An Incentive Mechanism and An Offline Trajectory Publishing Algorithm Considering Sensing Area Coverage Maximization and Participant Privacy Level

Qing Cao[1], Yunfei Tan[2(✉)], and Guozheng Zhang[2]

[1] Nokia Shanghai Bell Co., Ltd., Shanghai, China
[2] School of Computer Science, Shaanxi Normal University, Xi'an, China
tyf@snnu.edu.cn

Abstract. In response to the incentive mechanism design issue and privacy leakage risk of trajectory data release in mobile crowdsensing scenario, an incentive mechanism named MSASM for participant selection is firstly presented in the paper, which considers the constraints of maximizing sensing area based on similarity measurement and utilizes a greedy and knapsack mixed algorithm to select the optimal participant set. Then an offline differentially private trajectory publishing algorithm named DPOTCPA is designed, which compresses the trajectory of participants and adds Laplace noise into the compressed trajectories for publishing. Experimental results on a real dataset demonstrate the effectiveness of the MSASM mechanism and the DPOTCPA algorithm.

Keywords: mobile crowdsensing · incentive mechanism · trajectory publication · privacy protection · differential privacy

1 Introduction

With the wide application of wireless networks, sensors, and smart devices, Mobile Crowdsensing (MCS), as a new sensing paradigm, has experienced rapid development [1, 2]. Currently, there has no unified definition of Mobile Crowdsensing. A typical definition of MCS is a new sensing paradigm that empowers ordinary citizens to contribute data sensed or generated from their mobile devices, aggregates and fuses the data in the cloud for crowd intelligence extraction and people-centric service delivery [3]. With the proliferation of mobile devices carried by humans, the mobile crowd sensing system was launched, which outsources the aggregated sensory data to public crowds equipped with a variety of mobile devices. One of the fundamental problems of MCS is to effectively motivate people to participate [4].

As a complement to traditional paradigms, MCS leverages the mobility of participants, sensing capabilities embedded in smart devices, and existing wireless infrastructure to sense and aggregate diverse data. It can provide richer and more abundant

J. Cai et al. (Eds.): SPNCE 2023, LNICST 525, pp. 54–66, 2025.
https://doi.org/10.1007/978-3-031-73699-5_4

data information for applications in mobile social networks, environmental monitoring, traffic monitoring, public safety, smart cities, healthcare, and other domains [5]. MCS has attracted widespread attention from researchers due to its advantages, such as comprehensive network coverage, low deployment cost, diverse types of sensing data, high dynamism, and good scalability.

However, MCS applications is currently severely constrained by issues such as insufficient number of participants for sensing tasks [6] and low availability of sensing data [7]. The main reasons for these problems can be attributed to two aspects: Firstly, how to design a fair and equitable participant incentive mechanism. Most participants are not willing to provide sensing data without compensation and expect tangible rewards such as monetary payment or in-game currency in return for the sensing data they provide. Secondly, participants face risks of privacy disclosure during their involvement in sensing tasks. In MCS environments, participants may face privacy risks related to identity, location, etc.

These concerns pose significant challenges to the advancement of MCS applications. In response to above issues, an incentive mechanism satisfying the constraints of maximizing sensing area and a differentially private preserving participant trajectory publishing algorithm is proposed in the paper. The main contributions of this paper are summarized as follows:

1. A participant selection incentive mechanism satisfying the constraints of Maximizing Sensing Area based on Similarity Measurement (MSASM) is designed in the paper. The proposed mechanism selects a rough candidate participant set based on Pearson similarity and utilizes a greedy and knapsack mixed algorithm to select the optimal participant set while maximizing the sensing area.
2. A Differentially Private Offline Trajectory Compression and Publishing Algorithm (DPOTCPA) is given in the paper, which is suitable for MCS platform to execute. For offline scenario, the proposed algorithm firstly adopts the Douglas-Peucker algorithm to compress the trajectory of participants, and then adds Laplace noise into the compressed trajectories before publishing. The proposed algorithm achieves privacy protection for participants and reduce the storage required for trajectory data.
3. Experiments are conducted on a real dataset, and the results show the effectiveness of the MSASM mechanism and the DPOTCPA algorithm.

The rest of this paper is organized as follows. Section 2 presents the preliminaries and related works. Section 3 introduces the system model. Section 4 describes the proposed MSASM Incentive Mechanism in detail. And DPOTCPA algorithm is described in Sect. 5. Section 6 shows the experimental results and analysis of comparative experiments. Section 7 concludes this paper.

2 Preliminaries and Related Work

2.1 Differential Privacy

Differential privacy is based on the principle of data distortion. It aims to achieve privacy protection by adding random perturbation noise to the original data without altering the overall trend of the data. Sensitivity is a key parameter that determines whether the added noise is appropriate.

Definition 1. (ε-Differential Privacy [8]): For a given randomized function M and neighboring data sets D and D', with P_M representing the range of values for M, and S_M is any subset of P_M, representing any output result of M on the neighboring data sets D and D', if formula (1) holds true, the random algorithm M satisfies ε-differential privacy.

$$\frac{\Pr\left[M\left(D\right) \in S_M\right]}{\Pr\left[M\left(D'\right) \in S_M\right]} \leq \exp(\varepsilon) \tag{1}$$

In formula (1), $\Pr[M\left(D\right) \in S_M]$ represents the probability that the output of dataset D under algorithm M is S_M, which signifies the risk of privacy disclosure. The parameter ε represents the privacy budget [9], which measures the strength of privacy protection.

In differential privacy, the Laplace mechanism is suitable for numerical results. It achieves differential privacy by adding random perturbation noise following the *Laplace* distribution to the query result. Assuming a *Laplace* distribution with location parameter $\mu = 0$ and scale parameter b is denoted as Lap(b), its probability density function is given below:

$$Lap(x, b) = \frac{1}{2b} * e^{(-\frac{|x|}{b})} \tag{2}$$

Definition 2. (Laplace Mechanism): Given a dataset D, let $F : D \rightarrow R^d$ be a function with sensitivity Δf. Then the randomized algorithm $M\left(D\right) = f\left(D\right) + Y$ provides ε-differential privacy, where $Y \sim Lap(\Delta f / \varepsilon)$ is the random noise following the *Laplace* distribution with scale parameter $\frac{\Delta f}{\varepsilon}$.

Definition 3. (Sequential Composition): Let there be algorithms $M_1, M_2, ..., M_n$ with privacy budgets $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$, respectively. For the same dataset D, the composed algorithm $M\left(M_1(D), M_2(D), ..., M_n(D)\right)$, formed by these algorithms, provides $(\sum_{i=1}^{n} \varepsilon_i)-$ differential privacy protection.

2.2 Pearson Correlation Coefficient

The Pearson correlation coefficient is a measure used to describe the linear relationship between two samples. Given two samples X and Y, the Pearson correlation coefficient is defined as follows:

$$r(X, Y) = \frac{Cov(X, Y)}{\sqrt{Var|X|Var|Y|}} = \frac{\sum_{i=1}^{n}\left(x_i - \overline{x_i}\right)\left(y_i - \overline{y_i}\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i - \overline{x_i}\right)^2}\sqrt{\sum_{i=1}^{n}\left(y_i - \overline{y_i}\right)^2}} \tag{3}$$

Where n represents the feature dimension, $r(X, Y) \in [-1, 1]$ represents the degree of correlation. When r takes the values –1 or 1, it indicates that X and Y are perfectly correlated. When r takes the value 0, it indicates that X and Y are completely unrelated.

2.3 Perpendicular Euclidean Distance

Perpendicular Euclidean Distance (PED) refers to the shortest distance from a trajectory point P_m to a simplified trajectory segment $\overrightarrow{P_sP_e}$. The formula is defined as follows:

$$PED(p_m) = \frac{|(y_e - y_s)x_m - (x_e - x_s)y_m + x_e y_s - y_e x_s|}{\sqrt{(y_e - y_s)^2 + (x_e - x_s)^2}} \tag{4}$$

Where (x_s, y_s) represents the coordinates of the starting point P_s, (x_e, y_e) represents the coordinates of the ending point P_e, and (x_m, y_m) represents the coordinates of P_m.

2.4 Related Work

There exists a lot of works for privacy preserving MCS using traditional methods such as k-anonymity and cryptography. Wu et al. [10] proposed a holistic solution for trustworthy and privacy-aware mobile crowdsensing with no need of a trusted third party. Specifically, leveraging cryptographic technologies, they devised a series of protocols to enable benign users to request tasks, contribute their data, and earn rewards anonymously without any data link ability. Meanwhile, an anonymous trust/reputation model was seamlessly integrated into their scheme, which acted as reference for fair incentive design, and provided evidence to detect malicious users who degrade the data trustworthiness. Tao et al. [11] proposed an incentive mechanism for privacy-preserving mobile crowdsensing. More specifically, they introduced a trusted third party and combined partially blind signature, which could effectively reduce the correlation between participants and data and the number of interactions between users and task platform, to achieve high level participant privacy.

In recent years, differential privacy has gradually been applied to the field of MCS due to its rigorous and quantitative representation and proof of privacy leakage risks. Huang et al. [12] proposed a mechanism named TPA, to protect the trajectory as a whole part. The mechanism firstly computed the total amount of noise to satisfy differential privacy. Then it randomly allocated the noise to each coordinate of the trajectory. To improve the utility of the perturbed trajectory, the proposed mechanism also considered the correlations between each pair of perturbed and true trajectories. Different from the existing permission on-off control mechanism, Xu et al. [13] presented a configurable multi-strategy trajectory privacy-preserving framework, named MSPP in the participant's terminal. Based on the individual historical trajectory data stored locally and privacy preferences, participant could actively select the corresponding protection mechanism (Pathswap, Promesse, Geo-I, etc.) considering privacy metrics and data utility. Chen et al. [14] proposed a differentially private trajectory protection scheme with real-location reporting in MCS. Firstly, they presented the definition of trajectory privacy protection based on real path reporting under differential privacy. Secondly, they gave a trajectory privacy protection framework under Bayesian inference attacks. Chen et al. [15] applied differential privacy for trajectory privacy protection, by constructing a noisy prefix tree for counting query and adopting Laplace mechanism to achieve differential privacy. However, as the noisy prefix tree grows, the number of sequences entering a branch decreases rapidly, resulting in poor practicability.

3 System Model

The MCS system in this paper consists of a MCS platform, participants, and several service providers, as shown in Fig. 1. Service providers publish their requirements and purchase the necessary sensing datasets from the MCS platform. The MCS platform issues various types of sensing tasks to the participants, who autonomously select and bid for the tasks they wish to participate in. Using a monetary incentive mechanism, the MCS platform selects suitable task participants and aggregates the sensing data uploaded by the participants, providing the corresponding service providers with the processed data.

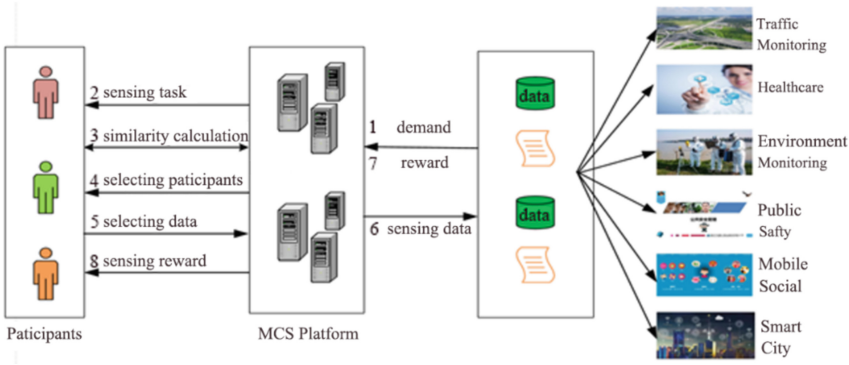


Fig. 1. System Model

In this paper, the MCS platform is assumed to be untrusted and curious about the sensing data uploaded by participants. The MCS system faces two main challenges in the process of implementing sensing tasks: (1) how to personalize the selection of participants while satisfying the constraint of maximizing sensing region coverage; (2) how to ensure privacy protection for the participants. Considering the diverse requirements of different types of service providers, the MCS platform issues various types of sensing tasks to the participants.

This paper adopts a vector Tv containing five attributes $\{T_{ty}, D_c, T_{ti}, N_r, P_r\}$ to describe the published perceptual task. Here,Tty represents the task type,D_c represents data accuracy,T_{ti} represents task time,N_r represents the number of participants required, and P_r represents perceptual reward. Simultaneously, a vector Pv containing five attributes $\{T_P,P_l,P_t,P_c,E_r\}$ is used to describe participants' task participation preferences. Here, T_P represents task preference, P_l represents privacy level, P_t represents sensing time, P_c represents personal reputation, and E_r represents expected reward.

Then, candidate participants are selected based on the similarity measurement between the task vector T_v and the participant vector P_v. Finally, a combination of greedy and knapsack algorithms is employed to select the optimal set of participants from the candidate participant pool, achieving personalized and precise participant selection while maximizing the sensing area.

4 MSASM Incentive Mechanism

Based on the system model described above, we propose an incentive mechanism satisfying the constraints of Maximizing Sensing Area based on Similarity Measurement (MSASM). Firstly, constructing the task vector Tv of each task and preference vector Pv of each participant. Secondly, utilizing the Pearson similarity coefficient to calculate the similarity between T_v and P_v, and then selecting a candidate set of participants based on the similarity values. Finally, according to the following objective function (formula (5)), using a greedy and knapsack mixed algorithm under the constraints of maximizing sensing area and privacy levels of participants, to find the optimal participants from the candidate set.

$$f[k][v] = max\{f[k-1][v], f[k-1][\mathrm{v}-1]+w[i]\} \tag{5}$$

Where f[k][v] represents the maximum sensing area covered by all participants in first k group with a total of v participants. k represents the number of connected graphs in the sensing area based on the duplicate coverage of participants (which is further explained in the following paragraph), and $w[i]$ represents the sensing area covered by participant i.

In the MSASM mechanism, the greedy and knapsack fusion algorithm selects the optimal participant set from the candidate set when the objective function achieves its maximum value. Specifically, the MSASM mechanism transforms the problem of selecting N_P participants with the maximum sensing area from the candidate set into a problem of selecting N_P circles with the smallest intersection.

Firstly, for each candidate participant, drawing a circle with his/her position as center and radius $r = 1$. If sensing area of participant i overlaps with that of participant j, adding an edge between them, where the edge weight is the area of the intersection between participant i and j. This process constructs a graph G, and a breadth-first search algorithm is used to partition G into a set of connected graphs, denoted as $\{ \mathrm{g}_1, \cdots, \mathrm{g}_k \}$. Then, isolated participants are selected from the set of connected graphs. Suppose that the number of isolated participants is $Count$. If $Count >= N_P$, we can return the indices and positions of the first N_P participants in the set of isolated participants. Otherwise, we initialize the knapsack volume as $v = N_P - Count$ and use the greedy and knapsack mixed algorithm to continually select candidates with high similarity according to the objective function. Finally, the top N_P optimal participants with maximized sensing areas are found.

The pseudo code of the MSASM mechanism is shown in algorithm 1.

Algorithm 1. MSASM mechanism

Input: task dataset $Task = \{task_1, task_2, ..., task_n\}$
participant dataset $P = \{P_1, P_2, ..., P_m\}$
participant position $Loc = \{loc_1, loc_2, ..., loc_m\}$
the number of participants selected N_P

Output: optimal participant set OP

1: **for** i=1 to n
2: construct vector Tv_i for each task $task_i$;
3: **for** j=1 to m
4: construct vector Pv_j for each participant P_j;
5: calculate the similarity between Tv_i and Pv_j according to formula (3);
6: **end for**
7: obtain candidate set TC_i of participants for each task $task_i$;
8: **end for**
9: obtain the candidate set $TC = TC_1 \cup TC_2 \cup ... \cup TC_n$;
10: **for** i=1 to n
11: construct graph G by drawing circles with a radius of 1 and using the position of each participant in TC as the center;
12: add edges if there is an intersection between the circles, and the edge weight is area of the intersection between the circles;
13: **end for**
14: use the breadth-first search algorithm to partition graph G into $\{g_1, g_2, ..., g_k\}$ and get the number of isolated participants $Count$;
15: **if** $Count >= N_P$
16: add the first N_P participants into OP;
17: **else**
18: for each graph g_k
19: **for** $v = N_P - Count$ to 0
20: **for** each participant i belonging to g_k
21: calculate the objective function according to formula (5);
22: **end for**
23: **end for**
24: **end for**
25: **end if**
26: **return** OP.

5 DPOTCPA Algorithm

After selecting an appropriate participant set using the MSASM incentive mechanism, considering the large scale of participant trajectory datasets and the privacy risks of publishing participant trajectory data, we address the demand for privacy-preserving participant trajectory publication. And for offline scenario, we propose a Differentially Private Offline Trajectory Compression and Publishing Algorithm (DPOTCPA) suitable for MCS platform to execute.

For the participant set, the DPOTCPA algorithm firstly uses the Douglas-Peucker algorithm [16] to perform offline compression on each participant's trajectory curve based on a given threshold, effectively reducing the storage space of participant trajectory data. Then, under the constraint of a given total privacy budget and according to different privacy levels of participants, the DPOTCPA algorithm allocates different privacy budgets for participants using formula (6) (all the participants with the same level are allocated the same privacy budget). In the proposed algorithm, the privacy protection of participants are classified into three levels: $level_1$(low privacy protection), $level_2$(medium privacy protection), and $level_3$(high privacy protection). And Laplace noise is added to the compressed trajectory data using formula (7). Finally, the algorithm publishes the noisy participant trajectory dataset.

$$\varepsilon_i = \frac{level_i}{level_1 + level_2 + level_3} \tag{6}$$

Where ε_{i} represents the privacy budget allocated for trajectory tr_i of participant P_i, and $level_i$ represents the privacy protection level of participant P_i.

$$f(tr_i^{''}) = f(tr_i\prime) + Lap(\Delta f/\varepsilon_i) \tag{7}$$

Where $f(tr_i\prime)$ represents the compressed trajectory of P_i, $f(tr_i^{''})$ represents the compressed and perturbed trajectory of P_i, $Lap(\Delta f/\varepsilon_i)$ represents the added Laplace noise and Δf is the global sensitivity.

The pseudo code of the DPOTCPA algorithm is given in algorithm 2.

Algorithm 2. DPOTCPA algorithm

Input: original participant trajectory set $Tr=\{tr_1,tr_2,...,tr_n\}$
participant privacy level $Level=\{level_1,level_2,level_3\}$
privacy budget ε, threshold $D_{\max}$

Output: compressed and perturbed participants trajectory set $Tr''=\{tr_1'',tr_2'',...,tr_n''\}$

1: **for** i=1 to n
2: **for** each trajectory tr_i
3: traverse all trajectory points, calculate the distance of each point to the straight-line AB formed by the starting point A and the ending point B. Find the point C with the maximum distance to AB, and record this maximum distance as MP_m
4: **if** $MP_m < D_{\max}$
5: use line AB as an approximation for tr_i;
6: **else if** $MP_m \geq D_{\max}$
7: split point C is used to split AB into two segments, AC and CB;
8: for AC and CB, execute step 3 and 4, respectively;
9: **end if**
10: **if** all the segments have been processed
11: connect all the split point to form the approximation for tr_i;
12: **end if**
13: **end for**
14: allocate privacy budget according to formula (6);
15: add Laplace noise according to formula (7);
16: **end for**
17: publish the result trajectory dataset Tr''.

6 Privacy Analysis

In this section, we conduct simulation experiments to analyze and evaluate the MSASM mechanism and DPOTCPA algorithm. The goal is to validate the feasibility and effectiveness of the proposed incentive mechanism and participant trajectory publishing algorithms.

6.1 Experiment Environment

The hardware environment used in this study includes an Intel(R) Core(TM) i7-5500U CPU @ 2.4 GHz, 16 GB of RAM, and 1 TB of hard disk space. The software environment consists of a 64-bit Windows 10 operating system.

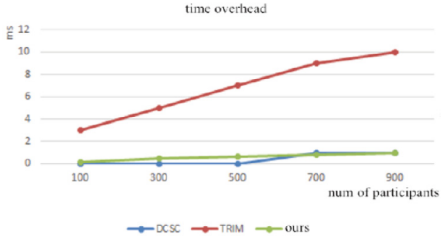
Regarding the proposed MSASM mechanism, the experimental dataset is generated using a pseudo-random number generator to create a set of task datasets and six sets of participant datasets with different numbers of participants. Attributes of each task dataset and participant dataset are described in Sect. 3.

Regarding the proposed DPOTCPA algorithm, the experimental dataset is taken from the real dataset GeoLife GPS Trajectories, a Microsoft research project known as GeoLife. This trajectory dataset contains 17,621 trajectories recorded from 182 participants between April 2007 and August 2012.

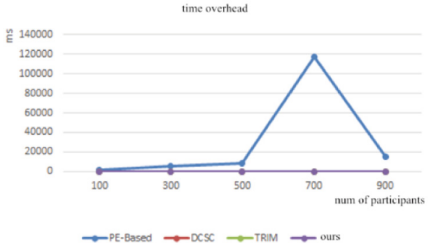
6.2 Experiment Result Analysis

In the first set of experiments, we compare the similarity calculation time overhead of the MSASM incentive mechanism, TRIM incentive mechanism [17], the incentive mechanism using the direct cosine similarity computing protocol (DCSC), and the incentive mechanism using the Paillier encryption-based (PE-based) protocol under different numbers of participants. The results are illustrated in Fig. 2.

The MSASM mechanism, TRIM mechanism, and the incentive mechanism using the DCSC protocol exhibit relatively small similarity calculation time overhead, as shown in detail in Fig. 2(a). Compared to the TRIM mechanism and the incentive mechanism using the PE-based protocol, the MSASM mechanism demonstrates a clear time advantage. When the number of participants is small, the incentive mechanism using the DCSC protocol has slightly lower time overhead. However, when the number of participants is large, the MSASM mechanism exhibits slightly lower time overhead. Overall, the time overhead of both the MSASM mechanism and the incentive mechanism using the DCSC protocol is comparable.



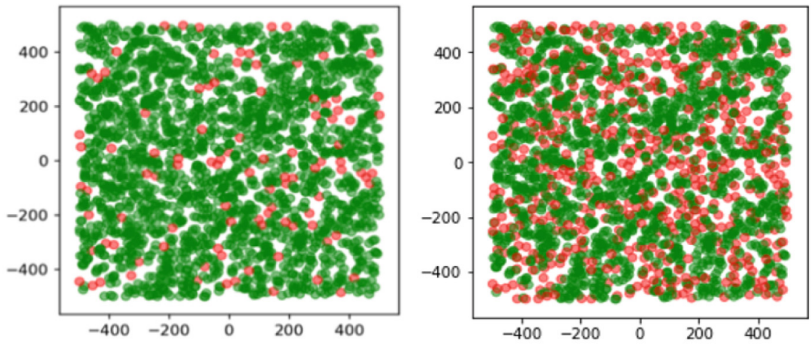
(a)



(b)

Fig. 2. Time overhead of different mechanisms

In the second set of experiments, with the number of participants set to 2000, we select the top 100 optimal participants and the top 500 optimal participants based on the highest similarity score, while also satisfying the constraints of maximizing the sensing area and privacy protection level. The experimental results are shown in Fig. 3(a) and (b). In Fig. 3, green circles represent participants, and red circles represent the selected optimal participants.



(a) (b)

Fig. 3. Optimal participant selection that satisfies the constraints of maximum sensing area and privacy protection level

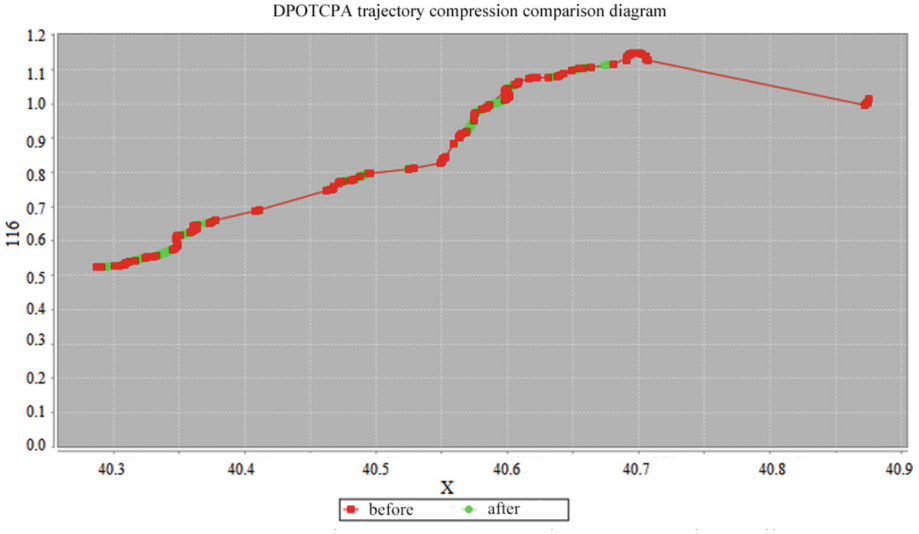


Fig. 4. DPOTCPA trajectory compression comparison diagram

The third set of experiments validates the trajectory compression of the DPOTCPA algorithm. We selected a participant from the GeoLife GPS Trajectories dataset, which

contains 3091 nodes in the trajectory curve. The DPOTCPA algorithm was applied to compress the trajectory curve. The comparison between the participant's trajectory before and after compression is shown in Fig. 4. The compression rate of the DPOTCPA algorithm is 0.05985118084762213, indicating that many nodes were discarded during the compression process, leading to a noticeable reduction in the curve in Fig. 4.

The fourth set of experiments validates the utility of privacy-protected trajectory data published by the DPOTCPA algorithm. We randomly selected 128 participants with 8173 trajectories and 181 participants with 12350 trajectories from the GeoLife GPS Trajectories dataset. Under total privacy budgets of 0.2, 0.4, 0.6, 0.8, and 1, the DPOTCPA algorithm was used to add noise perturbation to different participant trajectories. The RMSE (Root Mean Square Errors) between the perturbed dataset and the original dataset are shown in Fig. 5. It can be observed that the RMSE gradually decreases as the privacy budget increases.

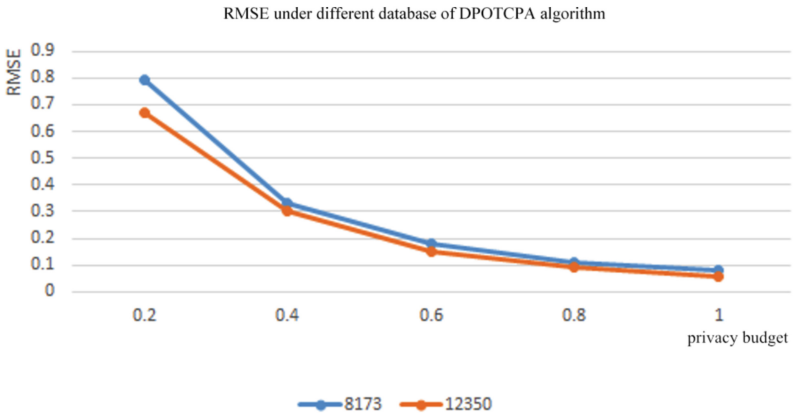


Fig. 5. RMSE under different datasets of DPOTCPA algorithm

7 Conclusion

To address the problem of incentive mechanism design and privacy leakage risks of participant trajectory data publishing in mobile crowdsensing scenario, a participant selection incentive mechanism named MSASM is firstly presented, which considers the constraints of maximizing sensing area based on similarity measurement and utilizes a greedy and knapsack mixed algorithm to select the optimal participant set. Then an offline trajectory publishing algorithm named DPOTCPA is given in the paper, which compress the trajectory of participants in advance and adds Laplace noise into the compressed trajectories for publishing.

In future work, we plan to make improvements in the following aspects: Firstly, the MSASM incentive mechanism exists the risk of participant privacy leakage during the candidate participant selection process. To mitigate this risk, we intend to utilize certain

lightweight data encryption algorithm to encrypt sensitive participant attributes. Secondly, although the MSASM incentive mechanism considers participant's reputation, it does not account for dynamic updates of reputation. We aim to construct a dynamic reputation function based on factors such as the number of completed tasks and task quality assessments to update participant's reputation values in a more practical environment.

References

1. Restuccia, F., Ghosh, N., Bhattacharjee, S., et al.: Quality of information in mobile crowdsensing: survey and research challenges. ACM Trans. Sens. Netw. (TOSN) **13**(4), 1–43 (2017)
2. Guo, B., Wang, Z., Yu, Z., et al.: Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm. ACM Comput. Surv. (CSUR) **48**(1), 1–31 (2015)
3. Guo, B., Yu, Z., Zhou, X., et al.: From participatory sensing to mobile crowd sensing. In: Proceedings of the 2014 IEEE International Conference on Pervasive Computing and Communication Workshops (PERCOM WORKSHOPS). IEEE, pp. 593–598 (2014)
4. Zhong, S., Zhong, H., Huang, X., et al.: Networking cyber-physical systems: algorithm fundamentals of security and privacy for next-generation wireless networks. Secur. Priv. Next Gener. Wirel. Netw., 33–48 (2019)
5. Sun, W., Liu, J.: Congestion-aware communication paradigm for sustainable dense mobile crowdsensing. IEEE Commun. Mag. **55**(3), 62–67 (2017)
6. Deterding, S., Dixon, D., Khaled, R., et al.: From game design elements to gamefulness: defining "gamification". In: Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments, pp. 9–15 (2011)
7. Wen, Y., Shi, J., Zhang, Q., et al.: Quality-driven auction-based incentive mechanism for mobile crowd sensing. IEEE Trans. Veh. Technol. **64**(9), 4203–4214 (2014)
8. Dwork, C.: A firm foundation for private data analysis. Commun. ACM **54**(1), 86–95 (2011)
9. Haeberlen, A., Pierce, B.C., Narayan, A.: Differential privacy under fire. In: Proceedings of the 20th USENIX Security Symposium (USENIX Security 2011) (2011)
10. Wu, H., Wang, L., Xue, G., et al.: Enabling data trustworthiness and user privacy in mobile crowdsensing. IEEE/ACM Trans. Networking **27**(6), 2294–2307 (2019)
11. Tao, D., Wu, T.Y., Zhu, S., et al.: Privacy protection-based incentive mechanism for mobile crowdsensing. Comput. Commun. **156**, 201–210 (2020)
12. Huang, H., Niu, X., Chen, C., et al.: A differential private mechanism to protect trajectory privacy in mobile crowd-sensing. In: Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6. IEEE (2019)
13. Xu, Z., Yang, W., Wang, J.: MSPP: a trajectory privacy-preserving framework for participatory sensing based on multi-strategy. In: Proceedings of the 2019 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2019)
14. Chen, X., Wu, X., Wang, X., et al.: Real-location reporting based differential privacy trajectory protection for mobile crowdsensing. In: Proceedings of the 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), pp. 142–150. IEEE (2019)
15. Chen, R., Fung, B., Desai, B.C.: Differentially private trajectory data publication. arXiv preprint arXiv:1112.2020 (2011)
16. Douglas, D.H., Peucker, T.K.: Algorithms for the reduction of the number of points required to represent a digitized line or its caricature. Cartographica Int. J. Geog. Inf. Geovisualization **10**(2), 112–122 (1973)
17. Xiong, J., Chen, X., Yang, Q., et al.: A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing. IEEE Trans. Netw. Sci. Eng. **7**(4), 2347–2360 (2019)