SPIR: A Secure and Privacy-Preserving Incentive Scheme for Reliable Real-Time Map Updates

Chengzhe Lai, *Member, IEEE*, Min Zhang, Jie Cao, and Dong Zheng

***Abstract*—The high-precision maps can provide additional information on roads and conditions, which plays an important role in autonomous vehicles (AVs) navigation. Compared with the existing map update methods, the real-time map updates based on crowdsensing have lower cost and higher accuracy. However, in the process of map update, the map service platform (MSP) cannot recruit enough vehicle users to obtain the sensing data due to a lack of incentive mechanism. Therefore, how to motivate more vehicle users to provide high-quality sensing data is the key for real-time map updates. In this article, we propose a secure and privacy-preserving incentive scheme for reliable real-time map updates, named SPIR. Specifically, under the condition of limited service platform budget and limited vehicle user's ability, an effective incentive mechanism based on reverse auction is presented, which can solve two core problems: i.e., payment control for MSP and completion quality for vehicle users. Meanwhile, a credit management and payment system based on the blockchain technique are designed. In addition, the partially blind signature technique is applied to guarantee the security of the incentive mechanism and protect the privacy of vehicle users. Both theoretical analysis and simulation results indicate that the proposed SPIR achieves near-optimal benefits, which can provide the fair reward for vehicle users and reasonable budget for the MSP. In the real-time map update services, SPIR can guarantee the computational efficiency and data reliability.**

***Index Terms*—Autonomous vehicles (AVs), blockchain, incentive, Internet of Vehicles, privacy, real-time map updates.**

I. Introduction

AUTONOMOUS vehicles (AVs) combine various sensors to perceive their surroundings, such as radar, computer vision, Lidar, sonar, GPS, odometry, and inertial measurement units. Advanced control systems interpret sensory information to identify appropriate navigation paths as well as obstacles. Autonomous driving has been an emerging area to achieve the ultimate in automobile safety and comfort, which will greatly change our lives [1]–[3]. Without human driving efforts, AVs must access large amounts of data from the map service platform (MSP) to make real-time control decisions for efficiency and safety [4]. As a supplement to the existing sensors of AVs, the vehicle map provides more reliable perception ability for AVs. The vehicle map plays an important role in the location, navigation, and control of the AVs [5], including intelligent public transport [6], real-time monitoring of traffic timetables by users, urban street information from FixMyStreet [7], and even critical information for people in case of accidents [8]. Maps can also be used to compare with real sensor data (e.g., real-time lidar and image data) on the ground to perform vehicle control operations along a given route [9].

Although digital maps based on satellite images have been widely used, they cannot accurately reflect the latest map data. Unlike traditional digital maps, vehicle maps need to be constantly updated. In order to accurately and effectively reflect the dynamics of maps, there are some schemes that have been proposed in recent years [5], [10], [11]. Particularly, mobile crowdsensing (MCS), which refers to the large-scale sensing work carried out by the participants, has attracted much attention [12]–[15]. Nowadays, vehicles have more abundant sensors, more powerful storage, and communication capabilities. Therefore, by recruiting vehicles as participants, there are many novel applications of MCS, including advertisement dissemination [16], [17], real-time traffic monitoring [18], parking service [19], and transportation data collection [20]. Vehicle map update can also be achieved through MCS, in which vehicle users upload their sensing data to the MSP.

In the process of MCS-based map updates, the insufficient number of vehicle users will seriously affect the realization of the vehicle map update since the MSP cannot obtain enough sensing data. Vehicle users may not be willing to spend their limited resources, such as battery energy, computing capability, and available network bandwidth, to assist map update without compensation. Consequently, how to motivate more vehicle users to provide high-quality sensing data is the key for real-time map updates. In addition, security and privacy concerns [21]–[25] are also a critical factor affecting the development of AV related applications. Karnouskos and Kerschbaum [26] examined the privacy and data integrity issues in the operation of fleets of cooperating, AVs, in which indicates that a series of security and privacy challenges should be first solved before the real-time map updates come into service.

In view of the above problems, this article proposes a secure and privacy-preserving incentive scheme for reliable real-time

Manuscript received August 30, 2019; revised October 11, 2019 and October 28, 2019; accepted November 6, 2019. Date of publication November 12, 2019; date of current version January 10, 2020. This work was supported in part by the National Natural Science Foundation of China Research under Grant 61872293 and Grant 61772418, in part by the National Key Research and Development Program of China under Grant 2017YFB0802002, in part by the Innovation Ability Support Program in the Shaanxi Province of China under Grant 2017KJXX-47, and in part by the Communication Soft Science Research Project of Ministry of Industry and Information Technology under Grant 2019R31. *(Corresponding author: Chengzhe Lai.)*

The authors are with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China (e-mail: lcz.xidian@gmail.com).

Digital Object Identifier 10.1109/JIOT.2019.2953188

map updates, named SPIR. Under the limited MSP budget and limited vehicle user's ability, SPIR can guarantee vehicle users' voluntary participation and real bidding, and make the MSP obtain satisfactory data quantity and quality. In addition, SPIR can achieve anonymity and conditional privacy by using the pseudonym management mechanism. Specifically, the contributions of this article are as follows.

1) In order to motivate more vehicle users to provide high-quality sensing data for real-time map update, we design an effective incentive scheme based on reverse auction, which can achieve payment control for the MSP and ensure completion quality for vehicle users. Meanwhile, the blockchain-based credit management system can guide vehicle users to attach importance to the quality of current tasks and maintain good activity.
2) Based on the partially blind signature technique, a secure pseudonym management mechanism is proposed to guarantee the security of the incentive mechanism and protect the privacy of vehicle users. Moreover, a blockchain-based payment system is equipped to ensure the secure distribution of rewards.
3) We make theoretical analysis and conduct extensive experiments to evaluate the performance of our proposed scheme. The results indicate that the proposed SPIR can guarantee the maximization of user revenue and enable the MSP to obtain adequate data. In the real-time map update services, SPIR can guarantee the computational efficiency and data reliability.

The remainder of this article is organized as follows. Related work is discussed in Section II. In Section III, we introduce our system model, incentive model, and design goals. Then, we present the secure and privacy-preserving incentive scheme in Section IV, followed by security analysis and performance evaluation in Sections V and VI, respectively. Finally, we draw our conclusion in Section VII.

II. Related Work

Incentive Mechanism: After recognizing the importance of user participation for a huge list of tasks in a variety of applications, many researchers began to design proper incentive mechanisms. A lot of valuable research works have gradually emerged over the years. Specifically, designing reasonable incentives to motivate enough users and provide high-quality data for MCS has been widely studied in recent years [27]–[30]. In MCS, there are different incentives according to the different application scenarios. Generally speaking, from the way of return, it can be divided into monetary incentives and nonmonetary incentives. Monetary incentive mainly encourages users to participate through payment. The most important monetary incentive is the auction mechanism.

As the earliest research article on auction-based incentive mechanism of MCS, Danezis *et al.* [31] designed a second price auction mechanism to encourage users to participate. However, the auction mechanism does not take into account the interests of users. Goldberg *et al.* [32] investigated two kinds of untruthful auctions, i.e., the optimal multiprice auction and the optimal single-price auction, and the relationship between their earnings has been established. Lee and Hoh [33] devised a dynamic pricing incentive mechanism based on reverse auction. In this mechanism, users sell data to service providers according to their own quotations. However, the auction mechanism is not real. That is to say, the author does not consider that users are selfish. Users may increase their earnings by making false offers. There is also a kind of incentive mechanisms based on the reverse auction. Zhang *et al.* [34] considered how to design an incentive mechanism under the premise of limited platform budget. Lin *et al.* [35] studied how to motivate participants to participate in the long term so that servers have stable data sources. However, the above work does not take into account both limited platform budget and limited user's ability. The fixed-price auction is proposed by [36], and Zhou *et al.* [37] extended it to reverse auction, which is the fixed-price reverse auction scheme and considers two factors above at the same time. Nevertheless, it does not consider the data quality problem. Pouryazdan *et al.* [38] proposed a framework to motivate users through a subgame perfect equilibrium (SPE). It is worth noting that the risk of privacy leakage is also critical since it may affect the enthusiasm of users. Therefore, payment control, completion quality and privacy issues mentioned above are the challenges in designing incentive mechanisms for reliable real-time map updates, which urgently needs to be solved in the current research work. In this article, we will adopt a real auction scheme to design our incentive mechanism, and maximize the benefits of the MSP.

Pseudonym Scheme: In recent years, lots of research works have emerged, proposing pseudonym solutions tailored to IoV. SECSPP [39] is a noninteractive ID-based scheme for V2V. It establishes a blind signature scheme and a trust relationship for V2I communication through the user's IDs. Authorized users can interact with roadside units and remain anonymous throughout the process without revealing any information. In this scheme, partial blind signature is used, and users and servers can negotiate public messages. Compared with blind signature, it enhances the controllability of signature on the premise of ensuring user privacy. Recently, Ali *et al.* [40] proposed SPATA, in which pseudonymity generation requires the participation of multiple certification entities in order to avoid the connection between real identity and pseudonymity. A single authority cannot reveal the known identity of the vehicle. The pseudonym of malicious vehicles is revoked and broadcasted. The size of certificate revocation list (CRL) will not increase. Therefore, the revoked pseudonym cannot be verified. Gao *et al.* [41] proposed an effective authentication scheme, which combines pseudonym with ID-based ring signature. Investigators can obtain pseudonyms from roadside units to reveal the true identity of the offender. Therefore, in their scheme, the real identity of the vehicle can be obtained through roadside units and trust authority. The pseudonym scheme in this article is also accomplished by many authorities, but it only needs a trace manager (TM) to complete the tracking of vehicle users. Moreover, TM does not participate in the whole process of signature issuance and verification. It only receives pseudonym from the server to track the identity of the user. Petit *et al.* [42] give an extensive overview

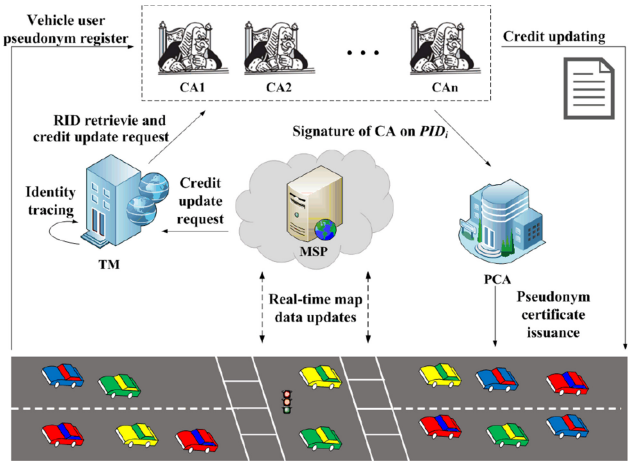

Fig. 1. System model.

and categorization of the state-of-the-art in this research area. Boualouache *et al.* [43] also presented a comprehensive survey and classification of pseudonym changing strategies. According to [42], the existing pseudonym schemes can be categorized into public key-based, identity-based cryptography, group signatures, and symmetric authentication.

III. System Model, Incentive Model, and Design Goals

In this section, we formalize the system model, the MCS-based incentive model, and identify our design goals.

A. System Model

Our system mainly consists of five entities: 1) the certificate authority (CA); 2) the pseudonym CA (PCA); 3) the TM, 4) the MSP; and 5) vehicle users, as shown in Fig. 1.

1) Certificate Authority: CA is mainly responsible for verifying the legitimacy of the vehicle user's identity and signing pseudonyms submitted by vehicle users, while CA does not know the content of the signed pseudonyms. Meanwhile, CA maintains a credit account for each vehicle user, in which the real identity of each vehicle user and its corresponding credit value is recorded. In our model, we employ multiple CAs to manage vehicle users located in different domains.

2) Pseudonym Certificate Authority: PCA is responsible for verifying the validity of the signature of the pseudonym submitted by the vehicle user. If the signature is valid, a pseudonym certificate is issued to the vehicle user; otherwise, the pseudonym is refused to be authenticated.

3) Trace Manager: TM can trace vehicle users, while it does not participate in the whole process of signature issuance and verification. Once TM verifies the activity of some vehicle user, the vehicle user's real identity can be directly recovered from the pseudonym and notified to CA. Then, CA calculates and updates the vehicle user's credit.

4) Vehicle User and Map Service Platform: In our system, vehicle users are responsible for data collection and provide reliable data to MSP.

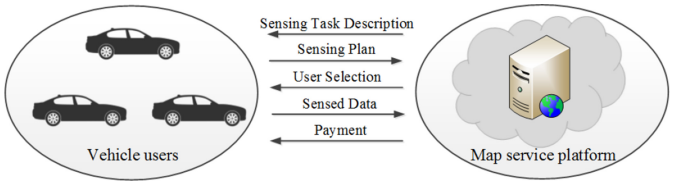

Fig. 2. MCS-based incentive model.

B. MCS-Based Incentive Model

Our MCS-based incentive model is presented based on [44], which consists of the MSP and n vehicle users, i.e., $V = (v_1, v_2, \ldots, v_n)$. In this model, the MSP acts as a buyer and the vehicle user acts as a seller. The MSP is interested in information, such as road conditions and vehicle users can collect this type of data and bid for it. According to the vehicle user's quotation, the MSP decides which vehicle user's data to buy. The MCS-based incentive model is illustrated in Fig. 2 and the workflow is as follows.

1) The MSP publishes required data types to vehicle users.
2) All vehicle users and MSP perform the auction process. Each vehicle user provides the MSP with data quotation $\overline{b}_i = <\overline{c}_i, \overline{q}_i>$. $\overline{c}_i$ represents the claimed unit cost of the MSP provided by the vehicle user v_i, and $\overline{q}_i$ represents the maximum amount of data that vehicle user v_i claims to be able to collect. We record the quotations of all vehicle users as $\overline{b} = (\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_n)$.
3) MSP decides the winner set $W(W \subseteq V)$ of the auction according to its own budget and vehicle user's quotation. MSP calculates the rewards f_i for vehicle user and the amount of data d_i that vehicle user is required to provide. We mark the reward of MSP to all vehicle users as $f = (f_1, f_2, \ldots, f_n)$, and the amount of data that all vehicle users need to provide as $d = (d_1, d_2, \ldots, d_n)$.
4) The winner provides data that fulfills the requirements of the MSP. After acceptance of the MSP, the vehicle user will be rewarded accordingly.

C. Design Goals

Our design goal is to design an SPIR. Specifically, the following three objectives should be attained.

1) *The Proposed Scheme Should Provide Effective and Fair Incentive:* Under the condition of limited vehicle user's ability and limited budget of the MSP, the proposed scheme should ensure that vehicle users participate voluntarily and bid authentically; according to the actual situation of the task, MSP should be able to control the quality of the selected vehicle users and obtain better benefits. Unqualified vehicle users shall not be able to participate in the future task and obtain high rewards.
2) *The Proposed Scheme Should Be Secure and Privacy-Preserving:* In the process of incentive, the secure pseudonym management mechanism should be proposed to guarantee the security of the incentive mechanism and

protect the privacy of the vehicle users. Moreover, a payment system should be equipped to ensure the secure distribution of rewards.

3) *The Proposed Scheme Should Ensure Reliability of Map Update:* In the process of map update, the proposed scheme should guarantee the data reliability and computational efficiency. In other words, the MSP should obtain satisfactory and reliable data. In addition, the incentive scheme should enable vehicle users to attach importance to the quality of current tasks and improve the service quality.

TABLE I
NOTATIONS

Symbol	Explanation
v_i	The vehicle user
K_{CA-V}	The shared key between CA and v_i
K_{MSP-TM}	The shared key between MSP and TM
Pub_v, Pri_v	Public key/secret key of v_i
Pub_{MSP}, Pri_{MSP}	Public key/secret key of MSP
e_{CA}, d_{CA}	Public key/secret key of CA
Pub_{TM}, Pri_{TM}	Public key/secret key of TM
$Info_{vc}$	Public information negotiated between CA and v_i
RID	The real identity of v_i
PID	The pseudonym of v_i
$pcert_i$	Pseudonym certificate

IV. Proposed Scheme

In this section, we first recall the basic building blocks used in our proposed scheme and give an overview of this scheme. Then, our SPIR is presented.

A. Randomized RSA-Based Partially Blind Signature

In this section, we briefly recall the basic building blocks used in our proposed scheme, i.e., randomized RSA-based partially blind signature [45], which includes five steps.

Step 1 (Initialization): At the beginning, the signer randomly selects two large prime numbers p and q, and then calculates $n = pq$ and $\varphi(n) = (p-1)(q-1)$. The signer randomly selects two integers e and d such that $e \cdot d \equiv 1 \bmod \varphi(n)$. Next, the signer publishes (e, n) and one-way hash function H. The public key of the signer is (e, n) and its private key is (p, q, d).

Step 2 (Blinding): The user chooses a message m to be signed "blindly", and prepares a string a negotiated and agreed by the user and the signer, in which a is a common information containing an expiration date and other optional items. The user sends string a to the signer. After verifying a, the signer randomly chooses $x \in Z_n^*$ and calculates $y = x^e \bmod n$. The signer sends y to the user. After receiving y, the user randomly chooses $u \in Z_n^*$ and the blind factor $r \in Z_n^*$. The user computes the blind message $\alpha = r^e u H(m \| u^e y) \bmod n$, and α is sent to the signer.

Step 3 (Signing): After receiving α, the signer calculates the blind signature $t = ((\alpha x)^{da})^{-1} \bmod n$, where the message (αx) to be signed is determined by both the user and the signer. The signer sends x, t to the user.

Step 4 (Unblinding): The user computes $c = ux \bmod n$, where x is the signer's contribution and u is the user's contribution. c is determined by both the user and the signer. The user calculates $s = r^a t \bmod n$ to remove the blind factor r from the blind signature t. The tuple (s, c, a) is the signature of the signer on message m.

Step 5 (Verifying): To verify the signature (s, c, a) of the message m, one can examine if $s^e (H(m \| c^e) c)^a \equiv 1 \bmod n$.

B. Overview

In order to provide the effective real-time vehicle map updates, a secure and privacy-preserving incentive scheme is desirable. In our scheme, the MSP first publishes the type of data it needs to vehicle users. Then, vehicle users can collect this type of data and bid for it. The MSP can decide the winner of the auction according to its own budget and vehicle user's quotation. Finally, the successful bidder provides data that meets the requirements of the MSP. After acceptance of the MSP, vehicle users will be rewarded accordingly. Specifically, our scheme involves a secure payment system based on blockchain for securely paying vehicle users. In order to protect the vehicle user's identity information, the pseudonym mechanism is used in this process. Meanwhile, the TM can conditionally recover the real identity of malicious vehicle users from pseudonyms, and further notify the CA. By equipped with a credit management system based on blockchain, the CA can deduct credit value from the malicious vehicle user's account and update the latest information to the blockchain that shared by all CAs. When these vehicle users want to register with the CA for pseudonym next time, the CA checks the vehicle user's credit account. If credit value of this user has fallen below a certain threshold, the CA refuses his registration request. The proposed scheme consists of pseudonym management mechanism, data report and reward distribution, and reward payment.

C. Pseudonym Management Mechanism

The MSP publishes the type of data it needs to vehicle users, and vehicle users can collect this type of data. The vehicle user can decide whether accept the task j ($j = 1, 2, \ldots, M$) by evaluating its cost and profit. Vehicle users use pseudonym PID to communicate with MSP and apply for the task j. After the MSP receives the request, the validity of PID is verified by the pseudonym certificate issued by the PCA. If it is invalid, the MSP rejects the request; otherwise, the MSP accepts the application.

During the whole process of incentive, a pseudonym management mechanism is equipped to provide anonymity and conditional privacy of vehicle users. The proposed pseudonym management mechanism consists of three steps: 1) vehicle user pseudonym register; 2) pseudonym certificate issuance; and 3) identity tracer and credit update, described as follows. The notations is shown in Table I.

Step 1 (Vehicle User Pseudonym Register): As shown in Fig. 3, the vehicle user generates a *Pseudonym Register Request* message combined with encrypted real identity (RID) and the number of pseudonyms applied by vehicle user (N) by using K_{CA-V}, i.e., $E_{K_{CA-V}}(\text{RID}||N)$. Then, the vehicle user generates $\text{Sign}_{\text{Pri}_v}[E_{K_{CA-V}}(\text{RID}||N)]$ and sends them to CA.

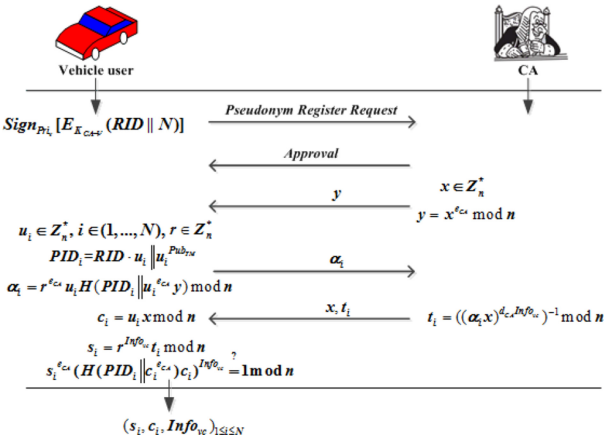

Fig. 3. Vehicle user pseudonym register.

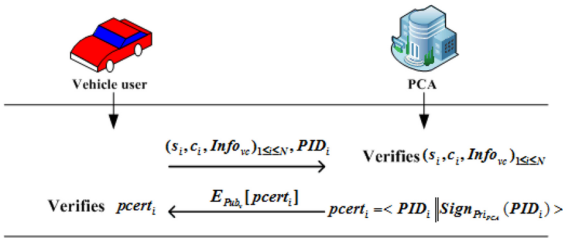

Fig. 4. Pseudonym certificate issuance.

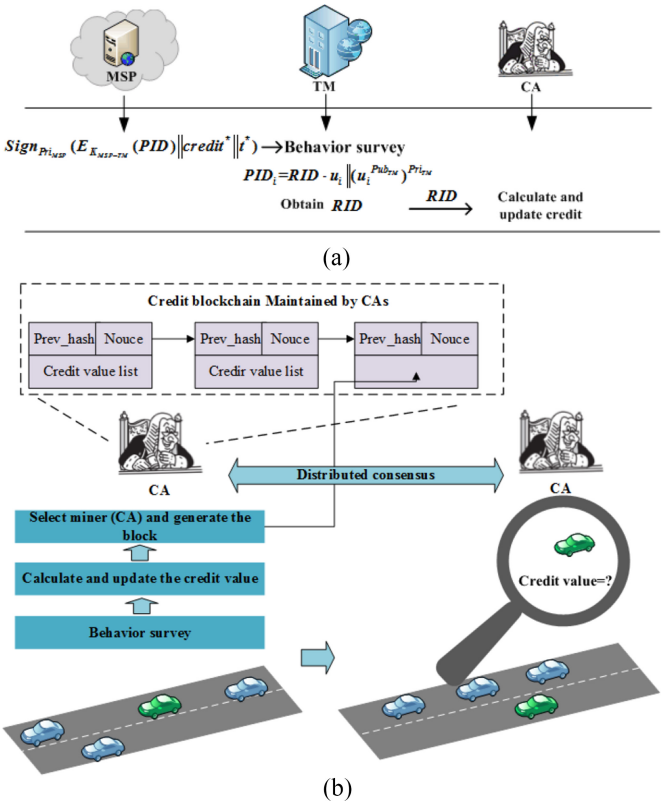

Fig. 5. Identity tracing and credit updating. (a) Identity tracing. (b) Credit updating.

Upon CA receives the message, it uses Pub_v to verify the validity of the signature and determines whether RID is valid. If it is invalid, the register request is rejected. Otherwise, CA sends *Approval* message to the vehicle user. After the vehicle user receives the message, it prepares an Info_{vc} negotiated and agreed by vehicle user and CA, in which contains an expiration date and other optional items. The vehicle user sends encrypted Info_{vc} to CA.

After verifying the Info_{vc}, CA randomly chooses $x \in Z_n^*$ and calculates $y = x^{e_{CA}} \bmod n$; then CA sends y to the vehicle user. When receiving y, the vehicle user randomly chooses $u_i \in Z_n^*$, $i \in (1, \ldots, N)$ and the blind factor $r \in Z_n^*$. The vehicle user constructs $\text{PID}_i = \text{RID} \cdot u_i \| u_i^{\text{Pub}_{\text{TM}}}$ and computes the blind message $\alpha_i = r^{e_{CA}} u_i H(\text{PID}_i \| u_i^{e_{CA}} y) \bmod n$; then α_i is sent to CA. After receiving α_i, CA calculates the blind signature $t_i = ((\alpha_i x)^{d_{CA}} \text{Info}_{vc})^{-1} \bmod n$, where the message $(\alpha_i x)$ to be signed is determined by both the vehicle user and CA. Next, CA sends x, t_i to the vehicle user, and then vehicle user computes $c_i = u_i x \bmod n$, where x is CA's contribution and u_i is the vehicle user's contribution. c_i is determined by both the vehicle user and CA. The vehicle user calculates $s_i = r^{\text{Info}_{vc}} t_i \bmod n$ to remove the blind factor r from the blind signature t_i. The tuple $(s_i, c_i, \text{Info}_{vc})$ is the signature of CA on PID_i. The vehicle user can verify the signature $(s_i, c_i, \text{Info}_{vc})$ of PID_i by examining if $s_i^{e_{CA}} (H(\text{PID}_i \| c_i^{e_{CA}}) c_i)^{\text{Info}_{vc}} \equiv 1 \bmod n$. If it is valid, the vehicle user accepts the CA's signature of the pseudonym. After N interactions, the vehicle user can obtain N pseudonym signatures $(s_i, c_i, \text{Info}_{vc})_{1 \le i \le N}$.

Step 2 (Pseudonym Certificate Issuance): As shown in Fig. 4, the vehicle user sends $(s_i, c_i, \text{Info}_{vc})_{1 \le i \le N}$ with PID_i to PCA and PCA verifies $(s_i, c_i, \text{Info}_{vc})_{1 \le i \le N}$. If these signatures are valid, it proves that the pseudonym has been certified by CA. PCA uses Pub_v to encrypt and send pseudonym certificate $pcert_i$ to the vehicle user. After the vehicle user receives the message, he decrypts it with Pri_v and obtains $pcert_i$. The vehicle user verifies the validity of certificate $pcert_i$. If the verification is valid, it means that the pseudonym has been authenticated by PCA, and $pcert_i$ can be used for future secure communication.

Step 3 (Identity Tracing and Credit Updating): A blockchain-based credit management system is designed to update the credit. As shown in Fig. 5(a), if the TM receives a *Credit Update Request* message with $\text{Sign}_{\text{Pri}_{\text{MSP}}}[E_{K_{\text{MSP-TM}}}(\text{PID}) \| \text{credit}^* \| t^*]$ from the MSP, where credit* denotes the credit value (+or−) that MSP uses to reward or punish vehicle users, and t^* is the current time. TM uses Pri_{TM} to decrypt $u_i^{\text{Pub}_{\text{TM}}}$ after verifying MSP's signature and investigating the behavior of vehicle users (malicious or goodwill). Then, the TM obtains the random number u_i and further obtains RID of vehicle users. Finally, TM securely sends RID and $\text{Sign}_{\text{Pri}_{\text{MSP}}}[E_{K_{\text{MSP-TM}}}(\text{PID}) \| \text{credit}^* \| t^*]$ to CAs. CAs verify the signature of MSP and calculate the vehicle user's new reputation value credit if verification is successful. As shown in Fig. 5(b), with the new reputation value for a vehicle, CAs can pack the result into a "block". Then, each CA will try to add their "blocks" to the trust blockchain by "mining." The trust blockchain is maintained by all the CAs via consensus mechanism.

D. Data Report and Reward Distribution

All vehicle users and MSP enter the auction process for real map data acquisition. Each vehicle user provides MSP with its quotation for the data. According to the reverse auction algorithm, the MSP decides the winner of the auction, and calculates the reward f and the amount of data d that vehicle users need to provide. After receiving f and d, the successful bidder, i.e., vehicle user, immediately carries on the corresponding sensing activities according to the requirements of MSP. The vehicle user encrypts the sensing data with the public key of MSP Pub_{MSP}. Subsequently, vehicle users also communicate with MSP using the pseudonym PID to send sensing data. The mathematical model and algorithm of reverse auction-based incentive in detail are described as follows.

1) Mathematical Model: We use reverse auction with budget constraints [37] to model our incentive scenario. Auctions consist of auctioneers and bidders. The bidder bids and the auctioneer sells the auctioned goods. Compared with auctions, reverse auctions only exchange the roles of buyers and sellers, that is to say, reverse auction is the sale of goods by bidders and bid by the auctioneer.

Definition 1 (Reverse Auction With Budget Restriction): In reverse auction with budget restriction, the MSP acts as an auctioneer and the vehicle user acts as a bidder. The MSP uses a limited budget to buy data provided by vehicle users.

For the convenience of the following description, we set the MSP's budget as R. Let the true quotation of all vehicle users as $b = (b_1, b_2, \ldots, b_n)$, in which $b_i = <c_i, q_i>$ is the true quotation for vehicle user v_i, where c_i represents the true unit cost of data collected by vehicle user v_i, and q_i represents the largest amount of data that vehicle user v_i can actually collect. We assume that vehicle user v_i can provide any number of data in $[0, q_i]$ intervals, and the unit cost of a vehicle user collecting different amounts of data is an approximate constant. The profit obtained by vehicle users participating in the auction is determined by the auction rules and their own quotations. The expected profit of the vehicle user determines whether he participates in the auction or not and the strategy he adopts in the auction. The following definition gives the calculation method of vehicle user's revenue.

Definition 2 (Vehicle User's Revenue): If v_i is the winner, the MSP will reward him f_i in return. Otherwise, he cannot obtain any rewards, and he does not need to collect any data. The revenue u_i of v_i is given by the following formula:

$$u_i = \begin{cases} f_i - c_i d_i, & v_i \in W, d_i \le q_i \\ -\infty, & v_i \in W, d_i > q_i \\ 0, & v_i \notin W. \end{cases}$$

As we can see, the most data collected by vehicle users is a fixed value. Under no circumstances can he provide data higher than this fixed value, otherwise his earnings will be $-\infty$. In this scheme, we want MSP to obtain as much data as possible. The following definition gives the calculation method of the MSP's revenue.

Definition 3 (The MSP's Revenue): Given the amount of data $d = (d_1, d_2, \ldots, d_n)$ that all vehicle users need to collect and the winner user set W, the revenue u_0 of the MSP is the sum of the amount of data provided by all winners

$$u_0 = \sum_{i:w_i \in W} d_i.$$

Definition 4 (Credit Factor): Credit value L_i can only be accumulated in the current month and cleared in the next month. Credit factor is a coefficient that represents the vehicle user's credit degree according to the credit value of the vehicle user who recently participated in map updating. In this article, the normalized tangent function [46] is chosen as the function of mapping the nearest credit value to the credit factor

$$\varepsilon_i = \frac{\arctan(L_i - \rho) + \arctan \rho}{\pi/2 + \arctan \rho}.$$

Definition 5 (History Factor): In this article, we introduce a variable of historical data reliability H_{ik}, which represents the data credibility of user v_i before completing the task for the kth. When user v_i completes the task on the kth time, $h_{ik} = 1$; otherwise $h_{ik} = 0$. After the kth task, the data reliability of the vehicle user is calculated as follows:

$$H_i = \theta H_{ik} + (1 - \theta) h_{ik}$$

where the parameter θ is called the history factor, and the range of the value of θ is $[0, 1]$.

Definition 6 (Data Reliability): User data credibility based on credit value reflects two factors of credit factor and user data credibility in the past. It is expressed in U and the calculation method is as follows:

$$U_i = \varepsilon_i * H_i.$$

Setting the user data credibility threshold U based on credit value can determine whether user v_i is allowed to perform tasks, such as

$$\begin{cases} U_i \ge U, & \text{Trust} \\ U_i \le U, & \text{Distrust.} \end{cases}$$

2) Reverse Auction-Based Incentive: In reverse auction-based incentive, all vehicle users are randomly divided into two parts. These two parts estimate each other's settlement price. We introduce credibility into this process. Credit can effectively adjust the credit factor of the vehicle users and encourage them to maintain a high degree of participation. It makes vehicle users with low reputation unable to have high data credibility, and avoids the possibility of high data credibility due to the small number of tasks. Data credibility can improve the impact of the results of the last task completion and make vehicle users pay more attention to the quality of completion.

The detailed algorithm of reverse auction-based incentive is given by taking the user set V as an example. In Algorithm 1, we use vehicle user quotation b on vehicle user set V, the MSP budget R and data reliability U as input. The output of the algorithm is the reward f of the MSP for all vehicle users and the amount of data d that all vehicle users need to collect. Algorithm 1 effectively solves the problem of payment control, and specific steps of Algorithm 1 are as follows:

Step 1: The MSP divides the user set V randomly into two user subsets T and Y, and distributes the budget equally into two parts. Then all vehicle users submit their quotations.

Algorithm 1 Reverse Auction-Based Incentive

Input: V, b, R, U;

Output: f, d;

1: The MSP randomly divides the user set V into two subsets T and Y, and then all vehicle users submit their respective quotations;
2: $Q_T \leftarrow OOA(T, R/2), Q_Y \leftarrow OOA(Y, R/2)$;
3: $FRA(T, R/2, UQ_Y), FRA(Y, R/2, UQ_T)$;
4: Collecting the outputs of the two subsets to get f and d;
5: **return** $\{f, d\}$;

Step 2: OOA algorithm is used to calculate the estimated values Q_T and Q_Y of the optimal auction data on user subset T and Y.

Step 3: Using UQ_Y as the estimation value of the data quantity obtained by the optimal auction on vehicle user subset T and UQ_T as the estimation value of the data quantity obtained by the optimal auction on vehicle user subset Y.

Step 4: Using the FPA algorithm, reverse auctions with a fixed price and budget constraints are carried out on vehicle user subsets T and Y, respectively.

Step 5: The MSP aggregates the results of auctions on vehicle user subsets T and Y, decides which vehicle user services to buy, and calculates f and d.

E. Reward Payment

The traditional banking model achieves a certain degree of privacy by restricting the access to a trusted third party. In SPIR, a blockchain-based payment system is equipped to pay rewards, which publishes all transactions publicly, while still protect privacy through anonymity. SPIR utilizes vehicle user's public key as the their pseudonym and the address is the hash value of the vehicle user's public key [47]. Each vehicle user has a private key and a public key. Private key is used for signing the transactions and public key is used for verifying signatures of transactions.

If the MSP wants to pay a vehicle user f, it makes a transaction $T_x = (T_y, \mathrm{Pub}_v, f, t, \mathrm{Sign}_{\mathrm{Pri}_{\mathrm{MSP}}}(T_y, \mathrm{Pub}_v, f, t))$, where t is the lock time and T_y represents the previous transaction. Its value is at least f, and there is no duplicate payment. If the signature is correct, the transaction is valid. This system uses input-script and output-script to define the transaction flexibly. Table II illustrates a standard transaction. In-script denotes the signature of MSP. Out-script is a verification statement with a value of reward f. The lock time t is a task deadline.

V. Security Analysis

In this section, we analyze the security properties of the proposed SPIR scheme. In particular, following the security and privacy preservation goals discussed earlier, our analysis mainly focuses on how the proposed SPIR scheme can provide secure pseudonym management.

TABLE II
Transaction T_x

T_x(in: T_y)
In-script: $Sign_{Pri_{MSP}}(T_y, Pub_v, f, t)$
Out-script:$(T_y, Pub_v, f, t, Sign_{Pri_{MSP}}(T_y, Pub_v, f, t))$
$Ver_v(T_y, Pub_v, f, t, Sign_{Pri_{MSP}}(T_y, Pub_v, f, t))$
Value: f
Lock time: t

A. Proposed SPIR Scheme Can Provide Secure Pseudonym Management

The SPIR scheme is proposed based on the randomized RSA-based partially blind signature, and the security of pseudonym management mechanism, including blindness, unforgeability has been proved in [45].

1) Correctness: The correction of the proposed pseudonym management mechanism can hold based on the following equation.

Proof:

$$
\begin{aligned}
& s_i^{e_{CA}} \left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}} \\
& \quad \equiv \left(r^{\mathrm{Info}_{vc}} t_i\right)^{e_{CA}} \left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}} \\
& \quad \equiv \left(r^{\mathrm{Info}_{vc}} \left((\alpha_i x)^{d_{CA}\mathrm{Info}_{vc}}\right)^{-1}\right)^{e_{CA}} \left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}} \\
& \quad \equiv r^{\mathrm{Info}_{vc}} \left((\alpha_i x)^{\mathrm{Info}_{vc}}\right)^{-1} \left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}} \\
& \quad \equiv r^{\mathrm{Info}_{vc}} \left(\left(r^{e_{CA}} u_i H\left(\mathrm{PID}_i \| u_i^{e_{CA}} y\right) x\right)^{\mathrm{Info}_{vc}}\right)^{-1} \\
& \qquad \times \left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}} \\
& \quad \equiv \left(\left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}}\right)^{-1} \left(H\left(\mathrm{PID}_i \| c_i^{e_{CA}}\right) c_i\right)^{\mathrm{Info}_{vc}} \\
& \quad \equiv 1 \bmod n.
\end{aligned}
$$

■

2) Privacy Preservation (Anonymity): In the process of incentive, SPIR can protect the privacy of vehicle users (i.e., anonymity) since vehicle users communicate with MSP using pseudonym PID to send sensing data. For CAs, they can verify the legitimacy of the vehicle user's real identity and sign pseudonyms submitted by vehicle users, while they do not know the content of the signed pseudonyms due to adopting the randomized RSA-based partially blind signature technique. For PCA, it can verify the validity of the signature of the pseudonym submitted by the vehicle user, while it does not know the vehicle user's real identity. For TM, it does not participate in the whole process of signature issuance and verification. TM can conditionally recover the real identity of malicious vehicle users from pseudonyms, and further notify the CA. In addition, vehicle users can change the pseudonyms randomly, and any adversary cannot predict the next pseudonym change.

3) Traceability: TM confirmes the behavior of vehicle users through investigation. The vehicle user's real identity can be directly recovered from the pseudonym due to $\mathrm{PID}_i = \mathrm{RID} \cdot u_i \| u_i^{\mathrm{Pub}_{\mathrm{TM}}}$. After intercepting $(u_i)^{\mathrm{Pub}_{\mathrm{TM}}}$, TM can decrypt the message by its own private key without any other data, i.e., obtain the secret value u_i. By using u_i, the real identity of the

TABLE III
COMPARISON OF EXISTING PSEUDONYM SCHEMES

Pseudonym Scheme	Asymmetric	Identity-based	Group sign	Symmetric	Ours
Pseudonym type	Asymmetric key pair, anonymous PKI certificate.	Pseudonymous node identifier as public key.	Group public key.	Short-term symmetric keys.	Asymmetric key pair, anonymous certificate.
Pseudonym issuance	Relies on PKI. Vehicles are registered to Certificate Authorities (CAs) to obtain identity. The pseudonym is issued by pseudonym provider (PP).	Pseudonym corresponding private keys and identifiers issued by Trusted Authority (TA). There's a key escrow facility.	Individual private keys and group public key generated by group management (GM). Sometimes no trusted entity can be found in the same class of vehicles	Vehicle user registered with ombudsman (OM). Individual short-term symmetric key is issued by RSU.	Vehicles are registered at CA, and then the vehicle constructs a pseudonym so that the CA can sign the pseudonym (CA does not know the pseudonym), and send this signature to PCA to obtain the pseudonym certificate.
Pseudonym use	Asymmetric message signature is generated by the sender and attached with a pseudonym certificate.	Asymmetric message signature is generated by the sender. The receivers verify signature by using sender's pseudonym identifier.	Asymmetric message signature is generated by the sender. The receivers verify signature by using known group public key. Batch validation reduces overhead.	The sender uses individual symmetric key to generate MAC. After the delayed key is released, the receiver waits for RSU computer or verification MAC.	Asymmetric message signature is generated by the sender and attached with a pseudonym certificate.
Pseudonym change	In order to prevent tracing based on public key certificates, pseudonym need to be changed. Different change strategies exist.	In order to prevent tracing based on identifier, pseudonym need to be changed. Different change strategies exist.	Group signature can ensures anonymity without changing the pseudonym.	Symmetric key change needed to restrict key validity in space and time.	Vehicles can change their pseudonyms at will.
Pseudonym resolution	PP stores identity pseudonym mapping. Solution require collaboration between multiple pseudonym resolution authorities (RAs). It enhances the privacy in pseudonym resolution and also increases communication overhead.	TA stores identity pseudonym mapping. The authority of identity resolution is concentrated in the same entity. No cooperation required.	GM can determine individual signer key. No cooperation required. Privacy is based on GM, which can disclose membership at will.	RSU and OM cooperate in identity escrow.	TM can determine violation users. Do not store pseudonym certificate and mapping. It only receives pseudonym from the server to track the identity of the user.

vehicle user can be obtained. When informing CA about the real identity of the vehicle user and its behavior, TM completes an identity tracking. Our pseudonym management mechanism avoids the abuse of pseudonyms and does not need to store any pseudonym certificate, thus saving the storage space of TM.

B. Comparisons

Petit *et al.* [42] give an extensive overview and categorization of the state-of-the-art in pseudonym schemes. The existing pseudonym schemes can be categorized into public key-based, identity-based cryptography, group signatures, and symmetric authentication. Based on [42], we further give a comprehensive comparison of the existing pseudonym schemes with our SPIR scheme, as shown in Table III.

Besides the security properties mentioned above, our scheme can resist the following attacks.

C. Resistance to Attacks

In the proposed SPIR, neither CA nor PCA can know the corresponding relationship between the vehicle user's real identity and its pseudonym. In the process of signature issuance and signature verification, Info is the public information of partial blind signature. Both signer CA and verifier PCA know its content. For CA, the pseudonym of vehicle users cannot be inferred from this information; For PCA, the real identity of vehicle users cannot be inferred from their pseudonyms or Info. Even if the two pseudonym issuers work together, there is no way to correspond to the exact relationship between the pseudonym and the real identity. TM's tracing of identity is independent of both sides. Therefore, on the premise of ensuring the security of the scheme, it prevents the leakage of identity information. In addition, it is not allowed to falsify pseudonym and certificates that are not related to some vehicle user's identity, or to tamper with the real identity of the vehicle user after CA compromised.

In addition, we have presented a pseudonym management mechanism, in which a tracking manager can track the malicious vehicle users' real identities when they violate the rules. Therefore, it is difficult for malicious vehicle users to perform long-term denial of service (DoS) attacks.

VI. THEORY ANALYSIS AND SIMULATION EVALUATION

In this section, we give a rigorous theory analysis of the SPIR and evaluate the performance of SPIR through a large number of simulations.

A. Theory Analysis

In this section, we prove that the designed SPIR can achieve a series of design objectives mentioned in Section III.

1) SPIR Has Authenticity: From Algorithm 1, it can be seen that the vehicle user cannot be divided into user set T or Y by changing his quotation. According to [37], the fixed price auction on user set T and Y is true, therefore, SPIR is also truthful and the theorem is proved. In Algorithm 1, all vehicle

users' quotations at auction are equal to their true quotations ($b = \overline{b}$). Thus, in step 2 of the algorithm, the estimated value of the data quantity obtained by the optimal auction of user sets T and Y are their true value.

2) SPIR Has Individual Rationality: According to Definition 2 and the fixed price BR auction [36], the vehicle user's profit can be expressed as follows:

$$u_i = \begin{cases} (p_V - c_i d_i), & R_r = 0, \overline{c_i} \le p_V, d_i \le q_i \\ -\infty, & R_r = 0, \overline{c_i} \le p_V, d_i > q_i \\ 0, & R_r > 0 \text{ or } \overline{c_i} > p_V \end{cases}$$

where R_r represents the remaining budget of the MSP after the fixed price BR auction [37], and p_V represents an estimate of the transaction price of the fixed price BR auction. Because SPIR is authenticity, vehicle user's unit quotations at auction are equal to their true unit quotations ($c_i = \overline{c_i}, q_i = \overline{q_i}$). Obviously $0 \le d_i \le q_i$. At this time, the upper form becomes the following form:

$$u_i = \begin{cases} (p_V - c_i d_i), & R_r = 0, c_i \le p_V \\ 0, & R_r > 0 \text{ or } c_i > p_V. \end{cases}$$

That is to say, if the vehicle user honestly offers his quotation, then his profit is not negative. Thus, the theorem is proved.

3) SPIR Has Budget Feasibility: That is to say, the sum of rewards received by all vehicle users does not exceed the MSP's budget.

4) SPIR Achieves Near Optimal Benefits: SPIR achieves near optimal benefits with limited MSP budget ($\sum_{i:w_i \in S} d_i p \le R$) and limited vehicle user's ability ($d_i \le q_i$). That is to say, given a clear price $p(c_i \le p)$ to solve this optimization problems

$$\begin{aligned} \max \quad & \sum_{i:w_i \in S} d_i \\ \text{s.t.} \quad & d_i \le q_i, \forall w_i \in S \\ & \sum_{i:w_i \in S} d_i p \le R \end{aligned}$$

where set $S = \{w_i | w_i \in V, c_i \le p\}$.

5) SPIR Has Incentive: According to the actual situation of the task, the MSP can adjust the data reliability threshold U to control the quality of the selected vehicle users and obtain better benefits. It can be seen that the threshold U directly determines the vehicle user's historical data reliability and credit value. When the threshold U required by the MSP is high, unqualified vehicle users will not be eligible to participate in the task, and they are not eligible for high rewards, which will motivate vehicle users to participate actively to improve credibility and historical data credibility.

6) SPIR Increases Data Reliability: The design of the SPIR scheme is inspired by the mechanism in [36] [profit extract partition auction (PEPA) mechanism] and [37]. The amount of data obtained by the PEPA mechanism is the smaller one in Q_T^* and Q_Y^*, i.e., $\min(Q_T^*, Q_Y^*)$. The amount of data that can be obtained is at least half that of Q_V^* [37]. SPIR follows the latter method of obtaining the data quantity. The data credibility is introduced in our scheme, which improves the data quality of the MSP significantly.

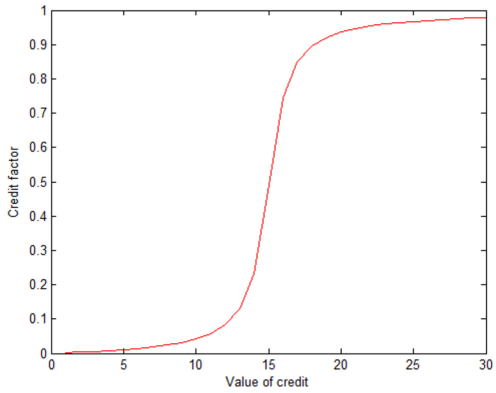

Fig. 6. Credit factor calculation function curve.

User data credibility based on credit value reflects two factors of credit factor and user data credibility in the past. According to Definition 6, the formula for calculating data reliability U is as follows:

$$U_i = \varepsilon_i * H_i.$$

In this article, the normalized tangent function is chosen as the function of mapping the nearest reputation value to the reputation factor

$$\varepsilon = \frac{\arctan(L - \rho) + \arctan \rho}{\pi/2 + \arctan \rho}.$$

The normalized tangent function is shown in Fig. 6, where parameter ρ plays a role in controlling the growth rate of credit factor. As can be seen from the figure, when the credit value $L = \rho$, the credit factor $\varepsilon = 0.5$. When L approaches ρ, the change rate of credit factor ε is larger. When L is far from ρ, the change rate of credit factor ε decreases. When $L > \rho$, one side is faster than 0.9, while when $L < \rho$, reputation factor is faster than 0.1. From this, we can see that $L = \rho$ is a demarcation line of user credit value. The MSP can control the average requirement of reputation value by adjusting the size of ρ, which effectively adjusts the credit factor of the vehicle user and encourage vehicle users to maintain a high degree of participation.

After the kth task, the data reliability of the vehicle user is calculated as follows:

$$H_i = \theta H_{ik} + (1 - \theta) h_{ik}$$

where the parameter θ is called the history factor, and the range of the value of θ is $[0, 1]$. When $(1 - \theta) < 1/k$, the impact of the current task on the overall data reliability is less than the average data reliability. When $(1 - \theta) > 1/k$, the impact of current tasks on overall data reliability is greater than that of average data reliability. When $(1 - \theta) = 1/k$, the impact of the current task on the overall data credibility is equal to the average data credibility. It can be seen that the history factor θ controls the impact of the proportion of data credibility that vehicle users have contributed to the results of their last task submission.

By introducing the credit factor, vehicle users with low reputation cannot have high data credibility, which avoids the

TABLE IV
HARDWARE CONFIGURATION

Hardware	Settings
CPU	Inter(R) Core(TM) i5-5200U
RAM	CPU at 2.20GHz
Operation System	Windows

TABLE V
PARAMETERS SETTING

Parameters	Settings
n	[10, 20]
c_i	[1, 4]
q_i	[5, 10]
R	180

possibility of high data credibility due to the small number of tasks. The introduction of historical factors can improve the impact of the results of the last task completion and make vehicle users pay more attention to the quality of completion.

7) Computational Complexity of SPIR Is $O(n \log n)$: The time complexity of running SPIR is mainly determined by the optimal auction OOA$(T, R/2)$ and OOA$(Y, R/2)$ [37]. The time complexity of the optimal auction is $O(n \log n)$, thus the time complexity of SPIR is $O(n \log n)$.

B. Simulation Evaluation

We use MATLAB to simulate this article. For SPIR, there are two reference objects. One is optimal auction, which is used to verify that the amount of data obtained by SPIR is very close to that obtained by optimal auction [32]. Another one is the PEPA mechanism proposed in [36], which is used to verify that the proposed SPIR scheme is superior to the previous auction schemes. Also, we will analyze the impact of reputation values and different history data credibility on data credibility.

1) Data Amount Test: We simulate systematically with a PC and the configuration is shown in Table IV. In Table V, we present the settings of simulation experiments to verify the performance of SPIR. The number of vehicle users ranges is [12, 20]. The unit cost of vehicle users c_i and the value of services of the vehicle users q_i is chosen uniformly at random from the numbers in the range given in the table. The budget R of the MSP is fixed at 180.

We use the settings in Table V to see how the number of vehicle users affects the amount of data that SPIR can obtain. As can be seen from Fig. 7, with the increase of the number of vehicle users, the amount of data obtained by the three auction mechanisms is increasing. The amount of data obtained by SPIR is very close to that obtained by optimal auction [32], which is much larger than that obtained by the PEPA mechanism [36].

2) Data Reliability Test: Data reliability based on credit value is calculated according to vehicle user historical data reliability and nearly 30 days reputation value. From the Definitions 4–6, we can see that ρ of control credit factor and historical factor θ indirectly affect the data reliability based on credit value. Credit value L can only be accumulated in the current month, plus one per day, and cleared in the next

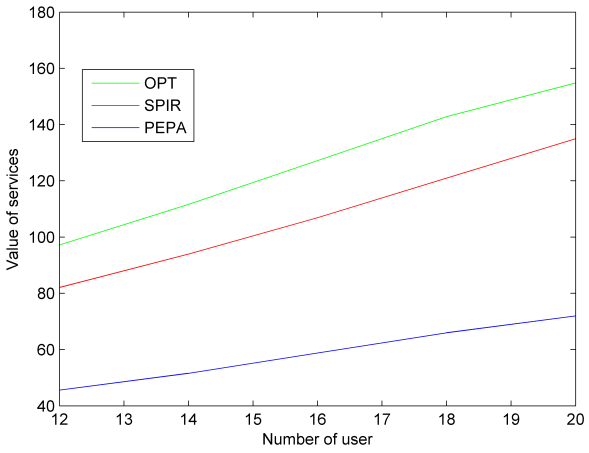

Fig. 7. Influence of the number of vehicle users on the amount of data obtained by the SPIR.

month. Therefore, the credit value [1, 30] and the historical data credibility [0.1, 0.9] are used to calculate data reliability based on credit value. $\rho = 10, 15, 20, 25$, data reliability curves are shown in Fig. 8.

Analysis of Credit Factor ε: Through the analysis of Fig. 8, we can see that ρ is a parameter to control the growth rate of ε. According to the four groups of curves on the graph, when $L > \rho$, ε increases rapidly to 0.9, while when $L < \rho$, ε decreases rapidly to less than 0.1. Therefore, $L = \rho$ is the dividing line to distinguish the credit value of vehicle users. ρ reflects the average requirement of the MSP for user credit value. In order to select vehicle users with higher credit value to accept tasks, the MSP can select vehicle users according to the number of tasks and set ρ. In order to achieve better benefits, when the number of tasks is small, let ρ = 20–30 to select better vehicle users; when the number of tasks is large, let ρ = 10–15, which can recruit more vehicle users to participate in tasks; when the task amount is moderate, setting $\rho = 15$ is more appropriate.

Analysis of Historical Factor θ: θ controls the proportion of vehicle user's last task resulting in total data reliability. It is emphasized that task completion near the current time has greater impact on data credibility than that far away from the current time. According to Fig. 8, when $L < 9$, vehicle users can obtain less than 0.2 user data reliability based on credit value, regardless of whether the historical data reliability is high or low. In order to highlight the proportion of data credibility after the completion of the current task, it is necessary to select the appropriate θ. As shown in Fig. 8, when $\rho = 15$ and the curve is $L \in [10, 20]$, the data reliability obtained by the vehicle user completing the current task has a greater impact on the overall data reliability. The analysis in Fig. 8. shows that $(1-\theta) > 1/L$ should be satisfied at this time, so $0 < \theta \leq 0.9$. As shown in Fig. 8, when $\rho = 10$, the curve varies greatly at $L \in [5, 15]$. Similarly, $0 < \theta \leq 0.8$. When $\rho = 20$, the curve varies greatly at $L \in [15, 25]$. Similarly, $0 < \theta \leq 14/15$. Therefore, it can be concluded that when $L \in [L - \rho, L + \rho]$,

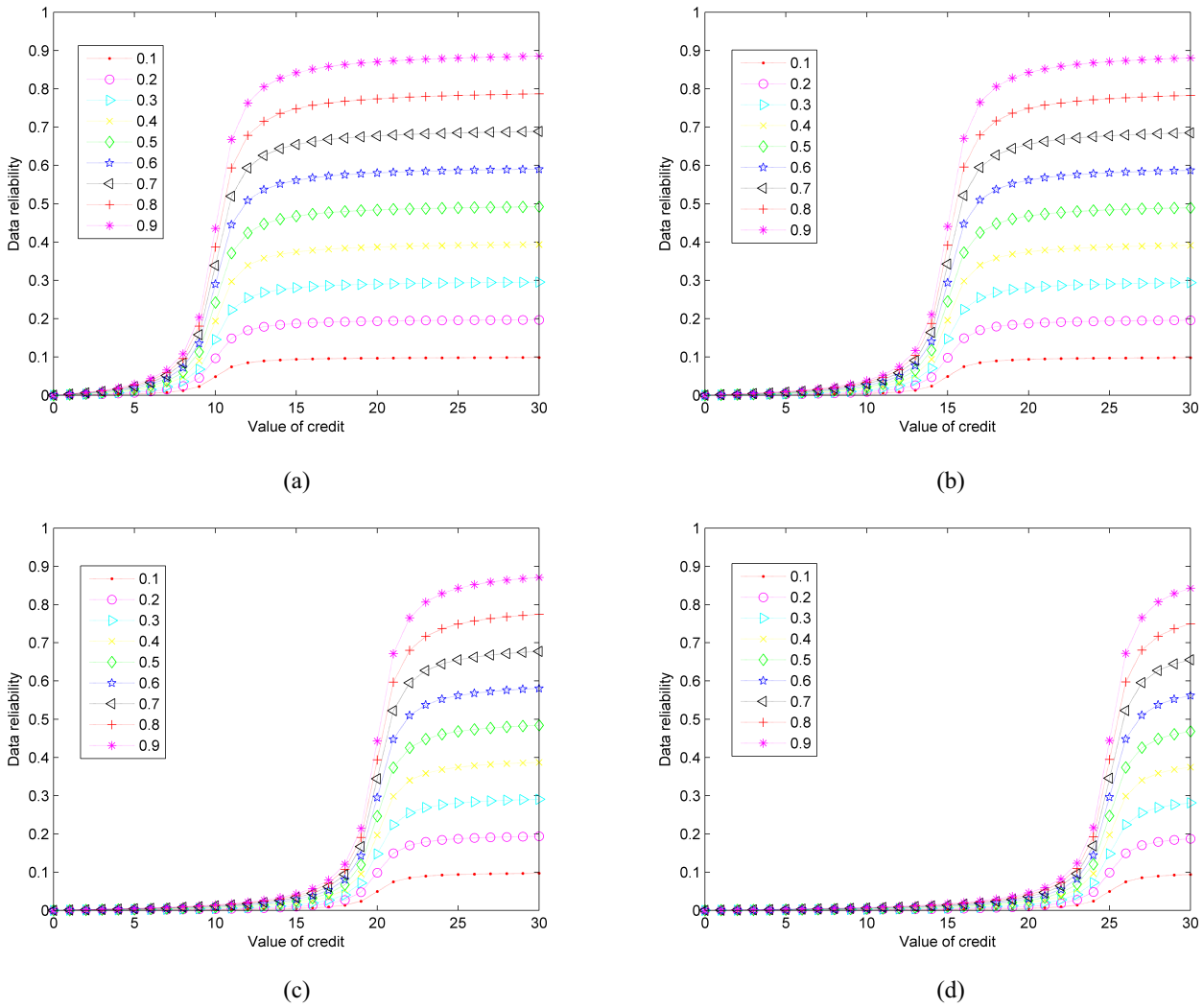

Fig. 8. Data reliability curves under different ρ. (a) $\rho = 10$. (b) $\rho = 15$. (c) $\rho = 20$. (d) $\rho = 25$.

the data reliability obtained by the vehicle user's current completion of the task has a greater impact on the overall data reliability. At this time, $0 < \theta \leq (L - \rho - 1)/(L - \rho)$.

Analysis of Data Reliability Threshold U: In user selection, the number of excellent vehicle users can be controlled by adjusting the data credibility threshold U. When the threshold U is too high, the vehicle users selected by the MSP are of high quality, but the number of vehicle users is small, which may lead to the extension of task completion time. When the threshold U setting is low, although the number of vehicle users is increased, the overall quality of the selected vehicle users is low. According to Fig. 8, it can be seen that the threshold directly determines vehicle user's historical data reliability and credit value. When the threshold $U \geq 0.5$, the MSP requires the credit value $L \geq \rho$ of the selected vehicle user. When the threshold U is higher than 0.7, only vehicle users whose historical data reliability is higher than 0.7 may meet the data credibility standard. According to the actual situation of the task, the MSP can adjust the threshold U to control the quality of the selected vehicle users and obtain better benefits.

The data credibility based on credit value proposed in this article plays an incentive role for vehicle users to attach importance to the quality of current tasks and maintain good activity.

VII. Conclusion

In this article, we have proposed an SPIR. Specifically, an effective incentive mechanism based on reverse auction is presented, which can achieve payment control for the MSP and ensure completion quality for vehicle users. Meanwhile, the blockchain-based credit management can guide vehicle users to attach importance to the quality of current tasks and maintain good activity. When the credit threshold U required by the MSP is high, unqualified vehicle users cannot be eligible to participate in the task, and they are not eligible for high rewards, which motivates vehicle users to participate actively to improve credibility and historical data credibility. In order to ensure the secure distribution of rewards, a blockchain-based payment system is equipped. Moreover, in order to ensure the security of the incentive mechanism and protect

the privacy of vehicle users, a secure pseudonym management mechanism is presented based on the partially blind signature technique. Security analysis shows that the scheme can provide secure pseudonym management and resist to attacks. In addition, SPIR can not only guarantee the maximization of vehicle user revenue but also enables the MSP to obtain as much reliable data as possible. The experimental results indicate that the amount of data obtained by SPIR is very close to that obtained by optimal auction, which is much larger than that obtained by the PEPA mechanism. In conclusion, SPIR can effectively motivate vehicle users to upload high-quality road information in real time to the MSP without revealing their privacy.

REFERENCES

[1] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018.

[2] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Mar. 2019.

[3] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.

[4] M. Hadian, T. Altuwaiyan, and X. Liang, "Privacy-preserving time-sharing services for autonomous vehicles," in *Proc. IEEE VTC-Fall*, 2017, pp. 1–5.

[5] H. Wang, M. Hadian, and X. Liang, "Efficient and privacy-preserving roadmap data update for autonomous vehicles," in *Proc. IEEE GLOBECOM*, 2018, pp. 1–6.

[6] *FixMyStreet*. Accessed: Aug. 15, 2019. [Online]. Available: http://www.fixmystreet.com/

[7] *Moovit*. Accessed: Aug. 15, 2019. [Online]. Available: http://www.moovitapp.com/

[8] L. Li *et al.*, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[9] M. Sweeney and A. Levandowski, "Deploying human-driven vehicles for autonomous vehicle routing and localization map updating," U.S. Patent App. 10 186 156, Jan. 22, 2019.

[10] İ. Demir *et al.*, "Generative street addresses from satellite imagery," *ISPRS Int. J. Geo Inf.*, vol. 7, no. 3, pp. 1–22, 2018.

[11] X. Chen, X. Wu, X.-Y. Li, X. Ji, Y. He, and Y. Liu, "Privacy-aware high-quality map generation with participatory sensing," *IEEE Trans. Mobile Comput.*, vol. 15, no. 3, pp. 719–732, Mar. 2015.

[12] X. Wang, W. Wu, and D. Qi, "Mobility-aware participant recruitment for vehicle-based mobile crowdsensing," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4415–4426, May 2018.

[13] X. Wu, P. Yang, S. Tang, X. Zheng, and Y. Xiong, "Privacy preserving RSS map generation for a crowdsensing network," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 42–48, Aug. 2015.

[14] C. Xiang *et al.*, "CARM: Crowd-sensing accurate outdoor RSS maps with error-prone smartphone measurements," *IEEE Trans. Mobile Comput.*, vol. 15, no. 11, pp. 2669–2681, Nov. 2015.

[15] G. Xu, H. Li, S. Liu, M. Wen, and R. Lu, "Efficient and privacy-preserving truth discovery in mobile crowd sensing systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3854–3865, Apr. 2019.

[16] J. Qin, H. Zhu, Y. Zhu, L. Lu, G. Xue, and M. Li, "POST: Exploiting dynamic sociality for mobile advertising in vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 6, pp. 1770–1782, Jun. 2016.

[17] J. L. Z. Cai, M. Yan, and Y. Li, "Using crowdsourced data in location-based social networks to explore influence maximization," in *Proc. IEEE INFOCOM*, 2016, pp. 1–9.

[18] J. Wan, J. Liu, Z. Shao, A. V. Vasilakos, M. Imran, and K. Zhou, "Mobile crowd sensing for traffic prediction in Internet of Vehicles," *Sensors*, vol. 16, no. 1, p. 88, 2016.

[19] J. Cherian, J. Luo, H. Guo, S.-S. Ho, and R. Wisbrun, "ParkGauge: Gauging the occupancy of parking garages with crowdsensed parking characteristics," in *Proc. IEEE Int. Conf. Mobile Data Manag.*, vol. 1, 2016, pp. 92–101.

[20] Y. Liu, X. Weng, J. Wan, X. Yue, H. Song, and A. V. Vasilakos, "Exploring data validity in transportation systems for smart cities," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 26–33, May 2017.

[21] I. Memon, Q. A. Arain, M. H. Memon, F. A. Mangi, and R. Akhtar, "Search me if you can: Multiple mix zones with location privacy protection for mapping services," *Int. J. Commun. Syst.*, vol. 30, no. 16, pp. 1–23, 2017.

[22] C. Lai, R. Lu, D. Zheng, and S. X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, to be published.

[23] J. Ni, *Security and Privacy Preservation in Mobile Crowdsensing*, Univ. Waterloo, Waterloo, ON, Canada, 2018.

[24] C. Lai, H. Zhou, N. Cheng, and X. S. Shen, "Secure group communications in vehicular networks: A software-defined network-enabled architecture and solution," *IEEE Veh. Technol. Mag.*, vol. 12, no. 4, pp. 40–49, Dec. 2017.

[25] G. Xu, H. Li, H. Ren, K. Yang, and R. Deng, "Data security issues in deep learning: Attacks, countermeasures and opportunities," *IEEE Commun. Mag.*, to be published.

[26] S. Karnouskos and F. Kerschbaum, "Privacy and integrity considerations in hyperconnected autonomous vehicles," *Proc. IEEE*, vol. 106, no. 1, pp. 160–170, Jan. 2018.

[27] A. Capponi, C. Fiandrino, B. Kantarci, L. Foschini, D. Kliazovich, and P. Bouvry, "A survey on mobile crowdsensing systems: Challenges, solutions and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2419–2465, 3rd Quart., 2019.

[28] X. Zhang *et al.*, "Incentives for mobile crowd sensing: A Survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 54–67, 1st Quart., 2016.

[29] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 370–380, Oct. 2015.

[30] K. Ota, M. Dong, J. Gui, and A. Liu, "QUOIN: Incentive mechanisms for crowd sensing networks," *IEEE Netw.*, vol. 32, no. 2, pp. 114–119, Mar./Apr. 2018.

[31] G. Danezis, S. Lewis, and R. J. Anderson, "How much is location privacy worth?" in *Proc. WEIS*, vol. 5, 2005, pp. 1–13.

[32] A. V. Goldberg, J. D. Hartline, and A. Wright, "Competitive auctions and digital goods," in *Proc. ACM-SIAM Symp. Discr. Algorithms*, 2001, pp. 735–744.

[33] J.-S. Lee and B. Hoh, "Dynamic pricing incentive for participatory sensing," *Pervasive Mobile Comput.*, vol. 6, no. 6, pp. 693–708, 2010.

[34] Q. Zhang, Y. Wen, X. Tian, X. Gan, and X. Wang, "Incentivize crowd labeling under budget constraint," in *Proc. IEEE INFOCOM*, 2015, pp. 2812–2820.

[35] G. Lin, F. Hou, and J. Huang, "Providing long-term participation incentive in participatory sensing," in *Proc. IEEE INFOCOM*, 2015, pp. 2803–2811.

[36] Z. Abrams, "Revenue maximization when bidders have budgets," in *Proc. 7th Annu. ACM-SIAM Symp. Discr. Algorithm*, 2006, pp. 1074–1082.

[37] Y. Zhou, Y. Zhang, and S. Zhong, "Incentive mechanism design in mobile crowd sensing systems with budget restriction and capacity limit," in *Proc. IEEE ICCCN*, 2017, pp. 1–9.

[38] M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, and P. Bouvry, "Game-theoretic recruitment of sensing service providers for trustworthy cloud-centric Internet-of-Things (IoT) applications," in *Proc. IEEE Globecom Workshops*, 2016, pp. 1–6.

[39] C.-T. Li, M.-S. Hwang, and Y.-P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, 2008.

[40] Q. E. Ali *et al.*, "SPATA: Strong pseudonym-based authentication in intelligent transport system," *IEEE Access*, vol. 6, pp. 79114–79128, 2018.

[41] T. Gao, X. Deng, Q. Li, M. Collotta, and I. You, "APPAS: A privacy-preserving authentication scheme based on pseudonym ring in VSNs," *IEEE Access*, vol. 7, pp. 69936–69946, 2019.

[42] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2014.

[43] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2017.
[44] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Trans. Netw.*, vol. 24, no. 3, pp. 1732–1744, Jun. 2016.
[45] T. Cao, D. Lin, and X. Rui, "A randomized RSA-based partially blind signature scheme for electronic cash," *Comput. Security*, vol. 24, no. 1, pp. 44–49, 2005.
[46] J. Yan, S. Ku, and C. Yu, "Reputation model of crowdsourcing workers based on active degree," *J. Comput. Appl.*, vol. 7, p. 39, Jul. 2017.
[47] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

Chengzhe Lai (M'15) received the B.S. degree in information security from the Xi'an University of Posts and Telecommunications, Xi'an, China, in 2008, and the Ph.D. degree from Xidian University, Xi'an, in 2014.

He was a visiting Ph.D. student with the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada, from 2012 to 2014. He is currently with the Xi'an University of Posts and Telecommunications, where he is also with the National Engineering Laboratory for Wireless Security. His research interests include wireless network security, privacy preservation, and VANET security.

Min Zhang is currently pursuing the master's degree with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, China.

Her main research interests include Internet of Vehicles and privacy protection in crowdsensing.

Jie Cao is currently pursuing the undergraduation degree with the Xi'an University of Posts and Telecommunications, Xi'an, China.

His main research interest includes wireless communication security.

Dong Zheng received the M.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1988, and the Ph.D. degree in communication engineering from Xidian University, Xi'an, in 1999.

He was a Professor with the School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai, China. He is currently a Professor with the Xi'an University of Posts and Telecommunications, Xi'an, where he is also with the National Engineering Laboratory for Wireless Security, Xi'an, China. His research interests include provable security and new cryptographic technology.