Chinese Journal of Electronics
vol.04, no.04, pp.1– 13, 2022
https://doi.org/123.123.123.123

Research Article

Reliable and Fair Trustworthiness Evaluation Protocol for Platoon Service Recommendation System

CHENG Hongyuan[1], TAN Zhiyuan[2], ZHANG Xianchao[3], LIU Yining[4]

1. *School of Computer Science & Engineering, LinYi University, Linyi 273300*
2. *School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Edinburgh 999020*
3. *College of Information Science and Engineering, Key Laboratory of Medical Electronics and Digital Health of Zhejiang Province, Engineering Research Center of Intelligent Human Health Situation Awareness of Zhejiang Province, Jiaxing University, Jiaxing 314001*
4. *College of Information Science and Engineering, Key Laboratory of Medical Electronics and Digital Health of Zhejiang Province, Engineering Research Center of Intelligent Human Health Situation Awareness of Zhejiang Province, Jiaxing University, Jiaxing 314001*

Corresponding author: LIU Yining; Email: lyn7311@sina.com.
Received March 22, 2023; Accepted March 20, 2024; Published March 22, 2024.

Abstract — Aiming at the problems of the communication inefficiency and high energy consumption in vehicular networks, the platoon service recommendation systems (PSRS) are presented. Many schemes for evaluating the reputation of platoon head vehicles have been proposed to obtain and recommend reliable platoon head vehicles. However, these trustworthiness evaluation protocols for PSRS fail to achieve both reliability and fairness. In this paper, we first provide a reliable trustworthiness evaluation method to ensure that the reputation level of platoon head vehicle can be calculated by cloud service provider (CSP) with the help of key agreement mechanism and truth discovery technology. Besides, the semi-trusted entity CSP may maliciously tamper with the reputation level of the platoon head vehicle. Thus, we also provide a reputation level confirmation method to ensure the fairness of trustworthiness evaluation. Formal security proof and security analysis are provided to show that our trustworthiness evaluation protocol can achieve the goals of privacy protection, reliability, fairness and resistance to several security attacks. Experiments demonstrate that this protocol can save execution time and achieve reliable and fair trustworthiness evaluation for PSRS.
Keywords — Reliability, Fairness, Privacy protection, Trustworthiness evaluation, Vehicle platoon.

I. INTRODUCTION

With the widespread deployment of fifth-generation (5G) networks and the flourishing development of intelligent Internet of Things (IoT) devices connected to vehicular networks, vehicle platooning [1] has received extensive attention as an effective way to reduce air pollution, decrease energy consumption, alleviate traffic congestion, and improve road capacity [2–4]. As a new driving pattern, vehicle platoon is essentially to maintain a group of vehicles running in a relatively close inter-vehicle distances, and the following vehicles can experience less air resistance [5], which reduces the overall fuel consumption and exhaust emissions. In the vehicle platoon, the platoon head vehicle is responsible for controlling the entire platoon, while the member vehicles automatically follow the platoon head vehicle [6].

The platoon head vehicle plays a crucial role in ensuring the safe and efficient operation of the entire vehicle platoon. However, a malicious platoon head vehicle may intentionally provide incorrect instructions to the platoon for personal gain, which pose a serious threat to the platoon's safety. Evaluating the platoon head vehicle's reputation and ensuring its trustworthiness has thus become a critical task in platoon service recommendation systems (PSRS) [7].

Many reputation-based schemes have been proposed as a promising solutions to prevent malicious behaviors of the platoon head vehicle in PSRS. Hu et al. [8] designed a reputation assessment scheme for platoon head vehicle in PSRS by collecting and modeling feedback from member vehicle. Cui et al. [9] proposed a centralized-based reputation scheme suitable for highways and urban roads, where the TA weights the feedback from different vehicles and updates the target's reputation score. Liu et al. [10] found most of these schemes assume that vehicle behavior can be accurately measured as reputation from the communication, disregarding the fact that malicious vehicles may exhibit intelligent behavior to avoid detection. As a solution, they proposed a hybrid reputation system (HDRS) which enables vehicles and roadside (RSU) to independently conduct reputation evaluations separately and provide mutual references. Datta et al. [11] con-

Chinese Journal of Electronics

sidered cognitive bias and proposed a trustworthy platoon head selection scheme to enhance secure platooning in vehicular networks. Furthermore, an effective reputation-based platoon recommendation scheme (RLE) is proposed in [12], which calculates vehicle's reputation score by constructing a multi-weight subjective logic model with the consortium blockchain. In fact, most of the aforementioned schemes that calculate the platoon head's reputation based on member vehicle's feedback often assign the same average weights to all member vehicles, which often results in inaccurate platoon head's reputation scores. This is because the quality of feedback provided by member vehicles differs due to variations in observation angles, wireless acquisition equipment, observation time, etc..

Thus, truth discovery technology [13–16] is introduced into the PSRS to identify the true information (truth) from a group of contradictory feedback. The reliability of the member vehicle providing feedback is evaluated during the truth discovery iteration, which is usually represented as the weight for calculating the truth. Accordingly, Zhang et al. [17] designed an effective and privacy-preserving quality-aware incentive mechanism based on blockchain, which deployed reputation management on blockchain using truth discovery technology and Dirichlet distribution to ensure user reliability. Yan et al. [18] proposed reputation-based truth discovery for the IoV with long-term vehicle reputation, reducing the number of iterations under the same criterion. A trust-based and privacy-preserving platoon recommendation scheme (TPPR) is proposed in [7], which calculates the platoon head vehicle's reputation score with the truth discovery algorithm and preserves vehicle's privacy with pseudonyms and Paillier cryptosystem. Gyawali et al. [19] found that TPPR suffers from high computational complexity due to the use of Paillier cryptosystem, which is not suitable for vehicle communication networks. Consequently, they designed a malicious behavior detection system based on the modified ElGamal cryptosystem, which efficiently identifies malicious behavior without disclosing vehicle privacy in vehicle communication networks.

1. Motivations

The main idea of the aforementioned schemes is to calculate the reputation score of platoon head vehicles by upper authorities based on member vehicles' feedback with the help of the truth discovery algorithm. While these schemes effectively improve the accuracy of calculating the reputation scores of platoon head vehicles, most of them often ignore the fact that malicious upper authorities may produce invalid reputation scores due to software/hardrware malfunctions or lazy behavior [20, 21]. This is because the aforementioned schemes often employ complex cryptographic operations (bilinear pairing, homomorphic encryption, etc.) to ensure the data integrity and vehicle privacy. Moreover, the execution process of the truth discovery algorithm typically involves multiple iterations of interactions between the upper authorities and the vehicles, resulting in substantial demand for computational resources. Hence, the upper authorities are incentivized to prioritize their interests by avoiding excessive calculations to save system overhead[22, 23].

Nonetheless, if the upper authorities fail to conduct reputation calculations honestly, the previous research efforts focused on truth discovery-based reputation evaluation schemes will become meaningless, leading to significant security concerns[24]. Considering this, it is crucial to establish supervision and verification mechanisms for PSRS to restrict the upper authorities' illegal behavior and ensure the provision of accurate and reliable reputation evaluation results. Specifically, a reliable and fair reputation mechanism between vehicles and the upper authorities needs to be established for PSRS.

2. Our Contributions

As introduced above, there are currently few studies achieve both reliability and fairness property, which prevent the upper authorities such as CSPs from providing incorrect platoon head vehicle's reputation scores to the platoon. In this paper, we present a reliable and fair trustworthiness evaluation protocol for PSRS. The main contributions lie in two aspects as follows.

(1) We propose a reliable trustworthiness evaluation scheme for PSRS based on the truth discovery algorithm and Elliptical curve cryptosystem (ECC). The proposed scheme adopts anonymous authentication mechanism to protect the identity privacy of member vehicles. Besides, session keys are utilized to ensure the security and privacy of feedback from member vehicles transmitted over open communication channels.

(2) We construct a reputation level confirmation method to ensure the fairness of trustworthiness evaluation, which enables member vehicles to confirm whether the platoon head vehicle's reputation score falls within their acceptable range, thereby further preventing semi-trusted CSP from conducting unfair evaluations.

II. PRELIMINARIES

Elliptical curve cryptosystem (ECC) and truth discovery are foundational elements in the proposed scheme. Hence, we introduce them in this section.

1. Elliptical Curve Cryptosystem and Assumptions

The Elliptic Curve E/F_p over a finite field is defined by the equation $y^2 = x^3 + a \cdot x + b(\bmod p)$, where $a, b \in F_p$ and p is a large prime number. An additive elliptic curve group G with order q and generator P consists of all points on the Elliptic Curve E and an infinity point O.

Scalar multiplication: The scalar multiplication over E can be denoted as $c \cdot P = P + P + \cdots + P(c \text{ times}), c \in Z_q^*$.

Discrete Logarithm Problem (DLP): Given two random

Chinese Journal of Electronics

points $P, Q \in G$, where $Q = w \cdot P$, $w \in Z_q^*$. The DLP assumption means that the probability of deducing w in probability polynomial time is ignored.

Computational Diffie-Hellman Problem (CDHP): Given two random points Q and Y on E, where $Q = w \cdot P$, $Y = c \cdot P$, and w, c are two random numbers. The CDHP assumption is that the advantage of calculating $w \cdot c \cdot P$ in probability polynomial time is negligible.

2. Truth Discovery

In this paper, truth discovery mechanism [25] with superior accuracy and efficiency is employed to infer the ground truth of platoon head vehicles by integrating the weights and feedback reports from member vehicles. The general procedure of truth discovery involves two phases: weight update and truth update. The detailed description is provided below.

Specifically, suppose that a total of M objects' data need to be collected and N denotes the number of vehicles in our system. Therefore, f_m^n denotes the objected values of the n-th user for the m-th value.

Weight update: Given the ground truth of each object, the individual weight ω_n can be calculated as follows.

$$\omega_n = \log(\sum_{n=1}^{N}\sum_{m=1}^{M} d(f_m^n - f_m^*)) - \log(\sum_{m=1}^{M} d(f_m^n - f_m^*)) \tag{1}$$

$d(\cdot)$ is a distance function that measures the difference between the observations and estimated truth. As observed from Eq. (1), vehicles that provide observations closer to the ground truth will be assigned higher weights.

Truth update: Similar to the weight ω_n update, iterative updating of the ground truth RS_m^* for each object of every vehicle is shown as follows.

$$RS_m^* = \sum\nolimits_{n=1}^{N} \omega_n \cdot f_m^n \Big/ \sum\nolimits_{n=1}^{N} \omega_n \tag{2}$$

Ultimately, the truth is updated iteratively and recursively until the function converges to the ground truth. It can be observed that the data provided by vehicles with higher weights are more likely to be considered as the truth.

3. System Architecture

As shown in Fig. 1, the participants involved in our protocol include the Trusted Authority (TA), Cloud Service Provider (CSP), Fog Nodes (FN), and vehicles equipped with onboard units (OBUs). Each participant and their corresponding responsibilities are described below.

TA: The Trusted Authority (TA) plays a major role in the overall system, which is responsible for the registration of entities (vehicles and FNs) and assigns pseudonyms and partial private keys to the vehicles. TA is the only entity that can obtain the real identity of malicious vehicles based on the messages they send. It also maintains a database and a blacklist

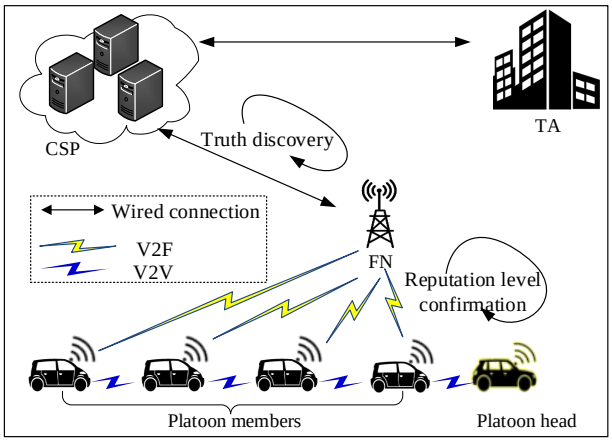

Figure 1 This is a test of figure and this is a very long caption and long caption.

for storing platoon head vehicle's reputations and all misbehaving platoon head vehicles, respectively.

CSP: With sufficient storage and computational capabilities, the Cloud Service Provider (CSP) triggers the truth discovery algorithm to calculate the reputation scores for the platoon head vehicles, with the assistance of the Fog Node (FN).

FN: Fog Nodes are typically deployed in fixed locations along the roadsides and are geographically closer to the vehicles than the CSP. The Fog Node acts as a gateway between the vehicles and the CSP, facilitating communication with them through wireless and wired means, respectively. FN possesses certain computing power and storage space, which it utilizes to verify the identities of member vehicles and forward vehicles feedback to CSP for assessing the reputation of platoon head vehicles.

Vehicle: Vehicles equipped with the on-board units (OBU) communicate with other vehicles and FNs via wireless network technologies such as DSRC, LTE-V2X and 5G-V2X. We assume that the secret cryptographic materials (pseudonyms, private keys, etc.) stored in the OBU are not accessible and available to anyone. Through vehicle-to-fog node (V2F) communication, vehicles upload feedback scores to the CSP via the fog node. Vehicles can be further divided into the following two categories.

* **Platoon head vehicles:** The platoon head vehicle controls and leads several member vehicles with the same origin and destination on the road. Vehicles with good driving habits and reputation can be selected as the platoon head vehicle. The reputation of the platoon head vehicle is calculated by CSP based on the feedback scores provided by member vehicles after each trip. There are a number of platoon head vehicles that form a set $P = \{PH_1, PH_2, \cdots, PH_k, \cdots\}$ in our protocol. If the current reputation score of a platoon head vehicle falls below the system threshold, it is unable to

Chinese Journal of Electronics

continue serving the vehicle platoon. Consequently, the CSP blacklists the vehicle and imposes a cash penalty.

* **Member vehicles:** Member vehicles automatically join a platoon led by the platoon head vehicle PH_k. Member vehicles receive instructions from the platoon head vehicle PH_k and provide feedback scores for evaluating the reputation of the platoon head vehicle PH_k. After a member vehicle completes a trip, it performs mutual authentication with the current FN and provides feedback scores to the FN without revealing identity privacy.

4. Threat Model

Following the threat model and security hypothesis presented in [7, 8], the proposed protocol mainly focuses on the discussion of internal and external threats as follows.

Internal threats: TA is the only entity within the PSRS that is fully trusted and can never be compromised. However, considering real-world scenarios, we acknowledge the presence of malicious CSPs, vehicles, and compromised FNs within the system, even though they are authorized by the TA. As semi-trusted entities, the CSP and FNs may be curious about the real identity and reputation score of a vehicle and try to deduce the vehicle's location and trajectory by linking its identity or reputation score. Furthermore, CSP outputs the reputation score of the platoon head vehicle with the help of member vehicles and FN. However, it may adopt a simplified method without performing the complete reputation calculation process, resulting in the output results inconsistent with the actual situation and misleading the reputation assessment of the platoon head vehicle.

For platoon head vehicle, its performance may vary across periods and trips, indicating that its reliability cannot be equally trusted. The proposed scheme assumes that the future performance (reputation) of the platoon head vehicle can be predicted based on its historical performance. The majority of member vehicles are honest, providing feedback on the performance of the head vehicle after each trip and confirming that the reputation evaluation output by the upper authorities is within an acceptable range. However, the varying performance among member vehicles affects the quality of the feedback and confirmation reports they provide, and some member vehicles may provide false reports for their own benefit.

External threats: Messages sent by legitimate entities in the PSRS on public channels may be intercepted, modified and forged by external attackers. Furthermore, an external attacker may be curious about the real identity of legitimate vehicles and the plaintext context of the reports being transmitted. Consequently, it can initiate various security attacks, including impersonation attacks, replay attacks and the modification attacks, thereby posing a significant threat to the communication security of the PSRS.

5. Evaluation Criteria

A common and comprehensive set of evaluation criteria plays a key role in the construction and unbiased evaluation of reputation assessment protocols. As far as we know, formal evaluation standards for reputation assessment schemes are currently lacking, primarily due to the diverse design goals and problem domains addressed by these schemes. Raya et al.[26] defined five basic attacks including fake information, heating with sensor information, ID or trajectory disclosure, denial of service, and masquerading. To resist the security threats and build a trust-based privacy-preserving head vehicle selection model, state-pf-the-art achievements [7, 8, 27] have presented the trustworthiness evaluation schemes for PSRS. Accordingly, we have taken all those trustworthiness evaluation schemes into account and proposed our evaluation criteria as follows.

EV1. Identity privacy preserving: The vehicle's real identity is highly sensitive. To realize the privacy protection of the vehicle's real identity, it should be ensured that the vehicle's identity information cannot be inferred from vehicle's message.

EV2. Mutual authentication: It means that the receiver of the message can authenticate the integrity of the message and the identity validity of the sender. That is to say, the proposed protocol should guarantee that messages sent by legitimate vehicles are complete and can only be exploited by legitimate fog nodes.

EV3. Reliability: Reliability is an important objective in our protocol. To ensure the security of the platoon service, the designed protocol must accurately calculate the reliable reputation of the platoon head vehicles based on their historical behavior.

EV4. Fairness: Considering that an incompletely credible CSP may make unfair reputation assessments of platoon head vehicles, the proposed protocol should ensure fairness of reputation evaluation.

EV5. Unlinkability: The misbehaving attacker remains incapable of linking two or more messages transmitted by a single vehicle or two different vehicles, thus ensuring privacy protection. More specifically, if the same vehicle transmits two messages M_i and $M_i{}'$ with a time interval more than ΔT (where ΔT represents a small time increment), then an adversary should not be feasible to determine whether M_i and $M_i{}'$ originate from the same sender based on message contents and where the message was received. Furthermore, if digital signatures are employed for authenticity, it is essential that the certificate lacks identifying information, and the keys are updated in a manner that prevents an eavesdropper from associating the old key with the new key.

EV6. Traceability: Although the real identity of the vehicle is hidden from any other vehicles, FNs and CSP. However, if necessary, the TA is able to track the real identity of the malicious vehicle immediately.

Chinese Journal of Electronics

Table 1 List of Symbols

Notation	Description
V_i, FN_j	i-th member vehicle, j-th Fog Node
PH_k	k-th platoon head vehicle
ID_{fj}	FN_j's identity
ID_{vi}, pid_i	V_i's real identity and pseudonym
G, q	Additive group, prime order
P	generator of G
s, P_{pub}	The private and public key of TA
(X_{i1}, X_{i2})	V_i's full public key
(x_{i1}, x_{i2})	V_i's full private key
(Y_j, sk_j)	The public-private key pair of FN_j
$h_i, i \in (0,3)$	One-way hash algorithms
a_i, b_j	Random numbers
σ_i, σ_{j1}	Signatures from V_i and FN_j
SK_{ij}, SK_{ji}, SK	Session key between V_i and FN_j
f_i, FR_i	V_i's feedback score and feedback report
$\|, \oplus$	Concatenation and XOR operation
$T_{1i}, T_{2i}, T_{1j}, T_{2j}$	The timestamps

EV7. Resistance to security attacks: To withstand the known passive and active attacks, particularly impersonation, replay and the known session key attacks.

III. PROPOSED PROTOCOL

The overall flow and function of our protocol are shown in Fig. 1. Our protocol mainly consists of five phases, which are outlined below.

In the first two phases, TA setups all necessary parameters and broadcasts public parameters. Vehicles register with TA and obtain the secret parameters for generating pseudonyms and full private keys. FN registers with TA and obtains its own private key. In the third phase, the vehicle and the FN authenticate each other and negotiate a session key that can be used in the next phase of communication. Fourth, after finishing a trip, the member vehicle generates feedback report, encrypts it with the session key and uploads it to the FN. Then, the FN collects multiple feedback reports and forwards them to CSP for evaluating the reputation of the platoon head vehicle. Finally, CSP triggers the truth discovery algorithm to calculate the reputation score of the platoon head vehicle and sends it to the member vehicles via the FN. In the fifth phase, the member vehicles need to confirm whether it is within their acceptable range and forward the confirmation result to FN. Then, FN consolidates the member vehicles' confirmation results and decides whether to re-evaluate the platoon head vehicle's reputation. Eventually, FN stores the reputation score of the platoon head vehicle in TA for platoon service recommendation, and TA gives a cash penalty to the platoon head vehicle whose reputation score is lower than the system threshold or removes it from the platoon head vehicle queue. Table 1 describes the notations used in this protocol.

1. System Setup Phase

In this stage, the system environment will be created by TA through the following operations. First, the TA generates the system parameters. Specifically, TA chooses a cyclic additive group G of Elliptic Curve over finite field, which is generated by P with the prime order q. Second, TA selects a random number $s \in Z_q^*$ as the system private key and calculates $P_{pub} = s \cdot P$ as the system public key. Third, TA selects several cryptographic hash functions $h_i, i \in (0,3)$, where $h_0 : \{1,0\}^* \rightarrow Z_q^*$, $h_1 : G \rightarrow Z_q^*$, $h_2 : G \times \{1,0\}^* \rightarrow \{1,0\}^l$, $h_3 : G \times \{1,0\}^* \rightarrow \{1,0\}^l$ and l represents the limited length of bit string. Finally, TA keeps s secretly and publishes the public system parameters $\{G, q, P, P_{pub}, h_0(\cdot), h_1(\cdot), h_2(\cdot), h_3(\cdot)\}$.

2. Registration Phase

This phase is performed under secure and private channels. Both the vehicle and FN need to register with the TA before joining the Internet of Vehicles (IoV). Through registration, the vehicles obtain the secret parameters used to generate valid pseudonyms and a full public-private key pair from the TA. After executing the registration phase, the FN can obtain a private key for signing its messages.

* **Vehicle registration:** V_i with the real identity ID_{vi} selects a number $x_{i1} \in Z_q^*$ and calculates $X_{i1} = x_{i1} \cdot P$. Then, $< ID_{vi}, X_{i1} >$ will be sent to TA. After receiving the registration request of V_i, TA picks a random number $w_i \in Z_q^*$ and computes $X_{i2} = w_i \cdot P$ and $VX_i = X_{i2} \oplus h_0(ID_{vi}) \cdot X_{i1}$. Last, TA generates partial private key x_{i2} for V_i by computing $x_{i2} = w_i + s \cdot h_1(X_{i1} || X_{i2}) \bmod q$. TA stores $< VX_i, x_{i2} >$ into the on-board units (OBU) of V_i. After that, V_i sets (x_{i1}, x_{i2}) as its full private key and sets (X_{i1}, X_{i2}) as its full public key.
* **Fog Node (FN) registration:** For FN_j with identity ID_{fj}, TA chooses $y_j \in Z_q^*$ and calculates $Y_j = y_j \cdot P$, $sk_j = y_j + s \cdot h_2(ID_{fj} \parallel Y_j) \bmod q$, where Y_j and sk_j are set as the public key and private key of FN_j. At last, TA returns $< Y_j, sk_j >$ to FN_j. Then, FN_j stores $< Y_j, sk_j >$ secretly.

3. Mutual Authentication Phase

In the proposed protocol, when the member vehicle V_i completes the trip Tr_k led by the platoon head vehicle PH_k, it is required to send a feedback report to the FN. Thus, both the vehicle and the FN should authenticate each other's identities when V_i is asked to provide the feedback report to the nearby FN FN_j. Due to the high-speed mobility of the vehicle, it is necessary to ensure the efficient mutual authentication between vehicles and FNs. The authentication between the vehicle and the FN (V2F) can be implemented as follows.

Step 1. When the vehicle V_i enters FN_j's area, it chooses a random number $a_i \in Z_q^*$ to compute $A_i = a_i \cdot P$. Then,

Chinese Journal of Electronics

it generates pseudonym pid_i by computing $pid_i = ID_{vi} \oplus h_3(a_i \cdot P_{pub} \parallel X_{i2} \parallel T_{1i})$, where T_{1i} is the latest timestamp. Then V_i computes $\alpha_i = h_2(pid_i \parallel X_{i2} \parallel A_i \parallel T_{1i})$ and generates the signature σ_i by computing $\sigma_i = x_{i2} + x_{i1} + a_i \cdot \alpha_i \bmod q$. Finally, V_i sends $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ to FN_j.

Step 2. Upon receiving the message $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ from V_i, FN_j first checks the validity of the timestamp T_{1i}. If the timestamp has expired, FN_j discards the message, otherwise it continues to verify the validity of the signature σ_i by Eq. (3).

$$\begin{aligned}\sigma_i \cdot P &= x_{i2} \cdot P + x_{i1} \cdot P + a_i \cdot \alpha_i \cdot P \\ &= w_i \cdot P + s \cdot h_1(X_{i1} \parallel X_{i2}) \cdot P + x_{i1} \cdot P + a_i \cdot \alpha_i \cdot P \\ &= X_{i2} + P_{pub} \cdot h_1(X_{i1} \parallel X_{i2}) + X_{i1} + A_i \cdot \alpha_i\end{aligned} \tag{3}$$

Where $\alpha_i = h_2(pid_i \parallel X_{i2} \parallel A_i \parallel T_{1i})$. If the Eq. (3) holds, FN_j chooses $b_j \in Z_q^*$ to compute $B_j = b_j \cdot P$. Then, FN_j generates the session key SK_{ji} with V_i, where $SK_{ji} = h_3(b_j \cdot A_i \parallel pid_i \parallel ID_{fj})$. Finally, FN_j calculates the hash value $\beta_{j1} = h_2(SK_{ji} \parallel B_j \parallel T_{1j})$ and the signature $\sigma_{j1} = sk_j + \beta_{j1} \cdot b_j \bmod q$, and sends $< ID_{fj}, B_j, Y_j, \sigma_{j1}, T_{1j} >$ to V_i, where T_{1j} is the current time.

Step 3. After receiving $< ID_{fj}, B_j, Y_j, \sigma_{j1}, T_{1j} >$ from FN_j, V_i first checks the freshness of T_{1j}. If T_{1j} is invalid, V_i discards the message. Otherwise, it calculates the session key SK_{ij} with FN_j by computing $SK_{ij} = h_3(a_i \cdot B_j \parallel pid_i \parallel ID_{fj})$. Then, it calculates $\beta_{j1} = h_2(SK_{ij} \parallel B_j \parallel T_{1j})$ for verifying whether the Eq. (4) holds.

$$\begin{aligned}\sigma_{j1} \cdot P &= sk_j \cdot P + \beta_{j1} \cdot b_j \cdot P \\ &= y_j \cdot P + s \cdot h_2(ID_{fj} \parallel Y_j) \cdot P + \beta_{j1} \cdot b_j \cdot P \\ &= Y_j + P_{pub} \cdot h_2(ID_{fj} \parallel Y_j) + \beta_{j1} \cdot B_j\end{aligned} \tag{4}$$

In the end, V_i and FN_j complete mutual authentication and establish a private session key $SK_{ij} = SK_{ji}$ to securely evaluate the reputation of the platoon head vehicle PH_k.

Batch verification: When FN receives multiple signatures from a set of member vehicles $\{V_i\}, i \in (1, k)$, it aggregates k signatures into a single signature with the help of batch verification technology. Then, the FN authenticates this single signature instead of individually authenticating each of the k signatures, greatly improving the authentication efficiency. The detailed process of batch verification performed on the FN side is shown below.

Step 1. FN checks the freshness of $T_{1i}, i \in (1, k)$. If it is fresh, FN proceeds.

Step 2. FN selects a vector $u = \{u_1, ..., u_i, ..., u_k\}$, where u_i is random selected in $[1, 2^t]$ and t is a very small integer. Then FN checks whether the Eq. (5) holds.

$$\begin{aligned}&(\sum_{i=1}^{k} u_i \sigma_i)P \\ &= (\sum_{i=1}^{k} u_i x_{i2})P + (\sum_{i=1}^{k} u_i x_{i1})P + (\sum_{i=1}^{k} u_i a_i \alpha_i)P \\ &= \sum_{i=1}^{k} (u_i w_i P) + (\sum_{i=1}^{k} u_i h_1(X_{i1} \parallel X_{i2}))sP \\ &+ \sum_{i=1}^{k} u_i x_{i1} P + \sum_{i=1}^{k} (u_i a_i \alpha_i P) \\ &= \sum_{i=1}^{k} (u_i X_{i2}) + P_{pub} \sum_{i=1}^{k} (u_i h_1(X_{i1} \parallel X_{i2})) \\ &+ \sum_{i=1}^{k} (u_i X_{i1}) + \sum_{i=1}^{k} (u_i A_i \alpha_i)\end{aligned} \tag{5}$$

If it holds, accept the signed message. Otherwise, there are one and more invalid signatures among the k signatures. Once the above situation occurs, binary search technology [28] can be used for detecting the invalid signatures.

4. Reputation Evaluation Phase

In our protocol, the platoon head vehicle PH_k is assumed to lead a group of member vehicles $\{V_i\}, i \in (1, k)$ in the trip Tr_k. Since the reputation of the platoon head vehicle PH_k mainly depends on the feedback provided by its member vehicles $\{V_i\}, i \in (1, k)$, we assess the reputation of PH_k by combing feedback reports from all member vehicles. The detailed process for evaluating PH_k's reputation is shown below.

Step 1. After the trip Tr_k, the member vehicle V_i with the pseudonym pid_i generates a feedback report reflecting the past behavior of the platoon head vehicle PH_k. The feedback report $FR_i = (pid_k, Tr_k, f_i, T_{2i})$ of V_i mainly includes the pseudonym of PH_k, the trip Tr_k and the feedback score $f_i \in Z_q^*$, where T_{2i} represents the current time. Finally, V_i encrypts the feedback report FR_i with the session key SK_{ij} and uploads $< pid_i, E_{SK_{ij}}(FR_i), T_{2i} >$ to FN_j.

Step 2. Upon receiving k encrypted feedback reports from the member vehicles $\{V_i\}, i \in (1, k)$, FN_j checks the freshness of the timestamp T_{2i} and then decrypts them with the session key SK_{ji}. Then, it selects $e_j \in Z_q^*$ to compute $E_j = e_j \cdot P$. Afterwards, it calculates the hash value $\beta_{j2} = h_2(sk_j \parallel E_j \parallel T_{2j})$ and the signature $\sigma_{j2} = e_j + \beta_{j2} \cdot e_j \bmod q$, and sends the aggregated report $< pid_k, Tr_k, \{pid_i, f_i\}_{i=1}^k, E_j, \sigma_{j2}, T_{2j} >$ to CSP, where T_{2j} is the current time.

Step 3. After receiving the aggregated report, CSP first verifies it by checking whether Eq. (6) holds.

$$\begin{aligned}\sigma_{j2} \cdot P &= e_j \cdot P + \beta_{j2} \cdot e_j \cdot P \\ &= E_j + \beta_{j2} \cdot E_j\end{aligned} \tag{6}$$

Where $\beta_{j2} = h_2(sk_j \parallel E_j \parallel T_{2j})$. If so, CSP will calculates the reputation score RS_{PH_k} of the platoon head vehicle PH_k. First, CSP calculates the weight w_k of each member vehicles according to the Eq. (1). Then, with the individual

Chinese Journal of Electronics

weights, CSP is able to estimate the reputation score of the platoon head vehicle PH_k according to the Eq. (2). Finally, CSP obtains the reputation score RS_{PH_k} of PH_k and sends it to FN_j.

5. Reputation Level Confirmation Phase

In fact, the CSP may intentionally lower the PH_k' reputation score to exclude it from the platoon head vehicle database or increase the reputation scores of the misbehaving PH_k to prevent punishment. To prevent the such situations, our protocol sets up a reputation level confirmation phase that allows member vehicles $\{V_i\}, i \in (1,k)$ to confirm whether the reputation score of PH_k calculated by the CSP is reasonable.

Step 1. After receiving the reputation score RS_{PH_k} of PH_k, FN_j broadcasts $< pid_k, RS_{PH_k} >$ within its communication range.

Step 2. Minimum acceptable reputation score $RS_{\min}$ are predefined for each member vehicle $\{V_i\}, i \in (1,k)$. Once V_i obtains the reputation score RS_{PH_k} of the platoon head vehicle PH_k with the pseudonym pid_k, it calculates whether the reputation score RS_{PH_k} provide by the CSP is within an acceptance range and outputs the following judgment result ξ_i.

$$\xi_i = \begin{cases} 1, & RS_{PH_K} \geq RS_{\min} \\ 0, & RS_{PH_K} < RS_{\min} \end{cases} \tag{7}$$

Eventually, the member vehicle V_i encrypts the judgment result ξ_i with the session key SK_{ij} and sends $< pid_k, E_{SK_{ij}}(\xi_i) >$ to FN_j.

Step 3. After receiving $< pid_k, E_{SK_{ij}}(\xi_i) >$ from member vehicles $\{V_i\}, i \in (1,k)$, FN_j encrypts them and checks whether $\sum_{i=1}^{k} \xi_i \geq k/2$ holds. If yes, FN_j uploads PH_k's RS_{PH_k} to TA for making decisions (penalty of reward) on PH_k. Otherwise, FN_j requests the CSP to re-evaluate the reputation of PH_k.

IV. SECURITY ANALYSIS

On the basis of formal security proof and informal security analysis, this section demonstrates the security of the proposed protocol.

1. Security Model

Referring to [1], the security model of our scheme is defined by playing a game between a simulator S and an adversary A. Let Π_{Ω}^{u} denote the u-th session of a participant $\Omega \in (V^i, F^j)$ (vehicles and FNs). In this query, A can make a set of queries, and S must answer them as described below.

* $h(m)$**:** S maintains a table L_h initialized to be vacant. After receiving the query, S inspects if (m,r) is recorded in L_h. If yes, return r to A. Else, S selects a random number r and sends it to A. The resulting entry (m,r) is then recorded into L_h.
* $Execute(ID_i, V_i)$**:** A passive attack is trapped by this query. S performs the proposed scheme normally and then reports messages $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_i >$ as the answer.
* $Send(\Pi_{\Omega}^{u}, m)$**:** Upon sending a message m from A, S runs the protocol according to its specification and returns a corresponding result to A.
* $\mathrm{R}eveal(\Pi_{\Omega}^{u})$**:** S gives back the current session key of Π_{Ω}^{u} as reply.
* $Test(\Pi_{\Omega}^{u})$**:** For the u-th session, S picks a bit $b \in \{0,1\}$. If $b = 1$, S returns the real session key to A; Otherwise, it returns a random element of the same bit length with the real session key to A.
* $Corrupt(\Pi_{\Omega}^{u}, a)$**:** S returns V^i's partial private key or F^j's private key to A.

The event in which A breaks the V2F authentication is denoted as E_1, and event where A breaks the F2V authentication is denoted as E_2. The event that A breaks AKA security of the proposed scheme is indicated as E_3. Then, the probability of the event E_1 and E_2 are denoted as $\Pr(E_1) = \varepsilon_1$ and $\Pr(E_2) = \varepsilon_2$, respectively. Therefore, the probability that A breaks the mutual authentication (MA) can be defined as $Adv_{\sum}^{A}(E_{MA}) = \Pr(E_1) + \Pr(E_2)$, where $\sum$ denotes the proposed scheme. Furthermore, the partnering definition describes that two participants should establish a session key which cannot be compromised by adversaries, while the freshness definition describes the freshness of the session key. Accordingly, the definitions of MA secure, AKA secure, partnering, freshness and correctness are as follows.

Definition 1 Mutual Authentication (MA) secure. A authentication scheme is mutual authentication (MA) secure if the probability $\Pr[Adv_{\sum}^{A}(E_{MA})]$ is negligible for any polynomial adversary A.

Definition 2 Authenticated Key Agreement (AKA) secure. After performing all queries in finite time, A guesses the value of b and produces its guessed value b'. The superiority that A corrupts the AKA of the proposed protocol $\sum$ is defined as $\mathrm{Adv}_{\sum}^{A}(E_{AKA}) = |2\Pr[b' = b] - 1|$. If the probability $\Pr[Adv_{\sum}^{A}(E_{AKA})]$ is negligible, then the scheme is AKA secure.

Definition 3 Partnering. V^i and F^j are considered partners if the following conditions are satisfied: 1) Both V^i and F^j accept; 2) Both V^i and F^j share the same session; 3) V^i is a partner of F^j, and vice versa.

Definition 4 Freshness. A session key constructed by an oracle and its partner is deemed fresh if it satisfies the following conditions: 1) If V^i and F^j do not initiate any Reveal-query, the session key SK constructed by them is $SK \neq NULL$; 2) At most one kind of Corrupt-query is made to $\Omega \in (V^i, F^j)$ from the beginning of the game.

Chinese Journal of Electronics

Definition 5 Correctness. If V^i and F^j are partnered and accepted, they will ultimately possess the same session key, denoted as $SK_V^i = SK_F^j$.

2. Formal Security Proof

Theorem 1 If neither $\Pr(E_1)$ nor $\Pr(E_2)$ is ignorable, the proposed scheme is MA secure.

Proof Suppose A has implemented the aforementioned oracles in the regular way and executes the $Send(\Pi_{V_i}^l, m)$-query. If successfully S calculates the value of $\sigma_i \cdot P = w_i \cdot P + s \cdot h(1) \cdot P + x_{i1} \cdot P + a_i \cdot \alpha_i \cdot P$, where $h(1) = h_1(X_{i1}, X_{i2})$, it means that the message $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ is valid. Subsequently, A can generate another valid message $< pid_i{}', A_i, X_{i1}, X_{i2}, \sigma_i{}', T_{1i} >$, which indicates that it can produce a valid s'. At last, A can obtain the system master private key $s = [\sigma_i{}' - \sigma_i + \alpha_i \cdot a_i - \alpha_i{}' \cdot a_i{}')]/(h'(1) - h(1))$ of the vehicles, as shown in the following equations:

$$\sigma_i \cdot P = w_i \cdot P + s \cdot h(1) \cdot P + x_{i1} \cdot P + a_i \cdot \alpha_i \cdot P \quad (8)$$

$$\sigma_i{}' \cdot P = w_i \cdot P + s \cdot h'(1) \cdot P + x_{i1} \cdot P + a_i{}' \cdot \alpha_i \cdot P \quad (9)$$

Thus, we obtain $s = [\sigma_i{}' - \sigma_i + \alpha_i \cdot a_i - \alpha_i{}' \cdot a_i{}')]/(h'(1) - h(1))$ as the result of the ECDLP. Furthermore, it requires a probability of $1/n \cdot q$ to forge a pair $(\sigma_i \cdot P, s)$. Hence, the probability that A can solve the ECDLP is $\varepsilon_1/n \cdot q$, which conflicts with the hardness of ECDLP. In a word, the probability of $\Pr(E_1) = \varepsilon_1$ is negligible.

Likewise, suppose A performs $Send(\Pi_{RSU_i}^l, m)$-query and if B successfully computes the value of $b_j \cdot A_i \cdot P$, then, A can generate $b_j \cdot A_i \cdot P$ as the instance $(b_j \cdot P, a_i \cdot P, P)$ of ECCDHP with probability ε_2/q_h, where q_h is the bounded number of hash queries. This contradicts the hardness of ECCDHP. In conclusion, the proposed scheme is MA secure.

Theorem 2 The proposed scheme is AKA secure if $\Pr(E_3)$ is negligible.

Proof If A accurately guesses the value of b in the $Test(\Pi_\Omega^l)$-query with a non-negligible probability ε_3, then there exists a S that solves the ECCDHP with a non-probability given by A.

Let E_{SK} be the event that A obtains the session key, E_{U_b} be the event that A guesses the correct value of b in user's instance, E_{R_b} be the event that A guesses the correct value of b in FN's instance. Since the probability of A successfully guessing the value of b is at least $1/2$, we can derive $\Pr[E_{SK}] \geq \varepsilon_3/2$. Furthermore, we get the following equations.

$$\begin{aligned}\Pr[E_{SK}] &= \Pr[E_{SK} \wedge E_{U_b}] + \Pr[E_{SK} \wedge E_{R_b} \wedge E_1] \\ &+ \Pr[E_{SK} \wedge E_{R_b} \wedge \neg E_1] \\ &= \Pr[E_{SK} \wedge E_{U_b}] + \Pr[E_1] \\ &+ \Pr[E_{SK} \wedge E_{R_b} \wedge \neg E_1]\end{aligned} \quad (10)$$

Thus, we obtain

$$\begin{aligned}&\varepsilon_3/2 - \Pr[E_1] \leq \Pr[E_{SK} \wedge E_{U_b}] \\ &+ \Pr[E_{SK} \wedge E_{R_b} \wedge \neg E_1] \\ &\leq \Pr[E_{SK} \wedge E_{U_b}] + \Pr[E_{SK} \wedge E_{U_b}]\end{aligned} \quad (11)$$

$\Pr[E_{SK} \wedge E_{U_b}] \geq 1/2(\varepsilon_3/2 - \Pr[E_1])$ is obtained according to the above equations. According to Theorem 1, $\Pr[E_1]$ is non-negligible, so $\Pr[E_{SK}]$ is also non-negligible. We assume that A can break the AKA secure and output $b_j \cdot a_i \cdot P$ as the solution to the ECCDHP of instance $(b_j \cdot P, a_i \cdot P, P)$ with a non-negligible probability, which is contradicts with the hardness of ECCDHP. Therefore, the proposed scheme is AKA secure.

3. Analysis of Evaluation Criteria

Identity privacy preserving. In our protocol, the vehicle generates dynamically updated pseudonym pid_i for each communication, where $pid_i = ID_{vi} \oplus h_3(a_i \cdot P_{pub} \parallel X_{i2} \parallel T_{1i})$. To extract ID_{vi} from $pid_i = ID_{vi} \oplus h_3(a_i \cdot P_{pub} \parallel X_{i2} \parallel T_{1i})$, the adversary computes $a_i \cdot P_{pub} = a_i \cdot s \cdot P$ from $P_{pub} = s \cdot P$ and $A_i = a_i \cdot P$. However, it is difficult for the adversary to compute $a_i \cdot P_{pub} = a_i \cdot s \cdot P$ according to the assumption of ECCDHP. Furthermore, although member vehicles' feedback scores and weights are in plaintext, the vehicle's identities are anonymous. Thus, the proposed protocol meets the requirement of identity privacy protection.

Mutual authentication. The vehicle and fog node will authenticate the received messages $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ and $< ID_{fj}, B_j, Y_j, \sigma_{j1}, T_{1j} >$, respectively. According to the formal security proof, the vehicle and fog node can authenticate the legitimacy of each other's identity by authenticating the signatures σ_{j1} and σ_i. Besides, no attacker can successfully forge a legitimate signature to convince the vehicle and fog node. Therefore, our protocol can achieve the requirement of mutual authentication.

Reliability. To accurately distinguish between well-behaved and badly behaved platoon head vehicles, this scheme utilizes truth discovery technology to obtain the reputation score f_k^* of the platoon head vehicle PH_k from the feedback report $< pid_i, E_{SK_{ij}}(FR_i), T_{2i} >$ provided by all member vehicles $\{V_i\}, i \in (1, k)$ in the trip Tr_k, where $FR_i = (pid_k, Tr_k, f_i, T_{2i})$. Then, if the reputation score of PH_k is exceeds the system threshold, it will be rewarded, otherwise it will be removed from the platoon head vehicle

queue and given corresponding penalties. Thus, this scheme provides reliability.

Fairness. The proposed protocol ensures the fairness of assessing the reputation of PH_k by constructing a credibility level confirmation phase. During the credibility level confirmation phase, member vehicles $\{V_i\}, i \in (1, k)$ is able to confirm whether the reputation score of PH_k calculated by the CSP is reasonable through Eq. (7) and send the judgment result ξ_i to FN. When $\sum_{i=1}^{k} \xi_i \geq k/2$ is not established, the FN requests the CSP to re-evaluate the reputation of PH_k.

Unlinkability. In the proposed protocol, vehicle V_i sends messages M_1, M_2 and M_3 in the mutual authentication phase, reputation evaluation phase and reputation level confirmation phase, respectively. Note that, $M_1 =< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$, $M_2 =< pid_i, E_{SK_{ij}}(FR_i), T_{2i} >$ and $M_3 =< pid_k, E_{SK_{ij}}(\xi_i) >$ For message M_1, different pseudonymspid_i, signatures σ_i and timestamps T_{1i} are generated by the vehicle for initial authentication with the FN. Therefore, it is impossible to link multiple sessions of the vehicle even if the FN colludes with each other. For message M_2, vehicles employ different pseudonymspid_i, session keys SK_{ij} and timestamps T_{2i} for communication with different FNs. As a result, the adversary is unable to link multiple messages M_2 originating from a specific vehicle. Even within the communication range of the same FN, the security of session keys and the randomness of pseudonyms and timestamps prevent any correlation between messages sent by the same vehicle. The unlinkability of M_3 can be analyzed in a similar way.

Traceability. In the proposed scheme, TA with its secret key s and X_{i2} can reveal the real identity ID_{vi} from the anonymity identity pid_i by computing $ID_{vi} = pid_i \oplus h_3(s \cdot A_i \parallel X_{i2} \parallel T_{1i})$. Thus, when the member vehicle V_i is flagged as controversial, TA can track it and broadcast its real identity. Therefore, our scheme fulfills the requirements of traceability.

Resistance to impersonation attacks. To impersonate a legal member vehicle V_i, the adversary needs to forge a signature σ_i that satisfies the equation $\sigma_i \cdot P = X_{i2} + P_{pub} \cdot h_1(X_{i1} \parallel X_{i2}) + X_{i1} + A_i \cdot \alpha_i$, and send message $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ to the FN. However, according to Theorem 1, it can be observed that the probability of successfully forging a signed message $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ in polynomial time without knowledge of the system private key s is negligible. Thus, the proposed scheme can effectively resist impersonation attacks.

Resistance to replay attack. The message $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ sent by the member vehicle and the message $< ID_{fj}, B_j, Y_j, \sigma_{j1}, T_{1j} >$ sent by the FN contain timestamp T_{1i} and T_{1j}. Thus, the recipient of the message can detect whether the message has been replayed by checking the freshness of timestamp T_{1i} and T_{1j}. Therefore, our scheme is capable of resisting replay attacks.

Table 2 Comparison of Achieved Evaluation Criteria

Schemes	EV1	EV2	EV3	EV4	EV5	EV6	EV7
[29]	✗	✓	✗	✗	✓	✗	✓
B-AGKA [30]	✓	✓	✗	✗	✓	✓	✓
[16]	✗	✓	✓	✗	✗	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓

Note that "✓" means achieving the corresponding goal, while "✗" not.

Resistance to modification attack. In this paper, a valid authenticated message $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$ contains its signature σ_i and pseudonym pid_i. If an adversary makes any modification on $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_{1i} >$, the FN can easily detect the modification by checking if the equation $\sigma_i \cdot P = X_{i2} + P_{pub} \cdot h_1(X_{i1} \parallel X_{i2}) + X_{i1} + A_i \cdot \alpha_i$ holds. As can be seen from Theorem 1, the designed scheme is resistant to modification attacks.

4. Comparison of Achieved Evaluation Criteria

To highlight the security, privacy and other characteristics of the proposed reputation assessment protocol, we compared it with existing works [29], B-AGKA [30] and [16] utilizing the predefined evaluation criteria discussed in Subsection 2.5, and the comparison results are summarized in Table 2.

As indicated in Table 3, both schemes in [29], B-AGKA [30] and [16] are incapable of achieving all the evaluation criteria. Specifically, [16] failed to ensure **EV1** and **EV5**, which compromises user privacy and discourages user from participation in reputation evaluation. Besides, [29] ignores the situation where TA tracks the real identity of the malicious vehicle during conflicts. Furthermore, all of these protocols fail to achieve both reliability and fairness. As mentioned earlier, any endeavors dedicated to building a reputation evaluation protocol would be in vain if reliability and fairness cannot be guaranteed. Taking all these aspects into consideration, the proposed scheme is the only one that achieves all the desirable evaluation criteria, therefore, it is better suited for PSRS compared to these existing schemes.

V. SIMULATION AND PERFORMANCE EVALUATION

This section demonstrates the implementation and experimental analysis evaluation of the proposed scheme.

1. Experimental Setup

This section implements the designed scheme and several related schemes to evaluate the actual performance on user's side and infrastructure's side. Our scheme performs moderate with JAVA programming language operating on the MIRACL library. The hardware platform consists of a clock frequency of 3.40GHz, 16GB of RAM, operating system of Windows 10 and Intel Core i5-8300 processor. The symbolic represen-

Chinese Journal of Electronics

tation and execution times of cryptographic operations are represented in Table 3.

Table 3 Cryptographic operation and execution times

Notation	Description of cryptographic operations	Execute time ms
T_{bp}	Execution time of bilinear pairing operation	3.6549
T_{bp}^{m}	Execute time of bilinear pairing-based multiplication operations	0.4600
T_{bp}^{a}	Time for bilinear pairing-based point addition operations	0.0500
T_{ecc}^{m}	Time of scalar multiplication operation based on elliptic curve cryptography	0.0200
T_{ecc}^{a}	Time for point addition operation based on elliptic curve cryptography	0.0014
T_h	Time of one-way hash operation	0.0001
T_{mtp}	The time of a hash-to-point operation	3.2400
$T_{\exp}$	The time of one exponential operation	0.3390

To analyze the performance of the pairing-based schemes and the ECC-based schemes, we select a symmetric bilinear pairing $\hat{e} : G_1 \times G_1 \rightarrow G_2$ with 80-bit security level and an addition group G with 80-bit security level, respectively. G_1 and G_2 denote additive and multiplicative groups with the same prime order q, respectively. The point $\bar{P}$ constructs the group G_1 on the super singular elliptic curve $\bar{E}$ defined by $y^2 = x^3 + x \mod \bar{p}$ with embedding degree 2, where q and $\bar{p}$ denote 160-bit and 512-bit primes, respectively. Similarly, G is generated by a point P on the nonsingular elliptic curve E defined by $y^2 = x^3 + a \cdot x + b \mod p$ with embedding degree 2, where p is 160-bit prime numbers and $a, b \in Z_q^*$. Thus, the sizes of groups G_1 and G are $|G_1| = 1024bits$ and $|G| = 320bits$, respectively. We assume that the length of values in all protocols is $|D| = 128bits$ for user identity, $\left|Z_q^*\right| = 160bits$ for a random value, $|h(\cdot)| = 256bits$ for hash function (SHA-256), $|ASE| = 256bits$ for ASE encryption and $|T| = 32bits$ for timestamp.

2. Experimental Analysis

In this section, simulation and performance analysis are presented to show the efficiency of the proposed scheme. The performance analysis results are obtained from MATLAB. The performance analysis mainly involves two aspects: computation overhead and communication overhead.

Computation Overhead Comparison

In the proposed scheme, we assume that there are n vehicles joining in the V2F mutual authentication and the reputation evaluation of the platoon head vehicle. Then, we evaluate the running time of our scheme from the perspective of vehicle and other entities. On the vehicles side, n vehicles verifies the FN's signature and performs feedback report perturbation and feedback report encryption, which costs $(5T_{ecc}^{m} + 2T_{ecc}^{a} + 5T_h) \cdot n \approx 0.253n(ms)$. Moreover, FN uses batch verification technology to verify the signatures of multiple member vehicles at once and negotiate the session keys with the member vehicles. Thus the execution time of the FN is $(3n+2)T_{ecc}^{m}+3T_{ecc}^{a}+4nT_h \approx 0.15n+0.104(ms)$. In Nikravan et al.[29] scheme, to realize user login and authentication, n vehicles need to perform two bilinear pairing operations, four multiplication operations based on bilinear pairing, two point addition operations based on bilinear pairing and six hash operations. Thus, the total computation cost of this step is $(2T_{bp}+4T_{bp}^{m}+2T_{bp}^{a}+6T_h)n \approx 11.821n(ms)$. Correspondingly, the entities (other vehicles and infrastructure) need to perform two bilinear pairing operations, two multiplication operations based on bilinear pairing, two point addition operations based on bilinear pairing and five hash operations to verify the legitimacy of n vehicles and the integrity of their messages. Thus, the total computation cost of this step is $(2T_{bp}+2T_{bp}^{m}+2T_{bp}^{a}+5T_h)n \approx 9.901n(ms)$. In B-AGKA [30], it needs the computation is $4T_{bp}+5T_{bp}^{m}+(n+1)T_{bp}^{a}+2T_h \approx 0.96n+20.61(ms)$ for n vehicles in the authentication and group key calculation phase. Then, the entities (other member vehicles and infrastructure) require computation of $8T_{bp}+6T_{bp}^{m}+(3n+1)T_{bp}^{a}+2T_h \approx 0.15n+37.33(ms)$ in the authentication and group key calculation phase. In [16], the computation required is $(5T_{bp}^{m}+2T_{mtp})n \approx 11.28n(ms)$ for n vehicles in the encryption and signature feedback phase. Then, the infrastructure (local authority) requires the computation is $(2T_{bp}+4T_{bp}^{m}+2T_{mtp})n \approx 18.2n(ms)$ in the feedback aggregation and feedback signature phase. The detailed comparison of the computation burden of our scheme and the related schemes is presented in the Table 4.

We analyzed the computation burden on the vehicle and FN side in each algorithm, which are summarized in Figs. 2 and 3. As shown in Fig. 2, the vehicle side of our scheme presents the lowest computational burden as the number of vehicles increases because the proposed scheme uses ECC and batch authentication techniques instead of complex pairing operations. Besides, Fig. 3 illustrates the total computational burden on the FN side as the number of vehicles increases. Compared with other schemes, the designed scheme has the smallest computation burden at the FN side. Thus, the proposed scheme is reasonable and suitable for practical application scenarios.

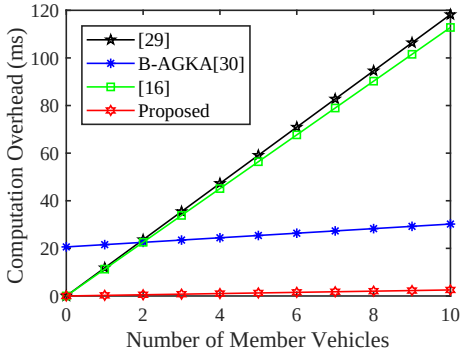

Figure 2 Comparison of computation burden on the member vehicle side.

Computation Overhead Comparison

Table 4 The computation cost of our scheme over other schemes.

Entity	[29]	B-AGKA [30]	[16]	Proposed
Vehicle	$(5T^m_{ecc} + 2T^a_{ecc} + 5T_h) \cdot n \approx 0.253n(ms)$	$(2T_{bp} + 4T^m_{bp} + 2T^a_{bp} + 6T_h)n \approx 11.821n(ms)$	$(5T^m_{bp} + 2T_{mtp})n \approx 11.28n(ms)$	$4T_{bp} + 5T^m_{bp} + (n+1)T^a_{bp} + 2T_h \approx 0.96n + 20.61(ms)$
Infrastructure	$(3n+2)T^m_{ecc} + 3T^a_{ecc} + 4nT_h \approx 0.15n + 0.104(ms)$	$(2T_{bp} + 2T^m_{bp} + 2T^a_{bp} + 5T_h)n \approx 9.901n(ms)$	$(2T_{bp} + 4T^m_{bp} + 2T_{mtp})n \approx 18.2n(ms)$	$8T_{bp} + 6T^m_{bp} + (3n+1)T^a_{bp} + 2T_h \approx 0.15n + 37.33(ms)$

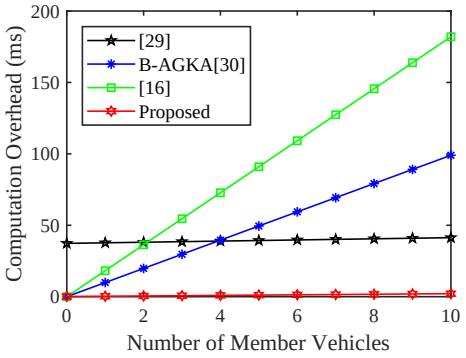

Figure 3 Comparison of computation burden on infrastructure side.

Table 5 The communication cost of our scheme over other schemes

Scheme	Entity	Verify one message (bytes)	Verify n messages (bytes)
[29]	Vehicles	224	$224n$
	Infrastructure	224	$224n$
B-AGKA [30]	Vehicles	1180	$1180n$
	Infrastructure	1156	$1156n$
[16]	Vehicles	788	$788n$
	Infrastructure	532	$532n$
Proposed	Vehicles	180	$180n$
	Infrastructure	180	$180n$

Communication cost refers to the number of bytes required for communication in the protocols. The communication overhead of all protocols on the side of the vehicle and other entities is described below.

In the proposed scheme, the message transmitted by the vehicle is $< pid_i, A_i, X_{i1}, X_{i2}, \sigma_i, T_i, E_{SK_{ij}}(FR_i) >$, where pid_i is the pseudonym, $(A_i, X_{i1}, X_{i2}) \in G$, $(\sigma_i, E_{SK_{ij}}(FR_i))$ is the integer and T_i denotes the timestamp. Thus, the total communication cost of the vehicle is $|D| + 3|G| + 2|Z^*_q| + |T| = 180bytes$. Besides, the message transmitted by the FN is $< ID_{fj}, B_j, Y_j, \sigma_{j1}, T_{1j}, pid_k, RS_{PH_k}, E_{SK_{ij}}(\xi_i) >$, where (ID_{fj}, pid_k) is the identity, $(B_j, Y_j) \in G$, $(\sigma_{j1}, RS_{PH_k}, E_{SK_{ij}}(\xi_i))$ is the integer and T_{j1} denotes the timestamp. Thus, the total communication cost of the FN is $2|D| + 2|G| + 3|Z^*_q| + |T| = 176bytes$. Similarly, in [29], the total communication cost of the vehicle is $|D| + |G_1| + 4|Z^*_q| = 224bytes$. Then, the total communication cost of the FN is $|D| + |G_1| + 4|Z^*_q| = 224bytes$. In B-AGKA [30], the total communication cost of the vehicle is $2|D| + 8|G_1| + 6|Z^*_q| + |T| = 1180bytes$. Then, the total communication cost of the FN is $2|D|+8|G|+5|Z^*_q| = 1156bytes$. In [16], the total communication cost of the vehicle is $1|D|+6|G_1|+|T| = 788bytes$. Then, the total communication cost of the infrastructure (local authority) is $|D| + 4|G| + |T| = 532bytes$. The detailed communication burden of the state-of-the-art works and our scheme is shown in Table 5.

We recorded the communication cost on the vehicle and infrastructure in all schemes, which are summarized in Figs. 4 and 5. The communication burden of vehicles and infrastructures increases with the number of messages. Fig. 4 demonstrates that the vehicles in our scheme have the lowest communication burden compared with the other two schemes. In Fig. 5, as the number of vehicles increases, the communication burden on the infrastructure side increases linearly, and our scheme achieves the lowest communication burden.

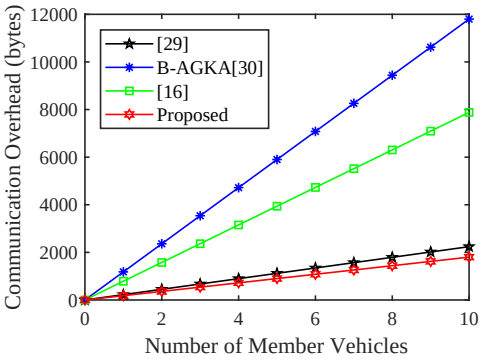

Figure 4 Comparison of communication delay on the member vehicle side.

VI. CONCLUSION

This paper proposes a reliable and fair trustworthiness evaluation protocol for platoon service recommendation systems (PSRS). Considering the uncertainty of platoon head vehicles' behaviors, we first design a reliable reputation evaluation protocol with the help of truth discovery algorithm to

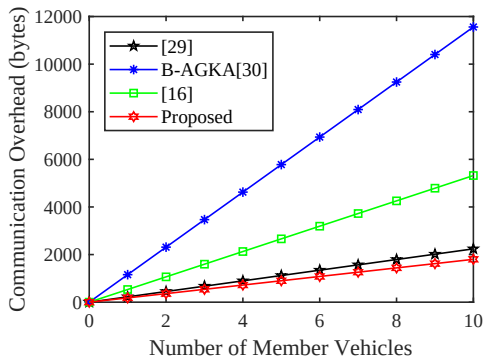

Figure 5 Comparison of communication delay on infrastructure side.

calculate platoon head vehicles' reputation score. Due to the adoption of session key and anonymous authentication mechanism, our scheme will not reveal vehicles' real identity and the privacy of the vehicle feedback transmitted in the open channel during the process of evaluating platoon head vehicles' reputation. In addition, we find that current trustworthiness evaluation protocols lack a complete system to ensure the fairness of platoon head vehicles' reputation level. To avoid unfair evaluations provided by malicious CSP, we design a credibility level confirmation method to ensure that member vehicles can confirm and feedback whether the platoon head vehicle's reputation calculated by CSP is within an acceptable range. Security proof and security analysis show that our scheme is secure for PSRS. We also conduct an implementation to evaluate our scheme, and compare the execution time and communication cost between our scheme and several related schemes to show the efficiency of our scheme.

References

[1] Y. Zhang, D. He, P. Vijayakumar, M. Luo, and X. Huang, "Sapfs: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for industrial internet of things", *IEEE Internet of Things Journal*, in press, doi:10.1109/JIOT.2023.3234178, 2023.

[2] R. Kianfar, B. Augusto, A. Ebadighajari, U. Hakeem, *et al.*, "Design and experimental validation of a cooperative driving system in the grand cooperative driving challenge", *IEEE transactions on intelligent transportation systems*, vol.13, no.3, pp.994–1007, doi:10.1109/TITS.2012.2186513, 2012.

[3] D. Jia, R. Zhang, K. Lu, J. Wang, *et al.*, "Improving the uplink performance of drive-thru internet via platoon-based cooperative retransmission", *IEEE Transactions on Vehicular Technology*, vol.63, no.9, pp.4536–4545, doi:10.1109/TVT.2014.2315741, 2014.

[4] Y. Zheng, S. E. Li, J. Wang, D. Cao, and K. Li, "Stability and scalability of homogeneous vehicular platoon: Study on the influence of information flow topologies", *IEEE Transactions on intelligent transportation systems*, vol.17, no.1, pp.14–26, doi:10.1109/TITS.2015.2402153, 2015.

[5] Y. Li, C. Tang, K. Li, S. Peeta, *et al.*, "Nonlinear finite-time consensus-based connected vehicle platoon control under fixed and switching communication topologies", *Transportation Research Part C: Emerging Technologies*, vol.93, pp.525–543, doi:10.1016/j.trc.2018.06.013, 2018.

[6] M. Hu, C. Li, Y. Bian, H. Zhang, *et al.*, "Fuel economy-oriented vehicle platoon control using economic model predictive control", *IEEE Transactions on Intelligent Transportation Systems*, in press, doi:10.1109/TITS.2022.3183090, 2022.

[7] C. Zhang, L. Zhu, C. Xu, K. Sharif, *et al.*, "Tppr: A trust-based and privacy-preserving platoon recommendation scheme in vanet", *IEEE Transactions on Services Computing*, in press, doi:10.1109/TSC.2019.2961992, 2019.

[8] H. Hu, R. Lu, Z. Zhang, and J. Shao, "Replace: A reliable trust-based platoon service recommendation scheme in vanet", *IEEE Transactions on Vehicular Technology*, vol.66, no.2, pp.1786–1797, doi:10.1109/TVT.2016.2565001, 2016.

[9] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "Rsma: Reputation system-based lightweight message authentication framework and protocol for 5g-enabled vehicular networks", *IEEE Internet of Things Journal*, vol.6, no.4, pp.6417–6428, doi:10.1109/JIOT.2019.2895136, 2019.

[10] X. Liu, O. Ma, W. Chen, Y. Xia, and Y. Zhou, "Hdrs: A hybrid reputation system with dynamic update interval for detecting malicious vehicles in vanets", *IEEE Transactions on Intelligent Transportation Systems*, in press, doi:10.1109/TITS.2021.3117289, 2021.

[11] S. Datta, P. Nikolaou, and M. K. Michael, "Trustph: Trustworthy platoon head selection considering cognitive biases to enhance secure platooning in intelligent and connected vehicles", in *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, IEEE, pp.1760–1766, 2021.

[12] Z. Ying, M. Ma, Z. Zhao, X. Liu, and J. Ma, "A reputation-based leader election scheme for opportunistic autonomous vehicle platoon", *IEEE Transactions on Vehicular Technology*, vol.71, no.4, pp.3519–3532, doi:10.1109/TVT.2021.3106297, 2022.

[13] C. Peng, D. He, J. Chen, N. Kumar, and M. K. Khan, "Eprt: An efficient privacy-preserving medical service recommendation and trust discovery scheme for ehealth system", *ACM Transactions on Internet Technology (TOIT)*, vol.21, no.3, pp.1–24, doi:10.1145/3397678, 2021.

[14] I. Rasheed, "Enhanced privacy preserving and truth discovery method for 5g and beyond vehicle crowd sensing systems", *Vehicular Communications*, vol.32, artilce no.100395, doi:10.1016/j.vehcom.2021.100395, 2021.

[15] Y. Zhu, A. Gupta, S. Hu, W. Zhong, *et al.*, "Driver behavior-aware parking availability crowdsensing system using truth discovery", *ACM Transactions on Sensor Networks (TOSN)*, vol.17, no.4, pp.1–26, doi:10.1145/3460200, 2021.

[16] J. Chen, Y. Liu, Y. Xiang, and K. Sood, "Rpptd: Robust privacy-preserving truth discovery scheme", *IEEE systems journal*, in press, doi:10.1109/JSYST.2021.3099103, 2021.

[17] C. Zhang, M. Zhao, L. Zhu, W. Zhang, *et al.*, "Fruit: A blockchain-based efficient and privacy-preserving quality-aware incentive scheme", *IEEE Journal on Selected Areas in Communications*, in press, doi:10.1109/JSAC.2022.3213341, 2022.

[18] L. Yan and S. Yang, "Trust-aware truth discovery with long-term vehicle reputation for internet of vehicles crowdsensing", in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, pp.558–563, 2021.

[19] S. Gyawali, Y. Qian, and R. Q. Hu, "A privacy-preserving misbehavior detection system in vehicular communication networks", *IEEE Transactions on Vehicular Technology*, vol.70, no.6, pp.6147–6158, doi:10.1109/TVT.2021.3079385, 2021.

[20] C. Ge, W. Susilo, J. Baek, Z. Liu, *et al.*, "A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds", *IEEE Transactions on Dependable and Secure Computing*, vol.19, no.5, pp.2907–2919, doi:10.1109/TDSC.2021.3076580, 2021.

[21] D. Lu, M. Li, Y. Liao, G. Tao, and H. Cai, "Verifiable privacy-preserving queries on multi-source dynamic dna datasets", *IEEE*

Transactions on Cloud Computing, in press, doi:10.1109/TCC.2022.3171547, 2023.

[22] K. Zhang, H. Xiao, and Q. Liu, "Data integrity verification scheme based on blockchain smart contract", in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, IEEE, pp.857–863, 2022.

[23] Q. Dong, J. Tang, S. Dang, G. Chen, and J. A. Chambers, "Blockchain-assisted reputation mechanism for distributed cloud storage", *IEEE Systems Journal*, in press, doi:10.1109/JSYST.2023.3277194, 2023.

[24] X. Zhang, J. Zhao, C. Xu, H. Wang, and Y. Zhang, "Dopiv: Post-quantum secure identity-based data outsourcing with public integrity verification in cloud storage", *IEEE Transactions on Services Computing*, vol.15, no.1, pp.334–345, doi:10.1109/TSC.2019.2942297, 2019.

[25] H. Cheng, X. Zhang, J. Yang, and Y. Liu, "Pprt: Privacy preserving and reliable trust-aware platoon recommendation scheme in iov", *IEEE Systems Journal*, in press, doi:10.1109/JSYST.2023.3264773, 2023.

[26] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks", *Journal of computer security*, vol.15, no.1, pp.39–68, doi:10.3233/JCS-2007-15103, 2007.

[27] J. Shen, C. Wang, J.-F. Lai, Y. Xiang, and P. Li, "Cate: Cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks", *IEEE Transactions on Vehicular Technology*, vol.68, no.11, pp.11213–11226, doi:10.1109/TVT.2019.2938968, 2019.

[28] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter", *IEEE transactions on vehicular technology*, vol.66, no.11, pp.10283–10295, doi:10.1109/TVT.2017.2718101, 2017.

[29] M. Nikravan and A. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the internet of things", *Wireless Personal Communications*, vol.111, no.1, pp.463–494, doi:10.1007/s11277-019-06869-y, 2020.

[30] Q. Zhang, Y. Li, R. Wang, J. Li, *et al.*, "Blockchain-based asymmetric group key agreement protocol for internet of vehicles", *Computers & Electrical Engineering*, vol.86, artilce no.106713, doi:10.1016/j.compeleceng.2020.106713, 2020.

CHENG Hongyuan received the B.E. degree from the School of Information Science and Technology, Taishan University, Tai An, China, in 2018, and the Ph.D. degree from the School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, China, in 2023. She is currently an Associate Professor with the School of Computer Science & Engineering, LinYi University, Linyi, China, and her research primarily focuses on fog computing, reputation evaluation, and privacy preservation in vehicular networks. (Email: hycheng649@163.com)

TAN Zhiyuan is an Associate Professor in the School of Computing at the Edinburgh Napier University (ENU). He holds a BEng degree (2005) with high distinction from the Northeastern University, China, and an MEng degree (2008) from the Beijing University of Technology, China. He was awarded a PhD degree in Computer Systems by the University of Technology Sydney (UTS), Australia in 2014. His current research interests include cybersecurity, machine learning, data analytics, virtualisation and cyber-physical system. Dr Tan has received AUD 27,800 funding from Commonwealth Scientific and Industrial Research Organisation (CSIRO) and UTS for his research on autonomous network intrusion detection, as well as £6,987 funding from ENU for his research on securing future 5G health care systems. Over the past nine years, he also has participated in other network security research projects funded by CSIRO, Minster of Education (Oman), and ITEA2-/CATRENE. (Email: Z.Tan@napier.ac.uk)

ZHANG Xianchao received the Ph.D. degree in Systems Engineering from Beihang University, Beijing, China in 2013. From 2013 to 2015, he was a Postdoctoral Fellow with Peking University, China. From 2018 to 2022, he was a Postdoctoral Fellow with Southeast University, China. From 2015 to 2021, he was a senior engineer with the China Academy of Electronic and Information Technology. He is currently a Professor with the Key Laboratory of Medical Electronics and Digital Health of Zhejiang Province and the Engineering Research Center of Intelligent Human Health Situation Awareness of Zhejiang Province, Jiaxing University, China. His research interests include artificial network, privacy computing. (Email: zhangxianchao@zjxu.edu.cn)

LIU Yining received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, China, in 1995, the M.S. degree in computer software and theory from the Huazhong University of Science and Technology, Wuhan, China, in 2003, and the Ph.D. degree in mathematics from Hubei University, Wuhan, China, in 2007. He is currently a Professor with the Guilin University of Electronic Technology, Guilin, China. His research interests include data privacy, security and privacy in VANETs, image security, and machine learning. (Email: lyn7311@sina.com)