MSPP:A Trajectory Privacy-Preserving Framework for Participatory Sensing Based on Multi-Strategy

1st Xu Zhenqiang
Institute of Geospatial Information
Information Engineering University
& Henan University of Technology
Zhengzhou, China
xuzhenqiang@haut.edu.cn

2nd Yang Weidong
College of Information Science and Technology
Henan University of Technology
Zhengzhou, China
yangweidong@haut.edu.cn

3rd Wang Jiayao
Institute of Geospatial Information
Information Engineering University
Zhengzhou, China
xzqzty@gmail.com

***Abstract*—With the continuous development of wireless communication and sensing technology, participatory sensing has broad applications in areas such as traffic detection, environmental detection, and road network update. However, this new data collection method may pose a serious threat to participants privacy as trajectories imply participants mobility patterns. In this paper, we propose a configurable trajectory privacy-preserving framework based on multi-strategy, named MSPP, in the participants' mobile devices. The MSPP does not rely on the trusted third-party server, and actively selects the corresponding protection mechanism based on the individual historical trajectory data stored locally in the participant terminal and the privacy preference setting. Finally, Experiments conducted on real datasets demonstrate that MSPP can meet the personalized privacy protection requirements of users in different application scenarios.**

***Index Terms*—Trajectory Privacy protection, Mobility Pattern, Participator Sensing**

I. Introduction

In recent years, with the strong support of mobile communication technology and Internet technology, participatory sensing (PS) has broad development space in many domains such as traffic monitoring [1], map generation [2] and so on.

However, PS applications face serious privacy problems. The collected data and the request service query contain the spatiotemporal context related to the participants. The attacker uses the spatiotemporal context in the data report uploaded by the participant to perform an inference attack to infer the user's individual sensitive information [3]. Once participants realize that their personal privacy is threatened, they are unwilling to provide sensing data to the application server. Finally, the effectiveness of participatory sensing campaign is likely to be severely affected. Meanwhile, corresponding service quality of PS will decline further. Therefore, the trajectory privacy preserving of sensing application participants has become an urgent problem to be solved in the research in this field.

At present, participants' trajectory privacy-preserving mechanism (TPPM) is technically similar to trajectory privacy technology in location-based services (LBS) and offline data publishing. It mainly includes trajectory suppression technique, dummy trajectories, trajectory k-anonymity and differential privacy. The inadequacy of previous privacy protection techniques lie in: a) adopting the same level of privacy-protection mechanism for all participants, failing to consider the user's personalized privacy protection requirements effectively in different scenarios, which may result in unnecessary information loss. b) the existing mechanisms focus on the trajectory privacy protection, but have not considered the protection privacy of the mobility patterns contained in the participant's trajectory. Relevant research shows that the trajectory of moving objects often has a high temporal and spatial regularity. c) Participants prefer to upload their trajectory data to the data collection server after they have been protected and processed, rather than through third-party servers for privacy protection [4]. If the data collection server is not trusted or attacked by an attacker, based on the historical trajectory data of the participants collected by the server, by analyzing and mining the mobility patterns of the participants, attackers can infer the sensitive information of the individual, such as home address and workplace, point of interest, living habits and even social attributes. In addition, the PS application data collectors hope to collect the most detailed and complete participants' spatial-temporal data, but in fact different sensing applications have different requirements for data collection, such as road network update and urban planning applications need long-term and accurate trajectory data; urban noise, air pollution, and other sensing applications are relatively weak for spatial data accuracy; while the application of surveying engineering requires lower accuracy in time domain. Therefore, these different utility goals also provide corresponding requirements for participants to choose different levels and degrees of privacy-preserving mechanisms. To achieve the trade-off between the different levels of privacy protection and data utility, this paper proposes a trajectory privacy-preserving framework based on configurable participant terminal, named MSPP. The main contributions of our work are summarized as follows:

- MSPP does not rely on a trusted third-party server, and adaptively selects a corresponding privacy protection scheme based on individual historical trajectory data and privacy preferences stored locally by the participant terminal;
- Based on user target privacy requirements and data util-

978-1-7281-0960-2/19/$31.00 ©2019 IEEE

ity objectives in different PS scenarios, MSPP provides participants with different TPPM.
- Experiments based on real trajectory datasets show that the privacy-preserving framework for PS applications proposed in this paper can meet the users' personalized privacy protection requirements.

The remainder of this paper is organized as follows. Section II presents the related work. In Section III, we propose the trajectory privacy preserving system framework for participatory sensing. In Section IV, we present the attack model with re-Identification attack. In Section V, we evaluate TPPMs in terms of privacy metric and utility metric. In Section VI, we run a set of simulations to evaluate the effectiveness of MSPP. Finally, we conclude this paper and present the future work in Section VII.

II. Related Work

Effective trajectory privacy-preserving mechanisms are required to resolve participants privacy concerns in the PS domain. Compared to single-point locations, trajectories that reflect user mobility patterns are more likely to present serious privacy challenges. It has been concluded that [5] the user's continuously updated trajectory is more vulnerable to attack. In this section, we review studies about trajectory privacy protection in PS system.

a) Trajectory Swapping Method: The typical operation of this method is to exchange the owned trajectory segments between the actual encountering participants. After the two participants meet, the path that one participant passes through is replaced by the path of the other. This exchange process is repeated in each encounter, resulting in a combined trajectory of multiple paths. In this way, the server side cannot disclose the actual path of individual participants. Reinhardt et al. [6] proposed to build k-anonymous regions through secure multi-party computing, and then exchange trajectory segments with each other to make trajectory swapping.

b) Mixed zone: This method is to identify some areas in advance, which can divide the user's travel path into segments and break the connection between the path segments, to achieve the anonymity when the user enters and leaves this area, such areas are called mixed zone. However, a single mix zone is insufficient to handle the inferential attack because side information leaks could occur in any part of a users trajectory. To enhance the effectiveness of privacy protection, Liu et al. [7] addressed the problem of optimal multiple mix zones placement.

c) Time-obfuscated Approach: The main idea of the approach [8] is to confuse the location and its adjacent timestamp to eliminate the server so that it does not know the precise trajectory of users. The randomness generated by the obfuscation process helps in providing strong protection to the trajectory privacy.

d) Noise-added approach: Differential Privacy (DP) [9] has been widely used for database privacy protection. Its main idea is to add controlled noise (such as with Laplace mechanism) to reduce the difference between two neighboring datasets of a unit record change. For trajectory protection, the record unit is a single trajectory [10]. For transportation trajectories, public accessible roads and railway topology can support the improvement process. This kind of priority has been explained in some studies to evaluate the DP approach with considering topology knowledge.

e) Elimination method: Elimination of removal of some sensitive samples to make the trajectory incomplete is a simple but effective method. Navigation PS App Waze uses this idea to eliminate the specified meter trajectory segment around the onset and end of the journey.

f) Suppression method: Suppression is a simple and effective method of privacy protection, which is to make the trajectory incomplete by deleting some sensitive spatiotemporal points. Primault et al. [8] uses this method to blur the start and end points of users' trajectories to make them less easily identifiable.

g) Dummy trajectory: The dummy-based method generate dummies and add fake trajectories along with the users real trajectory to confuse the adversaries. Virtual trajectory can be generated using random mode or transform mode [11].

III. Overview Of MSPP System

In this section, we firstly describe the architecture of a trajectory privacy-preserving framework (MSPP) for participatory sensing system, and then introduce the set of privacy protection mechanisms for participants to choose.

A. The Architecture of MSPP

Our MSPP has the architecture as shown in Fig.1. According to the different roles of function characteristics, the main components of MSPP are made up of the following entities.

Participants: The function of the participants is primarily to complete the task of data collection. Note that the involvement of participants in this sensing campaign is voluntary. The participant is required to store the original trajectory data of the individual locally. In addition, participants work also includes: a) constructing individual sensitive mobility patterns based on individual historical trajectory data, and b) independently selecting a proper privacy protection mechanism based on personalized privacy requirements and data utility objectives.

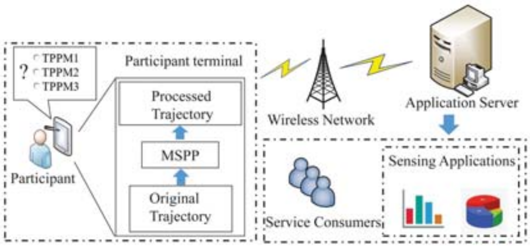

Fig. 1. Architecture of MSPP for participatory sensing.

Application Server: Every participant uploads the sensing data to the application server through the mobile network, and then the application server completes the pre-processing of the data, such as data aggregation, data classification, etc., and then performs data storage, data sharing and publishing. In the framework, we assume that the application server is untrustworthy, that is, it may leak participants sensitive information to an adversary.

Service Consumers: Service Consumers can be a participant himself, research institution or enterprises. They access and query the data reports gathered by the participants according to practical requirements. For example, traffic control departments uses route traffic information collected by participants (mobile phones or vehicles) to estimate future traffic flows. Then Consumers (users) can get traffic suggestions from traffic management.

B. The Collection of TPPMs

The Collection of TPPMs provides participants with different privacy protection strategies. Participants make decisions based on different requirements and preferences. In general, these TPPMs are classified into three categories depending on spatial or temporal transformation: spatio-temporal perturbation, spatial perturbation, and temporal perturbation. Next, the representative strategy for three types are used separately: Pathswap, Promesse, and Geo-I (as shown in Fig. 2). Notably, in Pathswap the participants collaborate to protect their privacy through swapping users' partial trajectory segments, but the latter two methods process the individual trajectory for each participant.

The following paragraphs discuss the principle of these strategies.

Pathswap The basic idea of Pathswap is to exchange the collected trajectory segments between participants who physically meet. For instance, as showed in Fig. 2a and Fig. 2b, by swapping two traces during a period of time, their mobility pattern become more atypical and less predictable. Through this operation, the prior path of one participant is replaced by that of another participant and vice versa. The repetition of such exchange process of each encounter results in a composed trajectory with sub-paths from multiple participants. As a result, the server-end cannot disclose the actual paths of individual participants [12]. In fact, Pathswap neither changes any location nor does it introduce any dummy locations.

Promesse Promesse [8] is a TPPM that has been developed in order to prevent the extraction of Points of Interests (users stop places) while maintaining a good spatial accuracy. The trace in Fig. 2c is the processed trace through Promesse. Its principle is to distort timestamps of location traces as well as remove and insert locations in a users trace in order to keep a constant distance between two events of the trace. One can see its behavior as adding temporal noise to a trace instead of spatial noise as in Geo-indistinguishability [10].

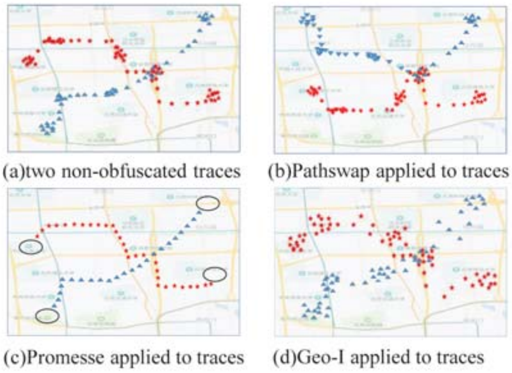
(a)two non-obfuscated traces (b)Pathswap applied to traces
(c)Promesse applied to traces (d)Geo-I applied to traces

Fig. 2. Illustration of TPPMs applied to mobility traces.

Geo-I The inspiration of Geo-indistinguishability (Geo-I for short) comes from one of the most popular approaches for differential privacy, namely a Laplace noise. It adjusts the amount of noise required to obfuscate the users location to get the service within an accepted utility level [10]. The effectiveness of Geo-I is dependent on the quantity of noise that has been added. It is a measurable noise controlled by the ε parameter. An example of applying Geo-I to a mobility trace of Fig. 2a is depicted in Fig. 2d.

IV. Threat Model

In this paper, we consider the problem of privacy preserving in a semi-honest model, in which the adversary can follow the specified protocol, but tries to obtain the sensitive information of the participants from the obtained data. The focus of this section is to illustrate the attacker's Re-identification attack by using the mobility patterns of participants.

A. Attack Scenario

We consider a set $U = \{U_1, U_2, \ldots, U_n\}$ of participants in PS application. The following assumptions were made for attack scenario:

- There are a set of unprotected trajectory data of participants in a period of time, i.e.,$KD = \{KD_1, KD_2, \ldots, KD_n\}$.
- The trajectories of participants are uploaded continuously to application server with sensing data in different time-intervals (one hour or longer period of time), and use pseudonym method (i.e., replace the participants real identifier with pseudonym) to realize anonymization. Those trajectories is noted $UD = \{UD_1, UD_2, \ldots, UD_n\}$.
- The adversary is able to access historical trajectories KD as his background knowledge and anonymization trajectory database UD. KD is not necessary to overlap with UD in time domain.

Next the adversary run a Re-identification attack A defined in (1).

$$Id(T^{'}) = A(T^{'}, KD) \tag{1}$$

where T' denotes an anonymous trajectory of UD and $Id(T')$ represents the Id corresponding to the anonymous track obtained by the attack algorithm. The attack process described below: a) The adversary builds respectively profile $p(KD_i)$ and $p(T')$ which characterize the mobility trajectory. b) Based on the particular distance measure, adversary compares $p(T')$ with $p(KD_j)$ as depicted in (2), and then get U_{id}.

$$Id(T') \leftarrow arg\ min_{0<j\leq|KD|}\ d(p(T'), p(KD_j)) \qquad (2)$$

B. Attack method

Participant profile that characterize mobility patterns depends on his Points of interests (POIs). Those POIs are extracted using clustering algorithms from the corresponding trajectory. We believe that the mobility Markov chains model can better describe the mobility patterns of participants. Therefore, Probabilistic Inter-POI Transition Attack (PIT-attack) method that adopt Markov chains runs re-identification attacks. Specifically, in order to get the similarity of two trajectories, it is necessary to compute the distance of the two moving Markov chains. The most effective distance measure method should involve the stationary distance and the proximity distance. This method not only take account of the geographical distance between POIs, but the weight of each POI. Specific implementation process have explained in [14].

V. Metric

Key to the evaluation of a protection mechanism is the definition of well-suited privacy and utility metrics. In this section, we introduce privacy metric and utility metric to evaluate the effectiveness of MSPP.

A. Privacy Metrics

1) Re-identification Rate

To evaluate the effectiveness of a TPPM, we apply it on a set of anonymous trajectory UD and then compute re-identification rate $r(A, KD, TPPM(UD))$ in (3).

$$r(A,KD,TPPM(UD)) = \frac{\sum_{UD_i} \begin{cases} 1 & \text{if } A(TPPM(UD_i), KD) = Id(UD_i) \\ 0 & \text{else} \end{cases}}{\mid UD \mid} \qquad (3)$$

Where A stands for PIT-attack in Section IV-B. In addition, A can be replaced with other attack methods based on various distance measure.

2) POIs Retrieval

For participants, POIs are very spatially delimited places. Mining trajectory of participants can reveal their POIs, which are sensitive places such as home or work. Consequently, the number of POIs adversary can be infer from a trajectory is generally considered as a privacy metric. Specifically, the set of POIs extracted from an original trajectory using clustering algorithm is noted $P = \{p_1, p_2, \ldots, p_m\}$ and the set of POIs extracted from a protected trajectory applied one TPPM is noted $P' = \{p'_1, p'_2, \ldots, p'_n\}$. We evaluate the level of privacy provided by one TPPM through computing the matching degree of P and P'.

The definitions of recall (r) (See (4)), precision (p) (See (5)) and $F - score$ (See (6)) are defined [15]:

$$r_\ell = \frac{\mid \{p' \in P' \mid \exists p \in P, d_\chi(p, p') \leq \ell\} \mid}{\mid P \mid} \qquad (4)$$

$$p_\ell = \frac{\mid \{p' \in P' \mid \exists p \in P, d_\chi(p, p') \leq \ell\} \mid}{\mid P' \mid} \qquad (5)$$

$$F - score = \frac{2 \times p_\ell(P, P') \times r_\ell(P, P')}{p_\ell(P, P') + r_\ell(P, P')} \qquad (6)$$

Where ℓ is a distance threshold of two POIs. p and p' are treated as the same point of interest if $d_\chi(p, p') \leq \ell$.

B. Utility Metrics

The metric of data utility is changing in different PS scenarios. Smartphone or Vehicle user periodically uploads its GPS samples, which be used to compute the traffic condition by the application server. In fact, the server does not need to associate samples to a specific user. It estimates traffic conditions only by some traffic statistics data. Our goal is to achieve a trade-off between participants privacy and data utility. The utility of anonymous trajectory dataset was evaluated by two metrics: range query distortion and spatial distortion.

1) Range Query Distortion

Range query is one of the classic operations in data analysis field. Specifically, spatio-temporal range query get the number of individuals within a specified time interval and a region. It is widely used in the prediction of urban hotspot and traffic flow scenarios. Range query distortion in [8] is used to measure data utility between original trajectory database D and protected database D' (See (7)). A range query Q needs to set two parameters: a time window and a geographical area.

$$RQD(T, T') = \frac{\mid Q(D) - Q(D') \mid}{Q(D)} \qquad (7)$$

2) Spatial Distortion

The use of TPPM will directly lead to spatial error, which will affect data utility. Spatial distortion metric assesses the imprecision between trajectories before and after the TPPM process. We assume that for each record in protected trajectory $T' = (r'_1, r'_2, \ldots)$ there is a minimal project on the corresponding original trajectory $T = (r_1, r_2, \ldots)$. The spatial distortion is the average of the minimal projection of all the records in T' (See (8)).

$$SD(T, T') = \frac{1}{\mid T' \mid} \sum_{r' \in T'} \min_{r \in T} d(r, r') \qquad (8)$$

VI. Experimental Evaluation

Before to demonstrate the effectiveness of MSPP through different experiments, we present the real trajectory datasets in section VI-A, and then describe the relevant experimental setup of our evaluation in section VI-B. Finally, in our experiments, we evaluate three strategies in MSPP using privacy and data utility metric.

A. Datasets

We used three real trajectory dataset to conduct our experiments [13]: Cabspotting, Geolife and MDC. The Cabspotting dataset contains the mobility of 536 cab drivers in San Francisco. The Geolife dataset collects GPS trajectories of users during 172 users daily life over four years in Beijing, while the MDC dataset contains the mobility data of 144 users in Geneva.

B. Experimental Setup and Configurations

We implemented a prototype system of MSPP and ran the simulation experiments on MATLAB platform. To evaluate the impact of different strategies on user privacy protection and data utility under different parameter settings, the parameters are set as follows. We configure Geo-I with various value of ε ($\varepsilon = \ln(4)/200$ marked as Geo-I (I); $\varepsilon = \ln(2)/200$, marked as Geo-I(II)). The lower ε, the higher the noise and the stronger the privacy guarantee and Promesses parameter α ($\alpha = 100m$, marked as Promesse(I), $\alpha = 200m$, marked as Promesse(II)). α represents the distance between two successive sampling points.

For POIs extraction algorithm a POI is defined as a place where users stay in a diameter of $200m$ during at least 15 minutes. The diameter of the clustering area and the minimum time of PIT-Attack in this section are respectively set to $200m$ and 20 minutes.

C. Privacy Evaluation

1) Resilience against PIT-Attack

In this section, we present the result of three TPPMs that protect users against re-identification rate of PIT-Attack (see Section IV-B) in the Fig. 3. NOBF means that no TPPM is used on the original trajectory dataset.

The results show that Pathswap and Promesse successfully decrease re-identification rate of PIT-Attack. In other words, Pathswap and Promesse are better at protecting user mobility patterns compared with Geo-I. So both of them are applicable to scenarios where participants are strongly willing to protect their cyclical behaviors. Especially, the rate ranges from 1% to 10% while the rate of Promesse and Pathswap is 1% and 3% respectively in Cabspotting dataset. The major cause is: a) Promesse hides participants POIs by smoothing speed along his trajectories; b) Pathswap confuses the sub-trajectories of users crossed, and the final trajectory is composed of sub-trajectories of different individuals. In this way, POIs originally belonging to a certain person are dispersed.

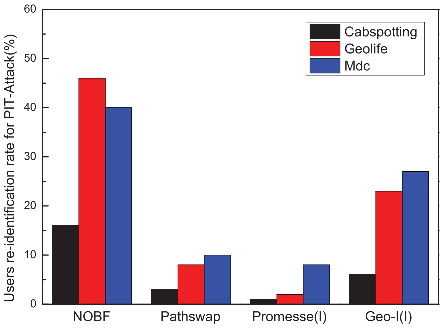

Fig. 3. Comparision of re-identification rate of different TPPMs.

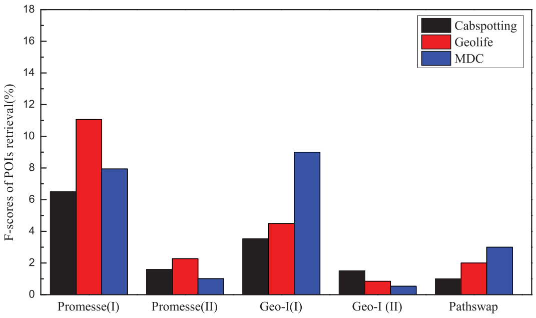

Fig. 4. F-scores of POIs retrieval.

2) POIs Retrieval

We only report on the F-score metric with $\ell = 100m$, which takes into account both precision and recall. Fig. 4 presents the detailed result of average F-score across all trajectories in each dataset.

Low F-Score means both a low precision and a low recall of POIs retrieval. For Promesse and Geo-I, we observe that the results depend on the parameters, and adaptively setting the parameters that meet the individual requirement is one of the future research contents. We also observe that trend of the metric of POIs retrieval was opposite to re-identification rate in Fig. 3 and Fig. 4, especially because of the principle of PIT-Attack. Intuitively, Pathswap can retain more POIs than Promesse and Geo-I, but it assigns POIs to different participants trajectories.

D. Utility Evaluation

To evaluate the data utility provided by different TPPMs, we use the two utility metrics (described in Section V-B): range query distortion and spatial distortion.

Range query distortion evaluate on trajectory dataset, rather than a single trajectory. There are two parameters needed to set: a region and a time interval. Similarly to [16], on account of the stochastic characteristics of range query, random durations and random regions under certain conditions are set. We randomly choose circular regions whose radius between 500 and $2000m$, and time interval with duration ranging from 2 to $6h$ in the experiments. Over 1000 different range queries are executed.

We notice that Pathswap outperforms all other TPPMs in term of range query distortion metric. Pathswap's average query distortion ranges from 4% to 12%, while Promesse has a query distortion ranging from 7% to 25% for $\varepsilon = 200m$. For Geo-I (I) it is from 5% to 26%. In fig. 5, we observe that this value of metric on Cabspotting is less sensitive than Geolife and MDC dataset. The fundamental reason lies in individual numbers of dataset. Meanwhile, from the perspective of individual location distribution, Pathswap does not add noise, but

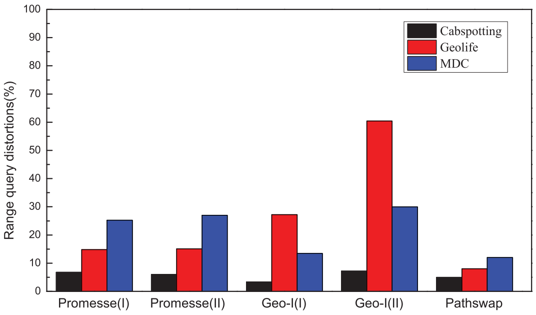

Fig. 5. Range query distortion.

TABLE I
AVERAGE SPATIAL DISTORTION

TPPM	Cabspotting	Geolife	MDC
Pathswap	50m	142m	163m
Promesse	11m	21m	30m
Geo-I(I)	62m	156m	183m
Geo-I(II)	113m	325m	378m

cuts off the link between individuals and trajectory segments. Compared with the other two strategies, Pathswap is more suitable for participatory sensing scenario of obtaining exact aggregated mobile data.

The table I presents the average spatial distortion for all trajectories in each dataset and we observe that Promesse provides the smallest spatial distort among the three TPPMs. Unlike the other two strategies, Promesse distorts time instead of distorting location and introduces spatial information losses because erasing some POIs. Spatial distortion of Geo-I is due to the fact that Geo-I adds noise depending on its ε parameter. Intuitively, for Pathswap the more trajectories intersect, the better the trajectory segments mix and the greater the spatial distortion, especially in a dense urban environment.

Our experiments results show that it might be difficult to use single (configuration) solution that fits all participants' privacy and utility objectives. Pathswap's performance in spatial error is weaker than Promesse, but it preserves the relative good aggregate information of spatial database and at the same time, provides anonymity to the individuals. Pathswap tends to protect participant's mobility patterns. Promesse has a better spatial utility but introduce time distortion. Geo-I provides strong privacy, but has lower utility. Note that, considering concrete privacy and utility requirements for different participatory sensing scenario, participants choose suitable TPPM and configure the corresponding parameter.

VII. CONCLUSION

Different from the existing permission on-off control mechanism, this paper has presented a configurable trajectory privacy-preserving framework for PS, named MSPP in the participants terminal. Based on the individual historical trajectory data stored locally and privacy preferences, participant actively selects the corresponding protection mechanism (Pathswap, Promesse, Geo-I, etc.) considering privacy metrics and data utility in PS scenarios. We illustrated the ability of our system to protect a user while keeping data utility using different mechanisms.

As future work, additionally to enrich the TPPMs and metrics, we plan to design visual interface for participant to fill the gap between non-technical users and privacy protection mechanisms.

ACKNOWLEDGEMENT

The work was supported by Program for Science and Technology Innovation Talents in Universities of Henan Province(19HASTIT027),and by the NSFC (61772173)

REFERENCES

[1] S. Hu, L. Su, H. Liu, H. Wang, T. F. Abdelzaher, ”Smartroad: Smartphone-based crowd sensing for traffic regulator detection and identification,” ACM Trans. Sens. Netw., vol. 11, no. 4, pp. 1-27, Dec.2015.

[2] X. Chen, X. Wu, X. Li, X. Ji, Y. He and Y. Liu, ”Privacy-Aware High-Quality Map Generation with Participatory Sensing,” IEEE Trans. Mob.Comput., vol. 15, no. 3, pp. 719-732, 1 March 2016.

[3] Z. Xiao, J. Yang, M. Huang, L. Ponnambalam, X. Fu and R. S. M. Goh, ”QLDS: A Novel Design Scheme for Trajectory Privacy Protection with Utility Guarantee in Participatory Sensing,” IEEE Trans. Mob.Comput., vol. 17, no. 6, pp. 1397-1410, 1 June 2018.

[4] D. Christin, ”Privacy in mobile participatory sensing: Current trends and future challenges”, J. Syst. Softw., vol. 116, pp. 57-68, June 2016.

[5] C. Y. Chow, M. F. Mokbel, ”Trajectory privacy in location-based services and data publication”, ACM SIGKDD Explor. Newsl., vol. 13, no. 1, June 2011.

[6] D. Reinhardt and I. Manyugin, ”OP4: An OPPortunistic Privacy-Preserving Scheme for Crowdsensing Applications,” IEEE LCN 2016.

[7] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, ”Traffic-aware multiple mix zone placement for protecting location privacy ”, IEEE INFOCOM 2012.

[8] V Primault, S.B Mokhtar, C Lauradoux, L Brunie, ”Time Distortion Anonymization for the Publication of Mobility Data with High Utility”, IEEE Trustcom/BigDataSe/ISPA 2015.

[9] C. Dwork, ”Differential privacy”, ACM ICALP 2006.

[10] M. E. Andrs, N. E. Bordenabe, K. Chatzikokolakis, C. Palamidessi, ”Geo-indistinguishability: Differential privacy for location-based systems”, ACM SIGSAC 2013.

[11] T. H. You, W. C. Peng, W. C. Lee, ”Protecting moving trajectories with dummies”, IEEE MDM 2007.

[12] D. Christin, D. M. Bub, A. Moerov, S. Kasem-Madani, ”A distributed privacy-preserving mechanism for mobile urban sensing applications”, IEEE ISSNIP 2015.

[13] M. Mohamed, S. B. Mokhtar, S. Bouchenak. ”HMC: Robust Privacy Protection of Mobility Data against Multiple Re-Identification Attacks.” ACM IMWUT 2018.

[14] S. Gambs, M.-O. Killijian, M. Nez del Prado Cortez, ”De-anonymization attack on geolocated data”, J. Comput. Syst. Sci., vol. 80, no. 8, pp. 1597-1614, Feb. 2014.

[15] V Primault, A Boutet, S.B Mokhtar, L Brunie, ”Adaptive Location Privacy with ALP.” IEEE SRDS 2016.

[16] O. Abul, F. Bonchi, and M. Nanni, Anonymization of moving objects databases by clustering and perturbation, Inf. Syst., vol. 35,no. 8, pp. 884-910, Jan 2010.