A Multi-task Mobile Crowdsensing Scheme with Conditional Privacy Preserving for Vehicle Networks

Zhe Xia[1,2(✉)], Shiyun Liu[1], Yichen Huang[1], Hua Shen[3], and Mingwu Zhang[3]

[1] School of Computer Science and Artificial Intelligence, Wuhan University of Technology, Wuhan, China
xiazhe@whut.edu.cn
[2] Hubei Key Laboratory of Transportation Internet of Things, Wuhan University of Technology, Wuhan, China
[3] School of Computer Science, Hubei University of Technology, Wuhan, Hubei, China

Abstract. Mobile crowdsensing recruits a group of users and utilizes their sensing devices to accomplish the sensing task. It can offer a flexible and scalable sensing paradigm with low deploying costs. As the development of vehicle networks, many works in the literature have investigated how to use vehicles as the sensing units for mobile crowdsensing. However, the majority of these works suffer some limitations. First, they can either achieve privacy preserving or supervision, but not both. Second, they mainly consider a single sensing task and overlook the management of users' reputations across multiple tasks. To address these limitations, we propose a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks. In our proposed scheme, the privacy preserving requirement and the supervision requirement can be harmonized, achieving a property called conditional privacy preserving. Moreover, each vehicle can participate in multiple sensing tasks at the same time. Specifically, privacy protection covers identity privacy, location privacy and reputation privacy simultaneously. And the reputation center does not need to store any internal information (e.g. random numbers or ephemeral keys) when updating the vehicles' pseudonyms, reducing the risks of Denial-of-Service (DoS) attacks. Therefore, it provides a more secure and practical solution for mobile crowdsensing. Security analyses prove that our scheme achieves the desirable security requirements, such as correctness, conditional privacy preserving and authentication. And efficiency analyses demonstrate that our scheme can be used efficiently in multi-task mobile crowdsensing.

Keywords: Mobile crowdsensing · Conditional privacy preserving · Reputation management · Vehicular networks

J. Chen et al. (Eds.): EISA 2022, CCIS 1641, pp. 21–36, 2022.
https://doi.org/10.1007/978-3-031-23098-1_2

1 Introduction

With the development of mobile Internet and the wide deployment of intelligent devices with sensors, the concept of mobile crowdsensing (MCS) [1] has been introduced. Due to its abilities in perceiving, collecting, and analyzing information about the surrounding environment, MCS has become a very attractive technique that has been widely used in various areas, such as transportation, medical treatment and healthcare. Recently, vehicles are equipped with more sensors and become more intelligent, and it is natural to use them as sensor nodes in mobile crowdsensing [2,3]. Moreover, vehicular networks enjoys many advantages, such as high mobility, low energy consumption, convenient installation and maintenance. Hence, their use in MCS has attracted more and more attentions both in the academia and industry. In vehicular networks, the MCS architecture mainly consists of three entities: *data requesters*, *a cloud server*, and *sensing vehicles*.

The sensing vehicles can perform sensing tasks when they moving round the rural and urban areas [2], which makes them suitable for applications with the mobility requirement. However, the openness of vehicular networks makes them vulnerable to various attacks. For example, the sensors and controllers of the vehicle might be controlled or tampered by adversaries. Malicious sensing vehicles can not only forge and tamper the data, violating the authenticity and integrity of data, but also steal sensitive information such as identity and location, decreasing users' acceptance about this new technology. To address this issue, the reputation value is often used to evaluate the trustworthy of the vehicles [4–6]. This value is normally issued and managed by the reputation center as follows: the cloud server evaluates the trustworthy of the vehicle through the accuracy of the sensing data, and it sends the feedback report to the reputation center, who then updates the reputation value of the vehicle accordingly. However, when the sensing vehicle participates in multiple sensing tasks simultaneously, it will become more challenging to manage the reputation value. Besides, achieving privacy protection in location and identity already cause large overheads in communication and computing. If the reputation value is also protected, the system may become even more complex.

In recent years, many MCS schemes have used the reputation value to evaluate the trustworthy of participants. However, most of these schemes only consider privacy protection of vehicle's identity [7] and location [8], but the reputation value was not considered [8,9]. The consequence is that malicious adversaries may use the reputation value to infer the vehicle's trajectory or even its identity. Besides, most existing schemes only consider a single sensing task, and they cannot be used in multi-task sensing. Moreover, in the existing privacy protection schemes based on pseudonyms, the cloud server needs to store the random numbers when updating pseudonyms. This not only causes large storage overheads, but also makes the system vulnerable to the denial-of-service (DoS) attacks.

Apart from the above issues, conditional privacy preserving is also a crucial requirement in vehicular networks [10]. On one hand, adversaries may intercept the communications to derive many sensitive information, which may cause serious consequences on privacy leakage. On the other hand, the trusted authority

needs to perform effective supervision, e.g. extract the real identity of some vehicle if necessary [11]. Therefore, conditional privacy preserving should be provided to harmonize the privacy preserving and the supervision requirements in vehicular networks. This stringent requirement requires that the trusted authority must be the only entity who can extract the real identity, location, and reputation value of a vehicle.

To address the above challenges, we propose a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicular networks. The major contributions of this paper are summarized as follows:

- The proposed scheme can be used in multi-task sensing, and it achieves conditional privacy preserving for identity, location, and reputation value simultaneously.
- When updating the pseudonyms of the sensing vehicles, the reputation center does not need to record any internal status (such as random numbers or ephemeral keys), which not only reduce the risks of DoS attacks, but also lowers the storage overheads.
- Security analyses prove that our scheme achieves the desirable security requirements, such as correctness, conditional privacy preserving and authentication, and efficiency analyses demonstrate that our scheme can be used efficiently in multi-task mobile crowdsensing.

The rest of the paper is organized as follows. Section 2 reviews some related works. Section 3 describes some preliminaries that will be used in our proposed scheme. Section 4 introduces the system and security models, and Sect. 5 presents our proposed scheme. Section 6 provides security and efficiency analyses. Finally, conclusion and discussion are included in Sect. 7.

2 Related Works

To achieve privacy protection in mobile crowdsensing based on vehicular networks, many existing schemes have considered identity and location privacy. Ni et al. [5] have used matrices to record the sensing area and sensing task, then randomized matrix multiplication is used to obtain matching of sensing tasks. Wang et al. [8] have proposed a novel area obfuscation mechanism by combining ε-differential-privacy with δ-distortion-privacy in sparse MCS to tackle the privacy protection for vehicle's location. Sun et al. [9] have used homomorphic encryption to achieve privacy protection. Zhao et al. [12] have assured statistics privacy using zero-knowledge proofs. However, the communication and computation overheads are quite heavy in these schemes, failing to meet the demands in real-world applications.

In order to evaluate the trustworthy of sensing vehicles, many researchers suggest to use the reputation value. Then, one can judge whether some vehicle is qualified to participate in the sensing tasks. In particular, some schemes have adapted the mechanism to update the reputation value in real time, e.g. at the end of each sensing task, the vehicle will be given a corresponding reputation value. However,

these schemes have not considered the multi-task environment [13]. Afterwards, some reputation value management schemes suggest that one should not only update the reputation value of a single task, but also calculate the weight of the new reputation value based on the reputation feedback report and the vehicle's original reputation value [14–16].

Obviously, vehicles' reputation values also need to be protected. Otherwise, if this information is leaked, the adversaries may use it to infer the trajectory and driving pattern. However, most existing schemes in the literature have not considered the protection of reputation values. For example, Liu [16] has proposed a reputation management scheme, in which the reputation value is used to collect high-quality sensor data, but it is easy to be intercepted or tampered with. Although the scheme in [5] has suggested to transmit and store the reputation value in a threshold fashion, the protection can only be enhanced to some extent and the reputation value still may be inferred by adversaries. Afterwards, the scheme in [17] replaces each reputation value with a hash value to achieve lightweight privacy preserving for reputation value. But since hash function is deterministic, adversaries can still learn some information of the reputation value if its space is limited.

Regarding the conditional privacy preserving requirement, Raya [11] has proposed a conditional privacy preserving authentication scheme with anonymous certificates. Many public/private key pairs and the corresponding certificates are pre-loaded into vehicles' OBUs to protect the identity. But this scheme suffers some disadvantages. First, both the vehicle and the trusted third party need large storage space to store the data. Second, when a malicious vehicle sends a faulty message, it takes a long time to recover its identity. To address these weaknesses, Lu et al. [10] have proposed a modified CPPA scheme using anonymous certificates, in which the vehicle obtains a temporary anonymous certificate when it drives pass an RSU. To achieve conditional privacy preserving, each vehicle has to request a new anonymous certificate from an RSU frequently, as the adversary can trace a vehicle if the certificate is used over a long period. Zhang et al. [7] have presented a novel CPPA scheme by leveraging pseudonyms. And the ID-based signature tied to pseudonymous is used to guarantee the entities' privacy in [19].

To sum up, the existing schemes still suffer some limitations. First, either they have not considered conditional privacy preserving, or the protection has not covered the reputation value. Second, they mainly consider a single sensing task and overlook the management of users' reputation across multiple tasks. To address these limitations. We propose a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicle networks. Hence, it provides a more secure and practical solution for mobile crowdsensing.

3 Preliminaries

In this section, we review some preliminaries that will be used to design our proposed scheme, including homomorphic encryption [20], and the BCP encryption scheme [22].

3.1 Homomorphic Encryption

Paillier' s cryptosystem [20] is one of the most widely used encryption scheme with the additive homomorphic property. Suppose we have N encrypted data under the same public key pk, denoted as $[m_i]_{pk}$ $(i = 1, 2, \ldots, N)$. The additive homomorphic encryption ensures that the following equation always holds

$$D_{sk}\left(\prod_{i=1}^{N}[m_i]_{pk}\right) = \sum_{i=1}^{N} m_i$$

where $D_{sk}()$ represents the corresponding decryption algorithm with private key sk. Liu [21] has proposed some extensions that can be used as toolkit for processing encrypted data, including *Secure Less Than* Protocol (SLT) and *Secure Equivalent Testing* Protocol (SEQ). Given two encrypted numbers $[x]_{pk}$ and $[y]_{pk}$, the SLT protocol can compute a bit in the encrypted form, depending on whether $x \geq y$ or $x < y$. And the SEQ protocol can compute a bit in the encrypted form, depending on whether the plaintext of the two encrypted data are equal (i.e. $x = y$).

3.2 The BCP Encryption Scheme

The BCP encryption scheme [22] works as follows:

KeyGen: Given two large primes p, q, and $n = p * q$. Let g and h be two elements of maximal order in G, where G is the cyclic group of quadratic residues modulo n^2. Note that, if h is computed as $g^x \bmod n^2$, where $x \in \left[1, \lambda\left(n^2\right)\right]$ and $\lambda(*)$ is the Euler function, then x is coprime with $\mathrm{ord}(G)$ with high probability, and thus h is of maximal order. The public parameters are n, g and $h = g^x \bmod n^2$, and the secret value is $x \in [1, \mathrm{ord}(G)]$

Enc: Given a message $m \in Z_n$, choose a random number r in Z_n^*. The ciphertext is computed as $[m] = (T, T') = \{h^r(1 + mn), g^r\} \bmod n^2$.

Decryption With Weak Private Key (WDec): with the secret key x, the plaintext m can be retrieved as follows: $m = L\left(T/\left(T'\right)^x \bmod n^2\right)$, where $L(u) = (u - 1)/n$.

Decryption With Strong Private Key (SDec): any ciphertext can be decrypted with the strong private key $SK = \lambda(n)$ by calculating:

$$T^{\lambda(n)} \bmod n^2 = g^{xr\lambda(n)}(1 + mn\lambda(n)) \bmod n^2 = 1 + mn\lambda(n)$$

Then, m can be recovered as follow:

$$m = L\left(T^{\lambda(n)} \bmod n^2\right) \cdot \lambda(n)^{-1} \bmod n$$

4 Models and Definitions

In this section, we describe the system model, security model, and security requirements.

4.1 System Model

The system model is shown as in Fig. 1 that consists of five entities: data requester, cloud server, reputation center, roadside unit, and sensing vehicle.

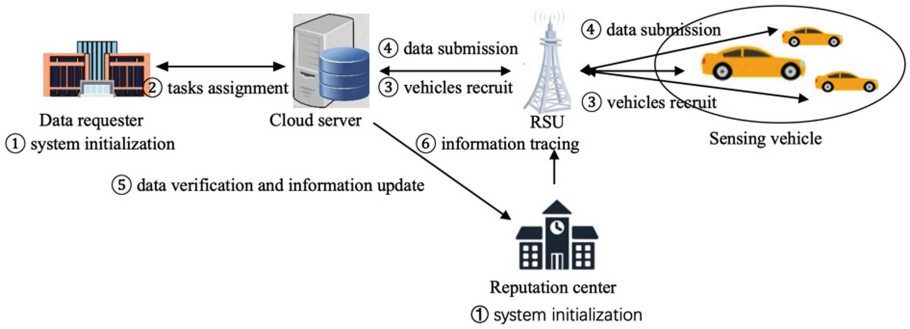

Fig. 1. The system architecture of proposed scheme.

Data Requester: It can be a management department, a service department, or an authorized individual. It assigns the sensing tasks in order to obtain some valuable information, such as road information, weather information, congestion level, etc.

Cloud Server: It collects, stores, and computes the encrypted sensing data. In addition, the cloud server evaluates the trustworthy of vehicles based on the accuracy of their submitted sensing data, and it generates the reputation feedback report. The cloud servers typically have strong storage and computing capabilities.

Reputation Center: It is responsible for verifying, storing, and distributing the reputation values and pseudonyms to each sensing vehicle. In addition, the reputation center updates the vehicles' reputation values based on the reputation feedback reports.

Roadside Unit (RSU): It is deployed on both sides of the road that is responsible for data transmission. Specifically, the RSU provides data transmission services between cloud servers and sensing vehicles, as well as between reputation centers and sensing vehicles.

Sensing Vehicle: It is generally equipped with various sensors, that are responsible for collecting and storing many types of environment data. Each sensing vehicle is also equipped with an on-board unit OBU [23,24] that can store secret information, such as secret keys, identities, locations, etc.

4.2 Security Model

The data requester, the cloud server, and the RSUs are all assumed to be honest-but-curious, i.e. they will follow the protocol, but they may try to obtain information beyond their authorization. For example, in the mobile crowdsensing environment based on vehicular networks, these honest-but-curious entities may intend to learn the location, identity, and reputation information of the sensing vehicles, called *inference attack* (includes location inference attack, identity inference attack, and reputation inference attack). Besides, if a malicious adversary intercepts a series of reputation values with respect to the same sensing vehicle, she may infer some other information such as its driving mode, and this attack is denoted as *reputation linkable attack*.

The reputation center is assumed to be fully trusted. The majority of the sensing vehicles are assumed to be honest, while the minority of dishonest vehicles may implement the following attacks:

- *Data pollution attack*. Malicious sensing vehicles may submit false sensing data, which may pollute the sensing results.
- *Sybil attack*. Malicious sensing vehicles may submit the same data many times or use fake identities in order to obtain a higher reputation or destroy the sensing results.
- *Reputation tamper attack*. Malicious sensing vehicles with low reputation value may tamper with the reputation value, so that they can participate in the sensing task that they are not authorized to.

4.3 Security Requirements

The following security requirements are considered in our proposed scheme:

- *Correctness*. If all participants execute the protocol honestly, the protocol will generate correct outputs.
- *Conditional privacy preserving*. Privacy protection are enforced on identity, location and reputation value from the adversaries, and this information can be retrieved by the trusted authority if necessary. In particular, identity privacy means that during the communication between the sensing vehicle and other entities, the adversaries cannot extract its real identity. Location privacy means that malicious adversaries cannot learn about the locations of sensing vehicles through messages. Reputation value privacy ensures that vehicles' reputation values should not be exposed or linked. However, the trusted authority can extract the real identity, location, and reputation value from the exchanged messages in a multi-task environment when necessary.
- *Authentication*. The exchanged messages cannot be tampered or fabricated by the adversaries without being detected.
- *Resistance to other attacks*. The proposed scheme is able to withstand various attacks in real-world applications, including the inference attack, reputation linkable attack, data pollution attack, Sybil attack, and reputation tamper attack.

5 The Proposed Scheme

In this section, we first give an overview of our proposed scheme, then its technical details are described. The proposed scheme consists of six phases: system initialization, task assignment, vehicle recruitment, data submission, data verification and information update, information tracing. The notations used in our proposed scheme are summarized as follows (Table 1):

Table 1. Formalized notations involved in the scheme

Notation	Definition
t_i	The ith sensing vehicle's reputation value
t_0	The threshold of sensing task's reputation
m	The content of a sensing task
$[m]$	The ciphertext of m
d	Sensing data
d_0	Sensing data's standard value
Δd	Sensing data's error threshold
PK_{DR}, SK_{DR}	Data requester's key pair
PK_{RC}, SK_{RC}	Reputation center's key pair
x, y	Sensing task's coordinate
r	Sensing task's radius
TSK	The sensing task list
RID	The real identity of a sensing vehicle
PID	The pseudonym of a sensing vehicle
T	The list that a sensing vehicle participate in

5.1 Overview of the Proposed Scheme

To simply the description, we first give an overview of the proposed scheme. We assume that there is a sensing task in an urban area. If the sensing vehicles desire to participate in the sensing task, their locations and reputation values should satisfy the location requirement and reputation threshold of this sensing task. For example, we assume that the data requester assigns a task and initializes the threshold for reputation as t_0. This means that the sensing vehicle's reputation value t should be no less than t_0, In addition, the position of the sensing vehicle should belong to the circle with radius r specified by the sensing task. As shown in Fig. 1, the proposed scheme includes the following steps:

– **System initialization.** The data requester and reputation center generate the system parameters and key pairs for the homomorphic encryption scheme. The reputation center initializes the reputation value for each vehicle, and sends each vehicle's pseudonym and reputation value to the corresponding

sensing vehicle. All these transmitted messages are also signed by the reputation center.

- **Task assignment.** The data requester assigns a sensing task to the cloud server, along with the location requirement and reputation threshold for this sensing task. Then, the cloud server broadcasts this sensing task to the sensing vehicles via RSUs.
- **Vehicles recruitment.** Each sensing vehicle verifies that its current position is within the effective area of this task. If the verification is satisfied, the cloud server will send the corresponding task to the sensing vehicle.
- **Data submission.** The sensing vehicles submit the sensing data to the cloud server via RSUs.
- **Data verification and information update.** The cloud server verifies the legitimacy of the sensing data submitted by each sensing vehicle, generates a reputation feedback report and sends it to the reputation center. The reputation center then updates the pseudonym and reputation value of the sensing vehicle.
- **Information tracing.** The reputation center retrieves the location, identity, and reputation information of the sensing vehicle using a master private key when necessary, e.g. when some vehicle is found malicious and the court demands this vehicle's information to be revealed.

5.2 Technical Details of the Proposed Scheme

Step 1. System Initialization

- **Initialization of system parameters and generation of key pairs:** Given a security parameter κ, two safe primes p, q are selected, such that $p' = (p-1)/2$ and $q' = (q-1)/2$ are also primes. Denote $n = pq$ and g_1 is with maximal order in $\mathbb{G}_1$, where $\mathbb{G}_1$ is the cyclic group of quadratic residues modulo n^2. The data requester and the reputation center select secret parameters $a \in [1, \mathrm{ord}(\mathbb{G}_1)]$ and $b \in [1, \mathrm{ord}(\mathbb{G}_1)]$ and generate their key pairs as $(PK_{DR} = g_1^a, SK_{DR} = a)$ and $(PK_{RC} = g_1^b, SK_{RC} = b)$.
- **Vehicle's pseudonym assignment:** The reputation center starts the registration phase, while the sensing vehicles' real identities are RID_i for $i = 1, 2, \ldots, m$. The reputation center selects a cyclic group $\mathbb{G}_2$ with order q, and g_2 is a generator of $\mathbb{G}_2$. For each vehicle with RID_i, the reputation center chooses a random number $w_i \in \mathbb{Z}_q^*$ and a secret value $x \in \mathbb{Z}_q^*$. Then, it uses ElGamal encryption to generate the pseudonym $PID_i = \{PID_1, PID_2\}$, where $PID_1 = {g_2}^{wi}, PID_2 = RID_i \cdot {h_{pub}}^{wi}$ and $h_{pub} = {g_2}^x$. As follows, the reputation center chooses a random number $r_i \in [1, \mathrm{n}/4]$, and uses the BCP encryption algorithm to generate the ciphertext for the reputation value $[t_i]_{PK_{RC}} = \{T_i, T_i'\} = \{{PK_{RC}}^{r_i} \cdot (1+n)^t, {g_1}^{r_i}\} \left(\mathrm{mod} n^2\right)$. Then, the reputation center generates a signature for $[t_i]_{PK_{RC}}$ as $\sigma_i = h^{xi}$, where $x_i \in \mathbb{Z}_q$ is the signing key, $h = H\left([t_i]_{PK_{RC}}\right)$ and H is a cryptographic hash function. The reputation center publishes the system parameter $\{n, g_1, g_2, \mathbb{G}_1, \mathbb{G}_2, h_{pub}, H, y, PK_{DR}, PK_{RC}\}$ and sends $\left\{PID, [t_i]_{PK_{RC}}, \sigma_i\right\}$ to the vehicle with the real identity RID_i through RSU.

Step 2. Task Assignment

- **Standard value assignment:** The data requester releases the sensor task data m, and uses the proxy re-encryption to calculate the initial ciphertext $[m]$, and then uses its own public key and BCP encryption algorithm to generate ciphertexts $[d_0]_{PK_{DR}}$ and $[\Delta d]_{PK_{DR}}$, where

$$[d_0]_{PK_{DR}} = \left\{T_{d_0}, T'_{d_0}\right\} = \left\{PK_{DR}^r * (1+n)^{d_0}, g_1^r\right\} \left(\mathrm{mod} n^2\right)$$
$$[\Delta d]_{PK_{DR}} = \left\{T_{\Delta d}, T'_{\Delta d}\right\} = \left\{PK_{DR}^r * (1+n)^{\Delta d}, g_1^r\right\} \left(\mathrm{mod} n^2\right)$$

- **Generation of the task list:** The data requester divides the entire area into n task ranges. For the ith task block, The reputation center first initializes the key pair (PK_{Ti}, SK_{Ti}) of the task block. Then, the data requester uses the corresponding private key and BCP encryption algorithm to encrypt the central point coordinates (x_0, y_0), the range radius r, and the reputation threshold t_0, obtaining the ciphertext $[x_0]_{PK_{Ti}}$, $[y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}$. After the current task is initialized, the data requester adds the task TSK_i to the task list TSK. Finally, the task list $TSK = \{TSK_1, TSK_2 \ldots TSK_n\}$ is generated, where $TSK_i = \left\{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}, PK_{Ti}\right\}$ for $i = 1, 2, \ldots, n$.
- **Broadcast the tasks:** After all tasks are initialized, the data requester sends $I_d = \left\{[m], [d_0]_{PK_{DR}}, [\Delta d]_{PK_{DR}}, TSK, PK_{DR}\right\}$ to the cloud server. After receiving I_d, the cloud server broadcasts $I_c = \{PK_{DR}\}$ in the crowdsensing area.

Step 3. Vehicle Recruitment

- **Location Match:** The sensing vehicle receives I_c and obtains the current position coordinates (x, y), and uses the data requester's public key and BCP encryption algorithm to obtain the ciphertext $([x]_{PK_{DR}}, [y]_{PK_{DR}})$ of the position coordinates. Where:

$$[x]_{PK_{DR}} = \left\{T_x, T'_x\right\} = \left\{PK_{DR}^r \cdot (1+n)^x, g_1^r\right\} \left(\mathrm{mod} n^2\right)$$
$$[y]_{PK_{DR}} = \left\{T_y, T'_y\right\} = \left\{PK_{DR}^r \cdot (1+n)^y, {g_1}^r\right\} \left(\mathrm{mod} n^2\right)$$

  After that, it sends $I_v = \left\{PID, [t_i]_{PK_{RC}}, \sigma_i, ([x]_{PK_{DR}}, [y]_{PK_{DR}})\right\}$ to the cloud server.
- **Vehicle selection:** After receiving I_v, the cloud server first verifies whether the pseudonym PID and signature σ_i are legal. If the verification fails, the communication with the vehicle will be terminated. Otherwise, the cloud server determines which tasks the vehicle is participating in, and verifies whether the vehicle reputation value t meets the threshold t_0. Specifically, for the task $TSK_i = \left\{[x_0]_{PK_{Ti}}, [y_0]_{PK_{Ti}}, [r]_{PK_{Ti}}, [t_0]_{PK_{Ti}}\right\}$ in the task list TSK, the cloud server uses the additive homomorphic property and Secure Less Than Protocol (SLT) [21] to compare whether $[t_i]_{PK_{RC}}$ and $[t_0]_{PK_{Ti}}$ satisfies the following relationships:

$$\begin{cases} t_i \geq t_0 \\ (x - x_0)^2 + (y - y_0)^2 \leq r^2 \end{cases}$$

If the location and reputation value of the vehicle is legal, the cloud server adds the task sequence number i to the current vehicle's task list T.

– **Re-assign task:** After filtering the task list T, the cloud server re-encrypts the task message $[m]$ into the final ciphertext $[m]'$ using the proxy re-encryption algorithm. Finally, the cloud server sends $I_c = \{[m]', T\}$ to the sensing vehicle.

Step 4. Data Submission. The sensing vehicle receives the ciphertext $[m]'$ and decrypts it, obtaining the task information m. The sensing vehicle starts the sensing task and generates the sensing data d, and uses BCP encryption to generate the ciphertext of the sensing data $[d]_{PK_{Ti}}$. Finally, the sensing vehicle sends the $I_v = \{PID, [d]_{PK_{Ti}}, T\}$ to the cloud server.

Step 5. Data Verification and Information Update

– **Sensing data verification:** After receiving I_v, the cloud server first verifies the authenticity of the vehicle's pseudonym. If it passes the verification, the cloud server compares d' and Δd through $[d']_{PK\Sigma}$ and $[\Delta d]_{PK_{DR}}$. Specifically, the cloud server first calculates:

$$[d']_{PK\Sigma} = \begin{cases} [d - d_0]_{PK\Sigma} & d \geq d_0 \\ [d_0 - d]_{PK\Sigma} & d < d_0 \end{cases}$$

Then, the cloud server compares d' and Δd through $[d']_{PK\Sigma}$ and $[\Delta d]_{PK_{DR}}$. If $d' \leq \Delta d$, it means that the sensing data is valid. Otherwise, the cloud server refuses to receive this sensing data.

– **Generate reputation feedback report:** According to the verification result of sensing data, the cloud server generates a reputation feedback report F for each sensing vehicle and sends $I_c = \{PID, F\}$ to the reputation center, where

$$F = \begin{cases} 1 & d' \leq \Delta d \\ 0 & d' > \Delta d \end{cases}$$

– **Update reputation value and pseudonym:** the reputation center first verifies whether the PID is valid, if it is valid, the reputation center updates the reputation value of each sensing vehicle. Specifically, the reputation center calculates Δt of the vehicle's reputation value variation, and then calculates the updated reputation value as follows:

$$[t'_i]_{PK_{RC}} = \begin{cases} [t_i + \Delta t]_{PK_{RC}} = [t_i]_{PK_{RC}} * [\Delta t]_{PK_{RC}} \\ [t_i - \Delta t]_{PK_{RC}} = [t_i]_{PK_{RC}} * [\Delta t]_{PK_{RC}}{}^{n-1} \end{cases}$$

The reputation center generates a signature σ'_i for $[t'_i]_{PK_{RC}}$, and then updates the pseudonym of the vehicle as $PID' = \{PID'_1, PID'_2\}$, where $PID'_1 = g^{wi\prime}, PID'_2 = RID_i \cdot h_{pub}{}^{\mathrm{wi'}}$. Finally, the reputation center sends $\{PID', [t'_i]_{PK_{RC}}, \sigma'_i\}$ to the sensing vehicle whose real identity is RID_i. The sensing vehicle then updates its own identity and reputation value.

Step 6. Information Tracing

- **Identity tracing:** The vehicle's real identity RID is encrypted within $PID_i = \{PID_1, PID_2\}$, where $PID_1 = {g_2}^{wi}, PID_2 = RID_i \cdot {h_{pub}}^{wi}, h_{pub} = {g_2}^{x}$. Using the private key of the system, the reputation center can compute ${g_2}^{wi*x}$ and $RID_i = PID_2 \cdot {g_2}^{-wi*x} = RID_i \cdot {h_{pub}}^{wi} \cdot {g_2}^{-wi*x}$ to extracts the real identity of the sensing vehicle.
- **Reputation value tracing:** to trace the reputation value of sensing vehicles in multi-task crowdsensing, e.g. $[t_i]_{PK_{RC}} = \{T_i, T'_i{}_i\} = \{{PK_{RC}}^r * (1+n)^t, g_1^r\} \left(\mathrm{mod} n^2\right)$, using the master private key of the system $\lambda(n)$, the reputation center can first calculate $T_i^{\lambda(n)} \bmod n^2 = {g_1}^{b*r*\lambda(n)}(1+n)^{t*\lambda(n)} \bmod n^2 = (1+tn\lambda(n))$. Denote $L(x) = \frac{x-1}{n}$, the reputation center can calculate $t = L\left(T_i^{\lambda(n)} \bmod n^2\right) \cdot \lambda(n)^{-1} \bmod n$ to extracts the reputation value.
- **Location tracing:** to trace the location information of sensing vehicles in multi-task crowdsensing, we take $[x]_{PK_{DR}}$ as an example, using the master private key of the system $\lambda(n)$, the reputation center can calculate $x = L\left(T_i^{\lambda(n)} \bmod n^2\right) * \lambda(n)^{-1} \bmod n$. Similarly, the reputation center can calculate y and r to extracts the location information of the sensing vehicle.

6 Security and Efficiency Analysis

6.1 Security Analyses

In this section, we prove that our proposed scheme can achieve the desirable security properties, such as correctness, conditional privacy preserving and authentication.

Correctness: the detailed proof for this property is omitted because of page restriction. At a high level, one can easily see that encryption can be correctly decrypted and legitimate signature can be validated. Hence, if all participants are honest, the protocol will generate correct outputs.

Conditional Privacy Preserving: regarding this property, we prove that any vehicle's sensitive information, such as location, identity and reputation value, can be protected from the adversaries, and the trusted authority can retrieve this information if necessary.

- *Location privacy*: in the proposed scheme, the adversary $\mathcal{A}$ can obtain the message $I_v = \left\{PID, [t_i]_{PK_{RC}}, \sigma_i, ([x]_{PK_{DR}}, [y]_{PK_{DR}})\right\}$ sent by the sensing vehicle. Although $\mathcal{A}$ acquires the encrypted ciphertexts, she cannot derive the specific location coordinates of each sensing vehicle. In the tasks assignment and vehicle recruitment phases, BCP encryption is used to encrypt the location information. It has already been proved that BCP encryption is semantically secure under the DDH assumption over $\mathbb{Z}_{n^2}$. Hence, $\mathcal{A}$ cannot obtain the location of each sensing vehicle. Furthermore, during the sensing

task matching, the cloud server selects vehicles by comparing the vehicle's current location with the location required by the task. However, $\mathcal{A}$ cannot get the specific location of each sensing vehicle during this phase neither. Therefore, $\mathcal{A}$ cannot learn any information about the sensing vehicle's location. In other words, the proposed scheme can preserve location privacy.

- *Identity privacy*: In our proposed scheme, $\mathcal{A}$ may intend to learn the real identity RID of the sensing vehicle. The vehicle's real identity RID is encrypted in PID_i generated by the reputation center, where $PID_i = \{PID_1, PID_2\}, PID_1 = {g_2}^{wi}, PID_2 = RID_i \cdot {h_{pub}}^{wi}$ and $h_{pub} = g_2^x$. However, $\mathcal{A}$ cannot extract RID from $PID_2 = RID_i \cdot {h_{pub}}^{wi}$, because she does not have the corresponding secret key. Therefore, based on the DDH assumption over $\mathbb{Z}_{n^2}$, the proposed scheme preserves identity privacy.
- *Reputation value privacy*: In the proposed scheme, $\mathcal{A}$ may steal the sensing vehicle's reputation value t and sensing task's reputation threshold t_0, where $t_0 < t$. Specifically, from the task list TSK initialized by the data requester, $\mathcal{A}$ acquires the ciphertext but not the specific reputation value of each sensing task. Because the BCP encryption is semantically secure, $\mathcal{A}$ cannot learn any information about the sensing vehicle's reputation value, i.e. the proposed scheme can preserve reputation value privacy.
- *Traceability*: The vehicle's real identity RID is involved in pseudonym $PID_i = \{PID_1, PID_2\}$, where $PID_1 = {g_2}^{wi}, PID_2 = RID_i \cdot h_{pub}^{wi}, h_{pub} = {g_2}^x$. Using the private key of the system, the reputation center can compute ${g_2}^{wi*x}$ and $RID_i = PID_2 \cdot {g_2}^{-wi*x} = RID_i \cdot {h_{pub}}^{wi} \cdot {g_2}^{-wi*x}$ to extracts the real identity of the sensing vehicle. Similarly, the trusted authority can extract the location and reputation value of the proposed scheme. Therefore, the proposed scheme could provide traceability.

Authentication: in the proposed scheme, all transmitted messages are digitally signed by their sender. And the receiver will only accept the received messages if the verification of signature is valid. Based on the security of digital signature, the adversary cannot tamper or fabricate messages without being detected. Hence, our scheme achieves the authentication property.

Resistance to Other Attacks: our proposed scheme can resist the inference attack, reputation linkable attack, data pollution attack, Sybil attack, and reputation tamper attack.

- Based on the above analyses, the proposed scheme can prevent the data requester, the cloud server, and the RSUs from suffering location inference attack, identity inference attack, and reputation inference attack. In addition, because the reputation value is encrypted using a randomized encryption. The proposed scheme can resist the reputation linkable attack.
- In the real multi-task crowdsensing environment, malicious sensing vehicles may submit false sensing data, which may lead to unreliable sensing results. Specifically, the cloud server compares d' and Δd through $[d']_{PK_\Sigma}$ and $[\Delta d]_{PK_{DR}}$. If $d' \leq \Delta d$, it means the sensing data is valid. Otherwise, the

cloud server refuse to receive this sensing data. Hence, our scheme can resist data replacement attack.
– Because the pseudonym PID of each sensing vehicle is distributed and updated by the reputation center, a malicious sensing vehicle is unable to forge multiple identities. Thus, our scheme can resist the Sybil attack. To verify the reputation value of every sensing vehicle, the cloud server uses the additive homomorphic property and Secure Less Than Protocol (SLT) to compare whether $[t_i]_{PK_{RC}}$ and $[t_0]_{PK_{T_i}}$ satisfies the relationship $t_i \geq t_0$. Hence, the sensing vehicle cannot pass the verification if the reputation value is less than the reputation threshold. This implies that our scheme can resist the reputation tamper attack.

6.2 Efficiency Analyses

In the system initialization step, one first selects two large safe primes. This can be done via the Miller-Rabin algorithm and it only needs to be executed once. Then the data requester and the reputation center compute a key pair, each requires one exponentiation in G_1. As follows, the reputation center generates an ElGamal ciphertext and a BCP ciphertext. The former requires two exponentiations and one multiplication in G_2, while the latter requires three exponentiations and one multiplication in G_1. In the task assignment step, the data requester generates six BCP ciphertexts, requiring eighteen exponentiations and six multiplications in G_1. In the vehicle recruitment step, the sensing vehicle generates two BCP ciphertexts, requiring six exponentiations and two multiplications in G_1. In information tracing, identity tracing needs one exponentiation and one multiplication in G_2. In reputation value tracing, it needs one exponentiation and one multiplication in G_1, and in location tracing, it needs three exponentiations and three multiplications in G_1. All these computations can be done efficiently, hence the proposed scheme is generally efficient in pratical use.

7 Conclusion

In this paper, we have proposed a multi-task mobile crowdsensing scheme with conditional privacy preserving for vehicular networks. The conditional privacy preserving property covers identity privacy, location privacy, and reputation privacy simultaneously. And each sensing vehicle can participate in several sensing tasks at the same time. Besides, when updating the pseudonyms of sensing vehicles, the reputation center does not need to store any internal status (such as random numbers and ephemeral keys), which can effectively reduce the risks of DoS attacks. Moreover, theoretical analyses show that the proposed scheme overcomes the weaknesses in existing schemes and it is efficient for multi-task mobile crowdsensing. In the future, we plan to consider a more severe security model, removing the assumption that the data requester, the cloud server, the RSUs are honest-but-curious, and providing verification mechanisms for these entities.

References

1. Ganti, R.K., Ye, F., Lei, H.: Mobile crowdsensing: current state and future challenges. IEEE Commun. Mag. **49**(11), 32–39 (2011)
2. Chen, X., et al.: PAS: prediction-based actuation system for city-scale ridesharing vehicular mobile crowdsensing. IEEE Internet Things J. **7**(5), 3719–3734 (2020)
3. Huang, C., Lu, R., Choo, K.-K.R.: Vehicular fog computing: architecture, use case, and security and forensic challenges. IEEE Commun. Mag. **55**(11), 105–111 (2017)
4. Ma, L., Liu, X., Pei, Q., Xiang, Y.: Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. IEEE Trans. Serv. Comput. **12**(5), 786–799 (2019)
5. Ni, J., Zhang, K., Xia, Q., Lin, X., Shen, X.S.: Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing. IEEE Trans. Mob. Comput. **19**(6), 1317–1331 (2019)
6. Dai, M., Su, Z., Xu, Q., Wang, Y., Lu, N.: A trust-driven contract incentive scheme for mobile crowd-sensing networks. IEEE Trans. Veh. Technol. **71**, 1794–1806 (2021)
7. Zhang, C., et al.: TPPR: a trust-based and privacy-preserving platoon recommendation scheme in VANET. IEEE Trans. Serv. Comput. (2019)
8. Wang, L., Zhang, D., Yang, D., Lim, B.Y., Han, X., Ma, X.: Sparse mobile crowdsensing with differential and distortion location privacy. IEEE Trans. Inf. Forensics Secur. **15**, 2735–2749 (2020)
9. Sun, G., Sun, S., Yu, H., Guizani, M.: Toward incentivizing fog- based privacy-preserving mobile crowdsensing in the Internet of Vehicles. IEEE Internet Things J. **7**(5), 4128–4142 (2019)
10. Lu, R., Lin, X., Zhu, H., Ho, P.-H., Shen, X.: ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of the 27th Conference on IEEE INFOCOM, pp. 1903–1911 (2008)
11. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. J. Comput. Secur. **15**(1), 39–68 (2007)
12. Zhao, B., Tang, S., Liu, X., Zhang, X.: PACE: privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing. IEEE Trans. Mob. Comput. **20**(5), 1924–1939 (2020)
13. Gao, S., Chen, X., Zhu, J., Dong, X., Ma, J.: TrustWorker: a trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing. IEEE Trans. Serv. Comput. (2021)
14. Hu, H., Lu, R., Zhang, Z., Shao, J.: REPLACE: a reliable trust- based platoon service recommendation scheme in VANET. IEEE Trans. Veh. Technol. **66**(2), 1786–1797 (2016)
15. Hu, H., Lu, R., Huang, C., Zhang, Z.: TripSense: a trust-based vehicular platoon crowdsensing scheme with privacy preservation in VANETs. Sensors **16**(6), 803 (2016)
16. Liu, Z., et al.: BTMPP: balancing trust management and privacy preservation for emergency message dissemination in vehicular networks. IEEE Internet Things J. **8**(7), 5386–5407 (2021)
17. Liu, Z., et al.: LPPTE: a lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications. Inf. Fusion **73**, 144–156 (2021)
18. Cheng, Y., Ma, J., Liu, Z., Wu, Y., Wei, K., Dong, C.: A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing

in vehicular networks. IEEE Trans. Dependable Secure Comput. (2022). https://doi.org/10.1109/TDSC.2022.3163752
19. Nkenyereye, L., Islam, S.R., Bilal, M., Abdullah-Al-Wadud, M., Alamri, A., Nayyar, A.: Secure crowd-sensing protocol for fog-based vehicular cloud. Futur. Gener. Comput. Syst. **120**, 61–75 (2021)
20. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_16
21. Liu, X., Deng, R.H., Choo, K.R., Weng, J.: An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys. IEEE Trans. Inf. Forensics Secur. **11**(11), 2401–2414 (2016). https://doi.org/10.1109/TIFS.2016.2573770
22. Bresson, E., Catalano, D., Pointcheval, D.: A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 37–54. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40061-5_3
23. Engoulou, R.G., Bellaıche, M., Pierre, S., Quintero, A.: VANET security surveys. Comput. Commun. **44**, 1–13 (2014)
24. Guette, G., Heen, O.: A TPM-based architecture for improved security and anonymity in vehicular ad hoc networks. In: 2009 IEEE Vehicular Networking Conference (VNC), pp. 1–7. IEEE (2009)
25. He, D., Zeadally, S., Xu, B., Huan, X.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **10**(12), 2681–2691 (2015). https://doi.org/10.1109/TIFS.2015.2473820