Optimal Location Privacy Preserving and Service Quality Guaranteed Task Allocation in Vehicle-Based Crowdsensing Networks

Yongfeng Qian, Yujun Ma, Jing Chen, *Member, IEEE*, Di Wu, *Senior Member, IEEE*, Daxin Tian, *Senior Member, IEEE*, and Kai Hwang

***Abstract*— With increasing popularity of related applications of mobile crowdsensing, especially in the field of Internet of Vehicles (IoV), task allocation has attracted wide attention. How to select appropriate participants is a key problem in vehicle-based crowdsensing networks. Some traditional methods choose participants based on minimizing distance, which requires participants to submit their current locations. In this case, participants' location privacy is violated, which influences disclosure of participants' sensitive information. Many privacy preserving task allocation mechanisms have been proposed to encourage users to participate in mobile crowdsensing. However, most of them assume that different participants' task completion quality is the same, which is not reasonable in reality. In this paper, we propose an optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks. Specifically, we utilize differential privacy to preserve participants' location privacy, where every participant can submit the obfuscated location to the platform instead of the real one. Based on the obfuscated locations, we design an optimal problem to minimize the moving distance and maximize the task completion quality simultaneously. In order to solve this problem, we decompose it into two linear optimization problems. We conduct extensive experiments to demonstrate the effectiveness of our proposed mechanism.**

***Index Terms*— Location privacy preserving, mobile crowdsensing, service quality, task allocation, vehicular network.**

Manuscript received May 30, 2020; revised November 14, 2020; accepted January 19, 2021. Date of current version July 12, 2021. This work was supported in part by the National Natural Science Foundation of China under Grant 61902363, in part by the Shenzhen Institute of Artificial Intelligence and Robotics for Society (AIRS) under Grant AC01202107002, in part by the Open Research Project of the Hubei Key Laboratory of Intelligent Geo-Information Processing under Grant KLIGIP-2018B10, in part by the National Natural Science Foundation of China under Grant U1836202 and Grant 61772383, in part by the Foundation of Ministry of Education for Pre-Research Equipment under Grant 6141A02033341, and in part by the Henan Province Key Scientific Research Project of Colleges and Universities under Grant 18A520043. The Associate Editor for this article was N. Kumar. *(Corresponding authors: Yongfeng Qian; Kai Hwang.)*

Yongfeng Qian is with the School of Computer Science, China University of Geosciences, Wuhan 430074, China, and also with the Hubei Key Laboratory of Intelligent Geo-Information Processing, China University of Geosciences, Wuhan 430074, China (e-mail: yfqian@cug.edu.cn).

Yujun Ma is with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: yujun.hust@gmail.com).

Jing Chen is with the School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China (e-mail: chenjing@whu.edu.cn).

Di Wu is with the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China, and also with the Guangdong Key Laboratory of Big Data Analysis and Processing, Guangzhou 510006, China (e-mail: wudi27@mail.sysu.edu.cn).

Daxin Tian is with the School of Transportation Science and Engineering, Beihang University, Beijing 100191, China (e-mail: dtian@buaa.edu.cn).

Kai Hwang is with the School of Data Science, The Chinese University of Hong Kong (Shenzhen), Shenzhen 518172, China, and also with the Shenzhen Institute of Artificial Intelligence and Robotics for Society, Shenzhen 518129, China (e-mail: hwangkai@cuhk.edu.cn).

Digital Object Identifier 10.1109/TITS.2021.3086837

I. Introduction

With continuous development of crowdsensing and the tendency of various types and functions of sensors in mobile devices [1], [2], many tasks can be assigned to participants (i.e., people who participate in the task) [3]. Participants use their mobile devices to collect the data required by the task and finally feedback the data [4], [5]. For example, when determining the noise situation in a certain area, if noise detection devices are deployed directly, the task is too costly and requires too much time [6].

However, the use of mobile crowdsensing can assign the task to participants in the specific area. Only the corresponding incentive mechanism needs to be set to reward these participants [7], [8], which has great advantages in both cost and delay compared with traditional schemes [9].

Mobile crowdsensing users' moving speed is low, which leads to a limited sensing range. However, some tasks need the participants move a long distance to execute sensing tasks, such as in an air pollution sensing task when the executed location is at isolated areas with few people around. In such a situation, the task is difficult to recruit participants even though the task is important and the reward is high. One solution is utilizing vehicular crowdsensing [10], in which vehicles can execute tasks with their mobile phones [11], [12].

However, after the release of a task, how to select appropriate participants to perform the task, or task assignment, is a key issue. This strongly influences the completion rate and incentive mechanism of the task [13]. The traditional solution to the task assignment problem is to select the participant closest to the task location to perform the task according to the locations submitted by participants and the location required for task execution. As for such a task assignment process, it is easy to cause leakage of participants' location privacy [14], [15]. An attacker may infer the participant's information, such as their work place, home address, hobbies, and other variables, which would decrease the interest of

participants in task execution, thus the number of participants would decrease, and then effective assignment of tasks would be influenced [16], [17].

In order to encourage mobile crowdsensing users (i.e., vehicles in this paper) to join in the crowdsensing platform and execute tasks, location privacy must be satisfied [18], [19]. In order to effectively protect the location privacy of participants during task assignment [20], we can apply one of the following methods:

- Anonymized method [21], [22]. With anonymization technology, the identity information of the participant can be anonymized, so the location submitted by the participant will not be associated with their identity information [23], [24].
- Dummy location method. With this strategy, the participant can submit multiple locations, which can confuse the attacker's guess of the participant's true location [25].
- Location confusion method [26], [27]. With this strategy, the true location can be changed to other locations at submission, thus the attacker can only see the location of the participant after disturbance, instead of directly obtaining the true location.
- Location privacy protection based on differential privacy [28], [29]. Differential privacy can provide strict mathematical standards for data privacy protection. At the same time, no matter what prior knowledge an attacker has, appropriate strategies can be designed to meet the needs of users [30], [31].

From the above several strategies, an attacker with prior knowledge cannot be resisted with the first three strategies [32]. However, with the differential privacy strategy, the prior information of attackers can be well handled [33]. Therefore, the differential privacy mechanism is adopted in this paper to solve the problem of location privacy protection in the process of task assignment [34].

However, rather than directly applying differential privacy to location privacy protection, service quality should also be considered. In addition, considering the vehicular network environment, how to design an optimal task allocation mechanism is discussed in this paper. Thus, we utilize differential privacy to preserve location privacy of participants, and also guarantee each task to set task completion quality in the vehicle-based crowdsensing networks. With the objective to minimize participants' moving distance and maximize tasks' quality, we design an optimal mechanism in this paper. To be specific, the main contributions of this paper are as follows:

- We propose an optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks, which can preserve location privacy and improve task quality at the same time.
- We design an optimal mechanism with two objectives, which can minimize participants' moving distance and maximize the whole service quality at the same time. To solve the optimization problem, we decompose it into two linear optimization problems, which can be solved easily.

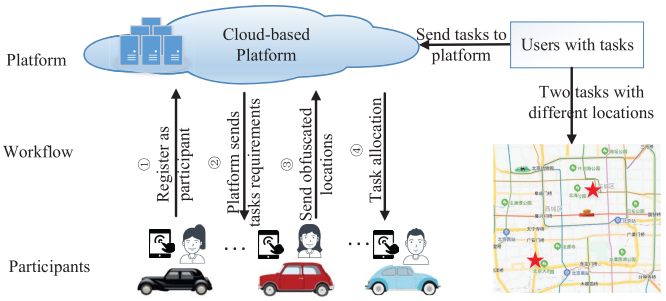


Fig. 1. Architecture of task allocation for vehicle-based crowdsensing networks.

- We conduct extensive experiments to verify that our proposed mechanism can reduce the distance and improve quality, compared with traditional methods.

The remainder of this paper is organized as follows. We introduce the system in Section II. We formulate the model in Section III, and conduct the performance evaluation in Section IV. Finally, we conclude this paper in Section V.

II. System Illustration

In this section, we first introduce the system model, and then describe the application of differential privacy to location privacy. This is followed by outlining the attack model, and finally setting out the main objectives of this paper.

A. System Model

In crowdsensing IoV, vehicles can take advantage of faster travel speeds and greater computing, communication, and storage resources to engage in the task at hand. As shown in Fig. 1, the whole vehicle-based crowdsensing network can be divided into three parts: (i) participants, i.e., vehicle users; (ii) task publishers, i.e., those who own the tasks, which may include detecting air pollution or traffic conditions; and (iii) the platform, which connects task publishers and participants, distributes task publishers' tasks to participants, and passes the data collected by participants to task publishers. Tasks in the network usually require the deployment of a large number of dedicated devices, but one of the drawbacks is a high cost. Through a crowdsensing platform, these tasks can be distributed to participants, and data collection can be distributed to and completed by the participants' own sensors.

In the system model considered in this paper, the focus is assingning task publishers' tasks to participants. It is common practice to choose participants who are closer to the task location to perform the task, but this requires the platform to know the actual location of participants in advance. In order to avoid leaking participants' private information, including their true locations, participant locations must be privacy-protected. The information protection model adopted in this paper is differential privacy, which perturbs the true location of participants and successfully obfuscates their information. Therefore, in the entire vehicle-based crowdsensing network system, after the platform publishes tasks, vehicles can submit which tasks they are interested in, along with their perturbed locations, to the platform.

While ensuring that participants submit perturbed locations, the platform must still select appropriate participants based on the quality of services (QoS) requirements of the task publishers' tasks. For this reason, QoS is used in our system model as an important metric to ensure that the optimal participants are selected. By combining the above two considerations, we use differential privacy to protect participants' location data; meanwhile, the quality of our selected participants reaches the required QoS of the task.

B. Differential Privacy

Differential privacy applied to location data has proven to be an effective form of privacy protection [9], [26], [29]. Differential privacy here converts the real location into a perturbed location as a probability function, and the subsequent task assignment is then based on the perturbed location.

We assume that the particular set of locations under consideration is L, and if the perturbation mechanism P satisfies $\epsilon-$differential privacy, then

$$p(l_o|l_r^1) \leq e^{\epsilon d(l_r^1, l_r^2)} p(l_o|l_r^2), \tag{1}$$

where $p(l_o|l_r^1)$ and $p(l_o|l_r^2)$ represent the probability of perturbing the true locations l_r^1 and l_r^2 to the perturbed location l_o, respectively. Without loss of generality, and assuming that l_r represents the true location, $P(l_o|l_r)$ denotes the probability of perturbing that true location l_r to the location l_o. $d(l_r^1$ and $l_r^2)$ denote the distance between the true locations l_r^1 and l_r^2, respectively. Meanwhile, ϵ represents the privacy budget. If the user has a higher privacy requirement, then a smaller ϵ can be set; conversely, for lower privacy requirements, a larger ϵ can be set.

The inequality (1) demonstrates that when applying differential privacy to location data protection, for any two real locations l_r^1 and l_r^2, the probability of mapping these two locations into perturbed locations l_o is similar. Moreover, the closer these two real locations l_r^1 and l_r^2 are to each other, the more difficult it is for the attacker to distinguish them.

C. Attack Model

In this paper, the platform is considered *honest-but-curious*, that is, the platform assigns tasks to participants based on their submitted perturbed locations, and at the same time, the platform is curious about the true locations of participants [35].

Given the aforementioned perturbation mechanism P, $p(l_r|l_o)$ is the probability of mapping the perturbed location l_o to the true location l_r. Based on probability theory, we can then obtain the following:

$$p(l_r|l_o) = \frac{p(l_o|l_r)p(l_r)}{p(l_o)} = \frac{p(l_o|l_r)p(l_r)}{\sum_{l_r} p(l_o|l_r)p(l_r)} \tag{2}$$

By (2), we find that the probability of the attacker (i.e., platform) to reconstruct the submitted perturbed location l_o into the true location l_r is $p(l_r|l_o)$, which is related to the probability of the true location $p(l_r)$ and $p(l_o|l_r)$. The former can be obtained from historical data, while the latter is determined by the perturbation mechanism P. Without loss of generality, we assume that the perturbation mechanism P is accessible to the attacker because, since the perturbation mechanism P is obtained externally, the mechanism is also easily obtained by the platform. Furthermore, it is clear that $p(l_r|l_o)$ is bounded. Therefore, although the attacker can obtain partial prior knowledge, the probability of reconstructing the true location l_r from the perturbed location l_o is still limited.

D. Quality Guaranteed for Tasks

Considering the tasks published on the platform, participant data must be collected by the platform to complete a given task. However, that each participant submits a perturbed location inevitably introduces an issue of decreasing accuracy in task assignment. For this reason, when setting up the task assignment mechanism, the QoS of each task must also be used as a metric during participant selection.

When performing task assignment, we must design a suitable participant selection mechanism that maximizes the quality of the selected participant performing the task. Therefore, the quality of each vehicle user's task completion needs to be obtained by the platform. A key question is how to obtain the quality of each vehicle user.

The quality of each vehicle user's task completion can be obtained by learning from historical data. For example, even though a vehicle user registered on the platform does not publish its real location data, the platform still has access to the user's registration ID and additional submitted data. Over time, each participant's historical data becomes available to the platform. However, this is not the case for newly registered users. Such users are called unknown workers. For unknown workers whose quality information cannot be obtained in advance, we can adopt a reinforcement learning approach that takes the quality of each user's task execution as a reward to learn which users are of higher quality.

E. Design Objectives

In this paper, we design a task assignment strategy using both location data protection and a QoS guarantee for crowdsensing IoV. The design objectives can be summarized as follows:

- **Preserving the location privacy of participants.** To encourage greater user participation in tasks and to avoid leaking participant location data, our first goal is to protect the locations of all participants using differential privacy.
- **Each published task's completion quality must meet predetermined quality requirements**. Since each participant submits their location after perturbation, task assignment will inevitably yield lower assignment accuracy than if tasks were assigned with true participant locations. Furthermore, each publisher pays a certain amount of money to each participant who submits data after completing the task. If there is no effective data feedback, task publishers are less motivated to participate on the platform. In order for task publishers to obtain valid data, we design a task assignment strategy that also meets the task publisher's task quality requirements. This is the second goal of the proposed mechanism.

Based on the above two objectives, we design an optimized task assignment policy that, (a) perturbs the real location of each participant to protect the privacy of the participant's location, and (b) ensures that each published task meets its quality requirements.

III. Model Formulation

In this section, we consider the use of vehicle users to complete tasks in a crowdsensing IoV, and ensure that the location privacy of each vehicle user is not compromised while also satisfying certain task quality requirements.

A. Problem Formulation

We assume that the number of all vehicle participants is m, and define their set as $W = \{w_1, w_2, \ldots, w_m\}$. The real location of each participant w_j is l_r^j, and the perturbed location after differential privacy protection is l_o^j. Since the task completion quality of each participant w_j can be obtained through learning, the participant's quality can be denoted as q_j. The set of qualities of all users is denoted as Q, and $Q = \{q_1, q_2, \ldots, q_m\}$.

Furthermore, we assume that the number of all tasks is n, and define their set as $T = \{t_1, t_2, \ldots, t_n\}$. For each task t_i, the location of the data to be collected is l_i^t. For each task t_i, when the task publisher publishes on the platform, it needs to publish the location, time, and reward of the data collection required by the task. The platform forwards this data to all vehicle users. If a vehicle user w_j is interested in the task t_i, then w_j returns $\{t_i, l_o^j\}$ to the platform.

Therefore, for each task t_i, the corresponding interested participants are the set W_{t_i}, and every element of W_{t_i} is participant w_j, that is, $w_j \in W$ and w_j applies for t_i. For each task t_i, the data to be collected may contain multiple locations. Thus, the number of participants needed to complete each task t_i is set to N_{t_i}. For this reason, appropriate participants need to be selected from the set W_{t_i} to perform each task.

It is necessary for the platform to use perturbed locations for task assignment. Thus, we denote $x(t_i, w_j)$ as the task allocation strategy, and $x(t_i, w_j) = 1$ means the participant w_j is selected for t_i, that is the task t_i has been allocated to w_j. $x(t_i, w_j) = 0$ means the task t_i has not been allocated to w_j. We write all $x(t_i, w_j)$ as the set X, where $w_j \in W_{t_i}$. The equation of $x(t_i, w_j)$ is formulated as follows:

$$x(t_i, w_j) = \begin{cases} 1 & \text{Task } t_i \text{ is allocated to } w_j \\ 0 & \text{Otherwise} \end{cases} \tag{3}$$

To preserve the location privacy of participants, any two participants w_i and w_j should satisfy

$$p(l_o|l_r^i) \le e^{\epsilon d(l_r^i, l_r^j)} p(l_o|l_r^j) \tag{4}$$

Appropriate participants are those closest to the task location based on their perturbed location to collect data. Suppose $d(w_j, t_i)$ denotes the distance from the real location of w_j to the task t_i. The true location of each w_j is not readily available, but can be obtained by the following equation:

$$d(w_j, t_i) = \sum_{w_j \in W_{t_i}} p(l_r^j) p(l_o^j|l_r^j) d(l_o^j, l_i^t) \tag{5}$$

where $d(l_o^j, l_i^t)$ denotes the distance from the perturbed location l_o^j of w_j to the task location l_i^t. One of the platform's goals of participant selection is to minimize the total distance from the participants to the task location. We denote the total distance as D:

$$D = \sum_{t_i \in T} \sum_{w_j \in W_{t_i}} x(t_i, w_j) p(l_r^j) p(l_o^j|l_r^j) d(l_o^j, l_i^t) \tag{6}$$

According to the task completion quality q_j of each vehicle user w_j, we need to design a task assignment mechanism $x(t_i, w_j)$ that maximizes the total completion quality of the selected participants. The task quality of each task t_i is $\sum_{w_j \in W_{t_i}} x(t_i, w_j) q_j$ according to the participants who are interested in the task. Then, the total quality is denoted as Q, which is expressed as follows:

$$Q = \sum_{t_i \in T} \sum_{w_j \in W_{t_i}} x(t_i, w_j) q_j \tag{7}$$

Our goal is to minimize the distance traveled by the selected participants and to maximize task completion quality, i.e., $\min D$ and $\max Q$, simultaneously. To unify these optimization objectives, we choose the variable $\xi \in [0, 1]$, unifying the two objectives as $\min(D - \xi Q)$. In summary, the task assignment mechanism we establish can be expressed as follows:

$$\underset{\mathbf{P},\mathbf{X}}{\text{minimize}} \ \{D - \xi Q\} \tag{8a}$$

$$\text{subject to } p(l_o|l_r^i) \le e^{\epsilon d(l_r^i, l_r^j)} p(l_o|l_r^j), \tag{8b}$$

$$\sum_{t_i \in T} x(t_i, w_j) \le 1, \tag{8c}$$

$$\sum_{w_j \in W_{t_i}} x(t_i, w_j) = N_{t_i}, \tag{8d}$$

$$\sum_{l_o \in L} p(l_o|l_r^j) = 1, \tag{8e}$$

$$p(l_o) = \sum_{j=1}^{m} p(l_o|l_r^j) p(l_r^j), \tag{8f}$$

$$x(t_i, w_j) = \{0, 1\}, \tag{8g}$$

$$q_j \in [0, 1], \quad j = 1, 2, \ldots, m. \tag{8h}$$

Our objective function is to select the appropriate $x(t_i, w_j)$ while minimizing the distance traveled by participants and maximizing the task completion quality. The first constraint to our function is to satisfy location indistinguishability under differential privacy. The second constraint is that each participant w_j can be assigned at most one task. The third constraint states that for each task t_i, the number of participants to be selected must satisfy a predefined N_{t_i} for that task. The fourth restriction states that when using differential privacy, the probability of perturbing any real location l_r^j to location l_o is 1, and L denotes all locations. The fifth restriction states that the proposed location-protecting differential privacy mechanism must satisfy the probabilistic condition that, for any one perturbed location l_o, its probability can be solved using the full probability formula. The sixth restriction states

TABLE I
FREQUENTLY USED NOTATIONS

Notations	Description
n	Total quantity of tasks
m	Total amount of participants
T	Task set
t_i	Task i
l_i^t	Location of task t_i
W_{t_i}	Participants for t_i
λ_{t_i}	Number of locations to completet_i
l_r^j	True locations of participant w_j
l_o^j	Disturbed locations of participant w_j
$x(t_i, w_j)$	Task allocation strategy
X	Set of $x(t_i, w_j)$
q_j	Task completion quality of w_j
N_{t_i}	Number of participants for t_i

the range of values for $x(t_i, w_j)$. The seventh constraint states the range of values for q_j.

B. Optimization Analysis

In this section, we analytically solve the above optimization problem. Since the problem is to optimize both the distance traveled by participants and the quality of task completion, we first decompose the optimization problem when solving it. From the perspective of optimization, the objective of maximizing task completion quality determines the task assignment policy X with higher task completion quality. Meanwhile, the objective of minimizing the distance traveled by participants determines the perturbation policy P. To this end, we convert the above optimization problem into two optimization problems, solving for task assignment X and location perturbation P policies.

The optimization problem with respect to the task assignment policy X is as follows:

$$\underset{\mathbf{X}}{\text{minimize}} \ -\xi Q \tag{9a}$$

$$\text{subject to} \sum_{t_i \in T} x(t_i, w_j) \le 1, \tag{9b}$$

$$\sum_{w_j \in W_{t_i}} x(t_i, w_j) = N_{t_i}, \tag{9c}$$

$$x(t_i, w_j) = \{0, 1\}, \tag{9d}$$

$$q_j \in [0, 1], \quad j = 1, 2, \ldots, m. \tag{9e}$$

Since the optimization problem of task assignment policy X has been transformed into a single objective optimization problem, the parameter ξ can be omitted. This improves the optimization objective, and allows us to obtain

$$\underset{\mathbf{X}}{\text{maximize}} \sum_{t_i \in T} \sum_{w_j \in W_{t_i}} x(t_i, w_j) q_j \tag{10a}$$

$$\text{subject to} \sum_{t_i \in T} x(t_i, w_j) \le 1, \tag{10b}$$

$$\sum_{w_j \in W_{t_i}} x(t_i, w_j) = N_{t_i}, \tag{10c}$$

$$x(t_i, w_j) = \{0, 1\}, \tag{10d}$$

TABLE II
SIMULATION SETTINGS

Variable	Value
n	[1,10,19,28,37]
m	[10,20,30,40,50]
k	[3,5,7,9,11]
q_i	Standard normal distribution
ϵ	[ln(1.5),ln(2),ln(2.5),ln(3),ln(3.5)]

$$q_j \in [0, 1], \quad j = 1, 2, \ldots, m. \tag{10e}$$

Based on the above optimization problem solving for X, we can obtain the task assignment policy X. The optimization problem regarding the location perturbation policy P can be obtained as follows:

$$\underset{\mathbf{P}}{\text{minimize}} \sum_{t_i \in T} \sum_{w_j \in W_{t_i}} x(t_i, w_j) p(l_r^j) p(l_o^j | l_r^j) d(l_o^j, l_i^t) \tag{11a}$$

$$\text{subject to} \ p(l_o | l_r^i) \le e^{\epsilon d(l_r^i, l_r^j)} p(l_o | l_r^j), \tag{11b}$$

$$\sum_{l_o \in L} p(l_o | l_r^j) = 1, \tag{11c}$$

$$p(l_o) = \sum_{j=1}^{m} p(l_o | l_r^j) p(l_r^j). \tag{11d}$$

Task assignment policy X can be easily solved by the first decomposition of the optimization problem. This is because the first optimization problem, which is already a linear optimization problem, can be solved by existing toolkits. The second optimization problem, with known X, is converted into a linear optimization problem on P. The location perturbation policy P is then obtained by a similar method.

IV. PERFORMANCE EVALUATION

In this section, we first introduce the experimental data and evaluation metric used. We then provide the benchmarks used and conclude with experimental results and analysis.

A. Parameter Setting

In order to conveniently indicate user locations, we set the targeted area to $k \times k$ grids, and the center of each grid is set to the location of all users in the coverage area. Note that the location here refers to the user's real location, and that the real locations of all users in the area are taken as the center of the grid. Each grid is set to $2km \times 2km$. In this experiment, k takes values in the range [3,5,7,9,11]. The number of all participants m is in the range [10,20,30,40,50]. Meanwhile, the number of all tasks n is in the range [1,10,19,28,37]. The quality of each task q_i obeys the standard normal distribution. The privacy budget ϵ takes is in the range of [ln(1.5), ln(2), ln(2.5), ln(3), ln(3.5)]. Table II shows the settings for different parameters.

B. Evaluation Metric

1) Average Task Quality (ATQ): Average task quality represents the whole task completion quality after task allocation,

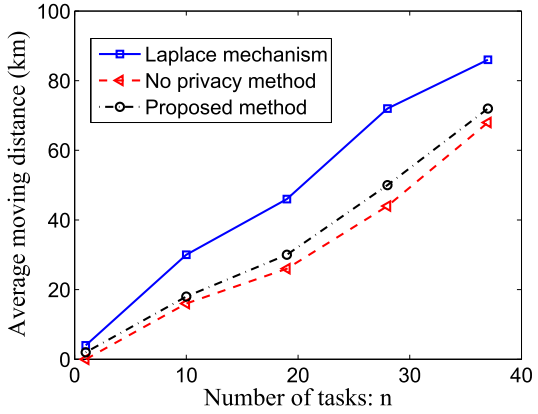


Fig. 2. Impact of the number of tasks on average moving distance.

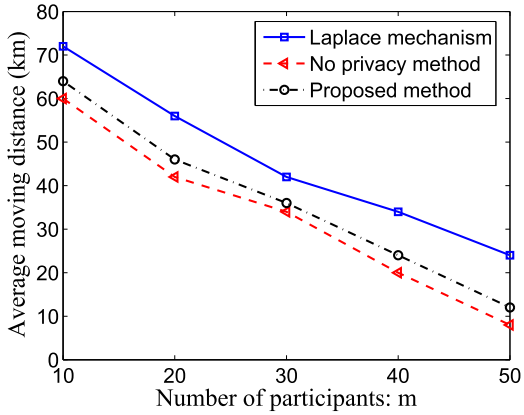


Fig. 3. Impact of the number of participants on average moving distance.

which can be denoted as follows,

$$ATQ = \frac{1}{n}\sum_{t_i \in T}\sum_{w_j \in W_{t_i}} x(t_i, w_j) q_j. \tag{12}$$

2) Average Moving Distance (AMD): The average moving distance represents the whole distance of all participants during the task assignment process. Its mathematical expression is as follows:

$$AMD = \frac{1}{m}\sum_{t_i \in T}\sum_{w_j \in W_{t_i}} x(t_i, w_j) p(l_r^j) p(l_o^j | l_r^j) d(l_o^j, l_i^t) \tag{13}$$

C. Benchmarks

In this experiment, we introduce two methods to compare with our mechanism.

- Laplace mechanism [29]. Laplace mechanism is to add Laplace noise when the differential privacy mechanism is applied.
- Optimal mechanism without privacy preserving. We utilize the optimal mechanism without the differential privacy technology when the platform to design task allocation, denoted by No-Privacy method.

D. Results

1) Impact of the Number of Tasks on Average Moving Distance: It can be seen from Fig. 2 that all the three algorithms (Laplace mechanism, No privacy method and our proposed method) will lead to the continuous increase of average moving distance, as the number of tasks n increases. In comparison of the three mechanisms, the average moving distance brought by Laplace mechanism is the largest. Compared with no privacy method, our proposed mechanism brings a larger moving distance. This is because the platform knows all participants' real locations in terms of no privacy method. However, our proposed method has little difference as for no privacy method, which also shows the effectiveness of our method. Moreover, compared with Laplace mechanism, our proposed method has smaller average moving distance.

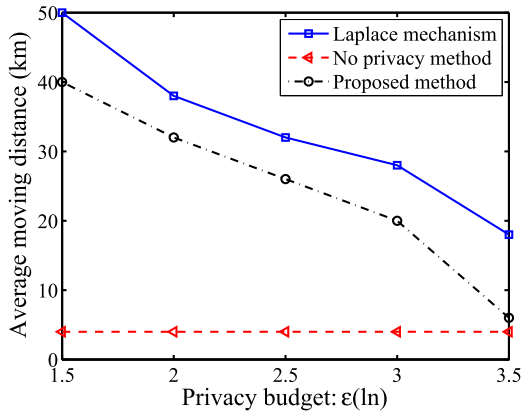


Fig. 4. Impact of privacy budget on average moving distance.

2) Impact of the Number of Participants on Average Moving Distance: Fig. 3 describes the relationship between the number of participants and the average moving distance. It can be seen from Fig. 3 that with the increase of number of participants, the average moving distance shows a downward trend. This is because when the number of participants increases, there are more choices to assign tasks for the task publishing platform to consider, which means that the optimal participant can be chosen through better selection. This reduces the average moving distance. Compared with Laplace mechanism, our method's average moving distance is smaller. As mentioned before, no privacy method's average moving distance is smaller than that of our method. However, the no privacy method does not preserve participants' locations, which makes it hard to apply in reality.

3) Impact of Privacy Budget on Average Moving Distance: Fig. 4 describes the influence of differential privacy budget ϵ on the average moving distance. As ϵ increases, the average moving distance decreases in terms of Laplace mechanism and our proposed method. This is because larger ϵ denotes the lower degree of privacy preserving, which leads to a lower interference of disturbance locations of participants on the accuracy of task allocation. Thus, the average moving distance shows a downward trend. In addition, privacy budget ϵ can not influence on the no privacy. Compared with Laplace method,

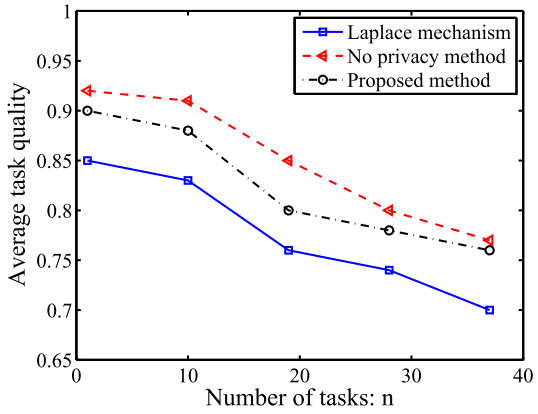


Fig. 5. Impact of the number of tasks on average task quality.

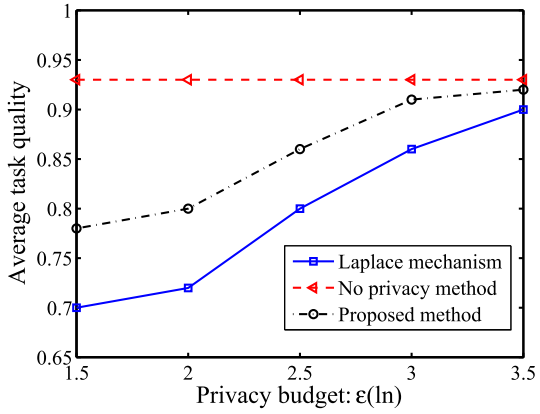


Fig. 7. Impact of privacy budget on average task quality.

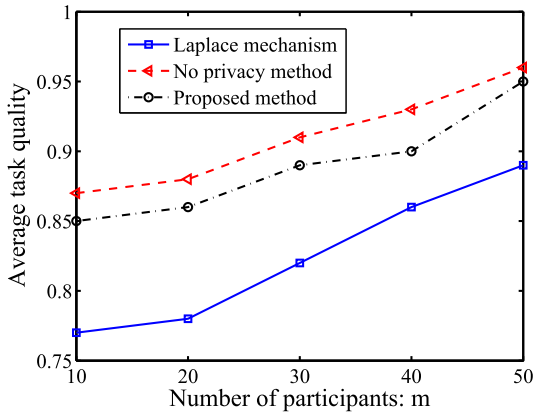


Fig. 6. Impact of the number of participants on average task quality.

our proposed method has a smaller average moving distance. This is because our mechanism can bring global optimization, while Laplace method can realize the local optimum.

4) Impact of the Number of Tasks on Average Task Quality: Fig. 5 describes the impact of the number of tasks on average task quality. From Fig. 5 we can observe, our proposed method has higher average task quality than Laplace mechanism, and lower task quality than no privacy method. Since no privacy method did not preserve participants' location privacy, the platform can obtain the real locations and thus achieve high performance. The other algorithms have protected location privacy, which brings an accuracy decrease is acceptable for both platform and task owners. In addition, the average task quality shows a slow downward trend as the number of task increases. With a greater number of tasks, fewer participants can be selected, and this ultimately reduces the task completion quality.

5) Impact of the Number of Participants on Average Task Quality: Fig. 6 shows the impact of the number of participants m on average task quality. From Fig. 6, we can observe, average task quality increases as m grows. With the increase of the number of participants, the platform can find more participants to execute each task, which leads to increased of task completion quality. Compared with Laplace mechanism, our proposed mechanism shows a higher average task quality as the number of participants increases.

6) Impact of Privacy Budget on Average Task Quality: Fig. 7 shows the impact of privacy budget ϵ on average task quality. As shown in Fig. 7, we can observe that ϵ has no effect on no privacy method, which is consistent with the impact of ϵ on the average moving distance. That is because no privacy method did not utilize the privacy budget, i.e., parameter ϵ, no influence on the result in turn. Compared with Laplace mechanism, our method proposed in this paper shows a higher average task quality.

V. Conclusion

In this paper, we proposed an optimal task allocation mechanism with considering location privacy preserving and service quality in vehicle-based crowdsensing networks. It utilizes differential privacy to preserve location privacy of participants. Moreover, it allows every task to set its completion quality. We design the optimal mechanism which aims at minimizing participants' moving distance and improving the service quality. In order to solve this optimization problem, we decompose it into two linear optimization problems. The proposed optimal mechanism is verified by extensive experiments.

References

[1] X. Jin, R. Zhang, Y. Chen, T. Li, and Y. Zhang, "DPSense: Differentially private crowdsourced spectrum sensing," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 296–307.

[2] M. Chen, Y. Hao, H. Gharavi, and V. Leung, "Cognitive information measurements: A new perspective," *Inf. Sci.*, vol. 505, pp. 487–497, Dec. 2019.

[3] B. Guo, Y. Liu, W. Wu, Z. Yu, and Q. Han, "ActiveCrowd: A framework for optimized multitask allocation in mobile crowdsensing systems," *IEEE Trans. Human-Mach. Syst.*, vol. 47, no. 3, pp. 392–403, Jun. 2017.

[4] S. Oya, C. Troncoso, and F. Pérez-González, "Back to the drawing board: Revisiting the design of optimal location privacy-preserving mechanisms," in *Proc. ACM CCS*, Oct. 2017, pp. 1959–1972.

[5] M. Khabbaz, M. Hasna, C. M. Assi, and A. Ghrayeb, "Modeling and analysis of an infrastructure service request queue in multichannel V2I communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 3, pp. 1155–1167, Jun. 2014.

[6] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2015, pp. 1017–1025.

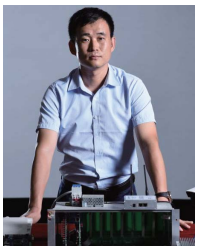
[7] Z. Wang, J. Li, J. Hu, J. Ren, Z. Li, and Y. Li, "Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2019, pp. 2053–2061.
[8] J. Xu, Z. Rao, L. Xu, D. Yang, and T. Li, "Incentive mechanism for multiple cooperative tasks with compatible users in mobile crowd sensing via online communities," *IEEE Trans. Mobile Comput.*, vol. 19, no. 7, pp. 1618–1633, Jul. 2020.
[9] L. Wang, D. Yang, X. Han, T. Wang, D. Zhang, and X. Ma, "Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation," in *Proc. 26th Int. Conf. World Wide Web*. Geneva, Switzerland: International World Wide Web Conferences Steering Committee, Apr. 2017, pp. 627–636.
[10] 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.
[11] G. Fan *et al.*, "Joint scheduling and incentive mechanism for spatio-temporal vehicular crowd sensing," *IEEE Trans. Mobile Comput.*, vol. 20, no. 4, pp. 1449–1464, Apr. 2021.
[12] G. Gao, M. Xiao, J. Wu, L. Huang, and C. Hu, "Truthful incentive mechanism for nondeterministic crowdsensing with vehicles," *IEEE Trans. Mobile Comput.*, vol. 17, no. 12, pp. 2982–2997, Dec. 2018.
[13] H. Li, M. Dong, and K. Ota, "Control plane optimization in software-defined vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7895–7904, Oct. 2016.
[14] H. Zhao, M. Xiao, J. Wu, Y. Xu, H. Huang, and S. Zhang, "Differentially private unknown worker recruitment for mobile crowdsensing using multi-armed bandits," *IEEE Trans. Mobile Comput.*, early access, Apr. 27, 2020, doi: 10.1109/TMC.2020.2990221.
[15] W. Jin, M. Xiao, M. Li, and L. Guo, "If you do not care about it, sell it: Trading location privacy in mobile crowd sensing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr. 2019, pp. 1045–1053.
[16] M. Chen, Y. Qian, K. Hwang, J. Chen, S. Mao, and L. Hu, "Privacy protection and intrusion avoidance for cloudlet-based medical data sharing," *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1274–1283, 2020.
[17] M. Chen, Y. Hao, C. Lai, D. Wu, Y. Li, and K. Hwang, "Opportunistic task scheduling over co-located clouds in mobile environment," *IEEE Trans. Service Comput.*, vol. 11, no. 3, pp. 549–561, 2018.
[18] C. Luo *et al.*, "Predictable privacy-preserving mobile crowd sensing: A tale of two roles," *IEEE/ACM Trans. Netw.*, vol. 27, no. 1, pp. 361–374, Feb. 2019.
[19] Z. Wang *et al.*, "Personalized privacy-preserving task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, pp. 1330–1341, Jun. 2019.
[20] J. Chen, K. He, Q. Yuan, M. Chen, R. Du, and Y. Xiang, "Blind filtering at third parties: An efficient privacy-preserving framework for location-based services," *IEEE Trans. Mobile Comput.*, vol. 17, no. 11, pp. 2524–2535, 2018.
[21] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 754–762.
[22] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-aware people-centric sensing," in *Proc. 6th Int. Conf. Mobile Syst., Appl., Services*, 2008, pp. 211–224.
[23] H. To, G. Ghinita, and C. Shahabi, "A framework for protecting worker location privacy in spatial crowdsourcing," *Proc. VLDB Endowment*, vol. 7, no. 10, pp. 919–930, Jun. 2014.
[24] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J. P. Hubaux, "Hiding in the mobile crowd: Locationprivacy through collaboration," *IEEE Trans. Depend. Sec. Comput.*, vol. 11, no. 3, pp. 266–279, Jun. 2014.
[25] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, "MobiCache: When k-anonymity meets cache," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 820–825.
[26] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2014, pp. 251–262.
[27] L. Wang, D. Yang, X. Han, D. Zhang, and X. Ma, "Mobile crowdsourcing task allocation with differential-and-distortion geo-obfuscation," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 2, pp. 967–981, Mar. 2021.
[28] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.* Berlin, Germany: Springer, 2008, pp. 1–19.
[29] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 901–914.
[30] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2015, pp. 1298–1309.
[31] L. Wang, D. Zhang, D. Yang, B. Y. Lim, and X. Ma, "Differential location privacy for sparse mobile crowdsensing," in *Proc. IEEE 16th Int. Conf. Data Mining (ICDM)*, Dec. 2016, pp. 1257–1262.
[32] R. Shokri, G. Theodorakopoulos, and C. Troncoso, "Privacy games along location traces: A game-theoretic framework for optimizing location privacy," *ACM Trans. Privacy Secur.*, vol. 19, no. 4, p. 11, Feb. 2017.
[33] B. Liu, W. Zhou, T. Zhu, L. Gao, T. H. Luan, and H. Zhou, "Silence is golden: Enhancing privacy of location-based services by content broadcasting and active caching in wireless vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9942–9953, Dec. 2016.
[34] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A distortion-based metric for location privacy," in *Proc. 8th ACM Workshop Privacy Electron. Soc.*, 2009, pp. 21–30.
[35] A. Boutet and S. Gambs, "Inspect what your location history reveals about you: Raising user awareness on privacy threats associated with disclosing his location data," in *Proc. 28th ACM Int. Conf. Inf. Knowl. Manage.*, Nov. 2019, pp. 2861–2864.

Yongfeng Qian received the Ph.D. degree from the School of Computer Science and Technology, Huazhong University of Science and Technology (HUST), in 2018. She is currently an Associate Professor with the China University of Geosciences, Wuhan, China. Her research interests include vehicular networks, security and privacy, mobile crowdsening, cloud computing, and the Internet of Things.

Yujun Ma was a Visiting Associate Professor with the Department of Electrical and Computer Engineering, The University of British Columbia, Canada, from 2018 to 2019. He has been an Associate Professor with the School of Computer and Software, Nanyang Institute of Technology, China, since 2016. His current research focuses on the Internet of Things, edge computing, body sensor networks, healthcare big data, and mobile cloud computing.

Jing Chen (Member, IEEE) received the Ph.D. degree in computer science from the Huazhong University of Science and Technology, Wuhan. Since 2015, he has been working as a Full Professor with Wuhan University. He has published more than 130 research articles in many international journals and conferences, such as IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON COMPUTERS, USENIX Security, and INFOCOM. His research interests in computer science are in the areas of network security and cloud security. He acts as a Reviewer for many journals and conferences, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and IEEE/ACM TRANSACTIONS ON NETWORKING.

Di Wu (Senior Member, IEEE) received the B.S. degree from the University of Science and Technology of China, Hefei, China, in 2000, the M.S. degree from the Institute of Computing Technology Chinese Academy of Sciences, Beijing, China, in 2003, and the Ph.D. degree in computer science and engineering from The Chinese University of Hong Kong, Hong Kong, in 2007. He was a Post-Doctoral Researcher with the Department of Computer Science and Engineering, Polytechnic Institute of New York University, Brooklyn, NY, USA, from 2007 to 2009, advised by Prof. K. W. Ross. He is currently a Professor and the Associate Dean of the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. His research interests include cloud computing, multimedia communication, Internet measurement, and network security. He is a member of the Council of China Computer Federation. He was a co-recipient of the IEEE INFOCOM 2009 Best Paper Award. He has also served as the MSIG Chair for the Multimedia Communications Technical Committee in the IEEE Communications Society from 2014 to 2016. He served as the TPC Co-Chair for the IEEE Global Communications Conference—Cloud Computing Systems, Networks, and Applications, in 2014, and the Chair for the CCF Young Computer Scientists and Engineers Forum-Guangzhou, from 2014 to 2015. He has served as an Editor for the *Journal of Telecommunication Systems* (Springer), *Journal of Communications and Networks*, *Peer-to-Peer Networking and Applications* (Springer), *Security and Communication Networks* (Wiley), and the *KSII Transactions on Internet and Information Systems*, and a Guest Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY.



Daxin Tian (Senior Member, IEEE) received the Ph.D. degree in computer science from Jilin University, Changchun, China, in 2007. He is currently a Professor with the School of Transportation Science and Engineering, Beihang University, Beijing, China. His research focuses on intelligent transportation systems, autonomous connected vehicles, swarm intelligence, and mobile computing.

Kai Hwang received the Ph.D. degree in EECS from the University of California at Berkeley. Prior to joining the Chinese University of Hong Kong (CUHK), Shenzhen, China, in 2018, he has worked at Purdue University and the University of Southern California for many years. He is currently a Presidential Chair Professor with CUHK. He has published ten scientific books and over 280 scientific articles. He has received the Outstanding Achievement Award in 2005 from the China Computer Federation and the Lifetime Achievement Award from IEEE CloudCom 2012. In 2020, he has also received the Tenth Wu Wenjun Artificial Intelligence Natural Science Award from the China's Artificial Intelligence Association for his recent work on AI-oriented clouds/datacenters.