cryptography

MDPI

Article

Privacy Protection Scheme for the Internet of Vehicles Based on Private Set Intersection

Quan Zhou [1,*], Zhikang Zeng [1], Kemeng Wang [2] and Menglong Chen [2]

[1] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China
[2] School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China
* Correspondence: zhouqq@gzhu.edu.cn

Abstract: Performing location-based services in a secure and efficient manner that remains a huge challenge for the Internet of Vehicles with numerous privacy and security risks. However, most of the existing privacy protection schemes are based on centralized location servers, which makes them all have a common drawback of a single point of failure and leaking user privacy. The employment of anonymity and cryptography is a well-known solution to the above problem, but its expensive resource consumption and complex cryptographic operations are difficult problems to solve. Based on this, designing a distributed and privacy-secure privacy protection scheme for the Internet of Vehicles is an urgent issue for the smart city. In this paper, we propose a privacy protection scheme for the Internet of Vehicles based on privacy set intersection. Specially, using privacy set intersection and blockchain techniques, we propose two protocols, that is, a dual authentication protocol and a service recommendation protocol. The double authentication protocol not only ensures that both communicating parties are trusted users, but also ensures the reliability of their session keys; while the service recommendation protocol based on pseudorandom function and one-way hash function can well protect the location privacy of users from being leaked. Finally, we theoretically analyze the security that this scheme has, i.e., privacy security, non-repudiation, and anti-man-in-the-middle attack.

Keywords: Internet of Vehicles; privacy security; service recommendation; dual authentication; private set intersection

Citation: Zhou, Q.; Zeng, Z.; Wang, K.; Chen, M. Privacy Protection Scheme for the Internet of Vehicles Based on Private Set Intersection. *Cryptography* **2022**, *6*, 64. https://doi.org/10.3390/cryptography6040064

Academic Editor: Josef Pieprzyk

Received: 18 October 2022
Accepted: 6 December 2022
Published: 7 December 2022

1. Introduction

Traffic congestion and road accidents are becoming increasingly severe with the increasing number of vehicles. It has caused great potential threats to their privacy, property, and even their lives. However, with the development of new generation mobile communication technologies, location-based services on the Internet of Vehicles (IoV) have become popular, which have alleviated the above problems to some extent and brought great convenience to people in their lives, such as carpooling [1,2], Ride-hailing [3–5], navigation [6,7] and finding parking spaces [8,9]. Unfortunately, however, it still poses a certain level of security threat to people. For example, the data traffic generated during data interaction can be analyzed by hackers to get the rest of the user's sensitive information [10–12].

Most of the existing privacy protection schemes for the IoV generally adopt a centralized location server, which then performs location-based services via user-initiated location service queries. However, such schemes suffer from shortcomings such as single points of failure and user privacy leakage. Based on this, some scholars have tried to secure the privacy of the IoVs in other ways, and blockchain technology is a good way to do this.

Blockchain is a distributed network that can secure privacy in the IoV with hash functions and cryptography, and is not tampered with, and also supports the traceability of vehicle information. Existing blockchains can be divided into two categories, public and federated, depending on whether they require licensing authority. Where a public chain is a fully decentralized blockchain system that does not require a trusted center for maintenance,

a federated chain is a partially decentralized or polycentric blockchain system. With the emergence of blockchain technology, some scholars have tried to combine blockchain technology with the IoV, and many schemes have been proposed [13–15]. However, since the public chain-based privacy protection scheme requires a consensus mechanism for inter-node maintenance, it runs slower compared to the federation chain-based privacy protection scheme.

Another issue that needs our attention is that privacy protection schemes based on anonymous, complex cryptographic algorithms can protect the privacy and security of users, but they consume enormous resources. Can we use the existing fundamental knowledge to propose a novel privacy protection scheme for vehicular networks? For this, we invoke the privacy set intersection (PSI). PSI is a specific problem in secure multi-party computation that allows participants to input private sets and jointly compute the intersection of private sets without revealing any information beyond the intersection. PSI-based privacy protection schemes can perform location-based services while protecting user privacy [16]. Nevertheless, it is still a great challenge to get a good application in the highly flexible and scalable vehicular networks.

1.1. Motivations

Existing privacy protection schemes for the IoV are difficult to protect users' identity and location privacy in a privacy-secure manner. The main objective of this paper is to propose a privacy protection scheme for the IoV based on private set intersection, and to analyze the security of the proposed scheme from a theoretical point of view.

1.2. Contributions

To address the privacy and security issues in the IoV as much as possible, this paper proposes a privacy protection scheme for the IoV based on privacy set intersection. The legitimate user in the scheme completes the location-based service by initiating a query for the location-based service. In this process, no additional personal information of the user is disclosed and no large and complex cryptographic operations are required.

Below, we conclude our main contributions as follows.

1. Privacy Security: This scheme can effectively protect the privacy and security of users from privacy and security threats caused by man-in-the-middle attacks.
2. Dual Authentication Protocol: The dual authentication protocol based on PSI can achieve dual guarantees: First, it ensures that both communicating parties have registration certificates issued by the trusted authority (TA) and are trusted users. Second, it ensures that both communicating parties have established secure and reliable session keys in the process.
3. Collaborative Recommendation of Location Services: Based on pseudorandom functions and secure one-way hash functions, we propose a privacy-secure PSI-based collaborative recommendation location service protocol. It can well protect the privacy and security of users without requiring large computational overhead and complex cryptographic algorithms.
4. Distributed Storage of Transaction Information: We construct a private blockchain formed by the location service provider (LSP) and record service recommendation information in its transaction ledger to reduce LSPs' storage costs.

1.3. Organization

The rest of this paper is organized as follows. We present the related work in Section 2, the scheme model and design goals in Section 3, some preparatory knowledge in Section 4, the main location privacy protection scheme in Section 5, the security analysis of our scheme and its comparison with existing schemes in Section 6, the performance analysis of our scheme and its comparison with existing schemes in Section 7, and finally a summary of the full paper in Section 8.

2. Related Work

We divided the related work into two main categories: authentication and privacy protection on the Internet of Vehicles.

2.1. Authentication

The IoVs refer to the all-around network connection of vehicles and people, vehicles and vehicles, vehicles and roads, and vehicles and service platforms with the help of a new generation of mobile communication technology, thus providing better location-based services for people. However, there are a number of factors that threaten people's privacy and security in this process. On the one hand, there exist certain devices that are vulnerable to attacks by malicious users, such as Road Side Units (RSU). If the RSU is attacked by a malicious user, it may tamper with the information received or sent by the vehicle, thus causing irreversible damage to the user. On the other hand, the Internet of Vehicles is highly dynamic and its devices are deployed in the open domain, which makes it vulnerable to various attacks such as surveillance and remote intrusion. To avoid the above attacks, scholars have proposed many different authentication protocols for the Internet of Vehicles. And identity authentication schemes can be traced back to the first identity-based authentication scheme proposed by Shamir in 1985 [17]. Subsequently, scholars have proposed an increasing number of authentication schemes based on vehicular networks [18–26].

Gupta et al. [18] proposed a blockchain-enabled game theory-based authentication mechanism. Specially, they also proposed a three-layer multi-trusted authorization solution that supports cross-region authentication of vehicles with almost no communication delay. Wu et al. [19] proposed an authentication protocol based on symmetric encryption and fog computing in the Internet of Vehicles. Specially, they also proposed a four-layer architecture to reduce the computational burden of cloud servers. Using bilinear mapping and a one-way hash function, Sikarwar et al. [20] proposed an efficient and lightweight batch verification scheme. Compared with the single message verification, they claim that their scheme has better security and efficiency. Zhang et al. [21] proposed a trust platform module (TPM)-based conditional privacy-preserving authentication protocol. In this protocol, they used bilinear mapping to accelerate the process of authentication of messages by entities in the Internet of Vehicles. Considering some resource-constrained mobile devices, Jan et al. [22] proposed a secure and efficient lightweight, and anonymous authentication and key establishment scheme which is applicable to "Vehicle to Vehicle (V2V)" and "Vehicle to RSU (V2R)". For forensic services on the Internet of Vehicles, it is critical to ensure data privacy of vehicles and the efficiency of data transfer between vehicles. Therefore, Zhang et al. [23] proposed a lightweight conditional anonymous authentication scheme for forensic services in IoV. Considering the vulnerability of onboard sensors of unattended vehicles to physical attacks, Jiang et al. [24] proposed a physically secure authentication and key exchange protocol using physical unclonable function. However, Ahmim et al. [25] argued that the scheme of Jiang et al. [24] has drawbacks such as a lack of message confidentiality. Based on this, Ahmim et al. [25] proposed some solutions and improved the security of the scheme of Jiang et al. [24]. Zhao et al. [26] proposed a federated learning collaborative authentication protocol for shared data. It can effectively protect user privacy and prevent data leakage.

2.2. Privacy Protection

The privacy security of users plays a very important role in the development of the Internet of Vehicles. Therefore, scholars have proposed many privacy protection schemes for the Internet of Vehicles based on anonymity and cryptography technologies, among which blockchain, as a distributed technology, has been continuously applied to privacy protection schemes on the Internet of Vehicles with the needs of application scenarios.

2.2.1. Anonymity

K-anonymity is a common approach in privacy-preserving schemes for the Internet of Vehicles. K-anonymity can be traced back to the work proposed by Sweeney in 2002 [27], but the first application to vehicular privacy protection was by Gruteser et al. [28]. And in order to be able to satisfy the level of privacy protection required by users, Kido et al. [29] proposed the first scheme to generate anonymous sets for users in the form of generated dummy users. However, this scheme suffers from unreliable dummy user data and the communication overhead increases as the number of dummy users increases. To solve the problem of unreliable virtual user data, scholars have proposed different K-anonymity based privacy preserving schemes for the Internet of Vehicles [30–34].

Sun et al. [30] proposed a region-of-interest division-based algorithm to preserve the location privacy of users. Specially, after considering the semantic location information, they also proposed an approach to generate dummy locations based on entropy, which can generate safe and secure dummy locations that do not contain the real location information of users. Considering frequent regions and time reachability, Liu et al. [31] proposed frequency-aware dummy-based method to the location privacy of users, which ensures that the generated dummy locations are as safe and reasonable as possible. Niu et al. [32] proposed a dummy-based privacy protection scheme for continuous location based services (LBSs). Especially, after considering factors such as time-sensitive side information, they proposed a dummy filtering algorithm to ensure that the dummy locations are realistic and reliable. Ni et al. [33] proposed an anonymous entropy-based location privacy protection scheme in mobile social networks. According to the population distribution method, the scheme contains two algorithms: an anonymous region constructing algorithm based on kd-trees in densely populated regions (K-DDCA) and an anonymous region constructing algorithm based on kd-trees in sparsely populated regions (K-SDCA). To ensure the validity, uncertainty and dispersion of virtual location, Xu et al. [34] proposed a location privacy-preservation method based on dummy locations under road restriction.

2.2.2. Cryptography

Due to the ability to provide higher quality of service and its communication overhead does not increase linearly with the number of users, cryptography-based privacy-preserving schemes for the Internet of Vehicles have numerous applications in carpooling [35,36] and hailing [37–40].

In view of the centralization problem existing in the traditional carpooling schemes, Li et al. [35] proposed an efficient and privacy-preserving carpooling scheme using blockchain-assisted vehicular fog computing. Using attribute-based proxy re-encryption, Wang et al. [36] proposed a secure ride-sharing scheme based on a consortium blockchain. All of their schemes ensure data security.

While online ride-hailing services bring a convenient way for people to travel, the privacy concern is also highly raised. Based on this, using somewhat homomorphic encryption, Yu et al. [37] proposed an efficient and privacy-preserving ride matching scheme for Online Ride Hailing services. Specially, they also proposed an efficient exact shortest road distance computation approach over encrypted data. And by this approach, they can find the taxi with the minimum road distance to serve a rider. Using paillier cryptosystem, Huang et al. [38] proposed a privacy-preserving online ride-sharing matching scheme. It also supports privacy-preserving ride-sharing between multiple riders. Using elliptic curve cryptosystem and digital signature technology, Wang et al. [39] proposed a blockchain-based anonymous ride-hailing scheme for autonomous taxi network. Using somewhat homomorphic encryption, Ma et al. [40] proposed a privacy-preserving cross-zone ride-matching scheme.

3. Problem Statement

3.1. System Model

The system model of this scheme consists of trusted authority (TA), road side unit (RSU), requesting users (RU_i), collaborating users (CU_j), and location service provider (LSP) which are depicted in Figure 1.

1. TA: A trust center, mainly responsible for user registration, generation of system private key *sk*, system public key *pk* and system parameters *params*.
2. LSP: A location service provider, which is the core component of this paper, is primarily responsible for the maintenance of the blockchain.
3. RSU: A roadside infrastructure is installed on both sides of the road with some computing and storage capacity, mainly responsible for message forwarding, functional verification, and PSI operations.
4. RU_i: Users who initiate location service queries.
5. CU_j: Users who respond to a location service query.

The key notations are listed in Table 1.

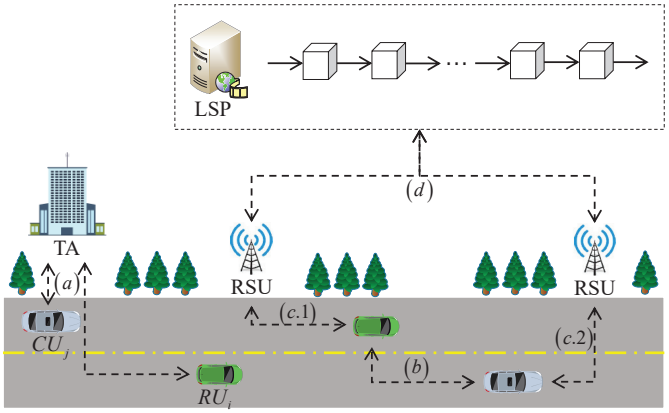

Figure 1. System model. Here, (a) the TA initializes the system, and then the user id_i register with the trusted authority and obtain the corresponding public-private key pair; (b) each user id_i (RU_i and CU_j) authenticates with each other; (c) the user id_i makes a service query (response) and sends it to the RSU, where (c.1) the RU_i initiates a service query and (c.2) the CU_j generates a service response; (d) the RSU writes the identity and transaction content of user id_i to the transaction and sends it to the blockchain network. Finally, the RU_i and CU_j will establish a personal channel to complete the relevant service recommendations.

Table 1. Symbol description.

Symbol	Description
λ, κ, p	Security parameter, prime number
$\mathbb{G}_1, \mathbb{G}_2, g_1$	Cyclic group, generator
e	Bilinear mapping
H_1, H_2, H_3, H_4	Hash function
C_{TA}	certificate of registration
pk, sk	The system public key and private key
$params$	The public parameter
id_{TA}	The identity of TA
id_i	The identity of user (RU_i and CU_j)
$sk_{i,1}, sk_{i,2}, pk_{i,1}$	The user's private key and public key
F_κ	Pseudorandom function
$PSI(X, Y)$	PSI operation of X and Y
SK	Session key
M	Service content
$Enc_{SK}(), Dec_{SK}()$	Encryption and decryption algorithm with SK

3.2. Threat Model

The main security threats to this scheme originate from the following components.

1. Most of the requesting users are honest and trustworthy, and will send real and reliable location service queries. However, a small percentage of requesting users will upload false location service queries or repeatedly initiate queries multiple times within a short period of time, thus reducing system security and query efficiency.
2. Most of the collaborative users are honest and trustworthy, and will generate true and reliable location service responses based on their historical experience, background knowledge. However, there exists a small percentage of collaborative users who will generate false service responses, thus reducing service efficiency.
3. A typical vulnerable attack during the communication between two parties is the man-in-the-middle attack, where a malicious user can perform acts such as wiretapping and forging messages during the communication between two parties.
4. Security threats due to physical factors are not considered.

3.3. Design Goals

The design goals of this scheme have the following main parts.

1. Identity Privacy: The user's identity information is anonymous to other users, RSUs and LSPs during the registration, authentication and service query process.
2. Location Privacy: Users' location information must be protected from remaining malicious users who may obtain it in an undisclosed manner and derive the rest of the user's sensitive information from it.
3. Route Privacy: The user's route information is known only to him/herself, and it is difficult for the rest of the users to infer the user's route from the available information.
4. Non-Repudiation: No user can repudiate the act of sending a message and the content of the message. TA can reveal the identity of users who have malicious behavior.
5. Anti-Man-in-the-Middle Attack: No man-in-the-middle attacks from malicious users during the communication between the two parties.

4. Preliminaries

In this section, we briefly revisit elemental techniques that are used to support the construction of the proposed scheme. These include bilinear pairing, the problem of collusion attack algorithm with k traitors (k-CAA), and private set intersection.

4.1. Bilinear Pairing

Assume $\mathbb{G}_1, \mathbb{G}_2$ are cyclic groups of prime order p, where g_1 is a generator in $\mathbb{G}_1$. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear pairing if the following conditions are satisfied.

1. Bilinearity: for all $z_1 \in \mathbb{G}_1, z_2 \in \mathbb{G}_2$ and $w_1, w_2 \in \mathbb{Z}_P^*$, $e(w_1 z_1, w_2 z_2) = e(z_1, z_2)^{w_1 w_2}$.
2. Non-degeneracy: $e(g_1, g_1) \neq 1$.
3. Computability: for all $z_1 \in \mathbb{G}_1$ and $z_2 \in \mathbb{G}_2$, $e(z_1, z_2)$ is efficiently computable.

4.2. k-CAA Problem

For any integer k and $s \in \mathbb{Z}_P^*, g_1 \in \mathbb{G}_1$, given $\left\{ v_1, \ldots, v_k \in \mathbb{Z}_p^*, g_1, sg_1, \frac{g_1}{s+v_1}, \ldots, \frac{g_1}{s+v_k} \right\}$, compute $\left(v, \frac{g_1}{s+v} \right)$, where $v \in \mathbb{Z}_p^*$ and $v \notin \{v_1, \ldots, v_k\}$.

4.3. Private Set Intersection

PSI means that the participants input the private set and jointly compute the intersection of the private set without revealing any information other than the intersection. And the most popular PSI scheme is the PSI scheme based on oblivious pseudo-random functions (OPRF-Based PSI), as shown in Figure 2.

1. Sender holds the set $Y = \{y_1, \ldots, y_n\}$, Receiver holds the set $X = \{x_1, \ldots, x_n\}$, k_i is Sender's private key, and F is an oblivious pseudo-random function.

2. Receiver sends $x_i \in X$ to OPRF. Then OPRF generates k_i and $F(k_i, x_i)$ and sends them to Sender and Receiver respectively.
3. When receiving k_i, Sender computes $F(k_i, y_1), \ldots, F(k_i, y_n)$ and sends it to the Receiver.
4. When receiving $F(k_i, y_1), \ldots, F(k_i, y_n)$ from Sender, Receiver contrasts $F(k_i, x_i)$ with $F(k_i, y_j)$, and then generates the PSI results for Sender and Receiver.

In Section 5.4, we construct a dual authentication protocol using PSI techniques and define a notation, i.e., $PSI(X, Y)$, which indicates that the PSI result of the set X and Y is $PSI(X, Y)$. For this, we make the following rules.

$$PSI(X, Y) \leftarrow \begin{cases} 1, & PSI(X, Y) = X = Y, \\ 0, & Otherwise. \end{cases} \quad (1)$$

If Sender and Receiver have the same set, i.e., $PSI(X, Y) = X = Y$, then we make $PSI(X, Y) \leftarrow 1$; otherwise we make $PSI(X, Y) \leftarrow 0$.

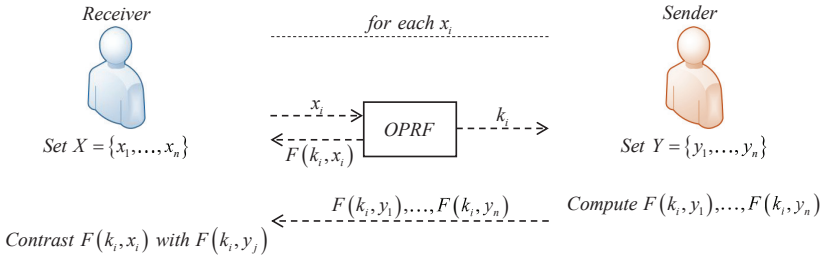

Figure 2. OPRF-Based PSI.

5. The Proposed Scheme

5.1. Overview

The scheme consists of the following parts: system initialization, user registration, dual authentication, service query (response), service recommendations and service transactions. The flow of the scheme is shown in Figure 3. Specifically, In (i), each user (requesting user and collaborating user) registers with the TA and generates the corresponding public-private key pair. In (ii), each user to be communicated authenticates with each other and generates a temporary session key. In (iii), the requesting user initiates a service request (and the collaborating user generates a service response) and sends it to the RSU. In (iv), the RSU performs signature verification of the requesting user (or collaborating user) and generates the corresponding service recommendation for the requesting user. Finally, in (v), the requesting user and the collaborating user establish a communication channel to complete the service recommendation.

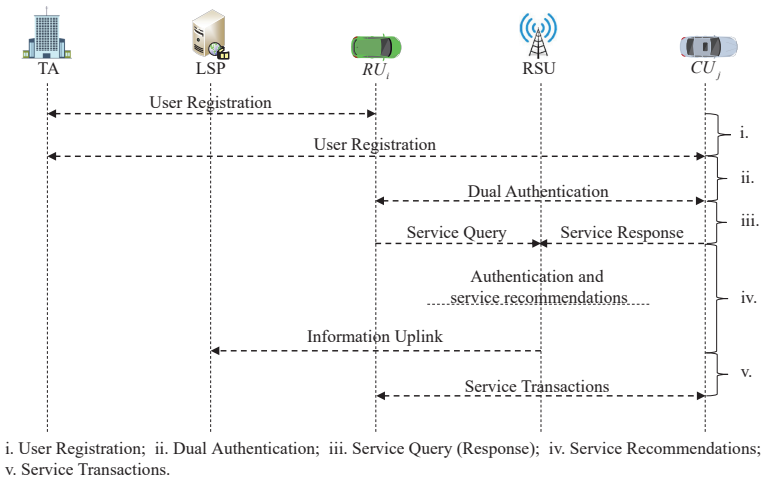

Figure 3. Overview of the proposed scheme.

5.2. System Initialization

Given a security parameter λ, the TA generates two cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ of prime order $p\left(p \geq 2^{\lambda}\right)$ and chooses a bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where g_1 is a generator in $\mathbb{G}_1$, and $g_2 = e(g_1, g_1)$. The TA chooses three hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_2 : \mathbb{Z}_p^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_p^*$, $H_3 : \{0,1\}^* \rightarrow \{0,1\}^{\kappa}$, and $H_4 : \{0,1\}^* \times \mathbb{Z}_p^* \rightarrow \{0,1\}^{l}$. Next, the TA chooses $s \in {}_R\mathbb{Z}_p^*$, computes $h_1 = sg_1$ and generates a user's certificate of registration $C_{TA} = H_1(id_{TA})^s$. Finally, the public key is $pk = h_1$, the private key is $sk = s$, and the public parameters is $params = \{\mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, p, pk, H_1, H_2, H_3, H_4\}$.

5.3. User Registration

Each user id_i (RU_i and CU_j) must register with the TA and generate their own public-private key pair, specifically.

1. The user id_i chooses $sk_{i,1} \in {}_R\mathbb{Z}_p^*$, computes $pk_{i,1} = g^{sk_{i,1}}$ and sends $(pk_{i,1}, H_1(id_i))$ to TA via a public channel.
2. When receiving $(pk_{i,1}, H_1(id_i))$ from user id_i, TA performs the following operations.
   - Compute $sk_{i,2} = \frac{1}{s+H_1(id_i)} g_1$.
   - Choose $\xi_1, \xi_2 \in {}_R\mathbb{Z}_p^*$, and compute $(h_2, h_3) \leftarrow \left(g^{\xi_1}, g^{\xi_2}\right)$.
   - Finally, send $(sk_{i,2}, h_2, h_3, C_{TA})$ to user id_i via a secure channel.

5.4. Dual Authentication

In this part, RU_i and CU_j verify each other and agree on a temporary session key.

1. RU_i randomly chooses a security parameter κ for pseudorandom function (PRF) and a number $\alpha \in {}_R\mathbb{Z}_p^*$. RU_i computes

$$\begin{cases} R_0 = g_1^{\alpha} (\mathrm{mod}\, p), \\ R_1 = \alpha(pk + g_1 \cdot H_1(id_i)), \\ R_2 = \frac{1}{\alpha + H_2(C_{TA}, R_1)} \cdot sk_{i,2}, \\ R_3 = H_3(C_{TA} \parallel R_0 \parallel R_1 \parallel R_2) \oplus (\kappa). \end{cases} \tag{2}$$

   Then RU_i sends (R_0, R_1, R_2, R_3) to CU_j via public channel.
2. When receiving (R_0, R_1, R_2, R_3) from RU_i, CU_j verifies

$$e(R_2, R_1 + H_2(C_{TA}, R_1)(pk + g_1 \cdot H_1(id_i))) \stackrel{?}{=} g_2. \tag{3}$$

   If the verification is correct, CU_j chooses a number $\beta \in {}_R\mathbb{Z}_p^*$ and computes

$$\begin{cases} \kappa = R_3 \oplus H_3(C_{TA} \parallel R_0 \parallel R_1 \parallel R_2), \\ C_0 = g_1^{\beta} (\mathrm{mod}\, p), \\ C_1 = \beta(pk + g_1 \cdot H_1(id_i)), \\ C_2 = \frac{1}{\beta + H_2(C_{TA}, C_1)} \cdot sk_{i,2}, \\ C_3 = R_0^{\beta}, \\ C_4 = H_3(F_{\kappa}(C_{TA}, C_3)). \end{cases} \tag{4}$$

   Then CU_j sends (C_0, C_1, C_2, C_4) to RU_i via public channel.
3. When receiving (C_0, C_1, C_2, C_4) from CU_j, RU_i verifies

$$e(C_2, C_1 + H_2(C_{TA}, C_1)(pk + g_1 \cdot H_1(id_i))) \stackrel{?}{=} g_2 \tag{5}$$

   If the verification is correct, RU_i computes $R_4 = C_0^{\alpha}$, $R_5 = H_3(F_{\kappa}(C_{TA}, R_4))$ and performs a intersection operation on (R_5, C_4). If $PSI(R_5, C_4) \leftarrow 1$, i.e., $PSI(R_5, C_4) = R_5 = C_4$, this indicates that CU_j and RU_i have the same registration certificate C_{TA}

issued by TA and generate a secure and reliable session key $SK = C_3 = R_4$, and indicates that CU_j is a reliable user. Then RU_i sends R_5 to CU_j via public channel; otherwise, interrupt process.

4. When receiving R_5 from RU_i, CU_j performs a intersection operation on (C_4, R_5). If $PSI(C_4, R_5) \leftarrow 1$, i.e., $PSI(C_4, R_5) = C_4 = R_5$, this indicates that RU_i and CU_j have the same registration certificate C_{TA} issued by TA and generate a secure and reliable session key $SK = R_4 = C_3$, and indicates that RU_i is a reliable user; otherwise, interrupt process.

The proof of correctness of the Equations (3) and (5) are demonstrated as shown below.

$$\begin{aligned} & e(R_2, R_1 + H_2(C_{TA}, R_1)(pk + g_1 \cdot H_1(id_i))) \\ &= e\Big(\tfrac{1}{\alpha + H_2(C_{TA}, R_1)} \cdot sk_{i,2}, \alpha(pk + g_1 \cdot H_1(id_i)) + H_2(C_{TA}, R_1)(pk + g_1 \cdot H_1(id_i))\Big) \\ &= e\Big(\tfrac{1}{(\alpha + H_2(C_{TA}, R_1))(s + H_1(id_i))} \cdot g_1, (\alpha + H_2(C_{TA}, R_1))(s + H_1(id_i))g_1\Big) \\ &= e(g_1, g_1) \\ &= g_2. \end{aligned} \tag{6}$$

$$\begin{aligned} & e(C_2, C_1 + H_2(C_{TA}, C_1)(pk + g_1 \cdot H_1(id_i))) \\ &= e\Big(\tfrac{1}{\beta + H_2(C_{TA}, C_1)} \cdot sk_{i,2}, \beta(pk + g_1 \cdot H_1(id_i)) + H_2(C_{TA}, C_1)(pk + g_1 \cdot H_1(id_i))\Big) \\ &= e\Big(\tfrac{1}{(\beta + H_2(C_{TA}, C_1))(s + H_1(id_i))} \cdot g_1, (\beta + H_2(C_{TA}, C_1))(s + H_1(id_i))g_1\Big) \\ &= e(g_1, g_1) \\ &= g_2. \end{aligned} \tag{7}$$

5.5. Service Query (Response)

In the service query (response) part, RU_i initiates a service query (CU_j generates a service response) and sends it to the RSU for service recommendations, specifically.

1. The user id_i chooses numbers $r_1, r_2 \in_R \mathbb{Z}_p^*$ and computes $D_1 = g^{r_1}, D_2 = g^{r_2}, D_3 = h_2^{r_1} h_3^{r_3} sk_{i,2}$.
2. The user id_i computes $E = H_3(F_k(M)), L_1 = H_1(D_1, D_2, D_3, E), L_2 = r_1 + sk_{i,1}L_1$, and $L_3 = r_2 + sk_{i,1}L_1$, where $M \in \{0,1\}^l$ is the service query contents of RU_i (or the service response contents of CU_j).
3. Finally, the user id_i sends $\sigma \leftarrow (E, D_1, D_2, D_3, L_1, L_2, L_3)$ to the RSU via public channel.

5.6. Service Recommendations

When receiving σ from different users id_i (RU_i or CU_j), the RSU performs the following operations:

1. Compute $D_1' = g^{L_2} pk_{i,1}^{-L_1}, D_2' = g^{L_3} pk_{i,1}^{-L_1}$, and $L_1' = H_1\big(D_1', D_2', D_3, E\big)$ and then verify the validity of $D_1' \stackrel{?}{=} D_1, D_2' \stackrel{?}{=} D_2$, and $L_1' \stackrel{?}{=} L_1$. If it is not valid, drop the corresponding query (response); otherwise, continue.
2. For two different users id_i (RU_i and CU_j) of $E_i \in \sigma_i$, compute $PSI\big(E_i, E_j\big)$ and send it to the RU_i
3. Write $\big\{(id_i, E_i), \big(id_j, E_j\big), E_i \cap E_j\big\}_{i \neq j}$ into the transaction and send it to the blockchain network.

The proof of correctness of the equations $D_1' \stackrel{?}{=} D_1, D_2' \stackrel{?}{=} D_2$, and $L_1' \stackrel{?}{=} L_1$ are demonstrated as shown below.

$$D_1' = g^{L_2} pk_{i,1}^{-L_1} = g^{r_1 + sk_{i,1}L_1} \Big(g^{sk_{i,1}}\Big)^{-L_1} = g^{r_1} = D_1. \tag{8}$$

$$D_2' = g^{L_3} pk_{i,1}^{-L_1} = g^{r_2 + sk_{i,1}L_1} \Big(g^{sk_{i,1}}\Big)^{-L_1} = g^{r_2} = D_2. \tag{9}$$

$$L_1' = H\big(D'_1, D'_2, D_3, E\big) = H(D_1, D_2, D_3, E) = L_1. \tag{10}$$

5.7. Service Transactions

In the service transactions part, the RU_i and CU_j will complete the relevant service recommendations via the personal channel. Specifically, the CU_j encrypts the relevant service response content, i.e., $Enc_{SK}(M) = H_4(SK, C_{TA}) \oplus (M)$, using the temporary session key $SK = C_3 = R_4$ and finally sends it to the RU_i. And the RU_i completes the location-based service query by computing $Dec_{SK}(Enc_{SK}(M)) = Enc_{SK}(M) \oplus H_4(SK, C_{TA}) = M$.

6. Privacy and Security Analysis

In this section, we analyze the privacy and security of the proposed scheme, which mainly includes identity privacy, location privacy, route privacy, non-repudiation, and anti-man-in-the-middle attacks.

6.1. Identity Privacy

In our scheme, we protect the privacy of the user's identity. During the user registration process, each user id_i must register with the TA to obtain the corresponding private key $sk_{i,2}$ and registration certificate C_{TA}. And in this process, all users are registered using the hash of their identity, i.e., $H_1(id_i)$, without revealing the user's identity information. In the dual authentication process, each user proves that he or she is secure and trustworthy via a registration certificate C_{TA} obtained at the time of registration, while maintaining the user's anonymity. In the service query (response) process, the user's identity information is secure because the user's identity (in this case, anonymous identity) is not involved. In summary, the user's identity information is anonymous to the rest of the users, RSUs and LSPs. However, the user's identity privacy is conditionally secure for the TA. This is because the user's private key $sk_{i,2}$ is issued by the TA. If the TA is compromised, the user's identity will be revealed.

6.2. Location Privacy

In the service query (response) process, we use a secure pseudo-random function and a one-way hash function to process the user's location data, i.e., $H_3(F_\kappa(M))$. And during the service transaction, we process the user's location data by its constructed session key, i.e. $Enc_{SK}(M)$. The location data processed in both ways will become indistinguishable, thus ensuring the privacy and security of the user's location.

6.3. Route Privacy

When RU_i initiates a service query (CU_j generates a service response), it is known from Section 6.2 that the user's location privacy is security. Moreover, the user uses a pseudo-random function and a hash function for its message content M, i.e., $E = H(F_\kappa(M))$, which prevents the adversary from determining that E and E' are generated by the same M. Finally, in the service transaction phase, we claim the following two facts. (1) RU_i cannot infer the routing information of CU_j from the location service sent by CU_j. For example, there are three routes available for driving from A to B. RU_i only knows that CU_j took one of the three routes, and does not know which one was taken. (2) CU_j also cannot infer the next routing information of RU_i from the location service it sends. On the one hand, the path selection of RU_i has a large uncertainty, and on the other hand, CU_j cannot know whether RU_i accepts the location service it sends.

6.4. Non-Repudiation

When there exists some malicious users who endanger the privacy and security of the rest of the users by means of message replay and forgery, TA can compute $D_3 \Big/ D_1^{\xi_1} D_2^{\xi_2}$ to obtain the private key of the malicious user and its corresponding identity.

The proof of correctness of the equations $D_3 \Big/ D_1^{\xi_1} D_2^{\xi_2}$ is demonstrated as shown below.

$$D_3 \Big/ D_1^{\xi_1} D_2^{\xi_2} = h_2^{r_1} h_3^{r_3} sk_{i,2} \Big/ (g^{r_1})^{\xi_1} (g^{r_2})^{\xi_2} = sk_{i,2}. \tag{11}$$

6.5. Anti-Man-in-the-Middle Attack

We have mainly considered man-in-the-middle attack resistance in the dual authentication phase. Specifically, under the random oracle and k-CAA assumptions, we prove by Theorem 1 that the proposed signature technique is resistant to existential forgery in the dual authentication phase. This ensures that the dual authentication protocol proposed in this paper is resistant to man-in-the-middle attacks.

Theorem 1. *The proposed scheme is existentially unforgeable in the random oracle model under the k-CAA assumption.*

Proof of Theorem 1. We assume that there exists an attacker $\mathcal{A}$ who adaptively selects messages and identities can break the scheme proposed in this paper with a non-negligible advantage ε after performing $n_{H_i}(i = 1, 2)$ times of $H_i(i = 1, 2)$ queries, n_E times of private key extraction queries and n_S times of signature queries within the time t. Then there exists a challenger $\mathcal{C}$ who can solve the $n_E - CAA$ problem with a non-negligible advantage ε' in time t'.

We assume that given a challenge to $\mathcal{C}$, i.e., given g_1, $h_1 = sg_1$, $v_1, v_2, \ldots, v_{n_E} \in \mathbb{Z}_p^*$, the goal of $\mathcal{C}$ is to output a solution $\left(v, \frac{g_1}{s+v}\right)$ of the $n_E - CAA$ problem, where $v \notin \{v_1, v_2, \ldots, v_{n_E}\}$.

1. Setup. $\mathcal{C}$ runs the system initialization algorithm, then chooses $\alpha_i \in \mathbb{Z}_p^*$, and computes $R_{i,1} = \alpha_i(pk + g_1 \cdot H_1(id_1))\left(1 \le i \le n_{H_1}\right)$. $\mathcal{C}$ constructs a list Q_{list} containing the array $(id_i, H_1(id_i), \alpha_i, R_{i,1})$, and finally sends the public parameter $\{\mathbb{G}_1, \mathbb{G}_2, g_1, g_2, e, p, pk, H_1, H_2, \{R_{i,1}\}_{i=1}^{n_{H_1}}\}$ to $\mathcal{A}$.
2. Queries. In response to the query of $\mathcal{A}$, $\mathcal{C}$ maintains list Q_1, Q_2, Q_3, Q_4 to track the H_1 query, H_2 query, private key extraction query and signature query of $\mathcal{A}$. The list Q_1, Q_2, Q_3, Q_4 is empty at the beginning. We assume that for each $id_i(1 \le i \le n_E)$, $\mathcal{A}$ has queried the H_1 value of id_i before performing H_2 query, private key extraction query and signature query for simplicity.
   - H_1 query. $\mathcal{C}$ maintains a list Q_1 containing the array $(id_i, H_1(id_i))$. Specifically, for id_i, $\mathcal{C}$ prepares a n_{H_1} response $\{H_1(id_i)\}_{i=1}^{n_{H_1}}$ and adds it to the Q_1. When $\mathcal{A}$ makes a H_1 query to id_i, $\mathcal{C}$ recovers $(id_i, H_1(id_i))$ from Q_1 and sends it to $\mathcal{A}$.
   - H_2 query. $\mathcal{C}$ maintains a list Q_2 containing the array $(id_i, C_{TA}, R_{i,1}, O_i)$. When $\mathcal{A}$ makes a H_2 query to $(C_{TA}, R_{i,1})$, $\mathcal{C}$ recovers $(id_i, H_1(id_i), \alpha_i, R_{i,1})$ from Q_{list} and chooses a number $O_i \in \mathbb{Z}_p^*$, so that $O_i = H_2(C_{TA}, R_{i,1})$. Then adds $(id_i, C_{TA}, R_{i,1}, O_i)$ to Q_2 and sends O_i to $\mathcal{A}$.
   - Private key extraction query. When $\mathcal{A}$ makes a private key extraction query to $id_i(1 \le i \le n_E)$, $\mathcal{C}$ recovers $(id_i, H_1(id_i), \alpha_i, R_{i,1})$ from Q_{list} and then verifies $H_1(id_i) \stackrel{?}{\in} \{v_1, v_2, \ldots, v_{n_E}\}$. If $H_1(id_i) \notin \{v_1, \ldots, v_{n_E}\}$, output "$\perp$" ("$\perp$" means failure). Otherwise there is $H_1(id_i) \in \{v_1, v_2, \ldots, v_{n_E}\}$ (i.e., there is $v_j \in \{v_1, \ldots, v_{n_E}\}$ such that $H_1(id_i) = v_j$), then computes $sk_{i,2} = \frac{g_1}{s+v_j}$. Finally, adds $(id_i, sk_{i,2})$ to Q_3 and sends $(\alpha_i, sk_{i,2})$ to $\mathcal{A}$.
   - Signature query. When $\mathcal{A}$ makes signature query to (id_i, C_{TA}), $\mathcal{C}$ recovers $(id_i, H_1(id_i))$ from Q_1 and verifies $H_1(id_i) \stackrel{?}{\in} \{v_1, \ldots, v_{n_E}\}$. If $H_1(id_i) \notin \{v_1, \ldots, v_{n_E}\}$, $\mathcal{C}$ outputs "$\perp$". Otherwise, $\mathcal{C}$ computes $R_{i,2} = \frac{sk_{i,2}}{\alpha_i + H_2(C_{TA}, R_{i,1})}$ and sends it to $\mathcal{A}$.
3. $\mathcal{A}$ outputs a message signature pair $\left(C_{TA}^*, R_{i,2}^*\right)$ about the id_i^*, and the signature satisfies the following equation.

$$e\left(R_{i,2}^*, R_{i,1}^* + H_2\left(C_{TA}^*, R_{i,1}^*\right)\left(pk + g_1 \cdot H_1(id_i^*)\right)\right) = g_2 \tag{12}$$

$\mathcal{C}$ verifies $H_1(id_i^*) \stackrel{?}{\in} \{v_1, v_2, \ldots, v_{n_E}\}$. If $H_1(id_i^*) \in \{v_1, v_2, \ldots, v_{n_E}\}$, output "$\perp$". Otherwise, we have that equation (12) holds. Therefore, $\mathcal{C}$ can compute $\frac{g_1}{s+H_1(id_i^*)} = \left(\alpha^* + H_2\left(C_{TA}^*, R_{i,1}^*\right)\right) R_{i,2}^*$ and thus output the array $\left(H_1(id_i^*), \frac{g_1}{s+H_1(id_i^*)}\right)$ as a solution to the $n_E - CAA$ problem, where $H_1(id_i^*) \notin \{v_1, v_2, \ldots, v_{n_E}\}$. And this contradicts the k-CAA assumption that it is a difficult problem.

□

We compare this scheme with existing work in Table 2 in terms of privacy and security. Only the proposed scheme can satisfy all the conditions. Generally speaking, some smart parking, carpooling and ride hailing schemes [1,2,4,8,41] based on location services can protect users' location privacy to a certain extent, but they can still lead to location and route information leakage due to malicious compromise by attackers.

Table 2. Comparison of privacy and security properties.

Scheme	Identity Privacy	Location Privacy	Route Privacy	Non-Repudiation	Anti-Man-in-the-Middle Attack
[1]	✓	×	×	✓	N/A
[2]	✓	×	×	N/A	N/A
[4]	✓	×	×	N/A	N/A
[5]	✓	✓	✓	N/A	N/A
[7]	✓	✓	✓	✓	N/A
[8]	✓	×	×	✓	N/A
[41]	✓	×	×	✓	N/A
[42]	✓	✓	N/A	✓	N/A
[43]	✓	N/A	N/A	✓	✓
[44]	✓	N/A	N/A	✓	✓
Our Scheme	✓	✓	✓	✓	✓

7. Performance Analysis

To instantiate our proposed scheme, we compare the proposed scheme with other existing schemes in terms of computational and communication overheads. The experimental performance verifies the efficiency and effectiveness of our scheme.

7.1. Experiment Setting

The experiments in our scheme were all conducted on a computer (Intel®Core™ i5-3470S CPU @ 2.90 GHz × 2, 3.8 GiB RAM) running Ubuntu 20.04.3 LTS 64-bit OS. We made use of modules such as hashlib and cryptography in Python. We first evaluate the time cost of the exponential operation T_e, hash operation T_h, and bilinear operation T_p, where the time cost of each operation is the average time after running 1000 times. Specifically, the time cost of each operation is $T_e = 0.0431$ ms, $T_h = 0.0293$ ms, $T_p = 4.6691$ ms. Next, we instantiated 100 users on a computer and compared the performance of our scheme with other schemes in terms of computation and communication overhead.

7.2. Computational Overhead

We experimentally evaluate the computational overhead of our scheme in the user registration, signature and signature verification phases and compare it with PiSim [7], SRPP [8], and ASAP [41], as shown in Figure 4.

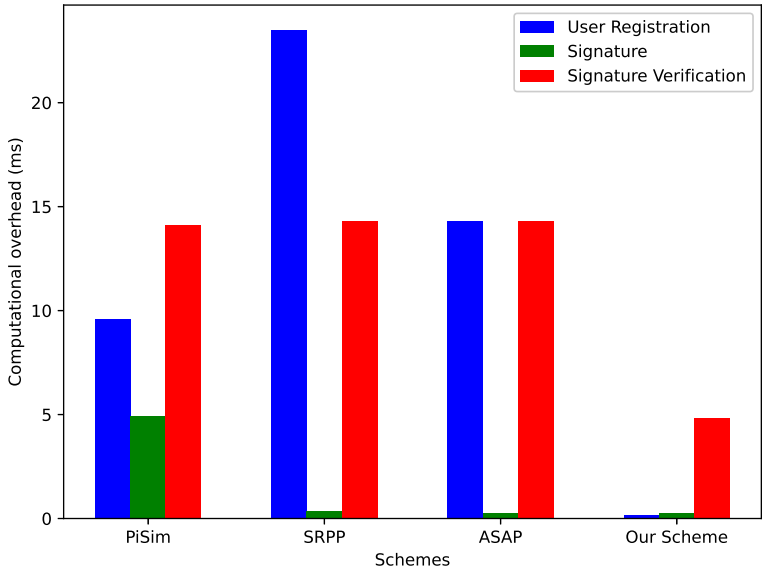

Figure 4. Comparison of computational overhead.

In user registration, we only use exponential and hash operations with low computational overhead, making the computational overhead of this paper only 0.1586 ms, which is much smaller than [7,8,41]. In signature, we use only 5 exponential operations and 2 hash operations, and its computational overhead is 0.2741 ms. Compared with [7,8,41], our scheme has a slight advantage. And in signature verification, although we use bilinear operations with high computational overhead, we can still have some advantages in this paper compared with [7,8,41].

7.3. Communication Overhead

Next, we analyze the communication overhead of the user's location service query during transmission.

In PPCS [30], the user generates a service query $L_q = (u_{id}, \{(x_1, y_1), \ldots, (x_n, y_n), R, C\})$, where u_{id} is the user's identity, $(x_1, y_1), \ldots, (x_n, y_n)$ are the location data, R is the the radius of the user's query scope, C is the service query content. Therefore, the total communication overhead is expressed as $|L_q| = |u_{id}| + |(x_1, y_1)| + \cdots + |(x_n, y_n)| + |R| + |C| \approx 1.52 + 0.0020n$ KBytes.

In RR-DLS [34], the user generates a service query $L_q = (u_{id}, \{(x_1, y_1), \ldots, (x_n, y_n), C_1, \ldots, C_n, V\})$, where C_i is the service query content at location (x_i, y_i), V is the degree of privacy protection. Therefore, the total communication overhead is expressed as $|L_q| = |u_{id}| + |(x_1, y_1)| + \cdots + |(x_n, y_n)| + |C_1| + \cdots + |C_n| + |V| \approx 1.5 + 0.03n$ KBytes.

In DK-A [45], the user generates a service request $R_i = \{name_i, pos_i, req_i\}$ and sends it to a trusted server for encryption. After the server receives n service requests R_i, it saves $\{name_i\}_{i=1}^{n}$ and generates two matrices O, E about the service requests. Finally, it outputs $O \times E$ as the user's service query, where $name_i$ is the user ID, pos_i is the location data, req_i is the service query content. Therefore, the total communication overhead is expressed as $|O \times E| \approx 0.0020n^2$ KBytes.

In our scheme, the user generates a service query $\sigma \leftarrow (E, D_1, D_2, D_3, L_1, L_2, L_3)$, then its total communication overhead is expressed as $|\sigma| = |E| + |D_1| + |D_2| + |D_3| + |L_1| + |L_2| + |L_3| \approx 0.10$ KBytes. Specifically, since the number of occupied bits of $D_1, D_2, D_3, L_1, L_2, L_3$ is fixed, and the number of bits of E is related to the hash function H_3. In the case that H_3 is deterministic, the number of bits of E is also fixed and does not change with the number of users. Therefore, the communication overhead of the service query of the users in our scheme is constant 0.10 KBytes.

The results of the communication overhead comparison for each scheme are shown in Figure 5. Through our analysis, we found that the service queries of [30,34,45] are

constructed based on anonymity sets, which makes their communication overhead increase linearly with the increase of anonymity sets. Although the increase of anonymity set can further improve the security of user's location privacy, its higher communication overhead is not tolerable for us. In contrast, this paper reduces the communication overhead to a constant 0.10 while guaranteeing user privacy security. Obviously, our paper has a greater advantage in terms of communication overhead compared to [30,34,45].

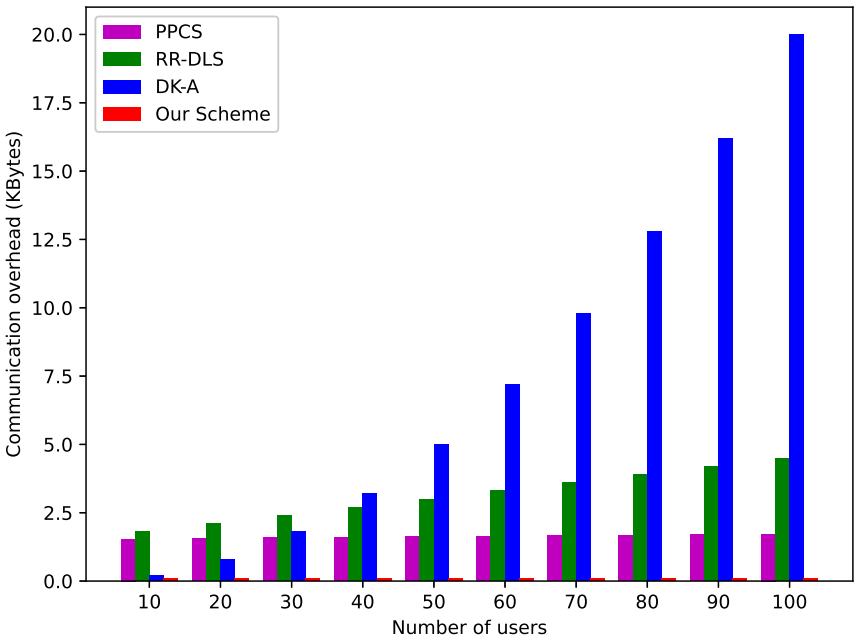

Figure 5. Comparison of communication overhead.

8. Conclusions

To better protect users' privacy and security, this paper proposes a privacy protection scheme for the Internet of Vehicles based on privacy set intersection. Specifically, we propose two privacy-secure protocols: a dual authentication protocol and a service recommendation protocol. The dual authentication protocol based on privacy set intersection has dual security guarantees. One can ensure that both sides of the authenticated communication are secure and trusted, and the other ensures that the session keys established by both sides in the process are secure and reliable. While in the service recommendation protocol, users are blinded to their location information by a pseudorandom function and a one-way hash function, making the user's location information available and invisible. Compared with existing schemes, our scheme is more security, achieving identity privacy, location privacy, routing privacy, non-repudiation, and anti-man-in-the-middle attack. Also, it is experimentally shown that our scheme is significantly better than the existing schemes in terms of computation overhead and communication overhead.

In the future, we will design a more fully functional privacy protection scheme, such as migrating the PSI operation in the service recommendation protocol to the smart contract of the blockchain. Thus, we can avoid the privacy leakage of users due to the excessive authority of RSU.

Author Contributions: Conceptualization, Q.Z. and Z.Z.; methodology, Z.Z.; formal analysis, Q.Z., K.W. and M.C.; writing—original draft preparation, Z.Z.; writing—review and editing, Q.Z. and Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China grant number 2021YFA1000600 and by the National Natural Science Foundation of China grant number 12171114.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Baza, M.; Lasla, N.; Mahmoud, M.M.E.A.; Srivastava, G.; Abdallah, M. B-Ride: Ride Sharing with Privacy-preservation, Trust and Fair Payment Atop Public Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 1214–1229. [CrossRef]
2. Nabil, M.; Sherif, A.; Mahmoud, M.; Alsharif, A.; Abdallah, M. Efficient and Privacy-preserving Ridesharing Organization for Transferable and Non-transferable Services. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1291–1306. [CrossRef]
3. Zhao, Q.; Zuo, C.; Pellegrino, G.; Lin, Z. Geo-locating Drivers: A Study of Sensitive Data Leakage in Ride-hailing Services. In Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–27 February 2019.
4. Yu, H.; Shu, J.; Jia, X.; Zhang, H.; Yu, X. Lpride: Lightweight and Privacy-preserving Ride Matching over Road Networks in Online Ride Hailing Systems. *IEEE Trans. Veh. Technol.* **2019**, *68*, 10418–10428. [CrossRef]
5. Yu, H.; Zhang, H.; Yu, X.; Du, X.; Guizani, M. Pgride: Privacy-preserving Group Ridesharing Matching in Online Ride Hailing Services. *IEEE Internet Things J.* **2021**, *8*, 5722–5735. [CrossRef]
6. Baruah, B.; Dhal, S. An Intelligent Privacy Preserving Vehicle Navigation System. In Proceedings of the 2019 IEEE Region 10 Symposium (TENSYMP), Kolkata, India, 7–9 June 2019; pp. 727–732.
7. Li, M.; Chen, Y.; Zheng, S.; Hu, D.; Lal, C.; Conti, M. Privacy-preserving Navigation Supporting Similar Queries in Vehicular Networks. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1133–1148. [CrossRef]
8. Zhang, Y.; Zhang, L.; Kang, B.; Ma, Y.; Chen, T. Secure and Reliable Parking Protocol Based on Blockchain for Vanets. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 29 March 2021–1 April 2021; pp. 1–6.
9. Wang, L.; Lin, X.; Zima, E.; Ma, C. Towards Airbnb-like Privacy-enhanced Private Parking Spot Sharing Based on Blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2411–2423. [CrossRef]
10. Jiang, S.; Zhu, X.; Wang, L. An Efficient Anonymous Batch Authentication Scheme Based on HMAC for Vanets. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 2193–2204. [CrossRef]
11. Arif, M.; Wang, G.; Bhuiyan, M.; Wang, T.; Chen, J. A Survey on Security Attacks in VANETs: Communication, applications and challenges. *Veh. Commun.* **2019**, *19*, 100179. [CrossRef]
12. Chen, J.; He, K.; Yuan, Q.; Chen, M.; Du, R.; Xiang, Y. Blind Filtering at Third Parties: An Efficient Privacy-preserving Framework for Location-based Services. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2524–2535. [CrossRef]
13. Karim, H.; Rawat, D.B. Tollsonly Please—Homomorphic Encryption for Toll Transponder Privacy in Internet of Vehicles. *IEEE Internet Things J.* **2022**, *9*, 2627–2636. [CrossRef]
14. Li, B.; Liang, R.; Zhou, W.; Yin, H.; Gao, H.; Cai, K. LBS Meets Blockchain: An Efficient Method with Security Preserving Trust in SAGIN. *IEEE Internet Things J.* **2022**, *9*, 5932–5942. [CrossRef]
15. Qureshi, K.N.; Shahzad, L.; Abdelmaboud, A.; Elfadil Eisa, T.A.; Alamri, B.; Javed, I.T.; Al-Dhaqm, A.; Crespi, N. A Blockchain-based Efficient, Secure and Anonymous Conditional Privacy-preserving and Authentication Scheme for the Internet of Vehicles. *Appl. Sci.* **2022**, *12*, 476. [CrossRef]
16. Li, Z.; Alazab, M.; Garg, S.; Hossain, M.S. Priparkrec: Privacy-preserving Decentralized Parking Recommendation Service. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4037–4050. [CrossRef]
17. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Proceedings of CRYPTO 84 on Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1985; Volume 196, pp. 47–53.
18. Gupta, M.; Kumar, R.; Shekhar, S.; Sharma, B.; Patel, R. B.; Jain, S.; Dhaou, I. B.; Iwendi, C. Game Theory-based Authentication Framework to Secure Internet of Vehicles with Blockchain. *Sensors* **2022**, *22*, 5119. [CrossRef]
19. Wu, T.-Y.; Guo, X.; Chen, Y.-C.; Kumari, S.; Chen, C.-M. SGXAP: Sgx-based Authentication Protocol in Iov-enabled Fog Computing. *Symmetry* **2022**, *14*, 1393. [CrossRef]
20. Sikarwar, H.; Das, D. Towards Lightweight Authentication and Batch Verification Scheme in Iov. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 3244–3256. [CrossRef]
21. Zhang, M.; Zhu, B.; Li, Y.; Wang, Y. Tpm-based Conditional Privacy-preserving Authentication Protocol in Vanets. *Symmetry* **2022**, *14*, 1123. [CrossRef]
22. Jan, S.A.; Amin, N.U.; Shuja, J.; Abbas, A.; Maray, M.; Ali, M. SELWAK: A Secure and Efficient Lightweight and Anonymous Authentication and Key Establishment Scheme for Iot Based Vehicular Ad Hoc Networks. *Sensors* **2022**, *22*, 4019. [CrossRef]
23. Zhang, M.; Zhou, J.; Cong, P.; Zhang, G.; Zhuo, C.; Hu, S. LIAS: A Lightweight Incentive Authentication Scheme for Forensic Services in Iov. *IEEE Trans. Autom. Sci. Eng.* **2022**, 1–16. [CrossRef]
24. Jiang, Q.; Zhang, X.; Zhang, N.; Tian, Y.; Ma, X.; Ma, J. Three-factor authentication protocol using physical unclonable function for IoV. *Comput. Commun.* **2021**, *173*, 45–55. [CrossRef]
25. Ahmim, I.; Ghoualmi-Zine, N.; Ahmim, A.; Ahmim, M. Security Analysis on "three-factor Authentication Protocol Using Physical Unclonable Function for Iov". *Int. J. Inf. Secur.* **2022**, *21*, 1019–1026. [CrossRef]

26. Zhao, P.; Huang, Y.; Gao, J.; Xing, L.; Wu, H.; Ma, H. Federated Learning-based Collaborative Authentication Protocol for Shared Data in Social Iov. *IEEE Sens. J.* **2022**, *22*, 7385–7398. [CrossRef]
27. Sweeney, L. K-Anonymity: A Model for Protecting Privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **2002**, *10*, 557–570. [CrossRef]
28. Gruteser, M.; Grunwald, D. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys '03, Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, San Francisco, CA, USA, 5–8 May 2003*; Association for Computing Machinery: New York, NY, USA, 2003; pp. 31–42.
29. Kido, H.; Yanagisawa, Y.; Satoh, T. An Anonymous Communication Technique Using Dummies for Location-Based Services. In Proceedings of the International Conference on Pervasive Services, Santorini, Greece, 11–14 July 2005; pp. 88–97.
30. Sun, G.; Cai, S.; Yu, H.; Maharjan, S.; Chang, V.; Du, X.; Guizani, M. Location Privacy Preservation for Mobile Users in Location-based Services. *IEEE Access* **2019**, *7*, 87425–87438. [CrossRef]
31. Liu, J.; Jiang, X.; Zhang, S.; Wang, H.; Dou, W. FADBM: Frequency-aware Dummy-based Method in Long-term Location Privacy Protection. In Proceedings of the 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), Tianjin, China, 4–6 December 2019; pp. 384–391.
32. Niu, J.; Zhu, X.; Shi, L.; Ma, J. Time-aware Dummy-based Privacy Protection for Continuous LBSs. In Proceedings of the 2019 International Conference on Networking and Network Applications (NaNA), Daegu, Republic of Korea, 10–13 October 2019; pp. 15–20.
33. Ni, L.; Tian, F.; Ni, Q.; Yan, Y.; Zhang, J. An Anonymous Entropy-based Location Privacy Protection Scheme in Mobile Social Networks. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 1–19. [CrossRef]
34. Xu, X.; Chen, H.; Xie, L. A Location Privacy Preservation Method Based on Dummy Locations in Internet of Vehicles. *Appl. Sci.* **2021**, *11*, 4594. [CrossRef]
35. Li, M.; Zhu, L.; Lin, X. Efficient and Privacy-preserving Carpooling Using Blockchain-assisted Vehicular Fog Computing. *IEEE Internet Things J.* **2019**, *6*, 4573–4584. [CrossRef]
36. Wang, D.; Zhang, X. Secure Ride-sharing Services Based on a Consortium Blockchain. *IEEE Internet Things J.* **2021**, *8*, 2976–2991. [CrossRef]
37. Yu, H.; Jia, X.; Zhang, H.; Shu, J. Efficient and Privacy-preserving Ride Matching Using Exact Road Distance in Online Ride Hailing Services. *IEEE Trans. Serv. Comput.* **2022**, *15*, 1841–1854. [CrossRef]
38. Huang, J.; Luo, Y.; Xu, M.; Hu, B.; Long, J. Pshare: Privacy-preserving Ride-sharing System with Minimum-detouring Route. *Appl. Sci.* **2022**, *12*, 842. [CrossRef]
39. Wang, K.; Liu, M.; Wang, J.; Wu, M.; Zhao, F. BBARHS: Blockchain-Based Anonymous Ride-Hailing Scheme for Autonomous Taxi Network. *Secur. Commun. Netw.* **2022**, *2022*, 8296608. [CrossRef]
40. Ma, H.; Ping, Y.; Zhang, Y. Privacy-Preserving Cross-Zone Ride-Matching for Online Ride-Hailing Service. *Math. Probl. Eng.* **2022**, *2022*, 5040766. [CrossRef]
41. Zhu, L.; Li, M.; Zhang, Z.; Qin, Z. ASAP: An Anonymous Smart-parking and Payment Scheme in Vehicular Networks. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 703–715. [CrossRef]
42. Kou, B.; Cao, S.; Lv, J. A Privacy Protection Scheme for Carpooling Service Using Fog Computing. *J. Phys. Conf. Ser.* **2020**, *1601*, 032019. [CrossRef]
43. Zhou, X.; He, D.; Khan, M.K.; Wu, W.; Choo, K.-K.R. An Efficient Blockchain-based Conditional Privacy-preserving Authentication Protocol for Vanets. *IEEE Trans. Veh. Technol.* **2022**, 1–12. [CrossRef]
44. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K.-K. R. BCPPA: A Blockchain-based Conditional Privacy-preserving Authentication Protocol for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 7408–7420. [CrossRef]
45. Xing, L.; Jia, X.; Gao, J.; Wu, H. A Location Privacy Protection Algorithm Based on Double K-anonymity in the Social Internet of Vehicles. *IEEE Commun. Lett.* **2021**, *25*, 3199–3203. [CrossRef]