Scientific Research Publishing

Journal of Information Security, 2022, 13, 1-22
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Trusted and Privacy-Preserving Carpooling Matching Scheme in Vehicular Networks

Hongliang Sun, Linfeng Wei*, Libo Wang, Juli Yin, Wenxuan Ma

College of Cyber Security, Jinan University, Guangzhou, China
Email: *lfwei_013@163.com

How to cite this paper: Sun, H.L., Wei, L.F., Wang, L.B., Yin, J.L. and Ma, W.X. (2022) A Trusted and Privacy-Preserving Carpooling Matching Scheme in Vehicular Networks. *Journal of Information Security*, **13**, 1-22.
https://doi.org/10.4236/jis.2022.131001

Received: December 15, 2021
Accepted: January 24, 2022
Published: January 27, 2022

Abstract

With the rapid development of intelligent transportation, carpooling with the help of Vehicular Networks plays an important role in improving transportation efficiency and solving environmental problems. However, attackers usually launch attacks and cause privacy leakage of carpooling users. In addition, the trust issue between unfamiliar vehicles and passengers reduces the efficiency of carpooling. To address these issues, this paper introduced a trusted and privacy-preserving carpooling matching scheme in Vehicular Networks (TPCM). TPCM scheme introduced travel preferences during carpooling matching, according to the passengers' individual travel preferences needs, which adopted the privacy set intersection technology based on the Bloom filter to match the passengers with the vehicles to achieve the purpose of protecting privacy and meeting the individual needs of passengers simultaneously. TPCM scheme adopted a multi-faceted trust management model, which calculated the trust value of different travel preferences of vehicle based on passengers' carpooling feedback to evaluate the vehicle's trustworthiness from multi-faceted when carpooling matching. Moreover, a series of experiments were conducted to verify the effectiveness and robustness of the proposed scheme. The results show that the proposed scheme has high accuracy, lower computational and communication costs when compared with the existing carpooling schemes.

Keywords

Vehicular Networks, Carpooling Matching, Travel Preference, Bloom Filter, Privacy Set Intersection, Trust Management

1. Introduction

Vehicular Networks [1] is an important part of the intelligent transportation system. In the vehicular networks, vehicles can use wireless communication

technology to communicate with nearby vehicles or infrastructure in a Vehicle-To-Vehicle (V2V) or Vehicle-To-Infrastructure (V2I) manner. With the development of vehicular networks, dynamic carpooling with the help of vehicular networks has become an important travel manner [2]. The dynamic carpooling service matches multiple passengers which have similar itineraries with the target vehicle based on the travel information provided by the passengers and the vehicle. Carpooling can improve the traffic environment [3], and reduce the number of vehicles on the road by increasing the utilization rate of vehicle seats to alleviate traffic congestion and improving road mobility. In addition, carpooling reduces fuel consumption and carbon emissions, thereby improving environmental pollution [4].

Privacy protection is an important concern in carpooling [5] since attackers usually launch attacks to eavesdrop on the private information of carpooling users, which will cause privacy leakage and reduce users' willingness to participate in carpooling. Moreover, the private information of carpooling users usually includes sensitive information such as location and address [6]. Attackers can guess the user's home address and other information by observing multiple carpooling information of users, which raises a major threat to the safety of carpooling users [7]. In recent years, many privacy-preserving schemes have been proposed to protect the anonymity and traceability of carpooling users [8]. These schemes may use encryption to protect the privacy of carpooling data [9] [10] or use anonymous identities to protect the privacy of carpooling users [11]. But anonymity and data encryption may cause difficulty in carpooling matching [12]. Some carpooling matching schemes have been proposed to solve the problem of difficulty in carpooling matching [13]. However, these schemes don't consider the individual needs of passengers. For example, there may be non-smokers who do not want to travel with smoking drivers, and female passengers don't want to travel with the smoking driver at night. If the individual needs of the passengers are ignored, it may cause a mismatch between the vehicle and the passengers. Therefore, the existing solutions can't achieve a balance between precise carpooling matching and privacy protection [14].

Trust management is another problem in carpooling since it enables users to judge the trustworthiness of the information before accepting it [15]. In recent years, a large number of trust management schemes have been proposed for Vehicular Networks [16]. Some schemes assign reputation certificates to vehicles, and the vehicles verify the reputation certificate to determine whether the information comes from a legitimate vehicle to ensure the legitimacy of the received information [17] [18]. There are also some schemes using reputation score trust management methods. The vehicle judges whether to trust a vehicle by comparing the reputation score of the vehicle sending message with the threshold set by itself, and then accepts the corresponding message [19]. However, a single reputation score makes it impossible for passengers to evaluate the trustworthiness of the vehicle from multi-faceted.

To solve the aforementioned problems, this paper proposes a trusted and pri-

vacy-preserving carpooling matching (TPCM) scheme in vehicular networks. The main contributions are as follows:

1) TPCM scheme adopts the privacy set intersection based on Bloom filter, and judges whether the vehicle fulfills the individual needs of the passengers according to the travel preferences selected by the passengers and the preference attribute set of the vehicle. The privacy of carpooling users will not be leaked in this process. It can also fulfill the individual needs of passengers. TPCM scheme overcomes the problem of mismatch between vehicles and passengers, which achieves a balance between precise carpooling matching and privacy protection.

2) This paper proposes a multi-faceted trust management model based on travel preferences to solve the trust lack between passengers and vehicles during carpooling matching. This model uses a reputation set based on travel preferences instead of a single reputation score. Each trust value in the reputation set represents the trustworthiness of a certain type of travel preference of the vehicle, which realizes the multi-faceted accurate trust evaluation of the vehicle and effectively depicts trust between passengers and vehicles.

The remainder of this paper is structured as follows. Section 2 introduces some related work on carpooling and its limitations. Section 3 revisits the preliminaries. Section 4 introduces the system model, threat model and travel preferences classification. Section 5 details the proposed TPCM scheme. Section 6 and Section 7 detail the security analysis and performance evaluation, followed by the conclusion in Section 8.

2. Related Work

In terms of privacy protection for carpooling matching, Yu *et al.* [7] proposed a privacy-preserving carpooling matching scheme which used encryption aggregation to calculate distance and protected the location privacy of vehicles and passengers by using homomorphic encryption. Hallgren *et al.* [20] proposed the scheme through the similarity between the starting point and the end point and trajectory matching to achieve carpooling matching, which adopted additional homomorphic encryption and threshold private set intersection protocol to protect user's privacy. Li *et al.* [13] presented the way to achieve one-to-many proximity matching by using privacy proximity test during carpooling matching, which protected the privacy of vehicles and passengers simultaneously. However, these schemes don't consider passenger's travel preferences in carpooling matching [21], which cannot achieve a balance between precise matching of passengers and vehicles and privacy-preserving and may cause a mismatch between passengers and vehicles. Passengers may give negative feedback to the vehicle after the carpooling journey ends. And it affects the user experience and reduces the effectiveness of carpooling.

In terms of trust management, Caballero-Gil *et al.* [22] proposed the reputation update algorithm which considered the relationship chain between users, and calculated the trust rating through friendliness and user ratings to generate a

trust rating between 0 and 1. Baza *et al.* [23] proposed a decentralized reputation system that generated two values based on whether the vehicle arrived at the agreed pick-up location and whether the carpooling journey was completed, and then used the two values to calculate the vehicle's reputation score. Sánchez *et al.* [24] presented a reputation management protocol which first aggregated the ratings of passengers, and then used negative truncation to normalize the reputation value of the vehicle. However, the aforementioned schemes only use a single reputation score to evaluate the trustworthiness of the vehicles, which not only causes reputation link attacks [25] but also cannot evaluate the trustworthiness of the vehicle from multi-faceted, such as the driver's driving skills and the degree of cleanliness.

3. Preliminaries

3.1. Bilinear Pairing

Let G_1 and G_2 be an addition cyclic group and a multiplication with the same prime order q. Let g be the generator of group G_1. Let $e: G_1 \times G_1 \to G_2$ denote a bilinear map which has following properties [26].

Bilinear: For all $a,b \in Z_q^*$, $e\left(g^a, g^b\right) = e\left(g, g\right)^{ab}$.

Non-degeneracy: $e\left(g, g\right) \neq 1$.

Computability: For all $g_1, g_2 \in G_1$, there is an effective algorithm for calculation $e\left(g_1, g_2\right)$.

3.2. ELGAMAL Encryption

The ElGamal encryption algorithm is a multiplicative homomorphic encryption algorithm. The process of the ElGamal encryption algorithm is as follows [27].

Key generation: Randomly select a large prime number q and a random number $s \in Z_q^*$. And calculate $o = g^s \bmod q$. Then the public key is $\left(o, g, q\right)$ and private key is s.

Encryption: Select a random number r that is relatively prime with $q-1$. And calculate the ciphertext of message M as

$$C = E\left(M\right) = \left(c_1, c_2\right) = \left(g^r \bmod q, s^r M \bmod \left(q-1\right)\right) \tag{1}$$

Decryption: Decrypt the ciphertext C as

$$M = D\left(C\right) = c_2 / c_1^s \left(\bmod q\right) = d\left(c_1^s\right)^{-1} \bmod q \tag{2}$$

3.3. BF-PSI

Bloom filter (BF) [28] is a probabilistic data structure that checks set membership and effectively saves space. The false negative rate of the Bloom filter is 0, but the Bloom filter has a certain false positive rate due to the collision rate of the hash function, the false positive rate p is calculated as [28]

$$p = \left(1 - \left(1 - \frac{1}{m}\right)^{k \cdot n}\right)^k \approx \left(1 - \mathrm{e}^{-\frac{k \cdot n}{m}}\right)^k \tag{3}$$

where m, k and n are the size of the bloom filter vector, the number of hash functions and the number of elements stored in the Bloom filter, respectively.

Privacy Set Intersection (PSI) [29] can judge whether there is an intersection between the input sets of the two parties without leaking privacy. The execution process of BF-PSI is: two parties A and B whose secret sets are $S_A = (a_1, a_2, \cdots, a_n)$ and $S_B = (b_1, b_2, \cdots, b_n)$, respectively. A and B choose random value r_a and r_b, and then use k independent hash functions with the number bits s to represent the set as BF_A and BF_B. Next, A and B exchange random values and BF. Finally, it determines the intersection of two parties A and B. For example, if A executes $PSI(S_A, BF_B, r_b)$, who uses $mem\_test()$ to judge whether $a_i (i = 1, 2, \cdots, n)$ appears in BF_B. If it returns a positive result, then $a_i \in BF_B$, and vice versa. In this way, A and B can learn $I_{A,B} = S_A \cap S_B$ without leaking the privacy of the two parties.

4. Problem Statement

4.1. System Model

The system model of the TPCM scheme proposed in this paper is shown in **Figure 1**, which includes four entities: Trusted Authority (TA), RSU, vehicle and passenger.

When the TPCM scheme is deployed in the carpooling system, TA assigns public key, private key and reputation certificates to registered entities. Only TA can reveal the true identities of malicious users and punish them when users have malicious behaviors. TA also is responsible for collecting trust feedback and updating the user's trust information. RSU is responsible for verifying the certificates and information signatures of vehicles and passengers and matching vehicles and passengers in carpooling. Passengers are responsible for sending

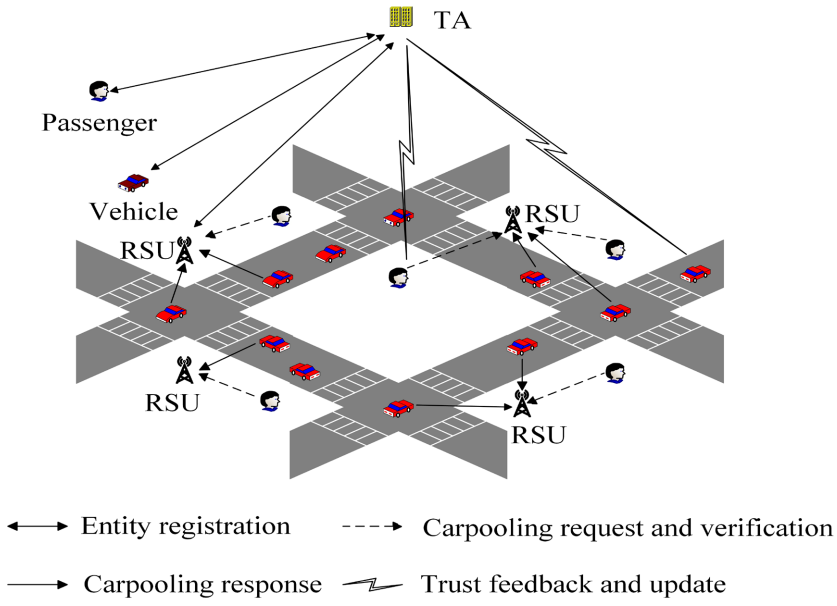

Figure 1. System model of carpooling matching scheme.

encrypted carpooling requests within the communication range of a certain RSU. The vehicles send an encrypted carpooling response after receiving the encrypted carpooling requests.

4.2. Threat Model

We assume that the TA is completely trusted, whereas RSU is honest and curious in the threat model of this paper. That is, the RSU honestly performs the steps in carpooling, but it is curious about the carpooling information broadcasted in the carpooling system and the user's private information. Specifically, RSU may launch passive attacks such as message eavesdropping attacks or privacy digging. Although it does not modify the information, it tries to obtain more private information from carpooling users. Vehicles and passengers may be malicious. They may launch passive attacks to eavesdrop on the private information in carpooling or launch active attacks to disrupt the carpooling network. For example, vehicles or passengers may launch message cheating attacks, and use a false identity to deceive other carpooling entities. And they may launch message modification attacks to modify the carpooling information.

4.3. Travel Preferences Classification

The classification and attributes of travel preferences for the TPCM scheme in this paper are shown in Table 1. Travel preferences are divided into 7 categories, where $I_1 \sim I_7$ represents the trust value corresponding to travel preferences. The trust value of travel preference I_m is $TV_{V_i(I_m)}$. The vehicle reputation set is composed of trust value, which is used to evaluate the trustworthiness of the vehicle from multi-faceted. Each travel preference has two attributes, $x_{1,1} \sim x_{7,2}$ represents the 14 attributes corresponding to the 7 travel preferences. The attributes of $I_1 \sim I_4$ is based on the range of trust values. That is, the attributes of preference $I_1 \sim I_4$ are converted from continuous variables to characters, where the range of trust values [ω_s, 0.5] is Good and the range (0.5, 1] is Very Good, ω_s is the score threshold. The attributes of $I_1 \sim I_4$ is constantly updated with the changes of the trust value. The attributes of $I_5 \sim I_7$ is unchanged based on the real information when vehicle registration, and the trust

Table 1. Travel preferences classification and attributes.

Travel preferences	Attribute
Driver's driving skill (I_1)	Very Good ($x_{1,1}$), Good ($x_{1,2}$)
Driver's sense of direction (I_2)	Very Good ($x_{2,1}$), Good ($x_{2,2}$)
Driver's attitude (I_3)	Very Good ($x_{3,1}$), Good ($x_{3,2}$)
Cleanliness of the vehicle (I_4)	Very Good ($x_{4,1}$), Good ($x_{4,2}$)
Driver smoking (I_5)	Yes ($x_{5,1}$), No ($x_{5,2}$)
Vehicle music (I_6)	Yes ($x_{6,1}$), No ($x_{6,2}$)
Driver's gender (I_7)	Male ($x_{7,1}$), Female ($x_{7,2}$)

value reflects the trustworthiness of the corresponding travel preference. One of the attributes of each travel preference constitutes the preference attributes set PA_{V_i} of the vehicle V_i, which is used to meet the individual needs of passengers.

5. Proposed Scheme

5.1. System Initialization

Given the security parameters 1^τ, TA generates the bilinear parameters (G_1, G_2, e), where G_1, G_2 is the cyclic group with prime order q, g_1, g_2 is the generator of G_1 and G_2, respectively. And the bilinear map $e: G_1 \times G_1 \to G_2$. Then TA calculates $e(g_1, g_2) = F$. Next, TA generates the master key $MSK_T = t$ and calculates $PK_T = g_1^t$ to be its public key, where $t \in Z_q^*$. TA selects two hash function: $H_1: \{0,1\} \to Z_q^*$, $H_2: \{0,1\} \times \{0,1\} \to Z_q^*$, and selects the filter function f, length l, and hash function set H_s for the Bloom filter. TA sets the distance threshold φ_s and φ_d, time threshold ψ_t and score threshold ω_s. Finally, TA publishes the system parameters $\Theta = (\tau, G_1, G_2, e, q, F, PK_T, f, l, H_s, \varphi_s, \varphi_d, \psi_t, \omega_s)$.

In order to prevent the vehicle from forging its travel preference attributes, TA will create preference attributes secret value as shown in Table 2, where Sv_i^λ is the secret value corresponding to the preference attribute x_i, λ is the time when TA generates all preference attributes secret value. The calculation method of Sv_i^λ is $Sv_i^\lambda = h_\lambda(x_i \| r_\lambda)$, where h_λ is the hash function for calculating the secret value and r_λ is a random number. Due to the collision rate of the hash function, if the secret value of two different preference attributes is the same, TA recalculates the secret value for all preference attributes until the secret value of all preference attributes is different. In addition, TA regularly updates the preference attributes secret value.

5.2. Entity Registration

When a passenger P_i with the identity RID_{P_i} registers with the carpooling system, TA generates the privacy key $SK_{P_i} = p$ and calculates the public key $PK_{P_i} = g_1^p$ for passenger P_i, where p is a random number and $p \in Z_q^*$. TA generates the reputation certificate $RCert_{P_i} = g_2^{1/(H_{P_i} + MSK_T + SK_{P_i})}$, where $H_{P_i} = H_1(RID_{P_i} \| PK_{P_i} \| PV_{P_i})$, PV_{P_i} is the validity period of the reputation certificate. The anonymous identity of passenger P_i is $PID_{P_i} = RID_{P_i} \oplus H_1(p \| PK_T \| PK_{R_i})$.

When vehicle V_i with the identity RID_{V_i} registers with the carpooling system, TA generates the privacy key $SK_{V_i} = v$ and calculates the public key $PK_{V_i} = g_1^v$

Table 2. Preference attributes secret value.

Preference attribute	$x_{1,1}$	$x_{1,2}$	…	$x_{7,1}$	$x_{7,2}$
Secret value	$Sv_{1,1}^\lambda$	$Sv_{1,2}^\lambda$	…	$Sv_{7,1}^\lambda$	$Sv_{7,2}^\lambda$

for vehicle V_i, where v is a random number and $v \in Z_q^*$. TA generates the reputation certificate $RCert_{V_i} = g_2^{1/(H_{V_i}+MSK_T+SK_{V_i})}$, where $H_{V_i} = H_1\left(RID_{V_i} \| PK_{V_i} \| PV_{V_i}\right)$. The anonymous identity of vehicle V_i is $PID_{V_i} = RID_{V_i} \oplus H_1\left(v \| PK_T \| PK_{R_i}\right)$. The reputation set of the vehicle V_i is $RS_{V_i} = \left(TV_{V_i(I_1)} \sim TV_{V_i(I_7)}\right)$, where $TV_{V_i(I_1)} \sim TV_{V_i(I_7)}$ represents the trust value of the 7 travel preference types of V_i, and the reputation set is used to evaluate the trustworthiness of V_i from multi-faceted. Since the travel preference $I_1 \sim I_4$'s trust value is initialized to 0.5 and the corresponding attributes are $x_{1,2}, x_{2,2}, x_{3,2}, x_{4,2}$, so the initial vehicle preference attribute set is $PA_{V_i} = \left(x_{1,2}, x_{2,2}, x_{3,2}, x_{4,2} x_a, x_b, x_c\right)$, where x_a, x_b and x_c are the real information registered by the vehicle V_i. PA_{V_i} is used to meet the individual travel preferences needs of passengers. TA retrieves the secret value corresponding to the preference attribute from **Table 2**, and then sends the preference attribute secret value set PAS_{V_i} to the vehicle V_i, where $PAS_{V_i} = \left(Sv_{1,2}^{\beta}, Sv_{2,2}^{\beta}, Sv_{3,2}^{\beta}, Sv_{4,2}^{\beta}, Sv_a^{\beta}, Sv_b^{\beta}, Sv_c^{\beta}\right)$.

When RSU registers with the carpooling system, TA generates the privacy key $SK_{R_i} = r$ and calculates the public key $PK_{R_i} = g_1^r$ for R_i, where r is a random number and $r \in Z_q^*$.

5.3. Carpooling Requesting

When a passenger P_i wants to carpool, who first chooses individual travel preferences, and then selects preference attributes from the attributes corresponding to the selected travel preferences. It is noted that passengers can only choose one of the two attributes corresponding to each travel preference. We assume that the preference attributes selected by the passenger are $x_m \sim x_n$, $I_{m'} \sim I_{n'}$ are the corresponding travel preferences. Next, the passenger P_i requests the secret value corresponding to the selected preference attributes from TA, and TA returns the corresponding secret value $Sv_m^{\alpha} \sim Sv_n^{\alpha}$ to the passenger P_i. We assume $PS_{P_i} = \left(Sv_m^{\alpha} \sim Sv_n^{\alpha}\right)$, then the passenger P_i selects a random number r_1 and injects PS_{P_i} into Bloom filter by using $Bf_{P_i} = Insert\left(H_s\left(PS_{P_i} \| r_1\right), Bf_{P_i}\right)$. The passenger sets a preference score threshold $\chi_{m\sim n}$. Finally, passenger P_i selects the starting position and destination to form a carpooling request

$$QM_{P_i} = \left(PID_{P_i}, RCert_{P_i}, Bf_{P_i}, \chi_{m\sim n}, loc_{P_i}, des_{P_i}, \alpha, T_{QM_{P_i}}\right) \tag{4}$$

where $T_{QM_{P_i}}$ denotes the timestamp when the carpooling request is generated. And then passenger calculates the signature $\delta_{QM_{P_i}} = g_2^{1/\left(H_2\left(QM_{P_i} \| PK_{P_i} \| PK_{R_i}\right)+SK_{P_i}\right)}$. When the passenger is within the communication range of a certain RSU, who uses ElGamal encryption and parameter $\left(g_1, PK_{R_i}\right)$ to encrypt QM_{P_i} to form a ciphertext

$$C_{P_i} = E\left(QM_{P_i}\right) = \left(c_1, c_2\right) = \left(g_1^{w_1} \bmod q, PK_{R_i}^{w_1} QM_{P_i} \bmod (q-1)\right) \tag{5}$$

Eventually passenger P_i sends $\left\{C_{P_i}, RCert_{P_i}, \delta_{QM_{P_i}}\right\}$ to R_i. After the R_i receives the information $\left\{C_{P_i}, RCert_{P_i}, \delta_{QM_{P_i}}\right\}$, which uses the decryption algo-

rithm and the private key to decrypt ciphertext C_{P_i} to obtain the passenger's carpooling request information, $QM_{P_i} = D\left(C_{P_i}\right) = c_2\left(c_1^{SK_{R_i}}\right)^{-1} \bmod q$. Then R_i obtains the current timestamp from the clock and verifies the freshness of the message by $\left|T_1 - T_{QM_{P_i}}\right| < \psi_t$. If it holds, then R_i verifies the validity of the passenger's reputation certificate and information signature by (6) and (7).

$$e\left(g_1^{H_{P_i}} \cdot PK_T \cdot PK_{P_i}, RCert_{P_i}\right) = F \tag{6}$$

$$e\left(g_1^{H_2\left(QM_{P_i} \| PK_{P_i} \| PK_{R_i}\right)} \cdot PK_{P_i}, \delta_{QM_{P_i}}\right) = F \tag{7}$$

when all verifications are passed, R_i will broadcast Msg_{R_i} to the nearby vehicles, where $T_{Msg_{R_i}}$ is the timestamp when Msg_{R_i} is generated.

$$Msg_{R_i} = \left(PID_{P_i}, Bf_{P_i}, loc_{P_i}, des_{P_i}, \alpha, T_{Msg_{R_i}}\right) \tag{8}$$

5.4. Carpooling Responding

When the vehicle V_i is within the communication range of R_i, who first obtains the current timestamp from the clock after receiving the information Msg_{R_i}, and then checks the freshness of the message by $\left|T_2 - T_{Msg_{R_i}}\right| < \psi_t$. If it holds, we assume the preference attribute secret value set of the vehicle V_i is $PAS_{V_i} = \left(Sv_p^{\beta} \sim Sv_q^{\beta}\right)$. In order to ensure the time consistency of the preference attribute secret value of the vehicle V_i and the passenger P_i, the vehicle first checks whether α is equal to β that in PAS_{V_i}. If it holds, the vehicle selects a random number r_2 and inserts PAS_{V_i} into the Bloom filter by using $Bf_{V_i} = Insert\left(H_s\left(PAS_{V_i} \| r_2\right), Bf_{V_i}\right)$; Otherwise, the vehicle requests to update secret value in PAS_{V_i} from TA, and then injects the updated PAS_{V_i} into the Bloom filter. Finally, vehicle sets the maximum number of carpooling to form a carpooling response

$$SM_{V_i} = \left(PID_{V_i}, RS_{V_i}, RCert_{V_i}, Bf_{V_i}, loc_{V_i}, des_{V_i}, CN_{\max}, T_{SM_{V_i}}\right) \tag{9}$$

where loc_{V_i}, des_{V_i} denotes the starting point and destination of vehicle, respectively, and $T_{SM_{V_i}}$ denotes the timestamps when the carpooling responding is generated. The vehicle calculates the signature $\delta_{SM_{V_i}} = g_2^{1/\left(H_2\left(SM_{V_i} \| PK_{V_i} \| PK_{R_i}\right) + SK_{V_i}\right)}$. Then vehicle V_i adopts ElGamal encryption and uses the parameter $\left(g_1, PK_{R_i}\right)$ to encrypt the carpooling response of the vehicle to form ciphertext

$$C_{V_i} = E\left(SM_{V_i}\right) = \left(c_3, c_4\right) = \left(g_1^{w_2} \bmod q, PK_{R_i}^{w_2} SM_{V_i} \bmod \left(q-1\right)\right) \tag{10}$$

Eventually vehicle V_i sends $\left\{C_{V_i}, RCert_{V_i}, \delta_{SM_{V_i}}\right\}$ to R_i.

5.5. Carpooling Matching

After receiving the information $\left\{C_{V_i}, RCert_{V_i}, \delta_{SM_{V_i}}\right\}$, R_i first uses the decryption algorithm and private key to decrypt the vehicle's carpooling response ciphertext C_{V_i} to obtain $SM_{V_i} = D\left(C_{V_i}\right) = c_4\left(c_3^{SK_{R_i}}\right)^{-1} \bmod q$. Then it checks the freshness of carpooling response information by $\left|T_3 - T_{SM_{V_i}}\right| < \psi_t$. If it holds, R_i

verifies the validity of V_i's reputation certificate and information signature by (11) and (12).

$$e\left(g_1^{H_{V_i}} \cdot PK_T \cdot PK_{V_i}, RCert_{V_i}\right) = F \tag{11}$$

$$e\left(g_1^{H_2\left(SM_{V_i} \| PK_{V_i} \| PK_{R_i}\right)} \cdot PK_{V_i}, \delta_{SM_{V_i}}\right) = F \tag{12}$$

After above verifications are passed, R_i verifies (13) to match the starting position and destination of the vehicle and passengers. Then it checks whether all the $TV_{V_i(I_1)} \sim TV_{V_i(I_7)}$ in RS_{V_i} is greater than $\chi_{m\sim n}$. In other words, it is to check whether the trust value corresponding to V_i's travel preference categories selected by the passenger meets the passenger's multi-faceted trust needs.

$$\left(\left|loc_{P_i} - loc_{V_i}\right| < \varphi_s\right) \wedge \left(\left|des_{P_i} - des_{V_i}\right| < \varphi_d\right) \tag{13}$$

Finally, R_i uses BF-PSI to determine whether there is an intersection In_{P_i,V_i} between V_i's preference attribute secret value set PAS_{V_i} and the set PS_{P_i} selected by P_i. If In_{P_i,V_i} and PS_{P_i} are the same, V_i fulfills all individual carpooling needs of passenger P_i. Then the vehicle and passengers are successfully matched and the message M_{P_i,V_i} is sent to the vehicle and passengers.

$$M_{P_i,V_i} = \left(PID_{P_i}, PID_{V_i}, S_{P_i,V_i}, T_{M_{P_i,V_i}}\right) \tag{14}$$

where S_{P_i,V_i} is the communication key between the vehicle and the passenger, and $T_{M_{P_i,V_i}}$ is the timestamp of the successful carpooling matching. In order to understand the process of carpooling matching in our TPCM scheme, Algorithm 1 describes the carpooling matching scheme based on BF-PSI in **Table 3**.

5.6. Trust Feedback and Reputation Updating

When the passenger P_i arrives at the destination, who will calculate the feedback score $Fs_{P_i\to V_i(I_{m'})} \sim Fs_{P_i\to V_i(I_{n'})}$ for the selected preference attribute ($x_m \sim x_n$) corresponds to the travel preferences ($I_{m'} \sim I_{n'}$) based on the actual experience in the carpooling journal. For $\forall I_i \in \left(I_{m'} \sim I_{n'}\right)$, the corresponding feedback score is $Fs_{P_i\to V_i(I_i)} \in \{0,1\}$, where 1 represents positive feedback and 0 represents negative feedback. Passenger P_i calculates feedback scores for all selected travel preferences by using above method and generates a travel preference feedback set $Fs_{P_i\to V_i} = \left(Fs_{P_i\to V_i(I_{m'})}, \cdots, Fs_{P_i\to V_i(I_{n'})}\right)$, which forms the passenger P_i's trust feedback tuple $Tf_{P_i\to V_i} = \left(PID_{P_i}, Fs_{P_i\to V_i}, PID_{V_i}, M_{P_i,V_i}\right)$ for the vehicle V_i.

Since there is more than one carpooling passenger, multiple trust feedback tuples about the vehicle V_i will be generated. These trust feedback tuples are aggregated by the RSU and sent to the TA in a safe manner. After the TA receives them, who first classifies and integrates this information into multiple preference feedback information sets about the vehicle based on the type of travel preference, for example

$$PFM_{V_i(I_{m'})} = \left(PID_{P_i}, Fs_{P_i\to V_i(I_{m'})}, \cdots, PID_{P_n}, Fs_{P_n\to V_i(I_{m'})}, PID_{V_i}\right) \tag{15}$$

Table 3. Carpooling matching scheme based on BF-PSI.

Algorithm 1: Carpooling matching scheme based on BF-PSI

Input: $QM_{P_i}, SM_{V_i}, \delta_{SM_{V_i}}$

Output: Result = "successful matching" or "failed matching"

$In_{P_i,V_i} = \varnothing$

if $\left|T_3 - T_{SM_{V_i}}\right| < \psi_t$ **then**

  R_i verifies the reputation certificate and signature of V_i

  if equation (11) and (12) hold **then**

    R_i matches the starting position and destination of the V_i and P_i

    if equation (13) holds **then**

      R_i verifies whether V_i meets P_i's multi-faceted trust needs

      if all the $TV_{V_i(I_1)} \sim TV_{V_i(I_7)} > \chi_{m-n}$ **then**

        V_i meets P_i's multi-faceted trust needs

      end if

    end if

  end if

end if

for $\forall p \in \{m, \cdots, n\}$ **then**

  if *mem_test* $\{Bf_{V_i}, r_2, x_p\}$ **then**

    $In_{P_i,V_i} = In_{P_i,V_i} \cup \{x_p\}$

  end if

end for

if In_{P_i,V_i} and PS_{P_i} are the same **then**

  Result = "successful matching"

else

  Result = "failed matching"

end if

TA updates the trust value of the travel preferences type selected by passengers in the reputation set RS_{V_i} of vehicle V_i based on $\left(PFM_{V_i(I_{m'})} \sim PFM_{V_i(I_{n'})}\right)$, the updating method is as follows:

$$TV_{V_i(I_i)}^{t+1} = \begin{cases} \dfrac{\sum_{PID_{P_i} \in PFM_{V_i(I_i)}} Fs_{P_i \to V_i(I_i)} \cdot Rs_{P_i}^t}{\sum_{PID_{P_i} \in PFM_{V_i(I_i)}} Rs_{P_i}^t}, & \text{if } \sum_{PID_{P_i} \in PFM_{V_i(I_i)}} Rs_{P_i}^t > \omega_s \\ \xi \cdot TV_{V_i(I_i)}^t, & \text{otherwise} \end{cases} \quad (16)$$

where Rs_{P_i} is the reputation score of passengers P_i, ξ is a decay factor. If a vehicle does not carpool for a long time, the trust value corresponding to its travel preference will decay over time.

Then TA updates the attributes of the first four items in the vehicle V_i's preference attribute set based on the updated trust value. Finally, TA sends the updated RS_{V_i} and PAS_{V_i} to the vehicle. In order to evaluate the overall trustworthiness of the vehicle, we use the weighted average method to calculate the

average reputation score of the vehicle, the calculation method is as follows:

$$Rs_{V_i}^{t+1} = \frac{w_s}{M}\sum\left(TV_{V_i(I_{m'})}^{t+1} + \cdots + TV_{V_i(I_{n'})}^{t+1}\right) + \frac{w_t}{N}\sum\left(TV_{V_i(I_{p'})}^{t} + \cdots + TV_{V_i(I_{q'})}^{t}\right) \quad (17)$$

where $I_{m'} \sim I_{n'}$ is the travel preferences of vehicle V_i corresponding to the preference attributes selected by passenger P_i, the number is M, corresponding to the updated trust value is $TV_{V_i(I_{m'})}^{t+1} \sim TV_{V_i(I_{n'})}^{t+1}$, and the total weight is w_s; $I_{p'} \sim I_{q'}$ is the travel preferences of vehicle V_i not selected by the passenger, the number is N, corresponding to the historical trust value is $TV_{V_i(I_{p'})}^{t} \sim TV_{V_i(I_{q'})}^{t}$, the total weight is w_t, where $w_t = 1 - w_s$.

6. Security Analysis

6.1. Conditional Privacy Preservation

For the TPCM scheme, the TA assigns a pseudonym PID_{V_i} to the vehicle when the vehicle is registered, and the vehicle uses the pseudonym identity to broadcast the carpooling information. Since the number v in PID_{V_i} is a random number, which is kept secretly by the TA. Therefore, the adversary cannot reveal the identity of the vehicle from the pseudonym PID_{V_i} to obtain private data. Only the TA can reveal the identity of the vehicle by using $RID_{V_i} = PID_{V_i} \oplus H_1\left(v \| PK_T \| PK_{R_i}\right)$ and punish the malicious vehicle. Therefore, the TPCM scheme not only protects the user's identity privacy, but also tracks the real identity of malicious users and realizes the conditional privacy protection of users' identities.

6.2. Carpooling Data Privacy Preservation

When the carpooling information is generated, this paper uses ElGamal encryption algorithm to encrypt it. That is, the vehicles or passengers use the public key of the RSU to encrypt the carpooling information, and the RSU decrypts the encrypted carpooling information by using its private key to verify the identity of the vehicles or passengers. Since a random number needs to be selected when the ElGamal encryption algorithm is used to encrypt a carpooling message and the private key of the RSU is used to decrypt the message. The private key of the RSU is a random number and is kept secretly by the RSU. The adversary cannot initiate an attack to get the plaintext information after the carpooling information is encrypted. Therefore, the TPCM scheme protects the privacy of carpooling data. In addition, the encrypted ciphertext of the same carpooling message is also different within the communication range of different RSUs by using the ElGamal encryption algorithm. Moreover, the carpooling matching method in this paper introduces travel preferences, which uses BF-PSI technology to match passengers and vehicles to meet the individual needs of passengers. The carpooling matching method by using the BF-PSI not only protects the preference privacy of vehicles and passengers, but also prevents mismatch between vehicles and passengers caused by ignoring the passenger's individual needs.

6.3. Resistance to Message Modification Attacks

The attackers may modify the carpooling message by launching a message modification attack to disrupt the carpooling network. However, for the TPCM scheme in this paper, the passenger P_i will calculate a signature $\delta_{QM_{P_i}}$ for the carpooling request QM_{P_i} when he issues it. After the RSU within the communication range of P_i receives QM_{P_i}, which uses Equation (7) to verify the validity of the passenger's carpooling request signature. If it holds, then the carpooling request QM_{P_i} has not been modified. Otherwise, the carpooling message will be discarded. Therefore, the TPCM scheme can resist the message modification attack.

6.4. Resistance to Message Cheating Attacks

Passengers or vehicles may initiate message cheating attacks and use false certificates to deceive each other. However, for the TPCM scheme in this paper, the reputation certificate of carpooling users has a validity period. When the reputation certificate expires, the TA will issue a new reputation certificate to the user. Although the internal attacker has a reputation certificate issued by the TA, the malicious user cannot repeatedly initiate a reputation certificate request to cover up his malicious behavior before the certificate expires. TA can reveal the identity of the internal attacker, who will reduce the trust value of a certain travel preference when the vehicle has malicious behavior. And TA will revoke the malicious vehicle when a certain trust value is lower than the score threshold. If an external attacker uses a fake reputation certificate to broadcast carpooling messages, who cannot pass the reputation certificate verification from RSU. Therefore, for the TPCM scheme in this paper, the reputation certificate with validity period can not only resist message cheating attacks and ensure the legitimacy of the carpooling user identity, but also avoid the communication delay of requesting the certificate every time for carpooling.

7. Performance Evaluation

7.1. Computation Cost

The computational cost of TPCM scheme mainly comes from ElGamal encryption and signature verification. We let T_m be the time to perform the maptopoint function operation, T_e be the time to perform the exponentiation operation, T_b be the time to perform bilinear pairing, and T_u be the time to perform multiplication. In the Intel i3-4170 3.7 GHz processor, 8 GB RAM and Windows 10 platform, the times of these operations are: $T_m = 3.7$ ms, $T_e = 3.9$ ms, $T_b = 4.5$ ms, $T_u = 0.6$ ms [30].

In order to compare the TPCM scheme with the FICA scheme [13] and SRSCB scheme [31], this paper considers the computation overhead of three stages of passenger carpooling request, information verification and vehicle carpooling response in **Table 4**. We let PCRG be the carpooling request generation stage,

Table 4. Computation cost of different carpooling schemes.

Scheme	PCRG	RMV	VCRG
FICA [13]	$2T_m + 9T_e + 2T_b + 6T_u$	$2T_m + 9T_e + 5T_b + 3T_u$	$2T_m + 9T_e + 2T_b + 6T_u$
SRSCB [31]	$4T_m + 10T_e + T_b + 2T_u$	$3T_e + 5T_b$	$2T_m + T_e + 2T_b$
TPCM	$T_m + 3T_e + T_u$	$2T_m + 3T_e + 2T_b + 3T_u$	$T_m + 3T_e + T_u$

RMV be the information verification stage, and VCRG be the carpooling response generation stage.

The computation cost comparison of different carpooling schemes is shown in **Table 4**. In the FICA scheme, the time consumption of passenger carpooling request generation, RSU information verification, and carpooling response is 55.1 ms, 66.8 ms, and 55.1 ms, respectively. In the SRSCB scheme (assuming the number of attributes is 1), the time consumption for the passenger generates an encrypted carpooling request, RSU information verification, and driver generates a carpooling response is 59.5 ms, 34.2 ms, and 20.3 ms, respectively. For the TPCM scheme, the time consumption of carpooling request generation, RSU information verification and carpooling response is 16 ms, 29.9 ms, and 16 ms, respectively.

Figure 2 and **Figure 3** show the computation cost of different carpooling schemes as the number of passengers and vehicles changes. We can see that the computation cost gradually increases as the number of passengers and vehicles increases, but the computation cost of our TPCM scheme increases more slowly compared with other schemes and is lower than the computation cost of other schemes.

7.2. Communication Overhead

We assume the pseudonym and key length are 16 bytes, the hash value length is 4 bytes, and the signature and homomorphic ciphertext length are 67 bytes and 512 bytes, respectively [30]. For our TPCM scheme, the length of passenger's carpooling information ciphertext is 595 bytes totally. The message length in the carpooling response and RSU verification phases is 595 bytes and 16 bytes, respectively. Comparing the communication overhead of our TPCM scheme with the FICA scheme [13] and PRIS scheme [32], **Figure 4** and **Figure 5** show the communication overhead of different carpooling schemes as the number of passengers and vehicles change. We can see that when the number of changes of passengers and vehicles from 100 to 1000, the communication overhead of our TPCM scheme is lower than other schemes regardless of whether the number of changes of passengers or vehicles. And it has a smaller growth rate compared with other schemes.

7.3. Probability of Successful Carpooling Matching

We propose a carpooling matching method that introduces travel preferences,

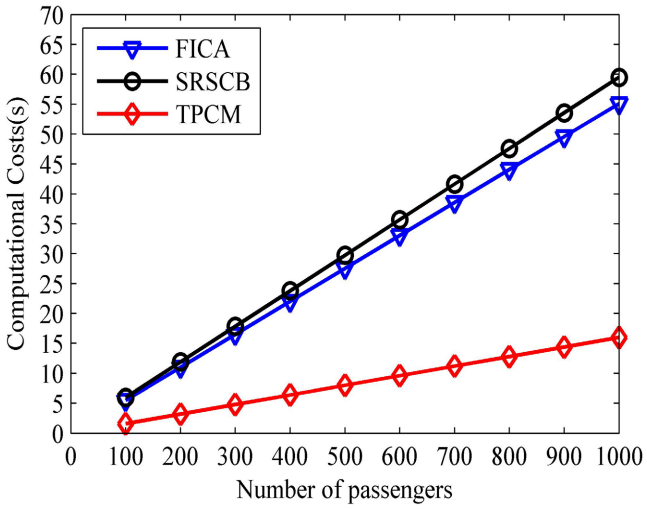

Figure 2. Time cost in passenger's carpooling requesting.

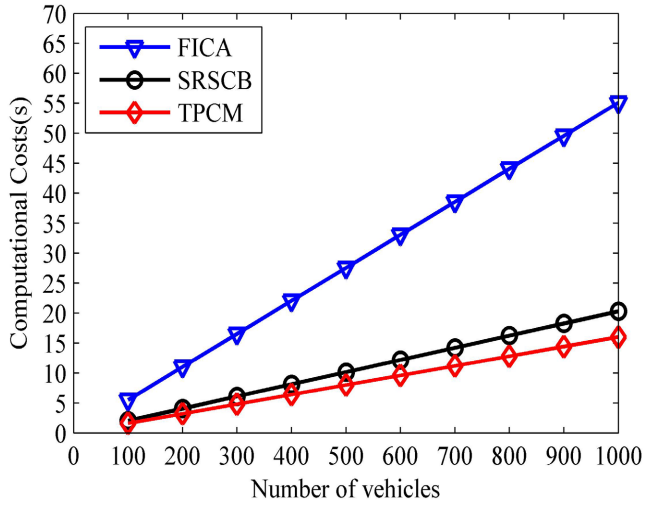

Figure 3. Time cost in vehicle's carpooling responding.

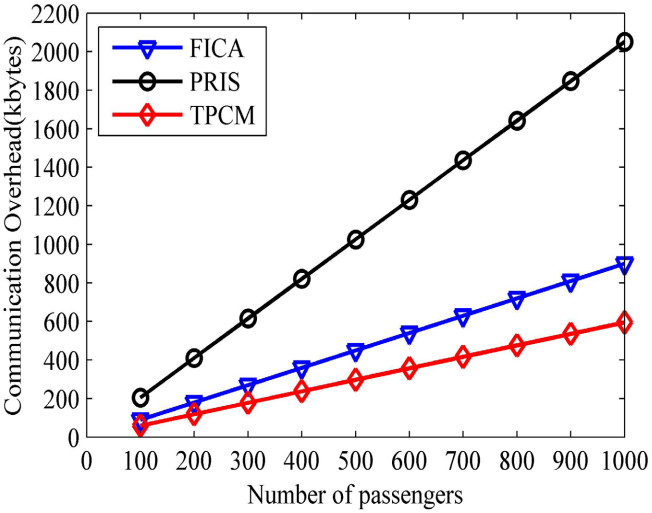

Figure 4. Communication overhead of passenger's carpooling requesting.

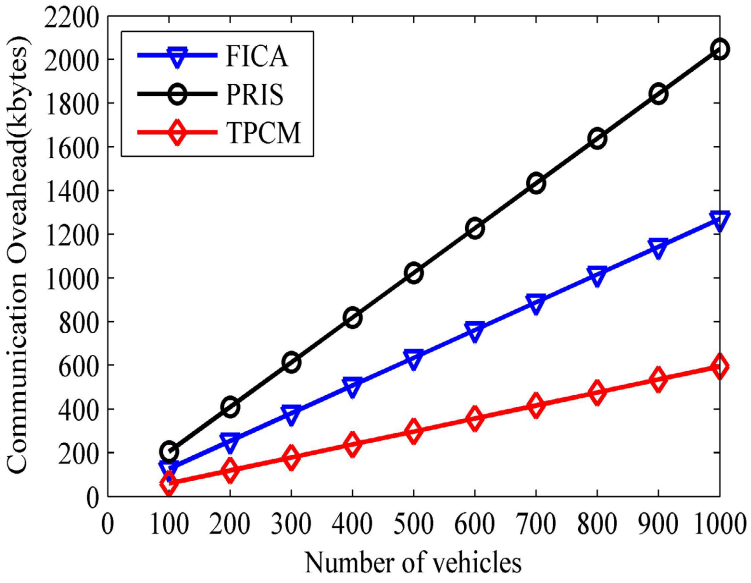

Figure 5. Communication overhead of vehicle's carpooling responding.

which uses the BF-PSI technology to match the vehicle's preference attribute secret value set with the preference secret value set selected by the passenger. **Figure 6** shows the change process of the probability that the carpooling is successfully matched n times with the size of the Bloom filter. We can see that with the increase of the size of the Bloom filter, the single matching success rate of our TPCM scheme is close to 100%, and the probability of multiple matching is almost 0. Therefore, the proposed carpooling matching scheme based on BF-PSI not only has high matching accuracy, but also has fast matching speed.

7.4. Evaluation of Trust Management Model

1) Simulation settings

In this section, we evaluate the robustness of the proposed trust management model. We mainly evaluate the robustness of the proposed model based on the changes in the average reputation scores of different carpooling vehicles. The factors that affect the average reputation score of a vehicle mainly include the percentage of malicious passengers in carpooling and the weight of passenger's feedback. The detailed simulation parameter setting is shown in **Table 5**.

In addition, we use *Rh* and *Rm* to evaluate the robustness of the proposed trust management model, where *Rh* denotes the average reputation score of honest carpooling vehicles; *Rm* denotes the average reputation score of malicious carpooling vehicles. The reputation score range of passengers is (0, 1], which is generated by random sampling and obeys a normal distribution, where $\mu = 0.5$, $\sigma = 0.5/3$.

$$f(x \mid \mu, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} * \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{18}$$

2) Robustness evaluation

Table 5. Simulation parameter settings.

Notations	Definition	Value
Pm	Percentage of malicious passengers	5%, 10%, 15%, 20%
w_s	Weight of passenger's feedback	0.6, 0.8

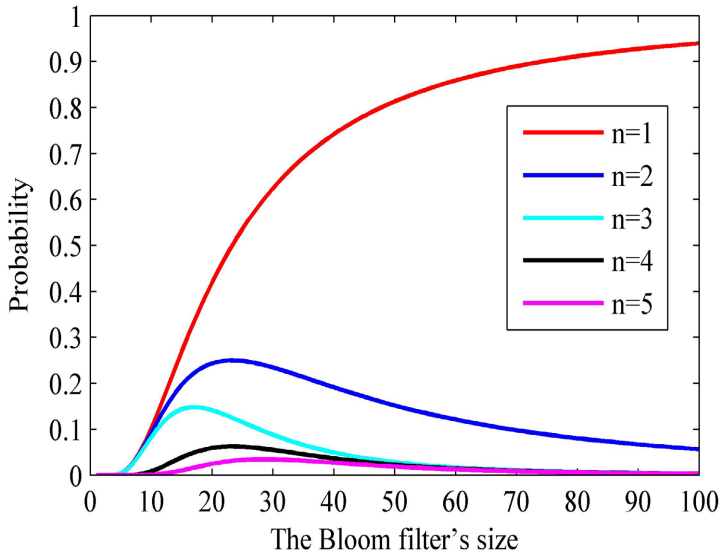

Figure 6. The probability of successful carpooling matching.

We mainly evaluate the robustness of proposed trust management model, that is, malicious passengers deliberately provide false trust feedback after carpooling to reduce or increase the trust value of certain travel preferences of the vehicle, thereby affecting the average reputation score of the vehicle. In this paper, the percentage of malicious passengers in carpooling is set to 5% - 25%. Each carpooling vehicle is first initialized and then performed 5 - 25 carpooling tasks respectively. The number of travel preferences selected by passengers is 1 - 7. After the interval, TA updates the trust value of each travel preference and preference attribute set of the unrevoked vehicle in the local database, and then updates the average reputation score of the vehicle based on the trust value of each updated travel preference. In the process of reputation update, the trust value of the travel preference of the carpooling vehicle that is not selected is 0.5 by default.

Figure 7 shows how the average reputation score of honest vehicles changes with the percentage of malicious passengers and weight w_s. We can see that when the percentage of malicious passengers gradually increases from 5% - 20%, the average reputation score of honest vehicles decreases slowly, which indicates that the presence of malicious passengers can't largely affect the average reputation score of honest vehicles. Therefore, our trust management model can resist attacks from malicious passengers. As w_s decreases, the average reputation score of honest carpooling vehicles decreases slightly, which is due to the fact that after the trust value of the travel preferences selected of honest vehicles are updated, the trust value of the corresponding travel preferences increases in a large extent

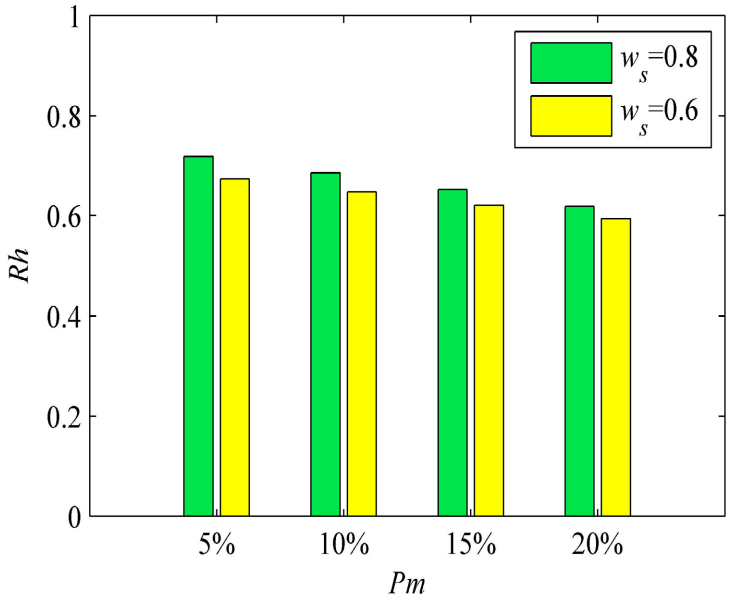

Figure 7. Average reputation score of honest vehicles.

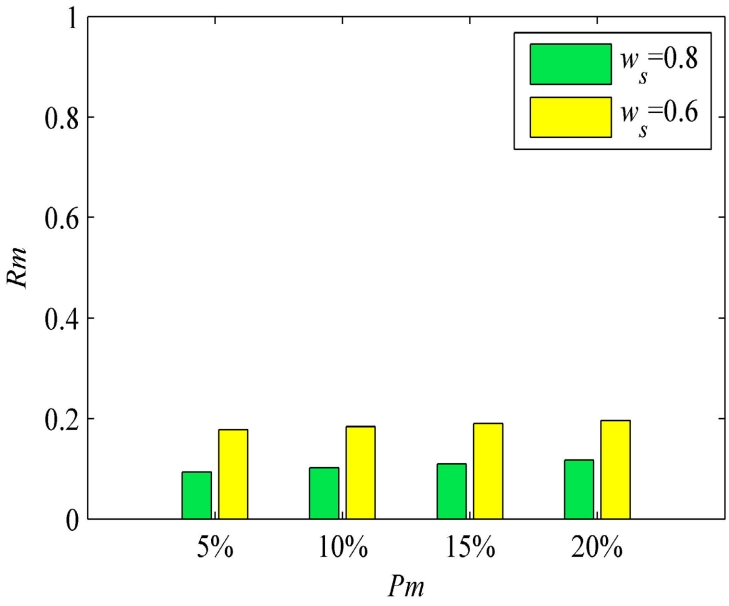

Figure 8. Average reputation score of malicious vehicles.

and is greater than the historical trust value of unselected travel preferences, reducing the weight w_s is equivalent to reduce the weight of the travel preference selected and updated by passengers, and the average reputation score of honest vehicles is reduced.

Figure 8 shows the changing process of the average reputation score of malicious vehicles with the percentage of malicious passengers and weight w_s. We can see that as the percentage of malicious passengers increases, the average reputation score of malicious vehicles increases very slowly, and the false feedback of malicious passengers can't greatly increase the average reputation score

of malicious vehicles. Therefore, the trust management model proposed in this paper shows robustness against malicious users' attacks. With the weight w_s decreases, the average reputation score of malicious vehicles has increased slightly, which is due to that after the trust value of travel preferences of vehicle reputation set selected by passengers is updated, the trust value rapidly decreases and is lower than the historical trust value of unselected travel preferences. Decreasing the weight w_s is equivalent to increase w_p, and the average reputation score of malicious vehicles is increased to a certain extent.

8. Conclusions

This paper adopts the privacy set intersection technology based on Bloom filter to propose a trusted and privacy-preserving carpooling matching scheme (TPCM). This scheme not only protects the privacy of vehicles and passengers during carpooling matching, but also solves the problem of carpooling mismatching caused by ignoring the individual needs of passengers by introducing travel preferences, which achieves a balance between precise carpooling matching and privacy protection; In addition, a multi-faceted trust management model is established to better describe the trust between the vehicles and the passengers, and to evaluate the trustworthiness of the vehicle from multi-faceted. Our TPCM scheme is robust against malicious attacks. Performance analysis shows that TPCM scheme can achieve fast and accurate carpooling matching, and has lower overhead compared with existing schemes.

In the future, we will consider the issue of batch authentication of multiple information, which will reduce the verification delay. And we will consider how to reduce the cost during the verification process and protect the privacy of the vehicle.

Acknowledgements

This work was in part supported by Fundamental Research Funds for the Central Universities of Jinan University (Grant No. 21621417), Natural Science Foundation of Guangdong Province of China (Grant No. 2017A030308013), Science and Technology Planning Project of Guangdong Province of China (Grant No. KTP20200022), National Natural Science Foundation of China (Grant No. 62032025, No. 62102167).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Liu, Z., Ma, J., Weng, J., Huang, F., Wu, Y., Wei, L. and Li, Y. (2021) LPPTE: A Lightweight Privacy-Preserving Trust Evaluation Scheme for Facilitating Distributed Data Fusion in Cooperative Vehicular Safety Applications. *Information Fusion*, **73**, 144-156. https://doi.org/10.1016/j.inffus.2021.03.003

[2] Chang, I.C., Hung, S.N. and Yen, C.E. (2019) Designing a Dynamic Carpooling System Integrated with the VANET-Based Route-Planning Algorithm. *Journal of the Chinese Institute of Engineers*, **42**, 132-142. https://doi.org/10.1080/02533839.2018.1552841

[3] Wang, Y., Gu, J., Wang, S. and Wang, J. (2019) Understanding Consumers' Willingness to Use Ride-Sharing Services: The Roles of Perceived Value and Perceived Risk. *Transportation Research Part C: Emerging Technologies*, **105**, 504-519. https://doi.org/10.1016/j.trc.2019.05.044

[4] Tamannaei, M. and Irandoost, I. (2019) Carpooling Problem: A New Mathematical Model, Branch-and-Bound, and Heuristic Beam Search Algorithm. *Journal of Intelligent Transportation Systems*, **23**, 203-215. https://doi.org/10.1080/15472450.2018.1484739

[5] Li, M., Zhu, L.H., Zhang, Z.J. and Xu, R.X. (2017) Achieving Differential Privacy of Trajectory Data Publishing in Participatory Sensing. *Information Sciences*, **400-401**, 1-13. https://doi.org/10.1016/j.ins.2017.03.015

[6] Sherif, A.B., Rabieh, K., Mahmoud, M.M. and Liang, X. (2016) Privacy-Preserving Ride Sharing Scheme for Autonomous Vehicles in Big Data Era. *IEEE Internet of Things Journal*, **4**, 611-618. https://doi.org/10.1109/JIOT.2016.2569090

[7] Yu, H., Jia, X., Zhang, H., Yu, X. and Shu, J. (2019) PSRide: Privacy-Preserving Shared Ride Matching for Online Ride Hailing Systems. *IEEE Transactions on Dependable and Secure Computing*, **18**, 1425-1440. https://doi.org/10.1109/TDSC.2019.2931295

[8] Wang, F., Zhu, H., Liu, X., Lu, R., Li, F., Li, H. and Zhang, S. (2018) Efficient and Privacy-Preserving Dynamic Spatial Query Scheme for Ride-Hailing Services. *IEEE Transactions on Vehicular Technology*, **67**, 11084-11097. https://doi.org/10.1109/TVT.2018.2868869

[9] Wernke, M., Dürr, F. and Rothermel, K. (2013) PShare: Ensuring Location Privacy in Non-Trusted Systems through Multi-Secret Sharing. *Pervasive and Mobile Computing*, **9**, 339-352. https://doi.org/10.1016/j.pmcj.2013.01.001

[10] Yu, H., Zhang, H., Yu, X., Du, X. and Guizani, M. (2020) PGRide: Privacy-Preserving Group Ridesharing Matching in Online Ride Hailing Services. *IEEE Internet of Things Journal*, **8**, 5722-5735. https://doi.org/10.1109/JIOT.2020.3030274

[11] Gruteser, M. and Grunwald, D. (2003) Anonymous Usage of Location-Based Services through Spatial and Temporal Cloaking. *Proceedings of the* 1*st International Conference on Mobile Systems, Applications and Services*, San Francisco, 5-8 May 2003, 31-42. https://doi.org/10.1145/1066116.1189037

[12] Kou, B., Cao, S. and Lv, J. (2020, July) A Privacy Protection Scheme for Carpooling Service Using Fog Computing. *Journal of Physics: Conference Series*, **1601**, Article ID: 032019. https://doi.org/10.1088/1742-6596/1601/3/032019

[13] Li, M., Zhu, L. and Lin, X. (2018) Efficient and Privacy-Preserving Carpooling Using Blockchain-Assisted Vehicular Fog Computing. *IEEE Internet of Things Journal*, **6**, 4573-4584. https://doi.org/10.1109/JIOT.2018.2868076

[14] Tyagi, A.K. and Sreenath, N. (2016) Vehicular Ad Hoc Networks: New Challenges in Carpooling and Parking Services. *International Journal of Computer Science and Information Security*, **14**, 13-24.

[15] Liu, Z., Ma, J., Jiang, Z., Zhu, H. and Miao, Y. (2016) LSOT: A Lightweight Self-Organized Trust Model in VANETs. *Mobile Information Systems*, **2016**, Article ID: 7628231. https://doi.org/10.1155/2016/7628231

[16] Tangade, S., Manvi, S.S. and Lorenz, P. (2020) Trust Management Scheme Based on Hybrid Cryptography for Secure Communications in VANETs. *IEEE Transactions on Vehicular Technology*, **69**, 5232-5243. https://doi.org/10.1109/TVT.2020.2981127

[17] Jaimes, L.M.S., Ullah, K. and dos Santos Moreira, E. (2016) ARS: Anonymous Reputation System for Vehicular Ad Hoc Networks. 2016 8*th IEEE Latin-American Conference on Communications* (*LATINCOM*), Medellin, 15-17 November 2016, 1-6. https://doi.org/10.1109/LATINCOM.2016.7811600

[18] Wang, S. and Yao, N. (2019) A RSU-Aided Distributed Trust Framework for Pseudonym-Enabled Privacy Preservation in VANETs. *Wireless Networks*, **25**, 1099-1115. https://doi.org/10.1007/s11276-018-1681-8

[19] Liu, Z., Guo, J., Huang, F., Cai, D., Wu, Y., Chen, X. and Konstantin Igorevich, K. (2021) Lightweight Trustworthy Message Exchange in Unmanned Aerial Vehicle Networks. *IEEE Transactions on Intelligent Transportation Systems*, 1-14. https://doi.org/10.1109/TITS.2021.3136304

[20] Hallgren, P., Orlandi, C. and Sabelfeld, A. (2017) PrivatePool: Privacy-Preserving Ridesharing. 2017 *IEEE* 30*th Computer Security Foundations Symposium* (*CSF*), Santa Barbara, 21-25 August 2017, 276-291. https://doi.org/10.1109/CSF.2017.24

[21] Salamanis, A., Kehagias, D.D., Tsoukalas, D. and Tzovaras, D. (2019) Reputation Assessment Mechanism for Carpooling Applications Based on Clustering User Travel Preferences. *International Journal of Transportation Science and Technology*, **8**, 68-81. https://doi.org/10.1016/j.ijtst.2018.08.002

[22] Caballero-Gil, C., Caballero-Gil, P., Molina-Gil, J., Martín-Fernández, F. and Loia, V. (2017) Trust-Based Cooperative Social System Applied to a Carpooling Platform for Smartphones. *Sensors*, **17**, Article No. 245. https://doi.org/10.3390/s17020245

[23] Baza, M., Lasla, N., Mahmoud, M., Srivastava, G. and Abdallah, M. (2019) B-Ride: Ride Sharing with Privacy-Preservation, Trust and Fair Payment Atop Public Blockchain. *IEEE Transactions on Network Science and Engineering*, **8**, 1214-1299. https://doi.org/10.1109/TNSE.2019.2959230

[24] Sánchez, D., Martínez, S. and Domingo-Ferrer, J. (2016) Co-Utile P2P Ridesharing via Decentralization and Reputation Management. *Transportation Research Part C: Emerging Technologies*, **73**, 147-166. https://doi.org/10.1016/j.trc.2016.10.017

[25] Abassi, R., Douss, A.B.C. and Sauveron, D. (2020) TSME: A Trust-Based Security Scheme for Message Exchange in Vehicular Ad Hoc Networks. *Human-Centric Computing and Information Sciences*, **10**, Article No 43. https://doi.org/10.1186/s13673-020-00248-4

[26] Farouk, F., Alkady, Y. and Rizk, R. (2020) Efficient Privacy-Preserving Scheme for Location Based Services in VANETSystem. *IEEE Access*, **8**, 60101-60116. https://doi.org/10.1109/ACCESS.2020.2982636

[27] Zhang, X. and Wang, D. (2019) Adaptive Traffic Signal Control Mechanism for Intelligent Transportation Based on a Consortium Blockchain. *IEEE Access*, **7**, 97281-97295. https://doi.org/10.1109/ACCESS.2019.2929259

[28] Kiss, S.Z., Hosszu, É., Tapolcai, J., Rónyai, L. and Rottenstreich, O. (2021) Bloom Filter with a False Positive Free zone. *IEEE Transactions on Network and Service Management*, **18**, 2334-2349. https://doi.org/10.1109/TNSM.2021.3059075

[29] Liu, Z., Huang, F., Weng, J., Cao, K., Miao, Y., Guo, J. and Wu, Y. (2020) BTMPP: Balancing Trust Management and Privacy Preservation for Emergency Message Dissemination in Vehicular Networks. *IEEE Internet of Things Journal*, **8**, 5386-5407. https://doi.org/10.1109/JIOT.2020.3037098

[30] Sun, G., Sun, S., Sun, J., Yu, H., Du, X. and Guizani, M. (2019) Security and Privacy Preservation in Fog-Based Crowd Sensing on the Internet of Vehicles. *Journal of Network and Computer Applications*, **134**, 89-99. https://doi.org/10.1016/j.jnca.2019.02.018

[31] Wang, D. and Zhang, X. (2020) Secure Ride-Sharing Services Based on a Consortium Blockchain. *IEEE Internet of Things Journal*, **8**, 2976-2991. https://doi.org/10.1109/JIOT.2020.3023920

[32] He, Y., Ni, J., Wang, X., Niu, B., Li, F. and Shen, X. (2018) Privacy-Preserving Partner Selection for Ride-Sharing Services. *IEEE Transactions on Vehicular Technology*, **67**, 5994-6005. https://doi.org/10.1109/TVT.2018.2809039