A Privacy-Preserving Pedestrian Dead Reckoning Framework Based on Differential Privacy

Tianyi Feng[*], Zhixiang Zhang[*], Wai-Choong Wong[*], Sumei Sun[+], Biplab Sikdar[*]
[*]*Department of Electical and Computer Engineering, National University of Singapore*, Singapore
[+]*Institute for Infocomm Research, Agency for Science, Technology and Research*, Singapore
Email: fengtianyi@u.nus.edu, e0320869@u.nus.edu, wong_lawrence@nus.edu.sg, sunsm@i2r.a-star.edu.sg, bsikdar@nus.edu.sg

***Abstract*—Pedestrian dead reckoning (PDR) is a widely used approach to estimate locations and trajectories. Accessing location-based services with trajectory data can bring convenience to people, but may also raise privacy concerns that need to be addressed. In this paper, a privacy-preserving pedestrian dead reckoning (P^3DR) framework is proposed to protect a user's trajectory privacy based on differential privacy. We introduce two metrics to quantify trajectory privacy and data utility. Our proposed privacy-preserving trajectory extraction algorithm consists of three mechanisms for the initial locations, stride lengths and directions. In addition, we design an adversary model based on particle filtering to evaluate the performance and demonstrate the effectiveness of our proposed framework with our collected sensor reading dataset.**

***Index Terms*—Pedestrian dead-reckoning, Trajectory privacy, Differential privacy, Location-based services**

I. Introduction

With the ubiquity of location-based services (LBS), indoor localization techniques have attracted more attention. Indoor positioning systems (IPSs) can support many applications to bring convenience to users. Hence, bountiful IPSs have been proposed according to different technologies, such as radio frequency identification (RFID), WiFi [1], Bluetooth, ultra-wideband (UWB), or their hybridization. PDR is another indoor positioning technique based on inertial sensors embedded in mobile terminals.

PDR [2] estimates movements and directions using the readings from an inertial measurement unit (IMU) incorporating an accelerometer, a magnetometer and a gyroscope. It generates trajectories for mobile users by adding estimated displacement to the previous location with three phases: step detection, stride length estimation, and orientation estimation. It can realize calibration-free indoor localization without additional preparations and infrastructures. With the increase of trajectory distance, PDR will produce cumulative error drifts.

With the rapid development of Internet of Things (IoT), an individual's trajectory data can be collected by service providers with high accuracy. Analysing human movement traces can help design more services such as navigation, social recommendations and delivery tracking. Such information and analysis can also help build a more intelligent city, e.g., urban planning, transportation management, and epidemiological analysis, etc. While publishing trajectory data brings great benefits, it also results in serious privacy threats to individuals since some sensitive information can be extracted, such as home address, relationships, religious beliefs and even health status. Therefore, it is important to protect trajectory privacy while accessing LBS and releasing trajectory data.

To address such privacy problems, numerous privacy preserving mechanisms have been proposed, such as k-anonymity [3], dummy trajectories [4], mix-zones [5] and confidence bounding [6]. Differential privacy [7] has also been applied to trajectory publishing, which is a mathematical construct to provide provable privacy protection to any individual whose data is in a statistical database. Mechanisms following such theory can provide a provable privacy guarantee.

Although trajectory data is spatio-temporal and discrete, the location correlations need to be considered. In addition, some partition-based approaches, like k-anonymity, mix-zones, and confidence bounding, are not suitable for publishing trajectories against many types of attacks, such as composition attack and foreground knowledge attack. To solve these problems, there has been some previous work on differentially private trajectory publishing. However, these works may be still vulnerable since most of them protect the user's trajectory privacy by generating synthetic trajectories with the received raw trajectories. Motivated by the weakness of traditional anonymization methods and the risk of synthesizing pseudo trajectories according to the original trajectories, we propose the P^3DR method to generate suitable and reasonable pseudo trajectories directly based on differential privacy.

The main contributions of this paper can be summarized as follows.

1) We propose a LBS system solution to preserve trajectory privacy and location privacy together based on differential privacy and find the tradeoff between privacy and data utility;
2) We introduce two metrics, trajectory correlation score and service performance score, to quantify privacy and data utility;
3) We present a privacy-preserving trajectory extraction algorithm based on PDR to generate pseudo trajectories;
4) We implement and evaluate our proposed framework with our collected mobile sensor dataset and design an adversary model to show the robustness of our system.

The rest of the paper is organized as follows. The related work on PDR and trajectory privacy is introduced in Section II.

Section III presents the theory and procedure of the traditional PDR. In Section IV, the preliminaries of differential privacy are introduced. The system model and our proposed Trajectory Privacy Preserving Mechanism (TPPM) are systematically presented in Section V. We also propose an adversary model in Section VI. In addition, the effectiveness evaluation and analysis are illustrated in Section VII. Section VIII concludes this paper.

II. Related Work

With the development of Micro-Electro-Mechanical Systems (MEMS), applications based on mobile sensors are widely used for localization and navigation. Jeong et al. [2] proposed a step, stride and heading determination method in the pedestrian navigation scenario. They derived the relationship between stride and accelerometer readings and proposed an integration scheme of gyroscope and magnetic compass. In [8], a map matching enhanced PDR algorithm was proposed to calibrate the location estimation together with the particle filter. They used the corridor information to calibrate the location and direction estimation with an improved particle filter and map filter. Wang et al. [9] proposed a landmark-aided PDR indoor positioning system, which combined WiFi and PDR techniques to define landmarks to correct cumulative errors. These are some localization methods to generate user trajectories based on PDR technique and IMU readings. While releasing trajectories for further services, trajectory privacy should be taken into consideration seriously.

Trajectory privacy has attracted many researchers and traditional trajectory privacy preserving mechanisms are based on anonymization and differential privacy. Nergiz et al. [10] proposed a generalization-based k-anonymity method to achieve trajectory anonymization. They enhance the privacy preserving effectiveness by a randomized reconstruction approach to generate representative trajectories. Soheila et al. [11] proposed a trajectory generative mechanism (TGM) based on differential privacy by encoding the given trajectories and generating synthetic trajectories. In their proposed framework, they used Laplace mechanism to add noise and Exponential mechanism to select locations adaptively with a directed budget restoring algorithm. In [12], a differential privacy trajectory synthesis system was proposed to synthesize mobility data. They used hierarchical reference systems with different resolutions to generate speed-varying trajectories.

Most of the above-mentioned approaches neglected the adversary's possible activities while designing privacy preserving mechanisms and published the generated or synthesized trajectory data according to the user's raw trajectories. However, the adversary model cannot be disregarded since it is crucial and necessary to evaluate the robustness of a TPPM. To address this open problem in this paper, we design an adversary model based on particle filter and validate the effectiveness and efficiency of our proposed framework. In addition, we propose a P^3DR framework to generate pseudo trajectories directly, rather than obtain raw trajectories first for further processing.

III. Traditional PDR

PDR is a pedestrian positioning solution that estimates the pedestrian's current position by adding the travelled displacement to the previously determined position, defined as:

$$l_t = l_{t-1} + \Delta l_t \cdot \begin{bmatrix} sin(\psi_t) \\ cos(\psi_t) \end{bmatrix} \tag{1}$$

where l_t is the position at step t, l_{t-1} is the position at step $t-1$, Δl_t is the step length and ψ_t is the walking direction at step t.

A. Step Detection

Peak detection algorithm can be used for step detection since accelerometer readings may present periodical variations [2], while the pedestrian is walking horizontally. Acceleration jitters may cause false detection of peaks and steps, so two thresholds need to be determined to constraint the magnitude and the time interval of peaks, namely the pedestrian's walking speed.

B. Stride Length Estimation

The simplest method to estimate stride length is setting a fixed step length according to the body characteristic of the pedestrian. According to pedestrian's walking features, some dynamic approaches are established, such as the Weinberg approach, the Kim approach and the Scarlet approach [2]. In particular, the Weinberg approach estimate the stride length by

$$L = K \times \sqrt[4]{a_{\max} - a_{\min}} \tag{2}$$

where K is a constant, a_{max} and a_{min} are the maximal and minimal acceleration in the vertical direction during one step. This method is based on the principle that the hip vertical displacement is proportional to the step length with some degree.

C. Orientation Estimation

The orientation can be obtained from the measurements of the accelerometer, gyroscope and magnetometer by the Euler angle algorithm and the quaternion algorithm [13]. In this paper, we use the quaternion-based algorithm to update attitude angle since it can avoid the singularity problem. The attitude quaternion can be defined as

$$\dot{q} = \frac{1}{2} q \otimes \omega \tag{3}$$

where $q = q_0 + q_1 i + q_2 j + q_3 k$ is the quaternion, $q_i(i = 0, 1, 2 and 3)$ is a real number, $\omega = 0 + \omega_1 i + \omega_2 j + \omega_3 k$ is the quaternion of the attitude angular velocity and $\otimes$ denotes the multiplication. The rotation matrix can be calculated as

$$R = \begin{bmatrix} q_0^2 + q_1^2 - q_2^2 - q_3^2 & 2(q_1 q_1 + q_0 q_3) & 2(q_1 q_3 - q_0 q_2) \\ 2(q_1 q_2 - q_0 q_3) & q_0^2 - q_1^2 + q_2^2 - q_3^2 & 2(q_2 q_3 + q_0 q_1) \\ 2(q_1 q_3 + q_0 q_2) & 2(q_2 q_3 - q_0 q_1) & q_0^2 - q_1^2 - q_2^2 + q_3^2 \end{bmatrix} \tag{4}$$

Since the magnetic field is unstable indoors, gravity is involved to calibrate the orientation estimation [8]. The roll and pitch can be calculated as

$$\begin{cases} roll &= \arctan\left(-\frac{-g_x}{\sqrt{g_y^2+g_z^2}}\right) \\ pitch &= \arctan\left(-\frac{-g_y}{\sqrt{g_x^2+g_z^2}}\right) \end{cases} \tag{5}$$

where g_x, g_y, and g_z are the triaxial gravity in the x, y, and z directions respectively. The regenerated ω^g can be determined as

$$\omega^g(i) = \omega(i) * R(roll(i-1), 1, 0, 0) \otimes R(pitch(i-1), 0, 1, 0), i \geq 2. \tag{6}$$

Finally, we can calculate the attitude angle update as

$$\Delta\theta = \frac{1}{6}\left(\omega_z^g(i-3) + 2\omega_z^g(i-2) + 2\omega_z^g(i-1) + \omega_z^g(i)\right) \times T_s, i \geq 4 \tag{7}$$

where T_s is the sampling period.

IV. Differential Privacy

A. Definition

Differential privacy was proposed by Dwork [14] and its basic principle is to make the probabilities of obtaining the same result be quite close by searching two adjacent datasets with only one different record.

Definition 1 (Differential Privacy): A randomized algorithm $\mathcal{M}$ gives ϵ-differential privacy if for all $\mathcal{S} \subseteq Range(\mathcal{M})$ and for all datasets D_1, D_2 such that $\|D_1 - D_2\|_1 \leq 1$,

$$\Pr\{\mathcal{M}(D_1) \in S\} \leq \exp(\epsilon) \times \Pr\{\mathcal{M}(D_2) \in S\} \tag{8}$$

where $\|D_1 - D_2\|_1$ is the distance between D_1 and D_2 to measure how many records differ in the two datasets.

B. Differential Privacy Mechanisms

There are two types of differential privacy, one is centralized differential privacy, the other is local differential privacy (LDP). The main approach to achieve centralized differential privacy is by adding Laplacian or Gaussian noise and such mechanisms are implemented in a server.

Definition 2 (Laplace Mechanism): Given any function f: $D \to \mathbb{R}$, the Laplace mechanism $\mathcal{M}_L$ is defined as

$$\mathcal{M}_L(D) = f(D) + Lap\left(\frac{\Delta f}{\epsilon}\right). \tag{9}$$

Laplacian and Gaussian mechanisms are two solutions for numerical data. Moreover, exponential mechanism is a method to randomize the results for non-numerical or categorical data. Randomized response, a research method always used in questionnaire or survey interview, is a major perturbation mechanism for LDP. LDP assumes that the data collector is not trustworthy, therefore, the mechanism should be implemented before sending original data to the data collector.

C. Composition theorems

In a privacy sensitive systems, it is possible to have more than one blocks or datasets. So we need to combine several privacy preserving mechanisms together to solve more sophisticated problems. There are two types of composition theorems: sequential composition [15] and parallel composition [16].

Theorem 1 (Sequential Composition): Suppose mechanisms $\mathcal{M}_1$, $\mathcal{M}_2$, $\cdots$, $\mathcal{M}_k$ sequentially access a private dataset D and each mechanism $\mathcal{M}_i$ satisfies ϵ_i-differential privacy, their combination $\mathcal{M} = \{\mathcal{M}_1, \mathcal{M}_2, \cdots, \mathcal{M}_k\}$ will provide ϵ-differential privacy with $\epsilon = \epsilon_1 + \epsilon_2 + \cdots + \epsilon_k$.

Theorem 2 (Parallel Composition): Suppose mechanisms $\mathcal{M}_1$, $\mathcal{M}_2$, $\cdots$, $\mathcal{M}_k$ access disjoint datasets $D_1, D_2, \cdots, D_k$ and each mechanism $\mathcal{M}_i$ satisfies ϵ_i-differential privacy, their combination in parallel will provide ϵ-differential privacy with $\epsilon = \max\{\epsilon_1, \epsilon_2, \cdots, \epsilon_k\}$.

V. P^3DR System

A. System Model

In traditional PDR systems, users request their initial locations from location service providers as the first step and forward their initial locations and mobile sensor readings to trajectory generation service providers to obtain their positions and trajectories. In our proposed P^3DR system, there are five entities as shown as Figure 1. To preserve the user's location privacy and trajectory privacy, the location service provider generates pseudo initial locations with the built-in location privacy preserving mechanism (LPPM) and the trajectory generation service provider estimates trajectories with the built in TPPM. The whole procedure of the P^3DR system follows the user's pre-defined privacy budgets. Since we have implemented three privacy preserving mechanisms together following the parallel composition principle and there are three privacy levels in our framework, namely, the privacy level ϵ_1 for initial locations, the privacy level ϵ_2 for stride lengths, and the privacy level ϵ_3 for angles, the total privacy budget ϵ can be computed as $\epsilon = \max\{\epsilon_1, \epsilon_2, \epsilon_3\}$. Finally, the trajectory generation service provider releases generated trajectories to the application service provider to access LBS. In our proposed system, we assume that an adversary may infer users' destinations by eavesdropping.

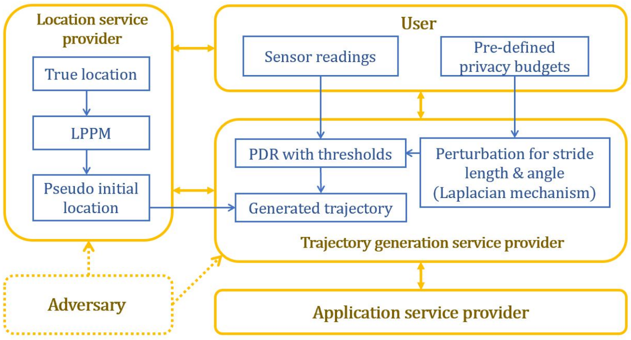
Location service provider
True location
LPPM
Pseudo initial location
User
Sensor readings
Pre-defined privacy budgets
PDR with thresholds
Perturbation for stride length & angle (Laplacian mechanism)
Generated trajectory
Trajectory generation service provider
Adversary
Application service provider

Fig. 1. System Model

B. Metrics

Two metrics, the trajectory correlation score and the service performance score, are introduced to quantify the trajectory privacy and trajectory data utility.

Definition 3 (Trajectory Correlation Score): For any user with a pair of the real trajectory $T = \{(x_i, y_i)|i = 1, 2, \cdots, n\}$ and the generated trajectory $T' = \{(x'_i, y'_i)|i = 1, 2, \cdots, n\}$, the trajectory correlation score S can be defined as

$$S = S(x) \times S(y), \tag{10}$$

where $S(x) = 1 - \prod_{i=1}^{n} \left\{1 - \exp\left(-\frac{|d_x^i|}{R}\right)\right\}$ and $S(y) = 1 - \prod_{i=1}^{n} \left\{1 - \exp\left(-\frac{|d_y^i|}{R}\right)\right\}$, $d_x^i = x_i - x'_i$ and $d_y^i = y_i - y'_i$ represent the distances of the latitudes and the longitudes between the positions on the real trajectory and the generated trajectory at i-th time slot, and R is the correlation range of the location distance to indicate the social relation.

Definition 4 (Service Performance Score): For a pair of the real trajectory and the generated trajectory, the service performance score $\mathcal{U}$ can be defined as

$$\mathcal{U} = \omega_1 \times \frac{1}{\Delta L} + \omega_2 \times \frac{1}{dis(l_n, l'_n)} + \omega_3 \times \frac{1}{d_{\text{diameter}}}, \tag{11}$$

where ΔL is the total trajectory length difference, $dis(l_n, l'_n)$ is the distance between the destination and the generated trajectory's ending position, $d_{\text{diameter}} = \max_{i,j} dis(l_i^u, l_j^u) - \max_{i,j} dis(l_i^{u'}, l_j^{u'})$ is the diameter error, and ω_1, ω_2 and ω_3 are the coefficients of these three factors.

C. LPPM

In our proposed P^3DR system, we introduce our previously proposed LPPM to protect the user's initial location privacy [17]. With a given initial location (x_i, y_i) and a privacy level ϵ_1, we can compute the Laplacian noise r_{Lap} added to the true location [18] within the location service quality threshold $(r_{\min}, r_{\max})$ by

$$r_{\text{Lap}} = \left| -\frac{1}{\epsilon}(W_{-1}(\frac{p-1}{e}) + 1) \right|, r_{\min} \leq r_{\text{Lap}} \leq r_{\max} \tag{12}$$

where $p = rand(1)$ is uniformly distributed in the interval $[0, 1]$ and W_{-1} is the LambertW function. Since $p \in [0, 1]$, r_{Lap} has its own range $(0, \frac{1}{\epsilon})$ and $(r_{\min}, r_{\max})$ should be within this range. The relationship among these parameters can be summarized as $0 \leq r_{\min} \leq r_{\text{Lap}} \leq r_{\max} \leq \frac{1}{\epsilon}$. Then, we can generate the pseudo initial location with a random direction $\theta = rand(1) \cdot 2\pi$ as

$$\begin{cases} x_i^{'} = x_i + r_{\text{Lap}} \cdot \cos(\theta) \\ y_i^{'} = y_i + r_{\text{Lap}} \cdot \sin(\theta). \end{cases} \tag{13}$$

D. TPPM

In our proposed P^3DR system, we propose a trajectory extraction algorithm based on the traditional PDR and preserve the user's trajectory privacy by adding constraints and Laplacian noise as shown in Figure 2. With the received pseudo initial locations and mobile sensor readings, our proposed TPPM adds Laplacian noise to the estimated stride lengths and angles to generate pseudo trajectories according to the user's pre-defined privacy budgets (i.e., privacy level ϵ_2 for stride lengths and privacy level ϵ_3 for angles). At the same time, we should also ensure the generated trajectories are reasonable. Therefore, we involve three constraints to limit the step speed, the stride length and the direction. We assume users cannot walk more than 5 steps per second and their stride lengths are always less than 1.5 meter. As for the direction, we use the turning detection before adding noise to the angle. While the user is not making a turn, the Laplacian noise will not be added to the angle and the current step will be assumed to continue as previously determined. The User's current pseudo positions are estimated by adding the perturbed displacement to the previously determined pseudo positions. The final generated trajectories are sent to the application service provider for accessing further services.

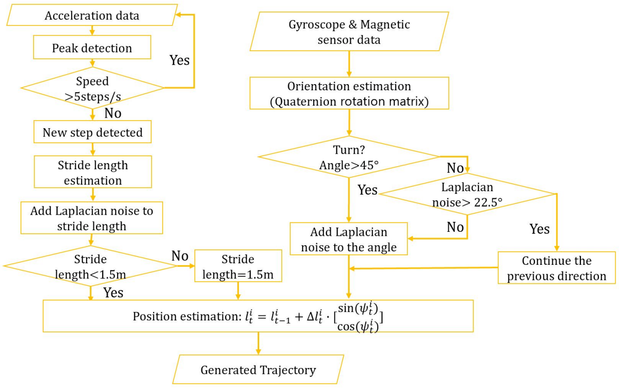
Acceleration data
Peak detection
Speed >5steps/s
Yes
No
New step detected
Stride length estimation
Add Laplacian noise to stride length
Stride length<1.5m
No
Stride length=1.5m
Yes
Gyroscope & Magnetic sensor data
Orientation estimation (Quaternion rotation matrix)
Turn? Angle>45°
No
Yes
Laplacian noise> 22.5°
No
Yes
Add Laplacian noise to the angle
Continue the previous direction
Position estimation: $l_t^i = l_{t-1}^i + \Delta l_t^i \cdot [\begin{smallmatrix}\sin(\psi_t^i)\\ \cos(\psi_t^i)\end{smallmatrix}]$
Generated Trajectory

Fig. 2. Trajectory Extraction Algorithm

VI. Adversary Model

In our proposed P^3DR framework, we assume the adversary's goal is to infer the users' actual destinations or the ending positions, because destinations can provide more valuable information for the adversary to explore the user's desired interests in some trajectory-related LBS. We also assume that the adversary can receive the released trajectories and has the prior knowledge of the walking area map. In particular, the walking area means the user can only walk in this area and cannot pass through obstacles such as rivers, buildings, etc. Therefore, we introduce two constrains for our

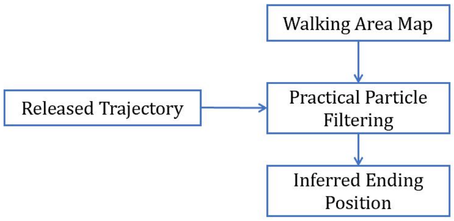

Fig. 3. Adversary Model

proposed adversary model. One constraint is that the user can only walk in the walking area, and the other is that the user's steps in a trajectory must be continuous. Then, we propose a practical particle filter algorithm for the adversary to infer the end positions as shown in Algorithm 1. Particle filtering has been applied in some indoor tracking systems since different particles with weights can represent the uncertainty of the location estimation. The weights and particles are updated for each step according to the distance error between the particles and the pseudo states. The pseudo states are the observable positions on the pseudo trajectory. So we use the particle filter to improve the inference results and involve the constraints to avoid generating unsuitable particles. The structure of our proposed adversary model can be illustrated as Figure 3.

```
Algorithm 1: Practical Particle Filter
Input: The released pseudo trajectory $Z$ and the
       waling area region $\mathcal{S}$
Output: The inferred ending position $P_e$
Initialize all the particles $P(:,i)$ as samples randomly
  distributed in the region $\mathcal{S}$, for $k = 1, i = 1 : N$;
for $k = 2 : T$ do
    Obtain the current observable position $Z(:,k)$ on
      the pseudo trajectory;
    Each particle predicts its next location $P(:,i)$ in
      the possible located area $\mathcal{S}$, for $i = 1 : N$;
    Compute the distance error between particles and
      the pseudo state
      $Err_{\text{dis}} = norm(P(:,i) - Z(:,k))$;
    Compute weights for each particle
      $\omega(i) = \left(1/\sqrt{R}/\sqrt{2\pi}\right) \times \exp\left(-\frac{Err_{\text{dis}}^2}{2R}\right)$;
    Normalize the weights;
    Re-sampling to update particles;
    Find the center of all the particles $PCenter(:,k)$;
Define the inferred ending position as the final center
  of the particles $P_e = PCenter(:,T)$;
Return $P_e$;
```

VII. Results and Evaluation

Figure 4 illustrates the P^3DR generated trajectories with different privacy levels. The red path shows the real trajectory of the user, and the yellow path is the generated trajectory by the traditional PDR with raw sensor readings. The rest of the paths in Figure 4 are the generated trajectories by our proposed P^3DR system with different privacy levels. In particular, the higher the differential privacy level, the lower the trajectory privacy preservation level the user obtains. Thus, the black path shows the P^3DR generated trajectory with a large differential privacy level, which is the closest result to the real trajectory. On the contrary, the blue path shows the P^3DR generated trajectory with the small differential privacy level, which is the most discrepant result to the real trajectory. According to the results shown in Figure 4, it can be concluded that our proposed P^3DR system can generate reasonable and suitable pseudo trajectories based on different differential privacy levels to protect the user's trajectory privacy.

To further evaluate our proposed system, we introduce an adversary model based on the use of particle filter. Figure 5 shows the initial state of our proposed practical particle filter algorithm. The yellow dots present the initialization of particles, which cannot be located on the motorways or inside the buildings. The red crosses are the points of interest (POIs) in our simulation scenario. The green dot is the user's initial position and the blue dot is the center of all the initial particles. In Figure 6, the red path shows the user's real trajectory, and the green path shows the generated pseudo trajectory by our proposed P^3DR system with the differential privacy level $\epsilon = 2$. The blue path shows the adversary inferred trajectory, which consists of the centers of all the particles. Our proposed adversary model can infer the user's possible destination to some extent since the end position of the blue path is closer to the user's destination than the pseudo destination.

To receive more general and convincing results, we simulate our proposed P^3DR system with different differential privacy levels from 0 to 10, and the interval of differential privacy level equals to 0.001. Figure 7 and Figure 8 illustrate the relationship between the trajectory privacy and the differential privacy level and the relationship between the trajectory data utility and the differential privacy level. Both the trajectory correlation score and the service performance score increase gradually with an increase in the differential privacy level. Thus, our proposed P^3DR system can protect the user's trajectory privacy and generate reasonable pseudo trajectories for the user according to her pre-defined privacy levels.

Figure 9 shows the performance of our proposed adversary model. Since we assume that the adversary's goal is to infer the user's destination, we compute the distances between the inferred final positions and the real destinations as the adversary final error to evaluate the adversary's performance. The adversary final error as shown as the black curve in Figure 9 is always below the blue curve, which is the pseudo final error. Therefore, our proposed adversary model can infer the user's possible destination to some extent, but not exactly. In addition, we compute the average distance between each pair of positions on the adversary's inferred trajectory and the real trajectory as the adversary average error, and the adversary model can also reduce the pseudo average error slightly. Therefore, our proposed framework is robust and can still preserve the user's trajectory privacy against the adversary.

VIII. Conclusion

This paper proposed the P^3DR framework for trajectory privacy preservation based on differential privacy and the technique of PDR. We introduced two metrics to quantify the trajectory privacy and the trajectory data utility, and proposed a trajectory extraction algorithm to generate pseudo trajectories. We also proposed an adversary model based on particle filter to evaluate the P^3DR system, and simulate with our collected

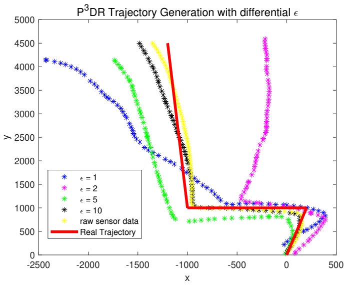

Fig. 4. P^3DR Trajectory Generation

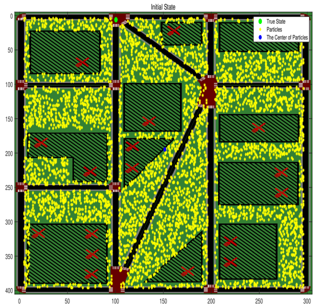

Fig. 5. Initial State

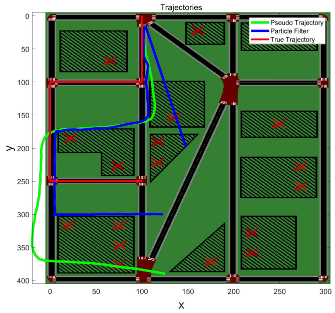

Fig. 6. True, Pseudo and Adversary-inferred Trajectories

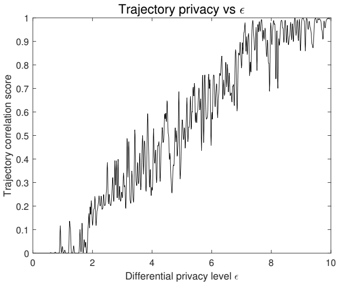

Fig. 7. Trajectory Privacy

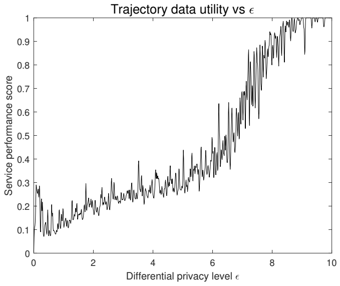

Fig. 8. Trajectory Data Utility

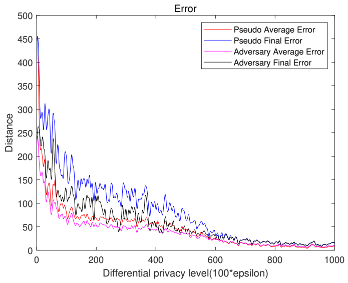

Fig. 9. Adversary Performance

mobile sensor dataset to show the detailed procedure of protecting the user's trajectory privacy and the robustness of our system. In our future work, we will consider the accelerometer based data privacy since publishing acceleration data alone is enough to extract some sensitive information including locations and trajectories. We plan to follow the LDP principle to design a acceleration privacy preserving mechanism to enhance the degree of users' privacy preservation.

Acknowledgment

This research/project is supported by the National Research Foundation, Singapore under its Strategic Capability Research Centres Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

References

[1] Y. Zhao, W.-C. Wong, T. Feng, and H. K. Garg, "Calibration-free indoor positioning using crowdsourced data and multidimensional scaling," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1770–1785, 2019.

[2] J. W. Kim, H. J. Jang, D. H. Hwang, and C. Park, "A step, stride and heading determination for the pedestrian navigation system," *Journal of Global Positioning Systems*, vol. 3, no. 12, pp. 273–279, 2004.

[3] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*. ACM, 2003, pp. 31–42.

[4] W. P. Tunhao You, "Protecting moving trajectories with dummies," in *International Conference on Mobile Data Management*, 2008.

[5] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*. IEEE, 2004, pp. 127–131.

[6] M. Terrovitis and N. Mamoulis, "Privacy preservation in the publication of trajectories," in *Mobile Data Management, 2008. MDM '08. 9th International Conference on*, 2008.

[7] C. Dwork, "Differential privacy," *Encyclopedia of Cryptography and Security*, pp. 338–340, 2011.

[8] B. Haitao and W. Wai-Choong, "A novel map-based dead-reckoning algorithm for indoor localization," *Journal of Sensor Actuator Networks*, vol. 3, no. 1, pp. 44–63, 2014.

[9] X. Wang, M. Jiang, Z. Guo, N. Hu, Z. Sun, and J. Liu., "An indoor positioning method for smartphones using landmarks and pdr." *Sensors (14248220)*, 2016.

[10] M. E. Nergiz, M. Atzori, and Y. Saygin, "Towards trajectory anonymization: a generalization-based approach," in *Sigspatial Acm Gis International Workshop on Security Privacy in Gis Lbs*, 2008.

[11] S. Ghane, L. Kulik, and K. Ramamohanarao, "Tgm: A generative mechanism for publishing trajectories with differential privacy," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2019.

[12] X. He, G. Cormode, A. Machanavajjhala, C. M. Procopiuc, and D. Srivastava, "Dpt: differentially private trajectory synthesis using hierarchical reference systems," *Proceedings of the Vldb Endowment*, vol. 8, no. 11, pp. 1154–1165, 2015.

[13] Z. Tian, Y. Zhang, M. Zhou, and Y. Liu, "Pedestrian dead reckoning for marg navigation using a smartphone," *Eurasip Journal on Advances in Signal Processing*, vol. 2014, no. 1, p. 65, 2014.

[14] C. Dwork, "Differential privacy," in *Proceedings of the 33rd international conference on Automata, Languages and Programming-Volume Part II*. Springer-Verlag, 2006, pp. 1–12.

[15] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Differentially private data publishing and analysis: A survey," *IEEE Transactions on Knowledge Data Engineering*, vol. 29, no. 8, pp. 1619–1638, 2017.

[16] F. Mcsherry, "Privacy integrated queries: An extensible platform for privacy-preserving data analysis," *Communications of the Acm*, vol. 53, no. 9, pp. 89–97, 2010.

[17] T. Feng, W.-C. Wong, S. Sun, Y. Zhao, and Z. Zhang, "Location privacy preservation and location-based service quality tradeoff framework based on differential privacy," in *2019 16th Workshop on Positioning, Navigation and Communications (WPNC)*. IEEE, 2019, pp. 1–6.

[18] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *the 2013 ACM SIGSAC Conference on Computer Communications Security*. ACM, 2012, pp. 901–914.