***get_reputation_from_chain***(*trd.vehicleId*);
$m \leftarrow$ ***get_miles***(*trd.vehicleId*);
$\delta \leftarrow$ ***get_reputation_change***(*trd.vehicleId*,*trd.periodEndTime*);
if ($\delta > 0$) **then**
  type $\leftarrow 1$;
else if ($\delta < 0$) **then**
  type $\leftarrow 2$;
else
  type $\leftarrow 3$;
$t \leftarrow$ ***cal_tax***(*type*,δ,*m*);
if ($t > \mathcal{R}$ OR $t < 0$) **then**
  rlt $\leftarrow$ false;
else if t = *trd.tax* **then**
  rlt $\leftarrow$ true;
else
  rlt $\leftarrow$ false;
return *rlt*;

A. Analysis of Security Goals

In the following, we first illustrate how $\mathcal{R}$-tracing can resist malicious attacks by proving that the reputation model can achieve a separation equilibrium, then demonstrate that $\mathcal{R}$-tracing can suppress selfish behaviors by introducing the tax mechanism, and finally prove that $\mathcal{R}$-tracing can also resist MOA and RSB by analyzing the whole system.

1) Resistance to Malicious Attacks: For an activity of reporting information, the utility function of the reputation value is shown in formula (6). If the vehicle reports information honestly, then its utility U_h can be calculated according to formula (7). Since the model requires that the reward obtained by the vehicle must be greater than the cost of reporting information, the value of U_h is always positive. If the vehicle reports false information for malicious attacks, its utility U_m can be calculated according to formula (8). Regardless of whether the number of malicious attacks exceeds the threshold thr_1, the value of U_m is less than or equal to 0. Therefore, the choice of honest reporting can improve the vehicle's reputation, while the choice of malicious attacks is very likely to reduce the reputation value.

$$U(e, f, \mathcal{R}) = W(e) - P(f, \mathcal{R}) - C(e, \mathcal{R}) \tag{6}$$

$$U_h(e, \mathcal{R}) = \beta e - \frac{e^2}{\alpha \mathcal{R}} > 0 \tag{7}$$

$$U_m(e, f, \mathcal{R}) = \begin{cases} -\frac{e^2}{\alpha \mathcal{R}} - \mathcal{R} & f > thr_1 \\ -\frac{e^2}{\alpha \mathcal{R}} - \left(1 - \left(\frac{1}{2}\right)^f\right) \mathcal{R} & f \le thr_1 \end{cases} \le 0 \tag{8}$$

The vehicles performing different behaviors need to set different optimal signal values to obtain the maximum utility. When reporting information honestly, the vehicle needs to set the optimal signal value e_h^* for maximum utility. As shown in formula (9), the value of e_h^* is solved to $\alpha\beta\mathcal{R}/2$ by setting the partial derivative of $U_h(e, \mathcal{R})$ equal to 0. By solving formula (10), it is obtained that the optimal signal value e_h^* should be set to 0 when the vehicle carries out a malicious attack. Assuming that all vehicles rationally make optimal choices, the model can reach a separation equilibrium. If an attacker sets the e of a forged information to 0, even if it doesn't pay any cost for this information, it will reduce its reputation due to severe penalty.

$$\frac{\partial U_h(e, \mathcal{R})}{\partial e} = \beta - \frac{2e}{\alpha \mathcal{R}} = 0 \tag{9}$$

$$\frac{\partial U_m(e, f, \mathcal{R})}{\partial e} = -\frac{2e}{\alpha \mathcal{R}} = 0 \tag{10}$$

2) Resistance to Selfish Behaviors: For the vehicle with selfish behaviors, the utility function of its reputation value is described in formula (11). If a vehicle does not report any information within a management period, there will be neither costs nor penalties, but tax must be paid. According to formula (5), as the vehicle's reputation value does not change, the tax is only related to its current reputation value $\mathcal{R}$ and the miles d driven during the management period. Since the values of $\mathcal{R}$ and d are non-negative, the utility of the selfish vehicle is less than or equal to 0. If the vehicle remains silent, it will be deducted a portion of its reputation value as tax at the end of each management period. Until the reputation value is cleared, the vehicle will be excluded from the system. It is worth noting that the taxes paid by vehicles are different. According to formula (11), a vehicle with a higher reputation value should pay a higher tax for its selfish behavior. This setting avoids a situation where vehicles gradually reduce their reporting after accumulating high reputations. Additionally, the more miles a vehicle has driven, the more tax it needs to pay for wasting more opportunities of reporting perceived information.

$$U_s = -\frac{1}{2}\left(\frac{\mathcal{R}}{\sum_{i=1}^{n_3} \mathcal{R}_i} + \frac{d}{\sum_{i=1}^{n_3} d_i}\right) S_3 \tag{11}$$

3) Resistance to Intelligent MA and SB: For MOA, $\mathcal{R}$-tracing takes defensive measures against it from both model and system aspects. First, the model sets a threshold thr_1 in formula (3) for the number of malicious attacks performed by the vehicle. Once the number exceeds thr_1, the vehicle's reputation value will be set to 0 directly. Second, in terms of system design, all updates of reputation value are recorded as transactions on the consortium blockchain. Since these records cannot be tampered with, managers can obtain the exact number of malicious behaviors by querying the distributed ledger. Therefore, $\mathcal{R}$-tracing can completely defend against MOA. For the vehicle with RSB, $\mathcal{R}$-tracing deducts its reputation value after each management period through the tax mechanism. Since the living space is gradually compressed, the vehicle with RSB have to report information to earn reputation values. Compared with the incentives brought by rewards, the tax mechanism can ensure that all vehicles must report perceived information to maintain their survival status.

B. Analysis of System Goals

In this subsection, we demonstrate through in-depth analysis that $\mathcal{R}$-tracing satisfies the system design goals of vehicle reputation management.

1) Distributed Management of Reputation: In $\mathcal{R}$-tracing, we build a distributed system for vehicle reputation management. In our system, DMV, PDs, and MOs are defined as different organizations in 5G intelligent transportation scenarios. To overcome the incomplete trust between organizations, the nodes belonging to different organizations are connected through a consortium blockchain. The decentralized and immutable advantages of blockchain are used to meet the requirements of distributed reputation management. In addition, three types of transactions are designed for the update reputation values. Each transaction needs to be submitted by one node and recorded on the ledger after reaching a consensus among all nodes.

2) Reputation Calculation is Publicly Verifiable: In $\mathcal{R}$-tracing, we design three types of transactions for the reputation update of vehicles. Each transaction needs to be stored on the consortium blockchain. As shown in Fig. 2, whether the transaction is for reported information, rewards, punishments, or periodic taxation, the transaction records will save detailed data. Thanks to the immutable nature of the blockchain, transaction records can provide a reliable calculation basis for publicly verifiable reputation management. In addition, $\mathcal{R}$-tracing regulates the reputation calculation process in the form of smart contracts. Any authorized user can execute a smart contract to check whether the reputation calculation in a transaction is correct. Therefore, the reputation calculation of $\mathcal{R}$-tracing is publicly verifiable.

3) Avoidance of Reputation Devaluation: In $\mathcal{R}$-tracing, we not only assign a reputation account to each vehicle, but also set up an official account for managers. In our system, reputation value is not allowed to be created or eliminated out of thin air. Its total amount must always remain the same. Therefore, whether in the management task for reporting information or in the management task for periodic taxation, the reputation value only flows between the official account and different vehicle accounts. As shown in formula (4), after a management period, the reputation value paid by the official account needs to be collected from the vehicle accounts through taxation. Therefore, in the same management period, if some vehicles' reputation values increase, the other vehicles' reputation values will inevitably decrease. To sum up, $\mathcal{R}$-tracing can avoid the occurrence of reputation devaluation.

VII. Experiments

Due to the limitation of experimental conditions, we cannot carry out large-scale experiments on an actual system, so we use a combination of software simulation and system testing. To verify that our reputation model can resist malicious attacks and selfish behaviors, we conduct simulation experiments involving 100 vehicles on MATLAB. In addition, we build a prototype system using multiple devices in our laboratory. By measuring the throughput, transaction confirmation latency, and storage overhead, we prove that $\mathcal{R}$-tracing achieves the system goals mentioned in Section III-C and meets the basic requirements of deployment in 5G-enabled intelligent transportation scenarios.

A. Performance of Vehicle Reputation Model

Whether our vehicle reputation model can effectively resist malicious attacks and selfish behaviors is the focus of $\mathcal{R}$-tracing verification. To achieve evaluations in large-scale traffic scenarios, we conduct comparative experiments on MATLAB instead of a system. According to the Manhattan model, a road network consisting of six roads in each direction is constructed, covering an urban area of 40×40 km^2. 100 vehicle nodes with different behaviors are set in the traffic scenario. To trigger the reporting activities of vehicles, 200 events are randomly arranged at different locations and times. Any vehicle that passes the designated location within the specified time can detect the corresponding event and behave according to its type. Before our experiment, we plan 10 routes for these vehicles. In each simulation, all vehicles should randomly choose a route and drive along it at a constant speed of 72 km/h. In terms of the communication model, we implement the constant speed propagation delay model on MATLAB and set the communication range of vehicles to 2 km. The duration of each simulation is 2000 seconds, and the statistical results of 10 repeated experiments are discussed in the following paragraphs.

First, a set of comparative experiments are performed to demonstrate the resistance of our vehicle reputation model to MA. It is worth noting that although the proportion of vehicles with MA in all vehicles may have an impact on the update process of all vehicles' reputation values, the changing trend of reputation value is fixed according to the results of our parameter tuning experiments. In the first comparative experiment, 30% of nodes are randomly set as vehicles with malicious attack behaviors (VMAB), and the remaining 70% of nodes are set as vehicles with honest behaviors (VHB). In addition, the classical linear reputation model (LRM) adopted in [16] and [35] is chosen for comparison. In this model, the reputation value will increase at a certain ratio after the vehicle honestly reports the information. Correspondingly, if a malicious attack is detected, the vehicle's reputation value will be deducted according to a certain ratio. Fig. 4 shows the reputation value changes of VHB and VMAB concerning two different models. Since both $\mathcal{R}$-tracing and LRM reward VHB and punish VMAB by increasing the reputation value, change trends of reputation values in Fig. 4(a) and (b) are similar. However, there are still three differences in the performance of the two models. (1) LRM deducts the reputation value at a fixed ratio. If a vehicle continues to report forged information, the punishment of LRM will gradually become lighter as the vehicle's reputation value decreases. By reading transaction records from the chain, $\mathcal{R}$-tracing can count the number of times a node play as VMAB. Therefore, the deducted reputation value in our model increases with the number of malicious attacks, which satisfies the principle of increasingly severe punishment. (2) The proportional deduction in LRM can reduce the reputation value of VMAB to a very low level but cannot kick the VMAB out of the system by clearing its reputation value to 0. The $\mathcal{R}$-tracing model requires that once the number of malicious

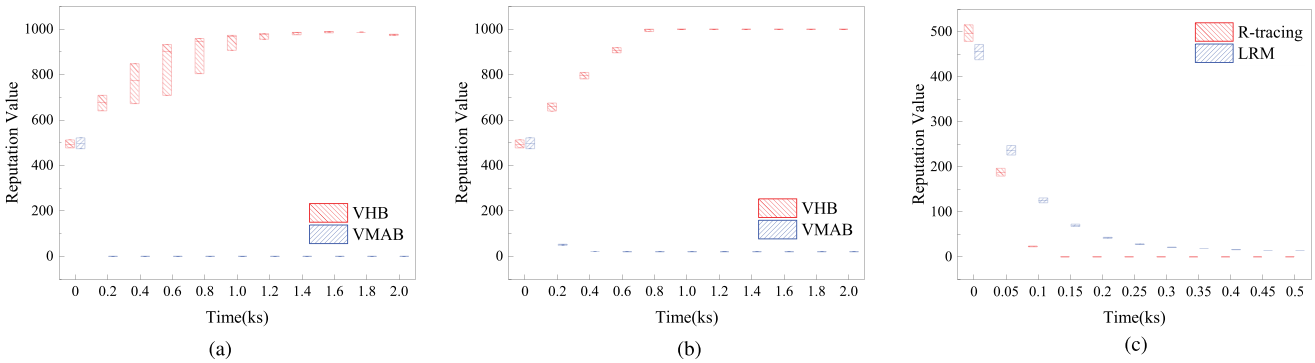


Fig. 4. Reputation value changes of VHB and VMAB with respect to two different models. (a) $\mathcal{R}$-tracing. (b) LRM. (c) Vehicle 20#.

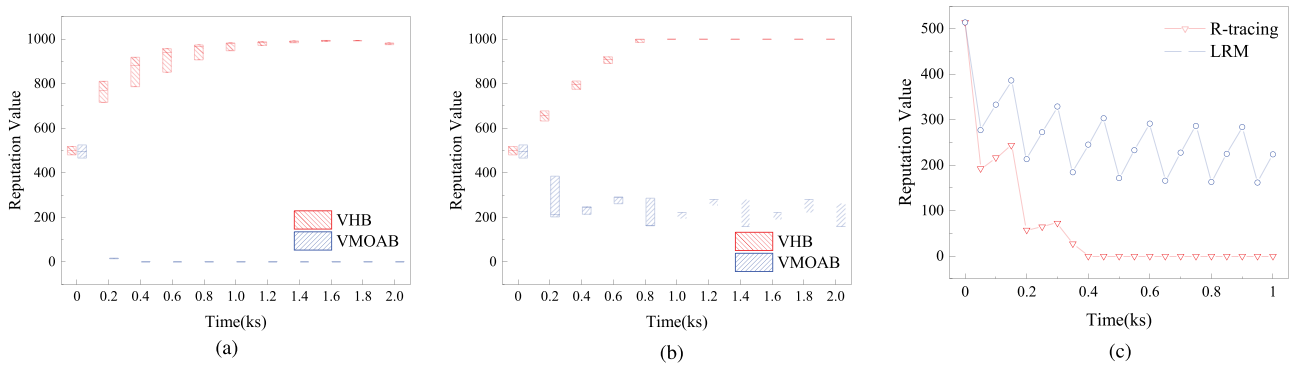


Fig. 5. Reputation value changes of VHB and VMOAB with respect to two different models. (a) $\mathcal{R}$-tracing. (b) LRM. (c) Vehicle 8#.

attacks exceeds thr_1, the reputation value of VMAB is directly cleared to 0, to quickly exclude it from the system. Fig. 4(c) shows the reputation value of vehicle 20# in an experiment. The R-tracing model can quickly reduce the reputation value to 0, while LRM cannot. (3) In LRM, the reputation value of VHB can reach the upper bound after enough honest reports. Once this situation occurs, the VHB may turn to selfish behavior because it cannot continue to accumulate its reputation value. According to the $\mathcal{R}$-tracing, each update of the vehicle's reputation value is treated as a transaction with the official. On the one hand, the reward VHB gets in each transaction gradually decreases with the increment of its reputation value. On the other hand, all vehicles periodically deduct a portion of the reputation value to pay taxes. Therefore, as shown in Fig. 4(a), the VHB can maintain a high reputation, but cannot reach the preset upper bound. Second, the resistance of the above two models to the malicious on-off attack is compared through experiments. Similar to the previous experiment, 30% of nodes are randomly set as vehicles with malicious on-off attack behaviors (VMOAB), and the remaining 70% are set as VHB. In addition, the form of MOA is defined as a cycle of three reports. Each VMOAB reports true information the first two times but false information the third time. Fig. 5 shows the reputation value changes of VHB and VMOAB with respect to two different models. Although both models reduce the reputation value of VMOAB, they perform differently. LRM can only reduce the reputation value to a certain extent but cannot impose continuous penalties on VMOAB. The model of $\mathcal{R}$-tracing can quickly reduce the VMOAB's reputation value to 0 by tracing its previous transactions. Fig. 5(c) shows the reputation value of vehicle 8# in an experiment. It clearly shows that LRM cannot defend against MOA, while our model is able to quickly kick VMOAB out of the system.

TABLE II
PARAMETERS IN REPUTATION MODEL

Parameter	Value
α	2
β	0.5
thr_1	4
thr_2	200
Speed	72km/h
Range	40×40km^2
Simulation duration	2000s
Number of vehicles	100
Number of accidents	200
Tax interval	200s
The maximum of reputation value	1000
γ_i	$1/3$
The communication distance of vehicle	2km

Finally, the inhibitory powers of two models on two types of selfish behaviors defined in Section III-C are compared. In experiments, 30% of nodes are randomly set as vehicles with selfish behaviors (VSB), 30% of nodes are randomly set as vehicles with rational selfish behaviors (VRSB), and the remaining nodes are set as VHB. According to the setup of experiments, once its reputation value falls below thr_2 shown in Table II, VRSB will switch from selfish silence to active reporting. Fig. 6 shows the reputation value changes of VSB and

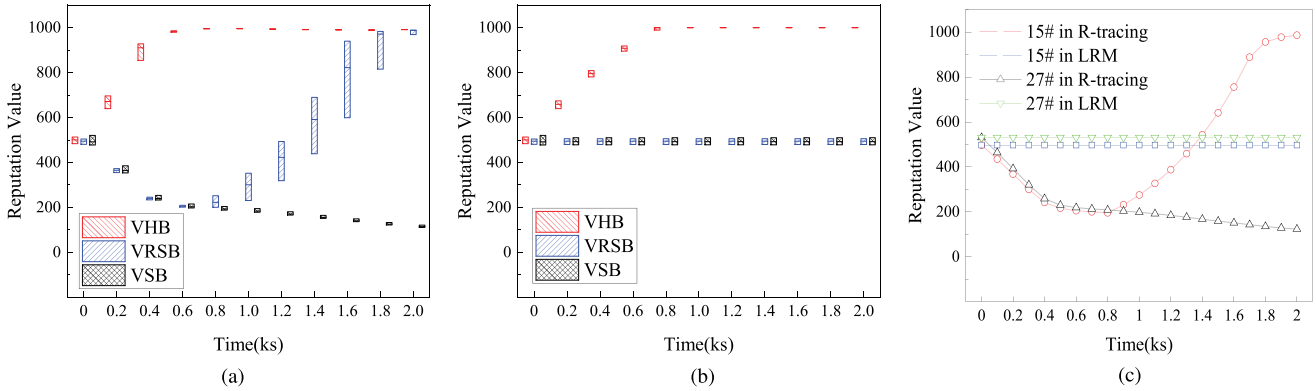


Fig. 6. Reputation value changes of VHB,VSB and VRSB with respect to two different models. (a) $\mathcal{R}$-tracing. (b) LRM. (c) Vehicle 15# and Vehicle 27#.

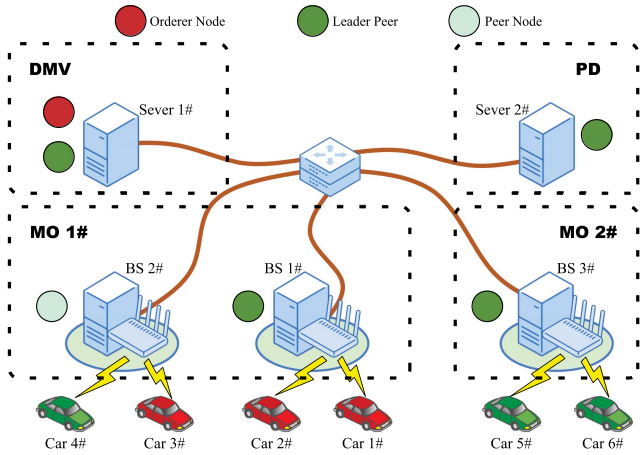


Fig. 7. Structure of prototype system.

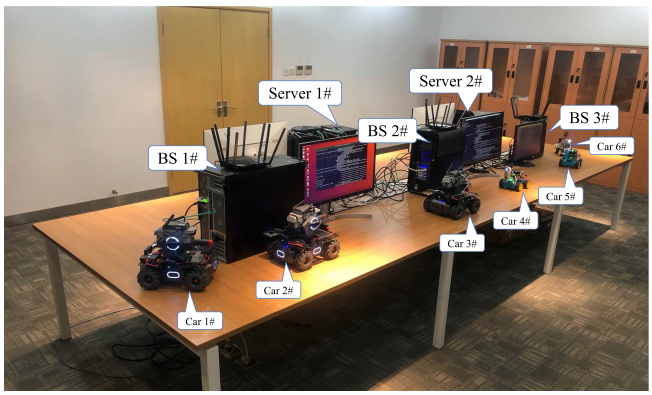


Fig. 8. Deployment of prototype system.

VRSB concerning two different models. The model of $\mathcal{R}$-tracing can cope with two types of selfish behaviors. As shown in Fig. 6(a), the reputation value of the selfish vehicle gradually decreases over time. Once a vehicle chooses to actively report information again, its reputation value increases rapidly. LRM cannot detect the selfish behaviors of vehicles. As shown in Fig. 6(b), the reputation values of VSB and VRSB are almost unchanged during the process of the experiment. Fig. 6(c) shows the reputation value changes of vehicles 15# and 27# in an experiment. Vehicle 15# is a VRSB, while vehicle 27# is a VSB.

TABLE III
DEVICES INFORMATION

Devices	Configurations	OS
Server 1#	Intel XEON SP; MEM:32G; SSD:256G	Ubuntu 18.04
Server 2#	Intel XEON SP; MEM:32G; SSD:256G	Ubuntu 18.04
BS 1#	Intel Core i9-10900; MEM:32G; SSD:512G	Windows 10
BS 2#	Intel Core i5-12400F; MEM:16G; SSD:512G	Windows 10
BS 3#	Intel Core i5-11400; MEM:16G; SSD:256G	Windows 10
Car 1#-3#	Raspberry Pi mainboard 4B 4G	Raspbian OS
Car 4#-6#	Raspberry Pi mainboard 4B 2G	Raspbian OS

Under the influence of our tax strategy, their reputation values gradually decrease over time. As vehicle 15# switches from the selfish state to the positive reporting state in time, its reputation value gradually increases after 800 seconds. This curve also proves that our reputation model can incentivize selfish vehicles to actively report information. In contrast, since LRM does not take any measures against selfish behaviors, the reputation values of vehicles 15# and 27# remain unchanged.

The above experimental results prove that the reputation model of $\mathcal{R}$-tracing not only resists malicious attacks through the reward and punishment strategy but also suppresses selfish behaviors through the tax strategy. With the traceability service provided by the consortium blockchain, our model has stronger adaptability in intelligent transportation scenarios than LRM.

B. Performance of Vehicle Reputation Management System

To test the system performance of $\mathcal{R}$-tracing, a prototype system is built in the laboratory environment using three kinds of devices listed in Table III. As shown in Fig. 7, all devices are deployed on a LAN. Each BS is emulated by connecting a wireless AP to a computer host. According to Table III, there are three BSs built in our experiment with different hardware configurations. Two BSs belong to MO 1#, and the other belongs to MO 2#. Besides, two servers are deployed in our experiment. One belongs to PD, and the other belongs to DMV. Based on these devices, a consortium blockchain consisting of six nodes is constructed. We select Hyperledger Fabric v2.2.0 as the implementation technology of our system in consideration of its high efficiency and wide application. It should be noted that $\mathcal{R}$-tracing can also be realized through other mainstream consortium blockchain technologies.

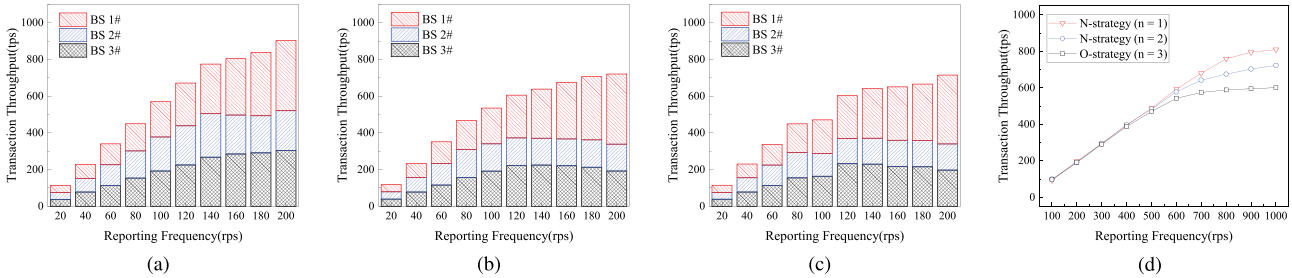


Fig. 9. Throughput of Type 1 and Type 2 transactions with different endorsement strategies. (a) N-strategy ($n = 1$). (b) N-strategy ($n = 2$). (c) O-strategy ($n = 3$). (d) Throughput of Type 2 transaction.

As shown in Fig. 7, two BSs managed by MO 1# serve as peer nodes, and BS 1# is selected as the leader peer. BS 3# is the only BS of MO 2#, so it is directly set as the leader peer. Similarly, there is also one leader peer on the two servers managed by DMV and PD. Due to the limited number of hosts, we adopt the Solo mode of HyperLedger Fabric and set only one orderer node on Server 1#. It is worth noting that the orderer node is only responsible for ordering submitted transactions, neither participating in any transactions nor keeping a ledger like a peer node. Fig. 8 shows the deployment of our prototype system. In our experiment, six smart cars developed based on Raspberry Pi are used to simulate vehicle nodes. Each car connects to one AP through wireless signals and reports information to our system. To test the performance of our prototype system, two agent programs are developed respectively on Raspberry Pi and Server 2#. In this way, smart cars can report information to BSs at a fixed frequency, and the PD can also submit investigation reports to the system at a preset frequency.

The throughput of different transactions is tested to verify the performance of our system. It is worth noting that the transactions for vehicle tax are periodically initiated by the peer node of DMV, and it does not generate many burst requests like the transactions for other usages. Therefore, only the first two types of transactions defined in Section V-A are tested in our experiments. Fig. 9 shows the throughput of Type 1 and Type 2 transactions concerning different endorsement strategies. Fig. 9(a) and (b) respectively show results of selecting one and two endorsing nodes when the N-strategy is adopted, while Fig. 9(c) shows results using the O-strategy. Since every transaction needs to be endorsed by at least one peer node from every other organization and our prototype system involves four organizations, the number of endorsing nodes for the O-strategy is set to 3. As the number of nodes increases, the endorsement time of each transaction is prolonged, and the system throughput gradually decreases. Fig. 9 shows the throughputs of the entire system and three BSs in the form of a stacked bar chart. Due to the difference in host configuration, the processing capability of BS 1# is better than the other two BSs. When the reporting frequency of each car reaches 100rps, other BSs have already discarded some transactions, but BS 1# can still work normally. Unlike Type 1 transactions, Type 2 transactions are triggered by the investigation report submitted by the PD node. In Fig. 9(d), as the sending frequency of the agent program on Server 2# increases, our system gradually reaches a performance bottleneck.

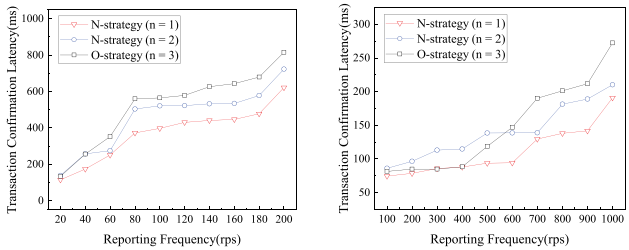


Fig. 10. Transaction confirmation latency of Type 1 and Type 2 transactions. (a) Type 1 transaction. (b) Type 2 transaction.

When the frequency is 800rps, many transactions are discarded because they cannot be updated to the chain on time. As shown in Fig. 9(d), although the number of endorsements affects the performance, the O-strategy recommended by $\mathcal{R}$-tracing still achieves the throughput of 600tps.

In addition to throughput, we also conduct comparative experiments on transaction confirmation latency and storage overhead. Transaction confirmation latency is equal to the time difference between the submission to the chain and the confirmation by all nodes. Fig. 10(a) shows the confirmation latencies of Type 1 transactions concerning different endorsement strategies. Since O-strategy uses three endorsing nodes, its confirmation latency is more than two cases with N-strategy. Furthermore, the confirmation latency grows as the reporting frequency increases. It is especially worth noting that when the reporting frequency of vehicles is higher than 200rps, our system reaches its performance bottleneck, resulting in a significant increase in transaction confirmation latency. Fig. 10(b) shows the confirmation latencies of Type 2 transactions. Their changing trends are similar to those of Type 1 transactions. Once the reporting frequency of the PD node reaches 1000rps, the transaction confirmation latencies will increase greatly. Fig. 11 shows the storage overhead of Type 1 and Type 2 transactions. With the increment of the reporting frequency, the storage overhead of both types of transactions also increases. According to the transaction records described in Fig. 2, since a Type 1 transaction occupies more bytes than a Type 2 transaction, the storage overhead of Type 1 transactions is larger than that of Type 2 transactions. When the reporting frequency of the vehicles reaches 200rps, our system takes 8.5 MB of storage per second, and when the

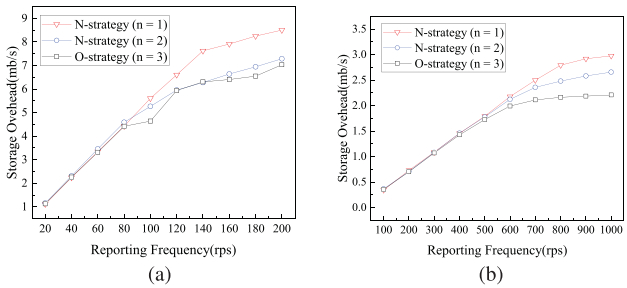


Fig. 11. Storage overhead of Type 1 and Type 2 transactions. (a) Type 1 transaction. (b) Type 2 transaction.

reporting frequency of the PD node reaches 1000rps, our system needs 3.1 MB of storage per second.

To sum up, thanks to the efficient consensus mechanism of the consortium blockchain, our $\mathcal{R}$-tracing has achieved a throughput of 600*tps* and a transaction confirmation latency of less than one second. In [17], the proposed scheme adopts the consensus mechanism of PoW. Since many hardware resources are used for complex computing tasks, its throughput is only 12*tps*. Although an improved consensus mechanism based on PoW is adopted in [18], the throughput achieved by the prototype system is 30*tps*. In contrast, the performance of our system can meet the requirements of vehicle reputation management in future 5G-IoV scenarios. However, the storage overhead of our system is not ideal. Although the reporting frequency in the actual scenarios is much lower than the limit tested in our experiments, the number of users will be much larger than the setting value. Therefore, reducing storage overhead becomes a huge challenge for the long-term operation of $\mathcal{R}$-tracing. In recent years, researchers have paid attention to the storage defect of blockchain and proposed some methods for off-chain transfer storage [36][37]. In the future, we will leverage these methods to optimize $\mathcal{R}$-tracing.

VIII. Conclusion

Malicious attacks and selfish behaviors displayed by vehicles in reporting information activities have become important security issues affecting future intelligent transportation applications. It is a promising idea to establish reputation for vehicles and carry out systematic management, but there are some defects in previous research. In this paper, we propose $\mathcal{R}$-tracing, a consortium blockchain-based vehicle reputation management scheme. Our work focuses on the design and implementation of $\mathcal{R}$-tracing, its main contributions can be summarized in three aspects. In terms of model design, we not only require that only the verified information can be used as the basis for reputation calculation, but also propose two different mechanisms to defend against malicious attacks and selfish behaviors of vehicles. In terms of system construction, we design a vehicle reputation management system based on a consortium blockchain. On the one hand, a distributed architecture is adopted to meet the needs of multi-party management. On the other hand, three smart contracts and an organization-based endorsement strategy are designed to provide publicly verifiable management services. Finally, through theoretical analysis and simulation experiments, we prove that our vehicle reputation model can not only effectively resist malicious attacks and selfish behaviors, but also meet challenges brought by vehicle intelligence. To verify the feasibility of $\mathcal{R}$-tracing, we also build a prototype system by using Hyperledger Fabric and demonstrate that its throughput far exceeds previous schemes. In summary, $\mathcal{R}$-tracing can help vehicles actively report real information in future 5G-enabled intelligent transportation scenarios.

References

[1] B. Ji et al., "Survey on the internet of vehicles: Network architectures and applications," *IEEE Commun. Standards Mag.*, vol. 4, no. 1, pp. 34–41, Mar. 2020.

[2] C. Yu, B. Lin, P. Guo, W. Zhang, S. Li, and R. He, "Deployment and dimensioning of fog computing-based internet of vehicle infrastructure for autonomous driving," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 149–160, Feb. 2019.

[3] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3832–3840, Jun. 2021.

[4] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5071–5080, Aug. 2021.

[5] C. Ge, L. Zhou, G. P. Hancke, and C. Su, "A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12481–12489, Aug. 2021.

[6] S. Safavat and D. B. Rawat, "On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based Internet of Vehicles for smart cities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5050–5059, Aug. 2021.

[7] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13784–13795, Nov. 2020.

[8] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[9] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021.

[10] J.-M. Chen, T.-T. Li, and J. Panneerselvam, "TMEC: A trust management based on evidence combination on attack-resistant and collaborative Internet of Vehicles," *IEEE Access*, vol. 7, pp. 148913–148922, 2019.

[11] H. Xia, S.-S. Zhang, Y. Li, Z.-K. Pan, X. Peng, and X.-Z. Cheng, "An attack-resistant trust inference model for securing routing in vehicular Ad Hoc networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 7108–7120, Jul. 2019.

[12] N. B. Truong, G. M. Lee, T.-W. Um, and M. Mackay, "Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the Internet of Things," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 10, pp. 2705–2719, Oct. 2019.

[13] H. Xiao, N. Sidhu, and B. Christianson, "Guarantor and reputation based trust model for social Internet of Things," in *Proc. IEEE Int. Wireless Commun. Mobile Comput. Conf.*, 2015, pp. 600–605.

[14] R. J. Atwah, P. Flocchini, and A. Nayak, "Towards smart trust management of VANETs," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, 2020, pp. 1–5.

[15] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[16] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020.

[17] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in Internet of Vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021.

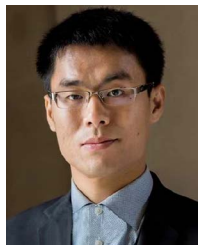
[18] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in Internet of Vehicles with blockchain," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11815–11829, Dec. 2020.
[19] J. Guo et al., "TROVE: A context-awareness trust model for VANETs using reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6647–6662, Jul. 2020.
[20] Z. Liu, J. Ma, Z. Jiang, H. Zhu, and Y. Miao, "LSOT: A lightweight self-organized trust model in VANETs," *Mobile Inf. Syst.*, vol. 2016, pp. 1–15, Dec. 2016.
[21] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 3, pp. 229–242, 2014.
[22] H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, "Blockchain-based trust management for Internet of Vehicles," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1397–1409, Jul.–Sep. 2021.
[23] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021.
[24] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, "NOTRINO: A novel hybrid trust management scheme for Internet-of-Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 9, pp. 9244–9257, Sep. 2021.
[25] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, "Software-defined vehicular networks with trust management: A deep reinforcement learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1400–1414, Feb. 2022.
[26] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "A job market signaling scheme for incentive and trust management in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3657–3674, Aug. 2015.
[27] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in vehicular ad hoc networks: An economic incentive model based approach," in *Proc. IEEE Comput., Commun. IT Appl. Conf.*, 2013, pp. 13–18.
[28] S. Ahmed, S. Al-Rubeaai, and K. Tepe, "Novel trust framework for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9498–9511, Oct. 2017.
[29] H. Hu, R. Lu, Z. Zhang, and J. Shao, "Replace: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.
[30] X. Chen and L. Wang, "A trust evaluation framework using in a vehicular social environment," in *Proc. IEEE Conf. Comput. Commun. Workshops*, 2017, pp. 1004–1005.
[31] F. Ahmad, V. N. L. Franqueira, and A. Adnane, "Team: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.
[32] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[33] J. Kang et al., "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.
[34] M. B. Mollah et al., "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.
[35] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
[36] J. Benet, "IPFS - content addressed versioned, P2P file system," 2014. [Online]. Available: https://arxiv.org/abs/1407.3561
[37] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "Biothr: Electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10857–10872, Jul. 2021.

Yuwei Xu (Member, IEEE) received the B.Eng. degree in information security and the Ph.D. degree in computer science from Nankai University, Tianjin, China, in 2007 and 2012, respectively. He was an Assistant Professor with the College of Computer and Control Engineering from 2012 to 2017, and an Associate Professor with the College of Cyber Science, Nankai University from 2018 to 2019. He is currently an Associate Professor with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. His research interests include the Internet of Things, future network architecture, and network security.

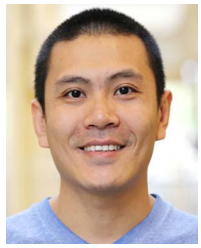
Enze Yu (Student Member, IEEE) received the B.Eng. degree in information security from Xinjiang University, Urumqi, China, in 2020. He is currently working toward the master's degree with the School of Cyberspace Security, Southeast Univerity, Nanjing, China. His research interests include network security and blockchain.

Yuxing Song received the B.Eng. degree in cyberspace security in 2021 from Southeast University, Nanjing China, where he is currently working toward the master's degree with the School of Cyberspace Security. His research interests include network security and blockchain.

Fei Tong (Member, IEEE) received the M.S. degree in computer engineering from Chonbuk National University, Jeonju, South Korea, in 2011, and the Ph.D. degree in computer science from the University of Victoria, Victoria, BC, Canada, in 2016. He is currently an Associate Researcher with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. From December 2016 to December 2018, he was a Postdoctoral Research Fellow with the Department of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include ad hoc networks, Internet of Things, and 4G/5G communication systems.



Qiao Xiang (Member, IEEE) received the bachelor's degree in information security and the second bachelor's degree in economics from Nankai University, Tianjin, China, in 2007, and the master's and Ph.D. degrees in computer science from Wayne State University, Detroit, MI, USA, in 2012 and 2014, respectively. He is a Faculty Member with Xiamen University, Xiamen, China. He was an Associate Research Scientist with the Department of Computer Science, Yale University, New Haven, CT, USA. His research interests include software-defined networking, resource discovery and orchestration in collaborative data sciences, interdomain routing, and wireless cyber-physical systems. From 2016 to 2016, he was a Postdoctoral Fellow with the Department of Computer Science, Yale University. From 2014 to 2015, he was a Postdoctoral Fellow with the School of Computer Science, McGill University, Montreal, QC, Canada.



Liang He (Senior Member, IEEE) is currently an Assistant Professor with the University of Colorado Denver, Denver, CO, USA. His research interests include cyber-physical systems, IoTs, and mobile computing. Before joining UCD, he was a Research Fellow with The University of Michigan at Ann Arbor, Ann Arbor, MI, USA, as a Research Scientist with Singapore University of Technology and Design, Singapore, and as a Research Assistant with the University of Victoria, Victoria, BC, Canada.