TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in VANET

Chuan Zhang, Liehuang Zhu, *Member, IEEE*, Chang Xu, Kashif Sharif, *Member, IEEE*, Kai Ding, Ximeng Liu, *Member, IEEE*, Xiaojiang Du, *Fellow, IEEE*, and Mohsen Guizani, *Fellow, IEEE*

Abstract—Vehicle platoon, a novel vehicle driving paradigm that organizes a group of vehicles in the nose-to-tail structure, has been considered as a potential solution to reduce traffic congestion and increase travel comfort. In such a platoon system, head vehicles' performances are usually evaluated by user vehicles' feedbacks. Selection of an appropriate and reliable head vehicle while not disclosing user vehicles' privacy has become an interesting problem. In this article, we present a trust-based and privacy-preserving platoon recommendation scheme, called TPPR, to enable potential user vehicles to avoid selecting the malicious head vehicles. The basic concept of TPPR is that each user vehicle holds a trust value, and the reputation score of the head vehicle is calculated via a truth discovery process. To preserve vehicles' privacy, pseudonyms and Paillier cryptosystem are applied. In addition, novel authentication protocols are designed to ensure that only the valid vehicles (i.e., the vehicles holding the truthful trust values and joining the vehicle platoon) can pass the authentication. A comprehensive security analysis is conducted to prove that the proposed TPPR scheme is secure against several sophisticated attacks in vehicular ad hoc networks. Moreover, extensive simulations are conducted to demonstrate the correctness and effectiveness of the proposed scheme.

Index Terms—Vehicle platoon, trust, privacy-preserving, recommendation

1 Introduction

The explosive growth in vehicle ownership has caused many critical social problems, such as road safety, traffic congestion, and air pollution. To deal with these challenges, a platoon-based driving pattern, also called vehicle platoon, has received considerable attention in recent years [1], [2], [3], [4]. Generally, a vehicle platoon is a road train which comprises of a head vehicle and several user vehicles. The head vehicle drives manually, and all user vehicles follow it automatically [5]. Compared with the traditional driving pattern, vehicle platoon provides many benefits. On one hand, the leader-follower mechanism requires lean inter-vehicle spacing which increases road capacity and alleviates congestion to a certain extent. On the other hand, by reducing air resistance, it can also reduce fuel consumption and air pollution [6].

Although many benefits can be gained by vehicle platoon, some new challenges arise. Since user vehicles hand over their driving control, the head vehicle will determine the platoon's driving route and driving style. Some head vehicles unintentionally or intentionally degrade driver experience by providing low-quality services, or even worse put drivers in dangerous situations. Thus, it is essential to identify such head vehicles before joining a vehicle platoon. Normally, the performances of head vehicles can be judged by user vehicles' feedbacks [1], [2]. However, the problem here is that the feedbacks given by different user vehicles may vary significantly due to different driving habits, incomplete views of observations, or even malicious evaluations. When aggregating these feedbacks, traditional methods such as voting or averaging, which treat all user vehicles equally are not suitable.

An ideal approach to resolve the above challenge is to involve trust values for all user vehicles and make the aggregated reputation scores closed to the feedbacks provided by reliable user vehicles. Nevertheless, another critical issue that must be addressed is the location privacy of user vehicles. Although pseudonymous [7] and anonymous authentication [8], [9] can be used to conceal driver's identity information, vehicles' location and trajectory privacy may still be disclosed by linking their trust values. To illustrate, we consider a scenario in Fig. 1. At time t_1, two vehicles (the green and blue) join a vehicle platoon, and at time t_2 and t_3, they join different vehicle platoons respectively. Although their pseudonyms have been changed, their trust values (i.e., Trust_A and Trust_B) remain unchanged in a certain period. By linking their trust values, the trajectories of the two vehicles can be easily reconstructed. Hence, it is important to design a trust-based head vehicle selection scheme which does not sacrifice user vehicles' privacy.

- *C. Zhang, L. Zhu, C. Xu, K. Sharif, and K. Ding are with the Beijing Engineering Research Center of Massive Language Information Processing and Cloud Computing Application, School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100811, China. E-mail: {chuanz, liehuangz, xuchang, 7620160009}@bit.edu.cn, deking@139.com.*
- *X. Liu is with the School of Information Systems, Singapore Management University, College of Mathematics and Computer Science, Fuzhou University, Fuzhou, Fujian 350002, China, and Fujian Provincial Key Laboratory of Information Security of Network Systems, Fuzhou, Fujian 350002, China. E-mail: snbnix@gmail.com.*
- *X. Du is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122 USA. E-mail: dxj2005@gmail.com.*
- *M. Guizani is with the Department of Computer Science and Engineering, Qatar University, Doha 2713, Qatar. E-mail: mguizani@ieee.org.*

Manuscript received 21 June 2019; revised 20 Nov. 2019; accepted 8 Dec. 2019. Date of publication 24 Dec. 2019; date of current version 8 Apr. 2022. (Corresponding authors: Liehuang Zhu and Chang Xu.)
Digital Object Identifier no. 10.1109/TSC.2019.2961992

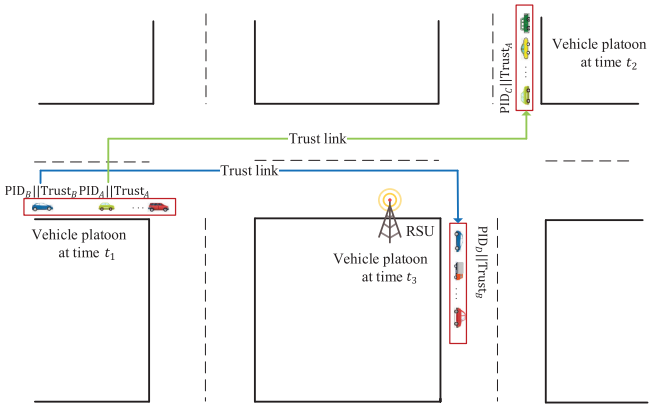


Fig. 1. Using trust values to link pseudonyms in a given period of time.

To address the above challenges, we present a trust-based and privacy-preserving platoon recommendation system, called TPPR, to accurately rank the head vehicles according to user vehicles' feedbacks while not disclosing their location privacy. The general process of TPPR can be described as follows. After finishing a trip with a platoon, user vehicles deliver their feedbacks and encrypted trust values to the roadside units (RSUs), which will collaborate with the Service Provider (SP) to calculate the head vehicle's reputation score using a weighted method. During the whole process, user vehicles' privacy will not be disclosed to any other parties. Below, we have summarized the major contributions of this work.

- First, we design a filtering truth discovery algorithm to process the feedback information received from user vehicles. By this algorithm, the proposed scheme can effectively estimate the performance of head vehicles and user vehicles. This allows the optimal selection of head vehicles in vehicle platoon.
- Second, we use pseudonyms and Paillier cryptosystem to protect user vehicles' privacy. Moreover, novel authentication protocols are designed to ensure that only legitimate vehicles can pass authentication. To the best of our knowledge, our work is the first attempt to resolve the security and privacy issues in head vehicle selection.
- Third, we conduct a comprehensive security analysis to demonstrate that the scheme presented is not only secure, but can also defend against different sophisticated attacks in vehicular ad hoc network *(VANET)*. Additionally, extensive simulations are performed to validate the correctness & effectiveness of TPPR.

This paper has been organized into 8 sections, where system and threat model along with design goals have been discussed in Section 2, followed by preliminary discussion in Section 3. The TPPR scheme functionality is explained in Section 4, and its security analysis & evaluation are presented in Sections 5 and 6. Related works and conclusion are detailed in Sections 7 and 8 respectively.

2 Models and Design Goal

To better present the proposed scheme, we first describe the system model, and give details of the threat model. Based on these, we develop the design goals of our proposed scheme.

2.1 System Model

The overall model considers a typical scenario of vehicle platoon. The RSUs are widely deployed in a given area and every vehicle can communicate with RSUs through an onboard unit. Particularly, the system consists of a trusted authority (TA), RSUs, a service provider (SP), and vehicles, as shown in Fig. 2.

- Trusted Authority (TA): This entity is in charge of all participating parties, and also maintains a database to store user vehicles' trust values. We assume that it is fully capable of storing and performing computation on data generated by other entities. After receiving user vehicles' trust values, it can predict their future behaviors based on historical data.
- Service Provider (SP): SP connects all RSUs and stores feedbacks and trust values sent from these roadside units. Upon receiving the data, SP executes a truth discovery based evaluation algorithm to calculate the reputation scores for head vehicles. Similarly, for the query of a potential user vehicle for the platoon join request, SP responds it by recommending the head vehicles with high reputation scores.
- Roadside Units (RSUs): RSUs are subordinates of SP. They are widely deployed and can cover a wide area. They collect user vehicles' feedbacks and trust values, and then forward them to SP. In particular, they have limited computation capacity, which ensures that they can authenticate user vehicles' identities and perform aggregation operations.
- Vehicles: The vehicles are equipped with onboard units, which enable direct communication with other vehicles, RSUs, and TA through wireless media. In a platoon scenario, vehicles can be classified as:
  - Head vehicles: The head vehicles, also known as platoon leaders, control the whole vehicle platoon. When a user vehicle joins a head vehicle's platoon, it should guide the vehicles toward the destination safely and satisfactorily. Besides, the head vehicle is required to maintain continuous connection with user vehicles and submit the proofs after finishing the trip.
  - User vehicles: These vehicles follow head vehicles automatically. They get instructions from head vehicles and build handshake proofs with them by Vehicle-to-Vehicle (V2V) connections. After finishing the trip, they will submit driving reports to RSUs. Besides, the user vehicles update their trust values from TA at regular intervals.

2.2 Threat Model

TA is fully trusted because it generates the public and private keys for all roles. We assume TA is under strong physical protection and cannot be compromised. SP and RSUs are both considered to be honest but curious. In other words, they will honestly perform the given tasks but try to infer user vehicles' location and trajectory privacy by linking their identities or trust values. Note that, SP and RSU will not collude with each other. This is a common assumption in existing fog-based applications [10], [11], [12]. The head vehicles are supposed to be reliable and trusted, since they control the whole

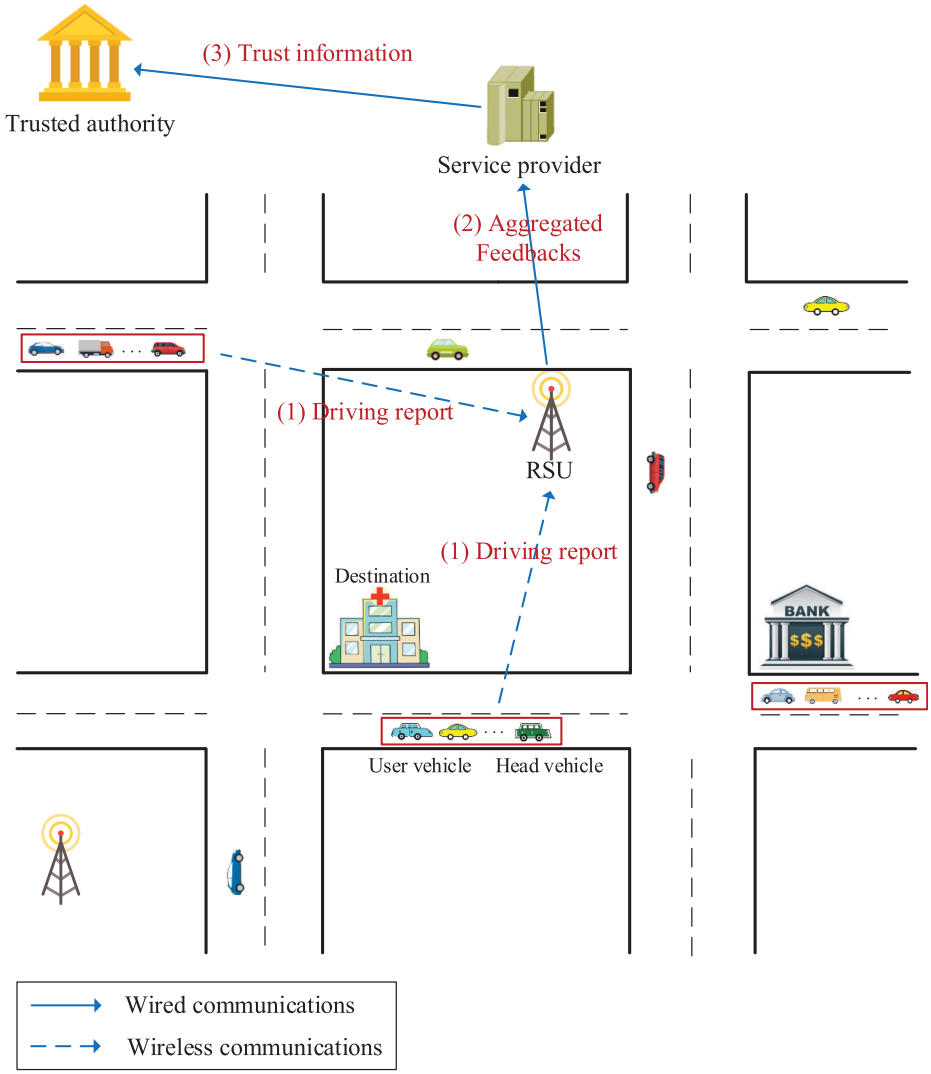


Fig. 2. System model.

platoon. However, their performances may vary differently due to different driving experience or driving style. For any head vehicle, its performance can change constantly in different trips. As for the user vehicles, they are required to submit their feedbacks and trust values after each trip. However, some selfish or malicious user vehicles may provide untruthful feedbacks, or some attackers outside the vehicle platoon may give fake feedbacks for their benefits or with the intention to disrupt the entire system. In particular, we assume there is no collusion between user vehicles and RSUs.

2.3 Design Goals

Using the earlier described system model, the goal is to build a trust-based and privacy-preserving head vehicle selection scheme for vehicle platoon. In particular, the following objectives should be captured.

- Privacy: The proposed scheme should preserve user vehicles' privacy. That is, other parties cannot infer user vehicles' location and trajectory information based on the given data.
- Security: The proposed scheme should defend against different sophisticated attacks, such as bad-mouth attack and on-off attack. In addition, some user vehicles may provide fake trust values and feedbacks. The proposed scheme must be resilient to these attacks.
- Accuracy: The proposed scheme should accurately calculate the reputation scores of the head vehicles according to user vehicles' feedbacks. Besides, the scheme should identify malicious and honest user vehicles, and further give a prediction of their future trust values.

3 Preliminaries

Bilinear pairing and Paillier cryptosystem are two foundation elements in the proposed scheme. Hence, we introduce them in this section.

3.1 Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of the same large prime order q. Then, the following three properties can be satisfied by a bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

- Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$, for all $P, Q \in \mathbb{G}$ and $a, b \in \mathbb{Z}_q^*$.
- Non-degenerated: $e(P, P) \neq 1$, for any $P \in \mathbb{G}$.

- Computable: $e(P,Q)$ can be efficiently computed for all $P,Q \in \mathbb{G}$.

We refer to [3], [13], [14] to provide a more comprehensive description and definition for this technique.

Definition 1. *A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm which takes a security number κ as input, and outputs a 5-tuple $(q, P, \mathbb{G}, \mathbb{G}_T, e)$, where q is a large prime with κ bits, $(\mathbb{G}, \mathbb{G}_T)$ are two multiplicative groups with the same order q, $P \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an efficiently computable bilinear group with the property of non-degeneracy.*

Definition 2 (Computational Diffie-Hellman (CDH) Problem). *Given the elements $(P, aP, bP) \in \mathbb{G}$, there exists no probabilistic and polynomial time algorithm to calculate $abP \in \mathbb{G}$ with a non-negligible probability of success.*

3.2 Paillier Cryptosystem

This cryptosystem is a form of encryption which supports multiplication operations on the ciphertexts. Due to the homomorphic properties, it has been widely used in various privacy-preserving applications [15]. Fundamentally, it consists of the following three algorithms:

- *Key Generation:* Given a large security parameter κ_1, and two large primes p_1, q_1, where $|p_1| = |q_1| = \kappa_1$. Then, $n = p_1 q_1$ and $\lambda = lcm(p_1 - 1, q_1 - 1)$ are computed, where $lcm(a, b)$ is a function to compute the least common multiple of a and b. Define a function $L(c) = \frac{c-1}{n}$, μ is calculated as $(L(g^\lambda \bmod n^2))^{-1} \bmod n$, where $g \in \mathbb{Z}^*_{n^2}$ is randomly chosen. Then, the public key pk and secret key sk are generated as $pk = (n, g)$ and $sk = (\lambda, \mu)$ respectively.
- *Encryption:* Given a message $m \in \mathbb{Z}_n$, the ciphertext is calculated as $c = E(m) = g^m \cdot r^n \bmod n^2$, where $r \in \mathbb{Z}^*_n$ is randomly chosen.
- *Decryption:* Given a ciphertext $c \in \mathbb{Z}^*_{n^2}$, the ciphertext can be decrypted as $m = D(c) = L(c^{\lambda \bmod n^2}) \cdot \mu \bmod n$. The correctness and security of the Paillier cryptosystem has been proven in [16].

In particular, the Paillier cryptosystem satisfies the following homomorphic properties:

- For any $m_1, m_2 \in \mathbb{Z}_n$, $E(m_1) \cdot E(m_2) = E(m_1 + m_2)$.
- For any $m_1, a \in \mathbb{Z}_n$, $E(m_1)^a = E(am_1)$.

4 TPPR Scheme

The proposed trust-based and privacy-preserving platoon recommendation scheme includes system initialization, system overview, report generation, report aggregation, feedback evaluation, and trust value evaluation.

4.1 System Initialization

Given security parameters κ and κ_1, TA first generates a 5-tuple $(q, P, \mathbb{G}, \mathbb{G}_T, e)$ by executing $\mathcal{G}en(\kappa)$, and generates the public key $(n = p_1 q_1, g)$ and private key (λ, μ) of the Paillier cryptosystem. Then, TA selects two secure cryptographic hash functions H and H_1, where $H : \{0,1\}^* \rightarrow \mathbb{G}$ and $H_1 : \{0,1\}^* \rightarrow \{0,1\}^\kappa$. Before joining the system, all vehicles and RSUs are required to register themselves with TA. Specifically, TA selects a secure symmetric encryption algorithm AES_{k_0} by choosing a symmetric key k_0. For every registered vehicle v_i with its real identity ID_i, TA creates a group of pseudonyms $\{PID_{i0}, PID_{i1}, \ldots, PID_{iN}\}$, and generates the public and private key pairs as $Y_{ij} = x_{ij}P$ for $j = \{0, 1, \ldots, N\}$, where $x_{ij} \in \mathbb{Z}^*_q$ is a random value and $PID_{ij} = AES_{k_0}(ID_i || x_{ij})$. Then, TA selects a secure number $\chi \in \mathbb{Z}^*_n$ to encrypt each vehicle's trust value T_i as $C_i = g^{T_i} \cdot (r_i \cdot H_1(t_c || \chi))^n \bmod n^2$, where t_c is the stipulated update time and $r_i \in \mathbb{Z}^*_n$, and then generates the corresponding trust signature as $\mathfrak{C}_i = g^{T_i} \cdot r_i^n \cdot g^{H_1(t_c||\chi)+PID_{ij}} = g^{T_i+H_1(t_c||\chi)+PID_{ij}} \cdot r_i^n \bmod n^2$. Note that the trust signature is used to verify if the trust value is fresh. For an RSU, TA selects a random element $x_r \in \mathbb{Z}^*_q$ as secret and calculates the public key $Y_r = x_r P$. Finally, TA sends $\{\{PID_{ij}, x_{ij}\}_{j=1}^N, t_c, C_i, \mathfrak{C}_i, n, \mathbb{G}, \mathbb{G}_T, e, H, H_1\}$ to vehicle v_i, $\{n, g, \chi, P, \mathbb{G}, \mathbb{G}_T, e, x_r, Y_r, H, H_1\}$ to RSU, and λ to SP.

4.2 Scheme Overview

When a user vehicle joins a vehicle platoon, it first creates a handshake proof with the head vehicle to prove that it has joined this platoon. After finishing the trip, both user and head vehicles are required to generate their driving reports and deliver them to RSU. Then RSU verifies the user vehicle's validity, i.e., to verify the user vehicle's driving report, handshake proof, and trust value. It then uses user vehicles' trust values and feedbacks to calculate the head vehicle's reputation score. Following this, the RSU delivers the reputation score and feedbacks to SP, which will be then used to evaluate the vehicles' performances. Finally, SP sends user vehicles' trust values to TA, and TA will predict their future performances based on the historical data. This complete process is shown in Fig. 3.

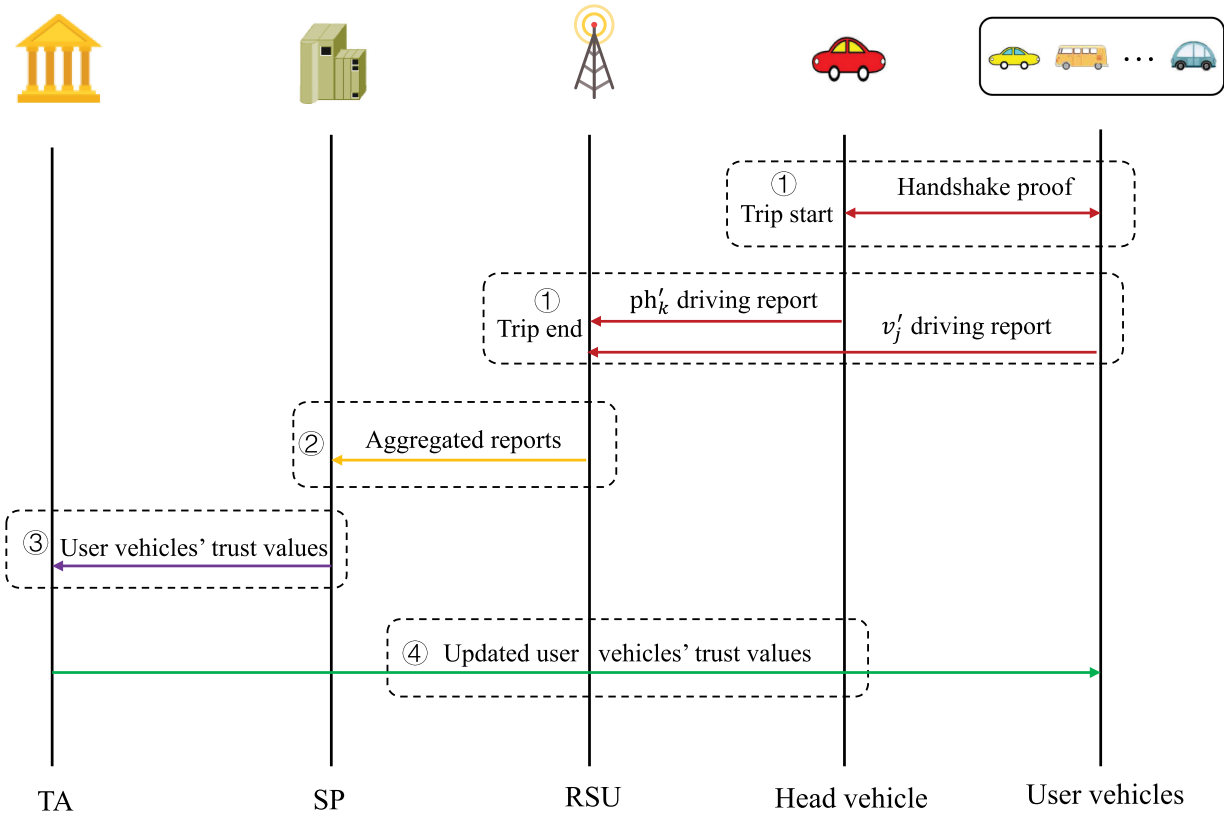
4.3 Report Generation

When a user vehicle v_j with $(\mathrm{PID}_j, x_j, C_j, \mathfrak{C}_j)$ finishes a vehicle platoon organized by a head vehicle ph_k, it is required to send a driving report to the nearby RSU, which is denoted as R_j. Specifically, v_j uses its onboard units (OBU) to generate the report, including the head vehicle ph_k, trip Tr_k, feedback f_j, and a handshake proof with ph_k. The handshake proof is used to prove that whether v_j actually joined the ph_k's platoon. This proof is generated as follows.

- Based on κ_1, the head vehicle ph_k generates its Paillier Cryptosystem's public key (n_k, g_k) and the secret key (λ_k, μ_k). Then, it broadcasts a random value $\alpha_k \in \mathbb{Z}^*_{n_k}$ and its public key to all user vehicles.
- The user vehicle v_j selects $\alpha_j, r_j \in \mathbb{Z}^*_{n_k}$ and uses the head vehicle's homomorphic encryption (n_k and g_k) to calculate $C_{\alpha_j} = g_k^{\alpha_j} \cdot r_j^{n_k} \bmod n_k^2$, which is the ciphertext of α_j. Then, the user vehicle delivers C_{α_j} to the head vehicle.
- After receiving the ciphertext, the head vehicle recovers α_j and calculates the proof as $\mathrm{proof}_{kj} = x_k H(\alpha_k + \alpha_j)$. Accordingly, the user vehicle calculates its proof as $\mathrm{proof}_{jk} = x_j H(\alpha_j + \alpha_k)$.

Then, to prevent the RSU or other attackers linking v_j's trust value, v_j selects a random value $r'_j \in \mathbb{Z}^*_n$ to perturb the trust ciphertext as $\widetilde{C}_j = g^{T_j} \cdot (r_j \cdot H_1(t_c||\chi))^n \cdot (r'_j)^n \bmod n^2$ [1].

1. In this paper, g is not public to the user vehicles. The user vehicles can only use the public key n to perturb the ciphertexts.



① Report generation ② Report aggregation ③ Reputation score estimation ④ Trust value estimation

Fig. 3. Overview of TPPR.

Accordingly, the trust signature is also recalculated as $\widetilde{\mathfrak{C}}_j = g^{T_j+H_1(t_c||\chi)+PID_j} \cdot r_j^n \cdot (r_j')^n \bmod n^2$. After that, v_j uses x_j to generate a signature as $\sigma_j = x_j H(PID_j||FR_j||TR_j||\ \text{proof}_{jk})$, where $FR_j = (\text{ph}_k||Tr_k||f_j)$ is the feedback report and $TR_j = (\widetilde{C}_j||\widetilde{\mathfrak{C}}_j||t_c)$ is the trust report. Finally, v_j submits the report $R_j = (PID_j, FR_j, TR_j, \text{proof}_{jk}, \sigma_j)$ to RSU when it finishes the trip. ph_k uploads its report $R_k = (\text{ph}_k, Tr_k, \{\text{proof}_{kj}\}_{j=1}^{sum}, \sigma_k)$, where sum is the total number of user vehicles in the trip Tr_k and $\sigma_k = x_k H(\text{ph}_k||Tr_k||\{\text{proof}_{kj}\}_{j=1}^{sum})$.

4.4 Report Aggregation

Upon receiving the reports, RSU first verifies the vehicle's signature σ_j, i.e., to check whether $e(P, \sigma_j) \stackrel{?}{=} e(Y_j, H(PID_j||FR_j||TR_j||\text{proof}_{jk}))$. If it does hold, the signature is valid and RSU will accept v_j's report, since $e(P, \sigma_j) = e(P, x_j H(PID_j||FR_j||TR_j||\text{proof}_{jk})) = e(Y_j, H(PID_j||FR_j||TR_j||\text{proof}_{jk}))$. To improve verification efficiency with less overhead, RSU can perform batch verification as:

$$\begin{aligned} e\left(P, \sum_{j=1}^{sum} \sigma_j\right) &= e\left(P, \sum_{j=1}^{sum} x_j H(PID_j||FR_j||TR_j||\text{proof}_{jk})\right) \\ &= \prod_{j=1}^{sum} e(P, x_j H(PID_j||FR_j||TR_j||\text{proof}_{jk})) \\ &= \prod_{j=1}^{sum} e(Y_j, H(PID_j||FR_j||TR_j||\text{proof}_{jk})). \end{aligned} \tag{1}$$

By this way, the verification can be completed by executing only $sum + 1$ rather than $2sum$ pairing operations.

After the validity checking, RSU will verify v_j's handshake proof, i.e., proof_{jk}, to check whether it has joined the vehicle platoon. Specifically, RSU verifies $e(Y_k, \text{proof}_{jk}) \stackrel{?}{=} e(Y_j, \text{proof}_{kj})$. If it holds, the proof is verified, since $e(Y_k, \text{proof}_{jk}) = e(x_k P, x_j H(\alpha_j + \alpha_k)) = e(x_j P, x_k H(\alpha_k + \alpha_j)) = e(Y_j, \text{proof}_{kj})$. Similarly, RSU can also perform batch verification, that is, to check if $e(Y_k, \sum_{j=1}^{sum} \text{proof}_{jk}) \stackrel{?}{=} \prod_{j=1}^{sum} e(Y_j, \text{proof}_{kj})$. The proof is given as follows.

$$\begin{aligned} e\left(Y_k, \sum_{j=1}^{sum} \text{proof}_{jk}\right) &= e\left(Y_k, \sum_{j=1}^{sum} x_j H(\alpha_j + \alpha_k)\right) \\ &= \prod_{j=1}^{sum} e(x_k P, x_j H(\alpha_j + \alpha_k)) \\ &= \prod_{j=1}^{sum} e(P, x_k x_j H(\alpha_j + \alpha_k)) \\ &= \prod_{j=1}^{sum} e(x_j P, x_k H(\alpha_j + \alpha_k)) \\ &= \prod_{j=1}^{sum} e(Y_j, \text{proof}_{kj}). \end{aligned} \tag{2}$$

Besides the above operations, it is also important to check if the trust value, i.e., $\widetilde{C}_j$, is truthful and fresh, as some malicious user vehicles may change their trust values. To achieve this goal, RSU first checks the time stamp t_c, and then checks the trust signature $\widetilde{\mathfrak{C}}_j$. Specifically, RSU checks if $\widetilde{C}_j \cdot g^{H_1(t_c||\chi)+PID_j} \bmod n^2$ equals to $\widetilde{\mathfrak{C}}_j \cdot (H_1(t_c||\chi))^n \bmod n^2$,

as $\widetilde{C}_j \cdot g^{H_1(t_c||\chi)+PID_j} = g^{T_j} \cdot (r_j \cdot H_1(t_c||\chi))^n \cdot (r'_j)^n \cdot g^{H_1(t_c||\chi)+PID_j} = g^{T_j+}\ H_1(t_c||\chi) + PID_j \cdot (r_j \cdot r'_j \cdot H_1(t_c||\chi))^n = \widetilde{\mathfrak{C}}_j \cdot (H_1(t_c||\chi))^n$. Similarly, RSU can perform batch verification to check $g^{H_1(t_c||\chi)} \cdot \sum_{j=1}^{sum}(\widetilde{C}_j \cdot g^{PID_j}) \stackrel{?}{=} (H_1(t_c||\chi))^n \cdot \sum_{j=1}^{sum} \widetilde{\mathfrak{C}}_j$. The proof is given as follows.

$$\begin{aligned} g^{H_1(t_c||\chi)} \cdot \sum_{j=1}^{sum}(\widetilde{C}_j \cdot g^{PID_j}) &= \sum_{j=1}^{sum}(g^{T_j+H_1(t_c||\chi)+PID_j} \\ &\quad \cdot (r_j \cdot r'_j \cdot H_1(t_c||\chi))^n) \\ &= (H_1(t_c||\chi))^n \cdot \sum_{j=1}^{sum} \widetilde{\mathfrak{C}}_j. \end{aligned} \tag{3}$$

Then, RSU performs the following steps to generate the aggregated report.

- Step 1. Compute the aggregated weighted data according to $\{f_j, \widetilde{C}_j\}_{j=1}^{sum}$ as

$$\begin{aligned} C_1 &= \prod_{j=1}^{sum} \widetilde{C}_j^{f_j} \bmod n^2 \\ &= \prod_{j=1}^{sum} g^{T_j f_j} \cdot (r_j \cdot r'_j \cdot H_1(t_c||\chi))^{nf_j} \bmod n^2 \\ &= g^{\sum_{j=1}^{sum} T_j f_j} \cdot \left(\prod_{j=1}^{sum} (r_j r'_j H_1(t_c||\chi))^{f_j} \right)^n \bmod n^2 \end{aligned} \tag{4}$$

$$\begin{aligned} C_2 &= \prod_{j=1}^{sum} \widetilde{C}_j \bmod n^2 \\ &= g^{\sum_{j=1}^{sum} T_j} \cdot \left(\prod_{j=1}^{sum} (r_j r'_j H_1(t_c||\chi)) \right)^n \bmod n^2. \end{aligned} \tag{5}$$

- Step 2: Use the private key x_r to generate a signature σ_r as

$$\sigma_r = x_r H(\mathrm{ph}_k||Tr_k||C_1||C_2||\{PID_j||f_j\}_{j=1}^{sum}). \tag{6}$$

- Step 3: Deliver the integrated report $R_r = (\mathrm{ph}_k, Tr_k, C_1, C_2, \{PID_j, f_j\}_{j=1}^{sum}, \sigma_r)$ to SP.

4.5 Reputation Score Evaluation

After receiving the report R_r, SP first validates the report by checking if $e(P, \sigma_r)$ equals to $e(Y_r, H(\mathrm{ph}_k||Tr_k||C_1||C_2||\{PID_j||f_j\}_{j=1}^{sum}))$. Then TA decrypts C_1, C_2 by using the secret key (λ, μ), and calculates the reputation score RS_k as follows.

$$\begin{aligned} RS_k &= \frac{D(C_1)}{D(C_2)} = \frac{L(C_1^{\lambda} \bmod n^2) \cdot \mu \bmod n}{L(C_2^{\lambda} \bmod n^2) \cdot \mu \bmod n} \\ &= \frac{\sum_{j=1}^{sum} T_j f_j}{\sum_{j=1}^{sum} T_j}. \end{aligned} \tag{7}$$

Note that, RS_k is calculated based on user vehicles' previous trust values. To evaluate the qualities of user vehicles' feedbacks in the trip Tr_k, we design a filtering truth discovery algorithm. The basic idea is to assign a higher weight to a user vehicle if its data is closer to the reputation score, and the data provided by a user vehicle with higher weight will be more likely to be considered as the truthful reputation score [11], [17], [18], [19], [20]. More specifically, $\mathcal{V}_k = \{v_1, v_2, \ldots, v_{sum}\}$ represents the set of vehicles which belong to the trip Tr_k, and is updated in each iteration since some user vehicles may be removed. The filtering truth discovery algorithm is achieved by the following steps.

- Data filtering: For a user vehicle $v_j \in \mathcal{V}_k^{(v)}$, SP calculates the difference between each user vehicle's feedback and the reputation score, and then removes the vehicle whose difference exceeds a predefined threshold value $U_{threshold}$, i.e.,

$$|f_j - RS_k^{(v)}| > U_{threshold}, \tag{8}$$

  where $RS_k^{(v)}$ denotes ph_k's reputation score in the vth iteration, $v \in [1, V]$. After this process, the set will be updated as $\mathcal{V}_k^{(v+1)}$.
- Weight update: SP calculates the difference between each user's feedback and the head vehicle's reputation score, and then updates each user's weight based on the aggregated differences. Without loss of generality, we adopt a logarithmic weight function, which has been widely used in truth discovery based applications [11], [19].

$$w_j^{(v+1)} = \log \left(\frac{\sum_{v_j \in \mathcal{V}_k^{(v+1)}} d(f_j, RS_k^{(v)})}{d(f_j, RS_k^{(v)})} \right), \tag{9}$$

  where $d(\cdot)$ is a distance function calculated as $d(f_j, RS_k^{(v)}) = (f_j - RS_k^{(v)})^2$.
- Reputation score update: Based on the uses' weights and feedbacks, the reputation score for the head vehicle can be estimated as

$$RS_k^{(v+1)} = \frac{\sum_{v_j \in \mathcal{V}_k^{(v+1)}} w_j^{(v+1)} \cdot f_j}{\sum_{v_j \in \mathcal{V}_k^{(v+1)}} w_j^{(v+1)}}. \tag{10}$$

The above procedures will be iteratively conducted until the change of the reputation score between two consecutive iterations is less than a predefined threshold. Then, SP publishes the head vehicle's reputation score. The general procedure of the filtering truth discovery algorithm is shown in Algorithm 4.5.

Algorithm 1. Filtering Truth Discovery Algorithm

Input: User vehicles' feedbacks $\{f_j\}_{j=1}^{sum}$
Output: Reputation score RS_k
Calculate the initial reputation score (see Eq. (7));
for $v = 1, 2, \ldots, V$ **do**
  for $v_j \in \mathcal{V}_k^{(v)}$ **do**
    Update the set of user vehicles (see Eq. (8));
    Update user vehicles' weights (see Eq. (9));
    Update the reputation score (see, Eq. (10));
return RS_k

4.6 Trust Value Evaluation

Based on the reputation score, SP can also obtain user vehicles' new trust values. Motivated by [2], we define a function to measure the qualities of user vehicles' trust values.

$$T_j = \begin{cases} 1 - |f_j - RS_k|^{V \cdot c_0} & v_j \in \mathcal{V}_k^{(V)} \\ T_0 & v_j \notin \mathcal{V}_k^{(V)} \end{cases}, \tag{11}$$

where V is the number of iterations. It is obvious that if there are more malicious user vehicles, V will be larger and it will be more difficult to obtain the accurate reputation score. Thus, V is used as a reward for the vehicles whose feedbacks contribute to the accurate reputation score calculation. Besides, we define another factor c_0 to control the reward sensitivity. If the vehicle is removed from the vehicle set (i.e., $v_j \notin \mathcal{V}_k^{(V)}$), then its feedback does not make any positive effect on the reputation score and hence the user vehicle will not obtain the reward. Then, SP delivers user vehicles' trust values $\{(PID_1, T_1), \ldots, (PID_{sum}, T_{sum})\}$ to TA.

On receiving trust values, TA first uses the symmetric key k_0 to retrieve user vehicles' real identities, and then predicts users' future trust values according to their historical behaviors. Here, we use the exponential weighted moving average (EMWA) technique to estimate user vehicles' future behaviors, as it gives more consideration of users' most recent performances [21], [22].

$$T_j^{(l+1)} = \alpha \times T_j^{(l-1)} + (1 - \alpha) \times T_j^l, \tag{12}$$

where $\alpha \in (0, 1)$ is an impact factor, and $T_j^{(l-1)}, T_j^l, T_j^{(l+1)}$ are the past, current, and future trust values respectively .

Note that, some user vehicles may behave well at the beginning to improve their trust values, and behave badly when these values are high enough. To counter the effect of this attack, we further design a trust value circuit-breaker mechanism as:

$$T_j^{(l+1)} = \begin{cases} T_0 & T_j^{(l-1)} - T_j^l > T_{threshold} \\ T_j^{(l+1)} & otherwise \end{cases} \tag{13}$$

From this equation, we can see if the decrease between two consecutive trust values is larger than a predefined threshold, the trust value will be set as the initialized value T_0. Moreover, to punish the on-off attacker, once the circuit-breaker is triggered, the predicted trust value will be decreased as $T_j^{(l+1)} = c_1 \cdot T_j^{(l+1)}$, where $c_1 \in (0, 1)$ is a forgetting factor. In this way, the attacker will take more time to bring its trust value to the previous level.

4.7 Discussion

Our scheme is based on the assumption that the RSUs are widely deployed. If there are not enough RSUs deployed in practice, or in a platoon's destination there is no RSU deployed, the user vehicles can submit their feedbacks when they pass by an RSU during the journey or after they end the journey. In these ways, our system can work normally.

If there are no RSUs deployed, a user vehicle can be selected to aggregate other users' feedbacks. Correspondingly, some new problems may occur in this scenario. For example, how to select the aggregator and guarantee the data integrity, and how to defend against the outside attacks and the collusion attacks. We will leave this to be our future work. The small amount of RSUs will affect the system's performance, as an RSU has to perform more authentication and computation tasks.

5 Security Analysis

In this section, we first give an analysis on how TPPR preserves user vehicles' privacy and then discuss some common attacks followed by the resistance analysis.

5.1 Privacy Analysis for User Vehicles

The user vehicle's identity is privacy-preserving. In system initialization, TA generates pseudonyms for user vehicles as $PID_i = AES_{k_0}(ID_i||x_i)$, where k_0 is the symmetric key and x_i is a random value selected by TA. Since k_0 and x_i are only known by TA, other entities cannot recover user vehicles' real identities from the pseudonyms. Thus, the user vehicle's identity is privacy-preserving.

The user vehicle's trust value is privacy-preserving. In the proposed scheme, each user vehicle's trust information is encrypted as a valid Paillier ciphertext $\overline{C}_j = g^{\overline{M}_j} \cdot \overline{R}_j^n \bmod n^2$ if we consider the trust values T_j in $(C_j, \widetilde{C}_j)$, $T_j + H_1(t_c||\chi) +$ PID_j in $(\mathfrak{C}_j, \widetilde{\mathfrak{C}}_j)$ as the message $\overline{M}_j$, and the random values $r_j \cdot H_1(t_c||\chi)$ in C_j, r_j in $\mathfrak{C}_j$, $r_j \cdot H_1(t_c||\chi) \cdot r'_j$ in $\widetilde{C}_j$, $r_j \cdot r'_j$ in $\widetilde{\mathfrak{C}}_j$ as $\overline{R}_j$. As the Paillier Cryptosystem can defend against the chosen plaintext attack [10], [16], the trust value achieves semantic security and privacy preservation. Hence, although an adversary may eavesdrop the ciphertext $\overline{C}_j$, it cannot identify the original data. After collecting user vehicles' reports, the RSU will compute C_1 and C_2 to aggregate all reports. However, the RSU or an adversary cannot get each individual's trust value without the secret key. Finally, SP can recover C_1 and C_2 as $\sum_{j=1}^{sum} T_j f_j$ and $\sum_{j=1}^{sum} T_j$. Nevertheless, since the decrypted data are aggregated results, it cannot get each user vehicle's trust value, i.e., $(T_1, T_2, \ldots, T_{sum})$. Therefore, the user vehicle's trust value is privacy-preserving.

The user vehicle's report achieves authentication and data integrity. The user vehicle's report is signed using the BLS short signature [23]. As the BLS signature has been proven to be secure under the CDH problem [24], any malicious behaviors of an adversary can be detected. Therefore, our proposed scheme can guarantee the report's authentication and data integrity.

The filtering truth discovery algorithm is conditional privacy-preserving. There are three steps in the filtering truth discovery algorithm, i.e., data filtering, weight update, and reputation score update. In these steps, although vehicles' feedbacks and weights are in plaintexts, the vehicles' identities are anonymous. Therefore, the RSU cannot infer each individual's privacy from these plaintexts.

5.2 Resilience Analysis Against Attacks Launched by Adversaries

Resilience to Link Attacks. From the TPPR scheme's perspective, a link attack means that an attacker may link a certain vehicle v_j to its identities or trust values. To prevent the identity link attack, v_j can change its pseudonym when it joins different trips, which will make them unlinkable. However, given that the trust value remains unchanged for some time, it may still be linked according to its trust value. In our proposed scheme, v_j does not submit its original trust values directly to the RSU. Instead, the trust value is encrypted, and v_j changes the ciphertext by multiplying a random value $(r'_j)^n$ when it takes part in a different vehicle platoon (i.e., $C_j \rightarrow \widetilde{C_j} = C_j \cdot (r'_j)^n \bmod n^2$). Besides, although SP owns the

TABLE 1
The Parameters for Evaluation

Notation	Definition	Value
κ	security parameter	$\kappa = 160$
κ_1	security parameter	$\kappa_1 = 512$
sum	maximum number of user vehicles	100
ρ	malicious user vehicles proportion	20%
T_0	initial trust value	0.01
c_0	reward sensitivity	0.1
c_1	forgetting factor	0.85
α	impact factor parameter	0.3
V	number of iterations	10
$U_{threshold}$	threshold which triggers set update	0.5
$T_{threshold}$	threshold which triggers circuit-breaker	0.5

secret key λ, it still cannot trace any individual user vehicle as the encrypted trust values have been aggregated in RSU.

Resilience to Fake Trust Value Attacks. In this scheme, the trust value is encrypted and hence the user vehicle has no method to know its real trust level. However, some malicious vehicle may still provide a fake trust value by colluding with other vehicles or using its previous data. In such a case, our scheme is still effective in defending against this attack as we use time stamp t_c and pseudonym PID_j to generate the trust ciphertext and trust signature, i.e., $(C_j = g^{T_j} \cdot (r_j \cdot H_1(t_c||\chi))^n$ *versus* $\mathfrak{C}_j = g^{T_j + H_1(t_c||\chi) + PID_j} \cdot r_j^n)$. Specifically, for the first collusion attack (v_j is in collusion with v_i for example), v_j submits its falsified trust report as $\widehat{C}_j = C_j \cdot C_i = g^{T_j+T_i} \cdot (r_j r_i (H_1(t_c||\chi))^2)^n \bmod n^2$, $\widehat{\mathfrak{C}}_j = \mathfrak{C}_j \cdot \mathfrak{C}_i = g^{T_j+T_i+2H_1(t_c||\chi)+PID_j+PID_i} \cdot (r_j r_i)^n \bmod n^2$. Since $\widehat{C}_j \cdot g^{H_1(t_c||\chi)+PID_j} \neq \widehat{\mathfrak{C}}_j \cdot (H_1(t_c||\chi))^n$, this malicious manipulation will be identified by RSU. For the second reply attack, v_j submits its previous trust report $C'_j = g^{T'_j} \cdot (r'_j H_1(t'_c||\chi))^n$, $\mathfrak{C}'_j = g^{T'_j + H_1(t'_c||\chi) + PID_j} \cdot (r'_j)^n$. Also, it still cannot pass the authentication, as $C'_j \cdot g^{H_1(t_c||\chi)+PID_j} \neq \mathfrak{C}'_j \cdot (H_1(t_c||\chi))^n$. Besides, the RSU will maintain a list and vehicles' pseudonyms will be added in the list once they have uploaded their reports. Thus, any other party cannot reuse other vehicles' pseudonyms and trust values.

Resilience to Badmouth Attacks. From the TPPR scheme's perspective, a badmouth attack means that the attackers may always provide low feedbacks for head vehicles. Specifically, the badmouth attackers can be categorized into internal and external attackers. For the external badmouth attackers, we design report authentication and handshake protocols to ensure that only the valid user vehicles which register with the system and join the vehicle platoon can pass the authentication. For the internal badmouth attackers, the proposed scheme incorporates a filtering truth discovery based algorithm to distinguish malicious vehicles.

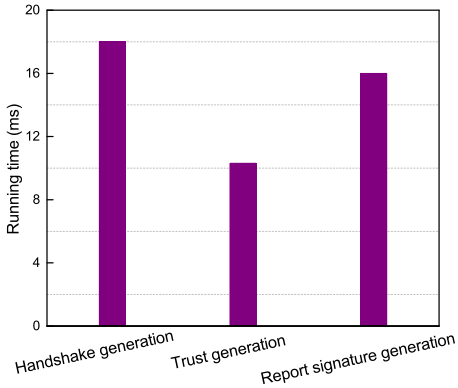


Fig. 4. Computational costs for report generation.

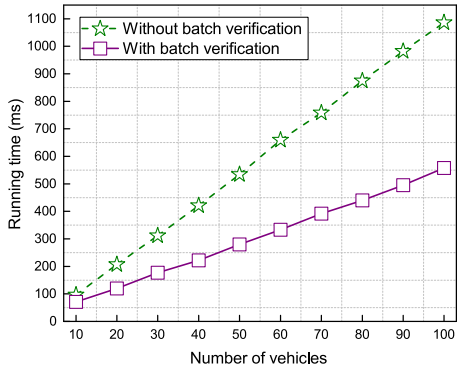


Fig. 5. Computational costs for report authentication.

Resilience to on-off Attacks. In the proposed scheme, an on-off attack means that some malicious user vehicles may perform well to hide themselves before launching attacks. When they attain high trust values, they launch attacks and then remain dormant for a certain period to regain their trust. This attack is hard to defend against using traditional methods. In our scheme, we design a circuit-breaker mechanism to handle this problem, which is motivated by a common human nature that people make great efforts to build up trust values and some bad behaviors will destroy them [2]. Specifically, we define $T_{threshold}$, and once the decrease of two consecutive trust values is larger than this predefined threshold, the circuit-breaker will be triggered. Besides, to punish the on-off attacker, its trust value will be decreased by multiplying a forgetting factor $c_1 \in (0, 1)$ in a long time. That is, the attacker will take a long time to build up its trust value to the previous level. Thus, our proposed scheme mitigates the on-off attack.

6 Performance Evaluation

Here, we evaluate the performance of TPPR in terms of efficiency and effectiveness in platoon selection. The proposed scheme is implemented in Java, and all experiments are conducted on an android phone with 6GB RAM and a system with Intel Core i7 2.5 GHz processor and 16GB RAM. The detailed parameter setting is shown in Table 1.

6.1 Efficiency Analysis

In this experiment, the aim is to evaluate the efficiency of TPPR on the vehicle and RSU sides. The android phone is used on the vehicle side and the laptop is used on the RSU and the SP side. Every experiment is executed 10 times and the average result is used for analysis. Note that, in the proposed scheme, three authentication protocols (i.e., report authentication, handshake authentication, and trust authentication) are designed for user vehicles' verification. We first show the computational costs on the vehicle side. As shown in Fig. 4, three operations are performed, which needs 18 ms for handshake generation, 10.3 ms for trust generation, and 16 ms for report signature generation. In Figs. 5, 6, 7, and 8, we plot the running time on the RSU side. Specifically, Figs. 5, 6,

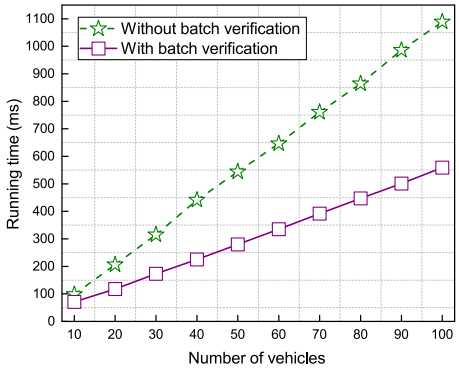


Fig. 6. Computational costs for handshake authentication.

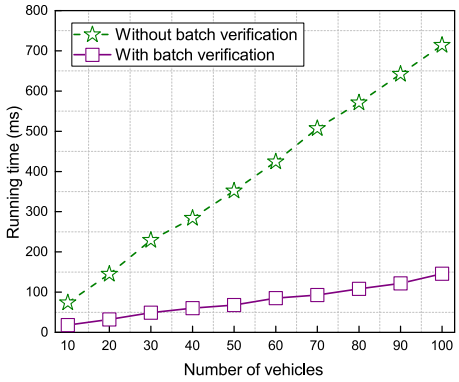


Fig. 7. Computational costs for trust authentication.

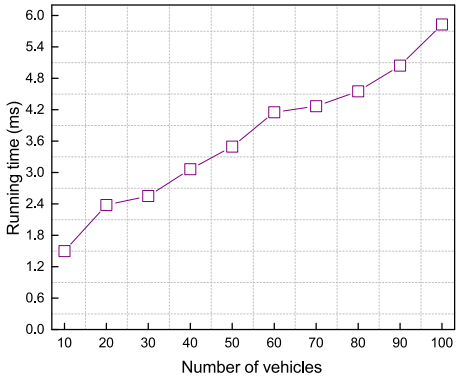


Fig. 8. Computational costs for ciphertexts aggregation.

and 7 illustrate the computational costs of the authentications varying against the number of user vehicles. As can be seen, since we use batch verification in each authentication, the verification is finished with fewer pairing and exponential operations, and accordingly, the running time is much less as compared to no batch verification. In Fig. 8, we plot the running time of ciphertexts aggregation. From this figure, we can observe that as the number of user vehicles increases, our scheme can efficiently perform the ciphertexts aggregation. This is evident from the fact that only 5.6 ms is required to execute the ciphertext aggregation for 100 user vehicles.

6.2 Effectiveness Analysis

To analyze the correctness of the system, we vary the percentage of malicious user vehicles. The malicious user vehicles will provide untruthful feedbacks, that is, their feedbacks are

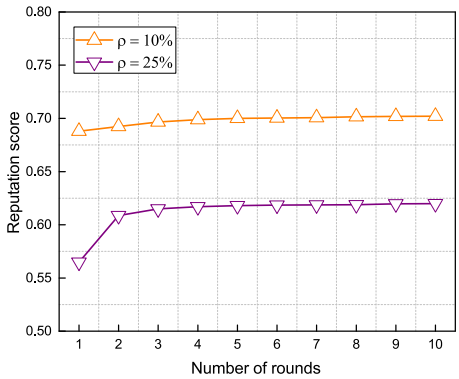


Fig. 9. Reputation score comparison ($\rho = 10\%$ and $\rho = 25\%$).

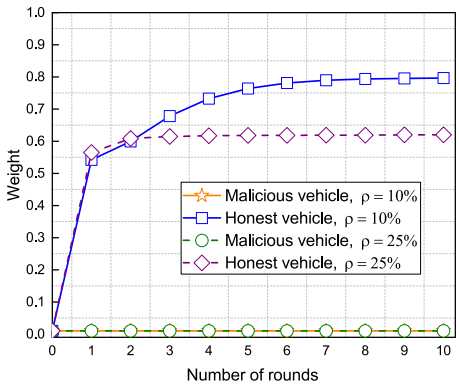


Fig. 10. Weight comparison for honest and malicious user vehicle.

much higher or lower than the truthful evaluation. All user vehicles are initialized with the same trust value T_0. After the execution of our proposed filtering truth discovery algorithm, we observe the value change of the head vehicle and user vehicles.

Figs. 9 and 10 plot the reputation score of the head vehicle and the weight of the user vehicle, where the percentage of malicious vehicles is set as 10 and 25 percent respectively, i.e., $\rho = 10\%$ and $\rho = 25\%$. The range of honest feedbacks is from 0.6 to 0.8 and the range of malicious feedbacks is from 0.01 to 0.1. From Fig. 9, we can see the reputation score tends to be stable after the fourth round. When the number of malicious user vehicles accounts for 10 percent of the total number of user vehicles, the reputation score is equivalent to 0.702. When there are more malicious feedbacks, the reputation score witnesses a downward trend, while is still in a reasonable range. Fig. 10 presents the weights of a single malicious user vehicle and a single honest user vehicle. It is obvious that the malicious vehicle gets the lower trust value after the experiments, which demonstrates the correctness of the TPPR scheme.

We also analyzed the effectiveness of the scheme for resilience to the on-off attack. Recall that an on-off attack means that a user vehicle behaves well to accumulate its trust value at the beginning, and give untruthful feedback when its trust value is high enough. To mitigate the effect of this attack, we design a circuit-breaker mechanism and apply the forgetting factor. As shown in Fig. 11, without the forgetting factor (i.e., the blue line), the user vehicle performs well in the first five vehicle platoons, and its trust value rises to 0.816. After launching the badmouth attack,

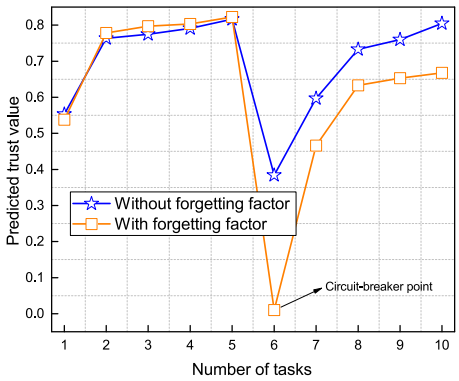


Fig. 11. Trust value comparison based on on-off attacks.

Fig. 12. Simulation area map.

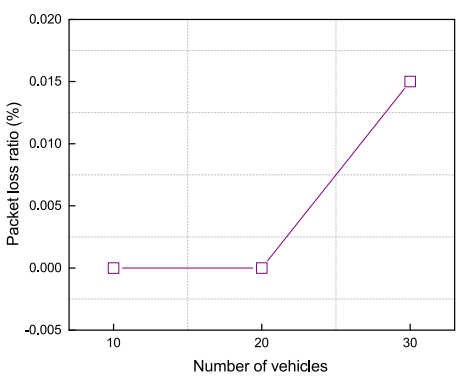


Fig. 13. Packet lose ratio in different numbers of user vehicles.

its trust value decreases quickly, which however rises to 0.804 after only four more vehicle platoons. In contrast, with the forgetting factor (i.e., orange line), it triggers the circuit-breaker at the sixth vehicle platoon, and its trust value rises slowly at the later vehicle platoon. That is, the attacker needs more time to bring its trust value to the previous level and hence demonstrates the effectiveness of the TPPR scheme.

6.3 NS-2 Experiment

We also realized our scheme in the NS-2 simulator to observe the network performance. Specifically, we used OpenStreetMap project to generate the road topography and used SUMO to generate vehicles' movement traces. As shown in Fig. 12, the scope of the simulation area map is set

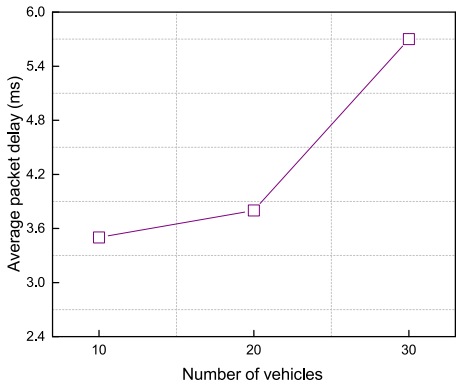


Fig. 14. Average packet delay in different numbers of user vehicles.

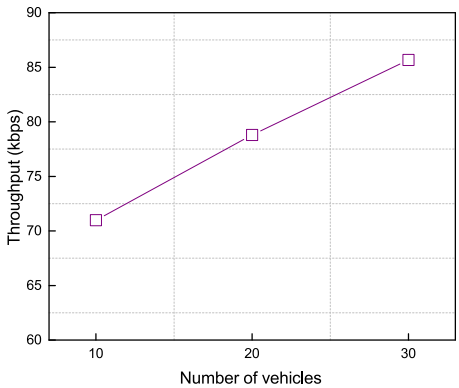


Fig. 15. Throughput in kilobytes per second in different numbers of user vehicles.

as 5.0 KM × 5.0 KM, which is a real-traffic environment located in Xi'an City of China. Especially, to give a more realistic simulation of vehicle platoon, we assume the user vehicles hold a same speed, which ranges from 16 m/s to 18 m/s, and accordingly the simulation area is extended to 50.0 KM × 50.0 KM in the simulator. The underlying protocol used to provide communications between vehicles is IEEE 802.11p. The communication range is set as 250 m. The vehicles form a fixed-size platoon, and the number of user vehicles is set as 10, 20, and 30 respectively. The performance metrics include packet loss ratio, average packet delay, and throughput.

From Fig. 13, we can see our proposed scheme remains a low packet loss ratio. The reason is that a vehicle platoon holds a stable topology and each user vehicle can send the packet in different time window to alleviate the problem of packet collision. From Fig. 14, we can observe that when the number of user vehicles ranges from 10 to 30, our proposed scheme can quickly transmit a packet from the user vehicle to the head vehicle, which also benefits from the unique driving paradigm of vehicle platoon. From Fig. 15, we can see the throughput in our scheme increases with the number of user vehicles, which is reasonable since more user vehicles need to send their packets to the head vehicle.

7 Related Work

By taking advantage of the unique feature of VANET and mobile crowdsensing systems [25], [26], [27], [28], vehicle platoon, has received considerable attention in recent years.

As a special driving pattern which links vehicles like a train, vehicle platoon can greatly save fuel and improve road capacity [29]. For example, the experiments in a California traffic automation program, also known as the PATH project, show that vehicles driving in the ten-car platoon can increase the lane capacity by three times. Besides, the project of Safe Road Trains for the Environment (SARTRE) [30], supported by the European Commission, shows that vehicle platoon can not only reduce fuel consumption, but also improve safety and driver comfort. Although many benefits can be obtained from the platoon, how to select a reliable head vehicle while not disclosing users' privacy is still an unsolved problem [31], especially considering that more and more people raise their concerns on security and privacy [32], [33].

To the best of our knowledge, none of the existing schemes have solved this problem. Generally, to find a reliable head vehicle and help user vehicles avoid selecting the misbehaving head vehicles, a potential approach is to evaluate the trustworthiness of the head vehicles and follower vehicles. Recently, many trust models have been proposed in VANET [2], [34], [35], [36], [37], [38], [39]. Specifically, in [34], Patwardhan *et al.* proposed a context-aware reputation management approach for vehicular ad hoc networks, which provides a bootstrapping method to enable vehicles to establish trust relationships. Raya *et al.* [35] presented a data-oriented trust establishment scheme. However, their framework is not efficient in handling a large amount of feedback data in a platoon scenario. Zhu *et al.* [37] described a trust management scheme for vehicular crowdsensing applications. Hu *et al.* [2] presented a reliable and trust-based platoon service recommendation scheme. By building a trust-based evaluation model, their scheme can defend against several sophisticated attacks in VANET. Although high accuracy can be obtained, their work is based on a strong assumption that the service provider is trusted. In contrast, we assume the SP is semi-honest and propose a novel trust-based and privacy-preserving platoon recommendation scheme. Besides, we also consider the outside attacks and design new authentication protocols to guarantee that only the user vehicles registering in the system, joining the vehicle platoon, and holding the truthful trust values can pass the authentication. Javed [38] presented a security adaptation scheme to improve the quality of service (QoS) of safety applications. In their scheme, several factors such as connectivity duration, near vehicles' centrality metrics, and security level are combined to calculate the trust level. Since this work is focused on the QoS in Vehicular Sensor Networks (VSNs), it is not suitable in the applications of vehicle platoon. Yang *et al.* [39] studied trust problems in online social networks (OSNs) and vehicular social networks (VSNs). In their work, the trust in VSNs is innovatively divided into direct trust and indirect trust, and any two vehicles can be connected by the trust link. Instead of just simply identifying the trust as trust or distrust, the trust is represented as a ternary value (i.e., belief, distrust, and uncertainty). Based on this, Liu *et al.* studied the subjective logic [40], [41] and proposed a three-valued subjective logical model [42] to model the trust in OSNs. With this model, they designed the AssessTrust algorithm to accurately calculate the trust between any two users. However, both schemes are focused on the trust measurements between vehicles in the social networks, so they are not appropriate for our RSU-based vehicle platoon recommendation systems. Besides, in [2], [8], [43], [44], the authors gave deep considerations about security and privacy issues in VANETs and wireless sensor networks, which inspires us to find out more potential concerns in vehicle platoons.

8 Conclusion and Discussion

In this article, we proposed a trust-based and privacy-preserving platoon recommendation scheme for user vehicles before they join a vehicle platoon. Considering the uncertainty of vehicles' behaviors, we design a filtering truth discovery based mechanism to calculate the head vehicles' reputation scores and user vehicles' trust values. Besides, authentication protocols are designed to ensure that only the valid user vehicles can pass the authentication. Security analysis and simulation results establish the security and effectiveness of the proposed scheme. In the future, we will try to design a vehicle platoon recommendation scheme where there are no RSUs deployed.

Acknowledgments

This research was supported in part by the National Natural Science Foundation of China (Grant Nos. 61972037, 61402037, 61272512, 61702105, 61872041, U1836212, and U1804263), and in part by the Graduate Technological Innovation Project of Beijing Institute of Technology (No.2019CX10014).

References

[1] H. Hu, R. Lu, and Z. Zhang, "TPSQ: Trust-based platoon service query via vehicular communications," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 262–277, 2017.

[2] 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.

[3] C. Xu, R. Lu, H. Wang, L. Zhu, and C. Huang, "TJET: Ternary join-exit-tree based dynamic key management for vehicle platooning," *IEEE Access*, vol. 5, pp. 26973–26989, 2017.

[4] H. Peng *et al.*, "Performance analysis of IEEE 802.11 p DCF for multiplatooning communications with autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2485–2498, Mar. 2016.

[5] D. Jia, K. Lu, and J. Wang, "A disturbance-adaptive design for vanet-enabled vehicle platoon," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 527–539, Feb. 2014.

[6] A. A. Alam, A. Gattami, and K. H. Johansson, "An experimental study on the fuel reduction potential of heavy duty vehicle platooning," in *Proc. 13th Int. Conf. Intell. Transp. Syst.*, 2010, pp. 306–311.

[7] J. Xu, K. Xue, Q. Yang, and P. Hong, "PSAP: Pseudonym-based secure authentication protocol for NFC applications," *IEEE Trans. Consum. Electron.*, vol. 64, no. 1, pp. 83–91, Feb. 2018.

[8] W. Hu, K. Xue, P. Hong, and C. Wu, "ATCS: A novel anonymous and traceable communication scheme for vehicular ad hoc networks," *Int. J. Netw. Security*, vol. 13, no. 2, pp. 71–78, 2011.

[9] Q. Yang, K. Xue, J. Xu, J. Wang, F. Li, and N. Yu, "Anfra: Anonymous and fast roaming authentication for space information network," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 486–497, Feb. 2019.

[10] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[11] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "LPTD: Achieving lightweight and privacy-preserving truth discovery in ciot," *Future Gener. Comp. Syst.*, vol. 90, pp. 175–184, 2019.

[12] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong, and N. Yu, "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 7–13, May/Jun. 2018.

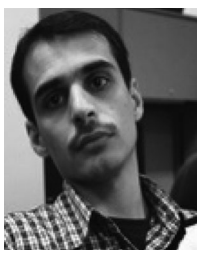
[13] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Int. Conf. Adv. Cryptology*, 2001, pp. 213–229.

[14] M. Abdalla, M. Bellare, and P. Rogaway, "The oracle diffie-hellman assumptions and an analysis of DHIES," in *Proc. RSA Conf. Topics Cryptology*, 2001, pp. 143–158.
[15] Y. Sang, H. Shen, and H. Tian, "Privacy-preserving tuple matching in distributed databases," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 12, pp. 1767–1782, Dec. 2009.
[16] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 1999, pp. 223–238.
[17] Q. Li, Y. Li, J. Gao, B. Zhao, W. Fan, and J. Han, "Resolving conflicts in heterogeneous data by truth discovery and source reliability estimation," in *Proc. Int. Conf. Manage. Data*, 2014, pp. 1187–1198.
[18] Y. Li *et al.*, "Conflicts to harmony: A framework for resolving conflicts in heterogeneous data by truth discovery," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 8, pp. 1986–1999, Aug. 2016.
[19] C. Miao *et al.*, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems," in *Proc. 13th ACM Conf. Embedded Networked Sensor Syst.*, 2015, pp. 183–196.
[20] C. Miao, L. Su, W. Jiang, Y. Li, and M. Tian, "A lightweight privacy-preserving truth discovery framework for mobile crowd sensing systems," in *Proc. IEEE Conf. Comput. Commun.*, 2017, pp. 1–9.
[21] F. Xia, L. Liu, J. Li, A. M. Ahmed, L. T. Yang, and J. Ma, "BEEINFO: Interest-based forwarding using artificial bee colony for socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 64, no. 3, pp. 1188–1200, Mar. 2015.
[22] L. Zhu *et al.*, "PRIF: A privacy-preserving interest-based forwarding scheme for social internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2457–2466, Aug. 2018.
[23] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
[24] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. ACM Conf. Comput. Commun. Security*, 1993, pp. 62–73.
[25] Y. Wu, F. Li, L. Ma, Y. Xie, T. Li, and Y. Wang, "A context-aware multi-armed bandit incentive mechanism for mobile crowd sensing systems," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7648–7658, Oct. 2019.
[26] C. Wu, T. Yoshinaga, Y. Ji, and Y. Zhang, "Computational intelligence inspired data delivery for vehicle-to-roadside communications," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12038–12048, Dec. 2018.
[27] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Social big-data-based content dissemination in internet of vehicles," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 768–777, Feb. 2018.
[28] Y. Li *et al.*, "Mp-coopetition: Competitive and cooperative mechanism for multiple platforms in mobile crowd sensing," *IEEE Trans. Serv. Comput.*, to be published, doi: 10.1109/TSC.2019.2916315.
[29] L. Xu, L. Y. Wang, G. G. Yin, and H. Zhang, "Communication information structures and contents for enhanced safety of highway vehicle platoons," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4206–4220, Nov. 2014.
[30] C. Bergenhem, Q. Huang, A. Benmimoun, and T. Robinson, "Challenges of platooning on public motorways," in *Proc. 17th ITS World Congr.*, 2010, pp. 1–12.
[31] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, Jan.-Mar. 2016.
[32] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2742–2750, Oct. 2017.
[33] S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo, and X. Liu, "Lightweight and expressive fine-grained access control for healthcare Internet-of-Things," *IEEE Trans. Cloud Comput.*, to be published, doi: 10.1109/TCC.2019.2936481.
[34] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. Int. Conf. Mobile Ubiquitous Syst.: Comput. Netw. Serv.*, 2006, pp. 1–8.
[35] M. Raya, P. Papadimitratos, V. D. Gligor, and J. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. 27th Conf. Comput. Commun.*, 2008, pp. 1238–1246.
[36] C. Chen, J. Zhang, R. Cohen, and P. H. Ho, "A trust modeling framework for message propagation and evaluation in vanets," in *Proc. Int. Conf. Inf. Technol. Convergence Serv.*, 2010, pp. 1–8.
[37] L. Zhu, C. Zhang, C. Xu, and K. Sharif, "Rtsense: Providing reliable trust-based crowdsensing services in CVCC," *IEEE Netw.*, vol. 32, no. 3, pp. 20–26, May/Jun. 2018.
[38] M. A. Javed, S. Zeadally, and Z. Hamid, "Trust-based security adaptation mechanism for vehicular sensor networks," *Comput. Netw.*, vol. 137, pp. 27–36, 2018.
[39] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Commun. Magazine*, vol. 53, no. 8, pp. 42–47, Aug. 2015.
[40] A. Jøsang and T. Bhuiyan, "Optimal trust network analysis with subjective logic," in *Proc. 2nd Int. Conf. Emerging Security Inf. Syst. Technol.*, 2008, pp. 179–184.
[41] A. Jsang, *Subjective Logic: A Formalism for Reasoning Under Uncertainty*. Berlin, Germany: Springer, 2018.
[42] G. Liu, Q. Yang, H. Wang, and A. X. Liu, "Three-valued subjective logic: A model for trust assessment in online social networks," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2019.2916366.
[43] X. Du, Y. Xiao, M. Guizani, and H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 24–34, 2007.
[44] X. Du, Y. Xiao, S. Ci, M. Guizani, and H. Chen, "A routing-driven key management scheme for heterogeneous sensor networks," in *Proc. IEEE Int. Conf. Commun.*, 2007, pp. 3407–3412.

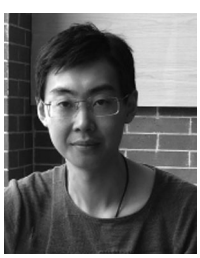
Chuan Zhang received the bachelor's degree in network engineering from the Dalian University of Technology, Dalian, China, in 2015. He is currently working toward the PhD degree in the School of Computer Science and Technology, Beijing Institute of Technology. His current research interests include secure data services in cloud computing, security & privacy in VANETs, and big data security.

Liehuang Zhu received the PhD degree in computer science from the Beijing Institute of Technology, Beijing, China, in 2004. He is currently a professor with the School of Computer Science & Technology, Beijing Institute of Technology. His research interests include security protocol analysis and design, group key exchange protocols, wireless sensor networks, and cloud computing. He is a member of the IEEE.

Chang Xu received the PhD degree in computer science from Beihang University, Beijing, China, in 2013. She is currently an associate professor with the School of Computer Science and Technology, Beijing Institute of Technology. Her research interests include security & privacy in VANET, and big data security.



Kashif Sharif (M'08) received the MS degree in information technology, in 2004, and the PhD degree in computing and informatics from the University of North Carolina, Charlotte, in 2012. He is currently an associate professor with the Beijing Institute of Technology, China. His research interests include wireless & sensor networks, network simulation systems, software defined & data center networking, ICN, and Internet of Things. He is a member of the IEEE and ACM.



Kai Ding received the MS degree in computer science and technology from the Beijing Institute of Technology, Beijing, China, in 2013. He is currently working toward the doctoral degree in the School of Computer Science and Technology, Beijing Institute of Technology. His current research interests include data security, network security, and blockchain.

Ximeng Liu (S'13–M'16) received the BSc degree in electronic engineering from Xidian University, Xi'an, China, in 2010, and the PhD degree in cryptography from Xidian University, China, in 2015. Currently, he is a research fellow with the School of Information System, Singapore Management University, Singapore, and qishan scholar in the College of Mathematics and Computer Science, Fuzhou University. He has published more than 80 research articles include *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Computers*, *IEEE Transactions on Services Computing*, and *IEEE Transactions on Cloud Computing*. His research interests include cloud security, applied cryptography and big data security. He is a member of the IEEE.

Xiaojiang Du (S'99–M'03–SM'09–F'20) received the BS and MS degrees in electrical engineering (Automation Department) from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the MS and PhD degrees in electrical engineering from the University of Maryland, College Park, in 2002 and 2003, respectively. He is a tenured full professor and the director of the Security and Networking (SAN) Lab in the Department of Computer and Information Sciences, Temple University, Philadelphia. His research interests are security, wireless networks, and systems. He has authored more than 400 journal and conference papers in these areas, as well as a book published by Springer. He been awarded more than six million US Dollars research grants from the US National Science Foundation (NSF), Army Research Office, Air Force Research Lab, NASA, the State of Pennsylvania, and Amazon. He won the Best Paper Award at IEEE GLOBECOM 2014 and the Best Poster Runner-up Award at the ACM MobiHoc 2014. He serves on the editorial boards of two international journals. He served as the lead chair of the Communication and Information Security Symposium of the IEEE International Communication Conference (ICC) 2015, and a co-chair of Mobile and Wireless Networks Track of IEEE Wireless Communications and Networking Conference (WCNC) 2015. He is (was) a Technical Program Committee (TPC) member of several premier ACM/IEEE conferences, such as INFOCOM (2007 - 2020), IM, NOMS, ICC, GLOBECOM, WCNC, BroadNet, and IPCCC. He is a fellow of the IEEE, and a life member of ACM.

Mohsen Guizani (S'85–S'89–SM'99–F'09) received the BS (Hons.) and the MS degrees in electrical engineering, and the MS and PhD degrees in computer engineering from Syracuse University, Syracuse, NY, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor with the Computer Science and Engineering Department, Qatar University, Qatar. Previously, he has served in different academic and administrative positions at the University of Idaho, Western Michigan University, University of West Florida, University of Missouri-Kansas City, University of Colorado-Boulder, and Syracuse University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He is the author of nine books and more than 500 publications in refereed journals and conferences. He has guest edited a number of special issues in the IEEE journals and magazines. He is a senior member of the ACM. He has also served as a member, the chair, and the general chair for a number of international conferences. Throughout his career, he has received three teaching awards and four research awards. He has also received the 2017 IEEE Communications Society WTC Recognition Award as well as the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and Ad-Hoc Sensor networks. He was the chair of the IEEE Communications Society Wireless Technical Committee and the chair of the TAOS Technical Committee. He is currently the editor-in-chief of the *IEEE Network Magazine*, and serves on the editorial boards of several international technical journals. He is the founder and editor-in-chief of the *Wireless Communications and Mobile Computing Journal* (Wiley). He has served as the IEEE Computer Society distinguished speaker and is currently the IEEE ComSoc distinguished lecturer. He is a fellow of the IEEE.