Protecting Personalized Trajectory with Differential Privacy under Temporal Correlations

Mingge Cao*, Haopeng Zhu*, Minghui Min*†, Yulu Li*, Shiyin Li*, Hongliang Zhang‡, and Zhu Han§

* School of Information and Control Engineering, China University of Mining and Technology, Xuzhou 221116, China.
† Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education and School of CyberScience and Engineering, Wuhan University, Wuhan 430072, China.
‡ School of Electronics, Peking University, Beijing 100871, China.
§ Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004, USA.

Abstract—Location-based services (LBSs) in vehicular ad hoc networks (VANETs) offer users numerous conveniences. However, the extensive use of LBSs raises concerns about the privacy of users' trajectories, as adversaries can exploit temporal correlations between different locations to extract personal information. Additionally, users have varying privacy requirements depending on the time and location. To address these issues, this paper proposes a personalized trajectory privacy protection mechanism (PTPPM). This mechanism first uses the temporal correlation between trajectory locations to determine the possible location set for each time instant. We identify a protection location set (PLS) for each location by employing the Hilbert curve-based minimum distance search algorithm. This approach incorporates the complementary features of geo-indistinguishability and distortion privacy. We put forth a novel Permute-and-Flip mechanism for location perturbation, which maps its initial application in data publishing privacy protection to a location perturbation mechanism. This mechanism generates fake locations with smaller perturbation distances while improving the balance between privacy and quality of service (QoS). Simulation results show that our mechanism outperforms the benchmark by providing enhanced privacy protection while meeting user's QoS requirements.

Index Terms—Location-based service, temporal correlation, trajectory privacy protection, differential privacy.

I. INTRODUCTION

Location-based services (LBSs) in vehicular ad hoc networks (VANETs), such as real-time traffic information reports and personalized navigation, significantly enhance our daily lives [1], [2]. However, to enjoy these convenient services, VANET users must provide their real-time location to the LBS server, raising concerns about privacy breaches [3]. Several location privacy protection mechanisms have been developed to address this issue. However, focusing solely on protecting location information is insufficient. Trajectory data, which consists of interconnected locations, holds valuable temporal information that potential attackers can exploit to

deduce users' activities and uncover sensitive personal information [4]. Besides, different users may have different location privacy and quality of service (QoS) requirements [5], and even the same user may have various sensitive information at different times and locations, and thus have different privacy protection demands. Therefore, ensuring the privacy of user trajectories and meeting their personalized demands is of utmost importance.

Most existing research focuses on privacy protection for individual locations. For instance, a privacy notion called geo-indistinguishability, based on differential privacy, is proposed in [6]. This notion aims to protect a user's location within a certain radius, guaranteeing "generalized differential privacy". However, this approach overlooks arbitrary prior knowledge that adversaries may possess, leading to potential privacy leakage [7], and the degree of privacy protection is not clearly defined. To address these shortcomings, authors in [8] combine geo-indistinguishability and expected inference error, leveraging their complementary properties to propose a personalized location privacy protection mechanism. However, this approach still fails to consider the temporal correlation between different locations on a trajectory.

A solution called "δ-location set" based differential privacy is proposed in [9], which combines the location privacy protection mechanism in [8] with the temporal correlation between locations on a trajectory. However, this approach assigns the same privacy budget to all locations and does not cater to users' personalized demands. A few trajectory privacy protection schemes use k-anonymity [10] to achieve privacy protection. These methods generalize and aggregate individual trajectory data, ensuring the trajectory remains protected while combining it with at least $k - 1$ other trajectories to form an anonymous region. However, these approaches rely on a trusted third party and fail to provide strict privacy guarantees [11], [12]. In summary, existing trajectory privacy protection schemes lack consideration of crucial aspects such as the temporal correlation between locations on a trajectory, meeting the user's personalized needs, and ensuring the protection of the user's actual location without relying on a trusted third party. Consequently, a novel trajectory privacy mechanism is needed to simultaneously satisfy these requirements.

In this paper, we develop a personalized trajectory privacy protection mechanism (PTPPM) that considers the temporal correlation between locations on a trajectory. The mechanism constructs a location transition probability matrix, deriving the potential location set for the user at each time point along the trajectory. To improve privacy, we leverage the complementary features of geo-indistinguishability [6] and distortion privacy [13] by employing the Hilbert curve-based minimum distance search algorithm [8] to identify a protection location set (PLS) encompassing all potential locations along the trajectory. Geo-indistinguishability can limit the attacker's posterior knowledge, but cannot quantify the similarity between the attacker's inferred location and the actual location. Distortion privacy can ensure that the attacker's expected inference error is greater than a certain threshold. However, it cannot prevent the leakage of posterior information. The combination of these two notions can effectively strengthen the resistance against location inference attacks. The mechanism also enables personalized user privacy protection by adjusting the privacy settings through two privacy parameters.

In addition, we introduce an extension of the Permute-and-Flip mechanism [14], originally designed for data privacy protection during data publishing, to serve as a location perturbation mechanism. This novel approach achieves a smaller perturbation distance, which has a better balance between location privacy and QoS. Simulation results demonstrate that PTPPM provides personalized trajectory privacy protection and offers superior privacy preservation compared to PIVE [8] under the same QoS loss. The main contributions of our work include:

1) We propose a personalized trajectory privacy protection mechanism called PTPPM, which can defend the attacker that obtains the temporal correlation between various locations within a trajectory. This mechanism combines two privacy notions of geo-indistinguishability and distortion privacy to enhance the system's robustness against location inference attacks.

2) We put forth a novel location perturbation mechanism, Permute-and-Flip. It has a smaller perturbation distance to release perturbed locations, thereby achieving a better balance between location privacy and QoS.

3) We conduct comprehensive simulations to study the impact of different privacy budgets and expected inference errors on users' personalized requirements. Additionally, we demonstrate the performance advantage of PTPPM over PIVE under the same QoS loss.

The remainder of this paper is organized as follows. Section II presents the system model. We present the trajectory privacy protection statement in Section III. A PTPPM framework is proposed in Section IV. The evaluation results are provided in Section V. Finally, we conclude this work in Section VI.

II. SYSTEM MODEL

To obtain real-time LBSs, we consider that VANET users share their location information with a roadside unit (RSU) or an LBS server at different times and locations [5], [15]. Users
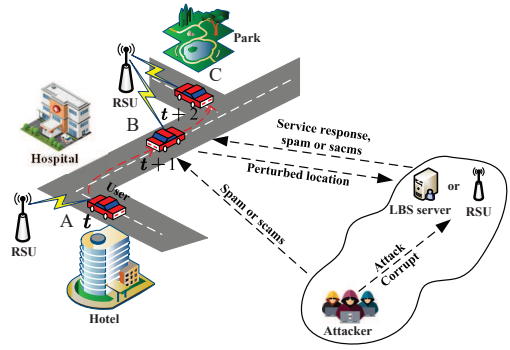

Fig. 1. Illustration of the trajectory privacy protection.

interact with the RSU to access road information, plan their destinations, and determine driving routes. Fig. 1 illustrates the user's driving trajectory, where A, B, and C are the user's locations at different times. To protect privacy, the user releases the perturbed locations. The untrusted LBS server, which an external attacker might also corrupt, can infer the user's sensitive information (e.g., the user's driving trajectory) at a particular time by analyzing the received temporally correlated location information and sending related spam or scams while providing feedback services.

A. User Model

We consider VANET users driving within a specific area of a city, which is divided into multiple grids. Each grid cell represents a distant location state of the user, and each cell is associated with a unique 2D coordinate. The state of all locations of the user in the area is $\mathcal{A} = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_n\}$, where n is the total number of location states. $\boldsymbol{x}_t$ represents the user's true location at time t, and $\boldsymbol{l}_t$ represents the two-dimensional coordinates of the user's location state at time t. For example, a shown in Fig. **??**, $\mathcal{A} = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_{22}\}$, $\boldsymbol{x}_t = \boldsymbol{a}_6 = [0,0,0,0,0,1,0\cdots,0]$, $\boldsymbol{l}_t = [2,4]$.

The user uses the location perturbation mechanism to remap the actual location $\boldsymbol{x}_t$ from the actual location set O_1 to the fake location $\boldsymbol{x}'_t$ from the perturbed location set O_2. The location perturbation probability distribution f is given by

$$f\left(\boldsymbol{x}'_t | \boldsymbol{x}_t\right) = \Pr\left(O_2 = \boldsymbol{x}'_t | O_1 = \boldsymbol{x}_t\right), \quad \boldsymbol{x}_t, \boldsymbol{x}'_t \in \mathcal{A}. \quad (1)$$

We use $\boldsymbol{p}_t$ to represent the user's location state at time t, where $\boldsymbol{p}_t[i] = \Pr(\boldsymbol{x}_t = \boldsymbol{a}_i) = \Pr(\boldsymbol{l}_t)$ represents the probability that the user's real location is in $\boldsymbol{a}_i$ at time t. Assuming that users are distributed with the same probability $\mathcal{A} = \{\boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_5, \boldsymbol{a}_7\}$, then the location probability distribution of users is $\boldsymbol{p}_t = [0, 0.25, 0.25, 0, 0.25, 0, 0.25, 0, \cdots, 0]$. We use $\boldsymbol{p}_t^-$ and $\boldsymbol{p}_t^+$ to represent the prior and posterior probabilities of the user before and after observing the released perturbed location $\boldsymbol{x}'_t$.

B. Attack Model

We consider the attacker to be an untrusted LBS server or an external attacker who may attack or corrupt the LBS
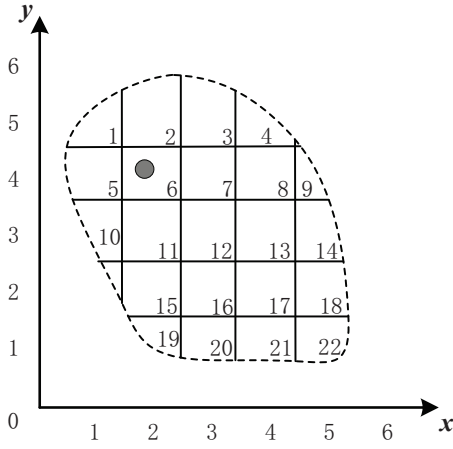
Fig. 2. User map coordinates and status coordinates.

server. They can access users' current location information for commercial profit or illegal purposes. We assume that the attacker knows the location perturbation probability distribution $f\left(x_t'|x_t\right)$, and can obtain the prior distribution $p_t^- = \Pr(x_t)$ of the user's current location through public tracking, check-in data set, or statistical information [16]. Then, the attacker can calculate the posterior probability distribution $p_t^+ = \Pr\left(x_t|x_t'\right)$ after observing the user's reported location x_t', i.e.,

$$p_t^+ = \Pr\left(x_t|x_t'\right) = \frac{\Pr(x_t) f\left(x_t'|x_t\right)}{\sum_{x_t \in \mathcal{A}} \Pr(x_t) f\left(x_t'|x_t\right)}. \quad (2)$$

A Bayesian adversary aims to infer the actual location at time t by minimizing the expected inference error against the posterior distribution. Therefore, the inferred location $\hat{x}_t$ is

$$\hat{x}_t = \arg\min_{\hat{x}_t \in \mathcal{A}} \sum_{x_t \in \mathcal{A}} \Pr\left(x_t|x_t'\right) d\left(\hat{x}_t, x_t\right). \quad (3)$$

We assume that the attacker can obtain the user's location transition probability matrix $\mathbf{M}$ based on the user's historical trajectory data and behavior habits [9]. Then, the attacker can infer the prior probability p_{t+1}^- of the user at time $t+1$, i.e.,

$$p_{t+1}^- = p_t^+ \mathbf{M}. \quad (4)$$

Since the posterior probability p_{t+1}^+ at time $t+1$ can be obtained according to (2), the attacker can perform an optimal inference attack on the user's location at time $t+1$ according to (3) to obtain the corresponding inferred location $\hat{x}_{t+1}$. Therefore, the attacker can obtain the inferred trajectory of the user in a certain period of time by performing the optimal inference attack on the user's location at each moment on the trajectory, thereby stealing the user's trajectory privacy.

III. Trajectory Privacy Protection Statement

In this section, we first list the main trajectory privacy notions and the condition for determining PLS, and then we present this paper's problem statement.

A. Location Transition Probability Matrix

Matrix $\mathbf{N}$ is the location transfer matrix, representing the number of times a user goes from one place to another. Let n_{ij} be an element in the ith row and jth column of matrix $\mathbf{N}$, and n_{ij} represents the number of times the user goes from region a_i to region a_j.

Through the location transition matrix $\mathbf{N}$, the location transition probability matrix $\mathbf{M}$ of the user can be analyzed. Let m_{ij} be an element in the ith row and the jth column of matrix $\mathbf{M}$, $m_{ij} = \dfrac{n_{ij}}{\sum_j n_{ij}}$ represents the probability of the user moving from a_i to a_j. The matrix $\mathbf{M}$ describes the temporal correlation of the user at different locations in a trajectory.

B. δ-Location Set

To protect locations frequently visited by users, δ-location set is proposed in [9], which represents the set of locations where the user is most likely to appear at time t, and we denote it as $\Delta\chi_t$.

$\Delta\chi_t$ denotes a set containing the minimum number of locations at time t with a prior probability sum not less than $1 - \delta$ ($0 < \delta < 1$).

$$\Delta\chi_t = \min\left\{a_i | \sum_{a_i} p_t^-[i] \geq 1 - \delta\right\}. \quad (5)$$

Note that since the δ-location set represents a set of possible locations with a high probability of the user appearing at time t, the real location x_t of the user may be eliminated with an extremely small probability. In this case, we substitute the closest location $\tilde{x}_t$ for the actual location x_t, given by

$$\tilde{x}_t = \arg\min_{\tilde{x}_t \in \Delta\chi_t} d\left(\tilde{x}_t, x_t\right). \quad (6)$$

If $x_t \in \Delta\chi_t$, then x_t is protected in $\Delta\chi_t$; if not, $\tilde{x}_t$ is protected in $\Delta\chi_t$.

C. Condition for Determining PLS

A two-phase dynamic differential location privacy framework PIVE was proposed in [8]. It studies the complementary relationship between geo-indistinguishability and distortion privacy and obtains the upper bound of posterior probability and lower bound of inference error through formula derivation. By combining these two privacy notions, PIVE introduces a user-defined inference error bound E_m to determine PLS.

First, to guarantee the expected inference error in terms of PLS, the conditional expected inference error is given by

$$ExpEr\left(x_t'\right) = \min_{\hat{x}_t \in \mathcal{A}} \sum_{x_t \in \mathcal{A}} \Pr\left(x_t|x_t'\right) d\left(\hat{x}_t, x_t\right). \quad (7)$$

Given that the adversary narrows possible guesses to the PLS Φ_t that contains the user's true location, we define

$$E\left(\Phi_t\right) = \min_{\hat{x}_t \in \mathcal{A}} \sum_{x_t \in \Phi_t} \frac{\Pr(x_t)}{\sum_{y_t \in \Phi_t} \Pr(y_t)} d\left(\hat{x}_t, x_t\right). \quad (8)$$

According to the lower bound on expected inference error,

$$ExpEr\left(\boldsymbol{x}_t^{'}\right) \geq e^{-\epsilon} E\left(\boldsymbol{\Phi}_t\right), \tag{9}$$

the authors in [8] (Theorem 1) obtain a sufficient condition,

$$E\left(\boldsymbol{\Phi}_t\right) \geq e^{\epsilon} E_m, \tag{10}$$

to satisfy the user-defined threshold, $\forall \boldsymbol{x}_t^{'}$, $ExpEr\left(\boldsymbol{x}_t^{'}\right) \geq E_m$.

D. Problem Statement

Considering the temporal correlation between locations on the trajectory, it is insufficient to protect only the user's current location, as attackers can still deduce the actual location by analyzing behavior patterns, geographical constraints, and other available information. Assuming the attacker possesses knowledge of the user's location transition probability matrix $\mathbf{M}$, they can calculate the prior probability of the user's current location based on previously published location information. To enhance the protection of the user's current location, we focus on protecting frequently visited locations with high prior probabilities [9].

Moreover, different types of LBS and varying contexts may impose different users' privacy requirements. Even for the same LBS, users may have various privacy needs for the same location at different times or in different locations. Therefore, we determine the possible location set $\boldsymbol{\Delta\chi}_t$ for each user at any given time based on the prior probability of locations along the trajectory. By combining the concepts of geo-indistinguishability and distortion privacy, we use a Hilbert-based minimum distance search algorithm to identify the set $\boldsymbol{\Phi}_t$ of possible locations in $\boldsymbol{\Delta\chi}_t$ at any location along the trajectory. We personalize user privacy by adjusting the privacy budget ϵ and the expected inference error threshold E_m. To enhance performance, we adapt the Permute-and-Flip mechanism, which was originally designed for data publishing scenarios, to serve as the location perturbation mechanism.

IV. PERSONALIZED TRAJECTORY PRIVACY PROTECTION MECHANISM

In this section, we propose a personalized trajectory privacy protection mechanism PTPPM, as shown in Fig. 3. Here, we consider the temporal correlation between different locations on the trajectory and combine geo-indistinguishability and distortion privacy to protect the user's personalized trajectory privacy. Specifically, we first use algorithm $\mathcal{F}_1$ to obtain the set of possible locations for the user at each time, leveraging the associated prior probability at each moment along the trajectory. Second, we employ algorithm $\mathcal{F}_2$ to dynamically select PLS for each possible location on the trajectory, incorporating both geo-indistinguishability and distortion privacy. Furthermore, our mechanism enables personalized trajectory privacy protection by adjusting different privacy settings (minimum inference error and privacy budget) for individual users. Finally, we put forth a novel Permute-and-Flip mechanism $\mathcal{K}$ to generate a perturbed location $\boldsymbol{x}_t^{'}$ for each location within
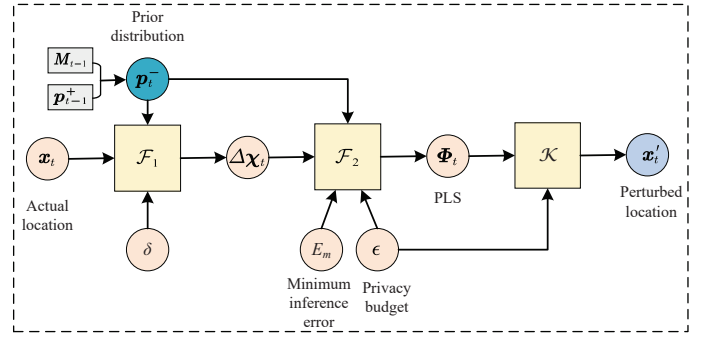

Fig. 3. The framework of PTPPM.

the PLS. These perturbed locations are selected with a smaller perturbation distance, ensuring a better QoS experience while providing robust and effective privacy protection.

A. Determine $\boldsymbol{\Delta\chi}_t$ at Continuous Times

The transition probability matrix $\mathbf{M}$ is constructed according to the user's historical trajectory data and behavior habits [9]. We eliminate all impossible locations ($\boldsymbol{p}_t^-$ is minimal or $\boldsymbol{p}_t^- = 0$) based on certain criteria to obtain the set of possible locations at time t, i.e., $\boldsymbol{\Delta\chi}_t$. If the actual location at time t is removed, we substitute it with $\tilde{x}_t$.

We calculate the posterior probability $\boldsymbol{p}_t^+$ according to (2) and then combine the location transition probability matrix $\mathbf{M}$ according to (4) to obtain the prior probability $\boldsymbol{p}_{t+1}^-$ at time $t+1$. In terms of $\boldsymbol{p}_{t+1}^-$, we get $\boldsymbol{\Delta\chi}_{t+1}$ at time $t+1$. We determine the size of $\boldsymbol{\Delta\chi}_{t+1}$ by setting the value of δ. Then, we obtain $\boldsymbol{\Delta\chi}_t$ at consecutive times by following the same process.

B. Determine Protection Location Set

After obtaining $\boldsymbol{\Delta\chi}_t$ for each time on the trajectory, we consider the protection of possible locations within $\boldsymbol{\Delta\chi}_t$ at any given time.

In order to improve the user's QoS, the smaller the diameter $D\left(\boldsymbol{\Phi}_t\right)$ of the circular area, the better. Since $D\left(\boldsymbol{\Phi}_t\right)$ is the diameter of the $\boldsymbol{\Phi}_t$, the distance between any two locations is less than or equal to $D\left(\boldsymbol{\Phi}_t\right)$. For $\forall \boldsymbol{x}_t, \hat{\boldsymbol{x}}_t$ in $\boldsymbol{\Phi}_t$, we have $D\left(\boldsymbol{\Phi}_t\right) \geq d\left(\boldsymbol{x}_t, \hat{\boldsymbol{x}}_t\right)$. By (10), we have

$$e^{\epsilon} E_m \leq E\left(\boldsymbol{\Phi}_t\right) \leq \min_{\hat{\boldsymbol{x}}_t \in \boldsymbol{\Phi}_t} \sum_{\boldsymbol{x}_t \in \boldsymbol{\Phi}_t} \frac{\Pr\left(\boldsymbol{x}_t\right)}{\sum_{\boldsymbol{y}_t \in \boldsymbol{\Phi}_t} \Pr\left(\boldsymbol{y}_t\right)} D\left(\boldsymbol{\Phi}_t\right) = D\left(\boldsymbol{\Phi}_t\right). \tag{11}$$

To effectively find the PLS with the smallest diameter at time t, the search method based on the Hilbert curve in [8] is adopted. For each possible location $\boldsymbol{x}_t$ in $\boldsymbol{\Delta\chi}_t$ on the trajectory, we search the neighborhood of $\boldsymbol{x}_t$ according to the search direction of the Hilbert curve. We identify the PLS for $\boldsymbol{x}_t$ that satisfies (10) and select the one with the smallest diameter as the PLS $\boldsymbol{\Phi}_t$.

On this basis, to prevent the single-direction search of the Hilbert curve might lead to an unreasonable protection area with a large diameter, we perform spatial rotation of the Hilbert curve to improve the opportunity of finding a

PLS for each location $\boldsymbol{x}_t$ with a smaller diameter. More specifically, similar to [8] we rotate 90, 180, and 270 degrees clockwise around the center point to generate three more Hilbert curves. After rotation, search for PLS where the user's location is under different Hilbert curves. Then, the group with the smallest diameter is selected from the four results as the PLS.

C. Differentially Private Mechanism in Protection Location Set

We put forth a new perturbation mechanism, Permute-and-Flip, to release the perturbed location with a smaller perturbation distance, which can better balance location privacy and QoS. The Permute-and-Flip mechanism was initially developed to protect privacy in the data publishing process [14]. We apply this mechanism for the first time to protect the location in the PLS $\boldsymbol{\Phi}_t$ through the mapping relationship between the utility function and the Euclidean distance. The Permute-and-Flip mechanism always selects the query option with the highest score when processing query options. Therefore, we take the difference between its distance and the maximum distance as a query function and define the sensitivity of the utility function as

$$\Delta u = \max_{\boldsymbol{x}_t' \in \mathcal{A}, \boldsymbol{x}_t, \boldsymbol{y}_t \in \boldsymbol{\Phi}_t} \left| d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right) - d\left(\boldsymbol{y}_t, \boldsymbol{x}_t'\right) \right|, \quad (12)$$

according to the triangle inequality, we have $\left| d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right) - d\left(\boldsymbol{y}_t, \boldsymbol{x}_t'\right) \right| \le d\left(\boldsymbol{x}_t, \boldsymbol{y}_t\right) \le D\left(\boldsymbol{\Phi}_t\right)$.

After obtaining $\Delta \boldsymbol{\chi}_t$ for each location on the trajectory, we can find the corresponding $\boldsymbol{\Phi}_t$ for each possible location in $\Delta \boldsymbol{\chi}_t$ using (10). Given the current location $\boldsymbol{x}_t$ and the PLS $\boldsymbol{\Phi}_t$, the probability of the output perturbed location $\boldsymbol{x}_t'$ is proportional to $\exp\left(\frac{-\epsilon(u(D,r) - \max(u(D,r)))}{2\Delta u}\right)$ according to the Permute-and-Flip mechanism. We have the perturbed locations' probability distribution

$$f\left(\boldsymbol{x}_t'|\boldsymbol{x}_t\right) = \omega_x \exp\left(\frac{-\epsilon\left(d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right) - \max d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right)\right)}{2D\left(\boldsymbol{\Phi}_t\right)}\right), \quad (13)$$

where ω_x is the probability distribution normalization factor, i.e.,

$$\omega_x = \left(\sum_{\boldsymbol{x}_t' \in \mathcal{A}} \exp\left(\frac{-\epsilon\left(d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right) - \max d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right)\right)}{2D\left(\Phi_t\right)}\right)\right)^{-1}. \quad (14)$$

V. SIMULATION RESULTS

In this section, we evaluate the effectiveness of our proposed PTPPM. We compare the trajectory privacy performance of PTPPM with that of PIVE [8] under the same QoS loss. To facilitate evaluation, we divide the 50 km × 50 km two-dimensional space evenly into 100 units, and each unit has the same area. These units serve as areas that VANET users may access, also known as the attacker's prior distribution. Each unit represents the location status of the user and has corresponding two-dimensional coordinates. We select 5 of them as the real locations of 5 consecutive moments on the user's trajectory, as depicted in Fig. 4.
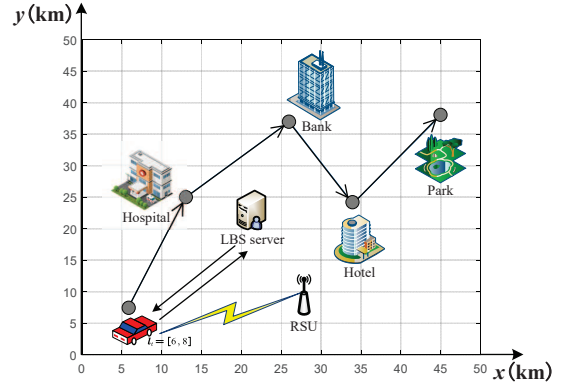

Fig. 4. Simulation setting of the trajectory of a user.

The location privacy p and QoS loss q are evaluated by the similar metrics in our previous work [5] which are given by

$$p = \sum_{\boldsymbol{x}_t, \boldsymbol{x}_t', \hat{\boldsymbol{x}}_t \in \mathcal{A}} \Pr\left(\boldsymbol{x}_t\right) f\left(\boldsymbol{x}_t'|\boldsymbol{x}_t\right) h\left(\hat{\boldsymbol{x}}_t|\boldsymbol{x}_t'\right) d\left(\boldsymbol{x}_t, \hat{\boldsymbol{x}}_t\right), \quad (15)$$

$$q = \sum_{\boldsymbol{x}_t, \boldsymbol{x}_t' \in \mathcal{A}} \Pr\left(\boldsymbol{x}_t\right) f\left(\boldsymbol{x}_t'|\boldsymbol{x}_t\right) d\left(\boldsymbol{x}_t, \boldsymbol{x}_t'\right). \quad (16)$$

First, we set different privacy budgets ϵ and inference error threshold E_m to evaluate their impact on users' personalized trajectory privacy protection performance in Figs. 5. We can see that two privacy parameters (ϵ and E_m) have a significant impact on trajectory privacy and QoS loss. More specifically, as shown in Figs. 5(a) and **??**, when ϵ is small, the trajectory privacy and QoS loss decrease with increased ϵ under different E_m. Besides, when ϵ is larger than a specific value, the trajectory privacy and QoS loss start to increase. That is because, according to (10), the increase of ϵ will cause $D\left(\boldsymbol{\Phi}_t\right)$ to sharply increase. The turning points under different E_m settings are different. Moreover, because $D\left(\boldsymbol{\Phi}_t\right)$ cannot be increased indefinitely in practical scenarios, the location privacy and QoS loss finally reach the upper limit value. Figs. 5(b) and 5(d) show that the trajectory privacy, QoS loss, and trajectory error increase with the increase of E_m under different ϵ. Given a ϵ, when E_m increases, the $D\left(\boldsymbol{\Phi}_t\right)$ of the protected area increases, thus increasing the trajectory privacy and QoS loss. Moreover, the effect of ϵ on $D\left(\boldsymbol{\Phi}_t\right)$ is exponential, much higher than that of E_m. Therefore, when ϵ is set to 1.5, with the increase of E_m, $D\left(\boldsymbol{\Phi}_t\right)$ changes significantly, so the trajectory privacy and QoS loss increase sharply, resulting in a steep curve. However, there is a limitation on the $D\left(\boldsymbol{\Phi}_t\right)$ of the protected area, so the trajectory privacy and QoS loss will converge to a finite value. We can see that the user's trajectory privacy and QoS loss reach the upper limit when ϵ is 0.1, regardless of the E_m setting. By adjusting different privacy settings, personalized trajectory privacy protection is realized.

Next, we quantitatively compare PF with PIVE in terms of trajectory privacy and QoS loss to verify its advantages. We set (16) equal to the set QoS loss value, and the only variable in
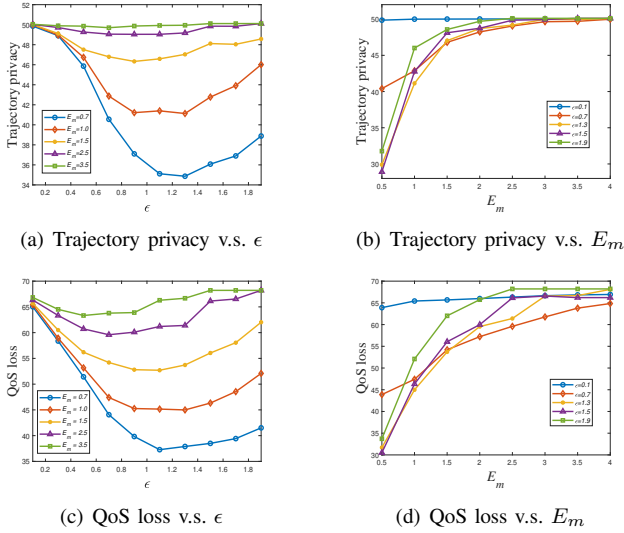
(a) Trajectory privacy v.s. ϵ (b) Trajectory privacy v.s. E_m

(c) QoS loss v.s. ϵ (d) QoS loss v.s. E_m

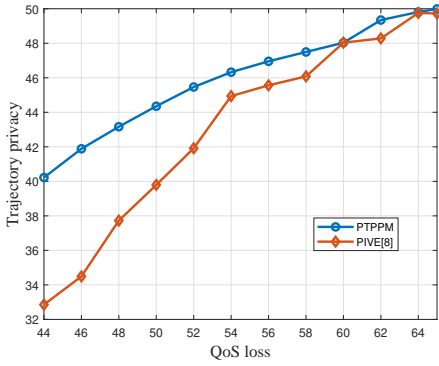Fig. 5. Impact of ϵ and E_m on personalized trajectory privacy protection.

Fig. 6. Performance of different LPPMs under different QoS loss.

this equation is the privacy budget ϵ. By solving this equation, ϵ corresponding to PF and PIVE can be obtained under the same QoS loss. By substituting (15), the corresponding privacy of PF and PIVE under the same QoS loss can be calculated. As shown in Fig. 6, we can see that PF can better protect privacy under the same QoS loss. For example, when QoS loss = 44, the privacy value of PTPPM is 22.4% which is higher than that of PIVE. That is because the proposed Permute-and-Flip mechanism provides a smaller perturbation distance while guaranteeing privacy demands in PLS. In addition, since $D(\Phi_t)$ cannot be infinitely enlarged in the actual scenario, privacy eventually reaches the upper limit. We can see that the proposed mechanism can better protect user privacy while meeting users' QoS requirements.

VI. CONCLUSION

In this paper, we have proposed a personalized trajectory privacy protection mechanism PTPPM. This paper has three novel contributions: First, we address the issue of attackers exploiting the temporal correlation between different locations

to compromise user privacy. To mitigate this threat, we design a robust trajectory privacy protection mechanism. Second, we combined the privacy notions of geo-indistinguishability and distortion privacy, enabling personalized privacy protection by adjusting the privacy budget and the expected inference error threshold to meet individual user needs. Third, we proposed a novel perturbation mechanism, Permute-and-Flip, which releases perturbed locations with smaller perturbation distances to better balance the trajectory privacy and QoS. Simulation results show that PTPPM offers improved privacy protection under the same QoS loss compared to PIVE. For instance, when QoS loss = 44, the privacy of PTPPM is 22.4% higher than that of PIVE.

REFERENCES

[1] N. U. Saqib, S. U. R. Malik, A. Anjum, M. H. Syed, S. A. Moqurrab, G. Srivastava, and J. C.-W. Lin, "Preserving privacy in the internet of vehicles IoV: A novel group leader-based shadowing scheme using blockchain," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21421–21430, Jul. 2023.

[2] W. Wang, M. Min, L. Xiao, Y. Chen, and H. Dai, "Protecting semantic trajectory privacy for vanet with reinforcement learning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019.

[3] M. Min, W. Wang, L. Xiao, Y. Xiao, and Z. Han, "Reinforcement learning-based sensitive semantic location privacy protection for VANETs," *China Commun.*, vol. 18, no. 6, pp. 244–260, Jun. 2021.

[4] J. Tang, H. Zhu, R. Lu, X. Lin, H. Li, and F. Wang, "DLP: Achieve customizable location privacy with deceptive dummy techniques in LBS applications," *IEEE Internet Things J.*, vol. 9, no. 9, pp. 6969–6984, Sep. 2021.

[5] M. Min, L. Xiao, J. Ding, H. Zhang, S. Li, M. Pan, and Z. Han, "3D geo-indistinguishability for indoor location-based services," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 7, pp. 4682–4694, Dec. 2021.

[6] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. & Commun. Secur.*, Berlin, Germany, Nov. 2013.

[7] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: optimal strategy against localization attacks," in *Proc. ACM Conf. Comput. Commun. Secur.*, Raleigh North, Carolina, Oct. 2012.

[8] L. Yu, L. Liu, and C. Pu, "Dynamic differential location privacy with personalized error bounds.," in *Proc. 24th Annu. Netw. Distributed Syst. Secur. Symp. (NDSS)*, San Diego, CA, Feb. 2017.

[9] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Denver, CO, Oct. 2015.

[10] L. Xing, X. Jia, J. Gao, and H. Wu, "A location privacy protection algorithm based on double k-anonymity in the social internet of vehicles," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3199–3203, Oct. 2021.

[11] F. Jin, W. Hua, M. Francia, P. Chao, M. Orlowska, and X. Zhou, "A survey and experimental study on privacy-preserving trajectory data publishing," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 6, pp. 5577–5596, May 2022.

[12] L. Wu, C. Qin, Z. Xu, Y. Guan, and R. Lu, "TCPP: Achieving privacy-preserving trajectory correlation with differential privacy," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 4006–4020, Jun. 2023.

[13] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *Proc. IEEE Symp. Secur. Priv.*, Oakland, CA, May 2011.

[14] R. McKenna and D. R. Sheldon, "Permute-and-Flip: A new mechanism for differentially private selection," *Adv. Neural. Inf. Process. Syst.*, vol. 33, pp. 193–203, Oct. 2020.

[15] S. Zeng, H. Zhang, B. Di, Z. Han, and L. Song, "Reconfigurable intelligent surface (RIS) assisted wireless coverage extension: RIS orientation and location optimization," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 269–273, Sep. 2021.

[16] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Constructing elastic distinguishability metrics for location privacy," *Proc. Priv. Enhanc. Technol.*, vol. 2015, no. 2, pp. 156–170, May 2015.