Personalized 3D Spatiotemporal Trajectory Privacy Protection with Differential and Distortion Geo-Perturbation

Minghui Min, *Member, IEEE*, Yulu Li, Gang Li, Meng Li, *Senior Member, IEEE*, Hongliang Zhang, *Member, IEEE*, Miao Pan, *Senior Member, IEEE*, Dusit Niyato, *Fellow, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—The rapid advancement of location-based services (LBSs) in three-dimensional (3D) domains, such as smart cities and intelligent transportation, has raised concerns over 3D spatiotemporal trajectory privacy protection. However, existing research has not fully addressed the risk of attackers exploiting the spatiotemporal correlation of 3D spatiotemporal trajectories and the impact of height information, both of which can potentially lead to significant privacy leakage. To address these issues, this paper proposes a personalized 3D spatiotemporal trajectory privacy protection mechanism, named 3DSTPM. First, we analyze the characteristics of attackers that exploit spatiotemporal correlations between locations in a trajectory and present the attack model. Next, we exploit the complementary characteristics of 3D geo-indistinguishability (3D-GI) and distortion privacy to find a protection location set (PLS) that obscures the real location for all possible locations. To address the issue of privacy accumulation caused by continuous trajectory queries, we propose a Window-based Adaptive Privacy Budget Allocation (W-APBA), which dynamically allocates privacy budgets to all locations in the current PLS based on their predictability and sensitivity. Finally, we perturb the real location using the allocated privacy budget by the PF (Permute-and-Flip) mechanism, effectively balancing privacy protection and Quality of Service (QoS). Simulation results demonstrate that the proposed 3DSTPM effectively reduces QoS loss while meeting the user's personalized privacy protection needs.**

Corresponding author: Minghui Min.

Minghui Min, Yulu Li, and Gang Li are with the School of Information and Control Engineering, China University of Mining and Technology, Xuzhou 221116, China (email: minmh@cumt.edu.cn; liyulu@cumt.edu.cn; ligang@cumt.edu.cn).

Meng Li is with the Key Laboratory of Knowledge Engineering with Big Data, Ministry of Education, Hefei University of Technology, Hefei 230009, China, also with the School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230009, China, also with the Anhui Province Key Laboratory of Industry Safety and Emergency Technology, Hefei 230601, China, also with the Intelligent Interconnected Systems Laboratory of Anhui Province (Hefei University of Technology), Hefei 230009, China, and also with the Department of Mathematics and HIT Center, University of Padua, Padua 35122, Italy (email: mengli@hfut.edu.cn).

Hongliang Zhang is with the School of Electronics, Peking University, Beijing 100871, China (email: hongliang.zhang92@gmail.com).

Miao Pan is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004, USA (email: miaopan.ufl@gmail.com).

Dusit Niyato is with the College of Computing and Data Science, Nanyang Technological University, Singapore (email: dniyato@ntu.edu.sg).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004, USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-70, South Korea (email: hanzhu22@gmail.com).

***Index Terms*—Location-based service, 3D space, spatiotemporal trajectory, trajectory privacy protection, differential privacy.**

I. Introduction

THE application of spatiotemporal trajectory data in 3D spaces has become increasingly widespread, particularly in areas such as smart cities [1], [2], traffic management, and low-altitude logistics [3], [4]. Users perform continuous location-based queries on trajectories to obtain location-based services (LBS) [5]. However, this querying process exposes a large amount of user data, including sensitive information such as health status, personally identifiable information, and other private details [6], [7]. If mishandled or exposed, it can pose significant risks to users' personal privacy [8].

There is a significant spatiotemporal correlation between different locations in spatiotemporal trajectory. Attackers with knowledge of these correlations can leverage this information to deeply analyze users' behavior patterns and activity regularities, thereby making more accurate predictions of users' real trajectories [9]. For example, in a smart city scenario, if a student takes an autonomous taxi to school at 8 a.m., an attacker with knowledge of spatiotemporal correlations could, by combining this with the user's historical behavioral data, infer that the taxi is likely to head towards the school in the subsequent time period, rather than the nearby bank. Such inferences may lead to serious privacy leakage, potentially exposing the student's daily routines and personal habits. Furthermore, as users perform continuous location-based queries, more trajectory data is incrementally exposed, this allows attackers to accumulate additional information, further enhancing their predictive capabilities and significantly amplifying the associated privacy risks [10]. Therefore, to effectively mitigate privacy leakage risks and protect users' trajectory privacy, it is essential to fully account for spatiotemporal correlations and limit the cumulative privacy leakage caused by continuous queries.

Moreover, compared to 2D trajectory data, 3D spatiotemporal trajectory data is larger in scale, higher in dimensionality, and contains richer semantic information. This complexity leads to significant variations in the sensitivity of different locations. In addition, the sensitivity of a given location may

dynamically change over time due to contextual or behavioral dynamics, causing users' privacy protection needs to vary even for the same location at different times [11]–[13]. Applying a uniform protection level to all locations may result in insufficient protection for high-sensitivity locations and excessive protection for low-sensitivity locations [14], [15]. Hence, it is essential to provide personalized privacy protection measures for different locations on 3D spatiotemporal trajectory based on users' specific privacy protection needs.

The PIM mechanism was proposed in [16] to protect trajectory privacy, considering the temporal correlation between locations in the trajectory. However, it does not fully account for the correlations between trajectory locations, overlooking spatial factors such as geospatial constraints, and applying a uniform protection level to all locations, which does not meet users' individualized privacy needs. To overcome these shortcomings, a spatiotemporal personalized trajectory privacy protection mechanism PTPPM was proposed in [17], which more comprehensively considers the spatiotemporal correlations between trajectory locations and provides varying levels of protection based on users' specific privacy requirements. Nevertheless, PTPPM overlooks the issue of cumulative privacy leakage caused by continuous queries along the trajectory, nor does it account for the potential variation in location sensitivity over time. Furthermore, the above mechanism is designed for 2D space and it is difficult to handle 3D spatiotemporal trajectory data that incorporates height information. Once attackers gain access to the height information of the trajectory, the risk of privacy leakage increases [18]–[20].

In 3D space, existing related mechanisms mainly focus on protecting individual location points, overlooking the spatiotemporal correlations between locations in a trajectory. Inspired by the concept of differential privacy [21], 3D geo-indistinguishability (3D-GI) was developed in [22], providing a rigorous method to quantify location privacy in 3D space, laying the foundation for 3D location privacy protection mechanisms. Building upon this, the complementary characteristics of 3D-GI and distorted privacy were analyzed, and a personalized location privacy protection mechanism, P3DLPPM, was proposed in [23], which enhances the robustness of the mechanism while meeting users' individualized needs. However, this mechanism is ineffective against attackers who exploit spatiotemporal correlations, directly applying it to trajectory privacy protection could lead to significant privacy leakage. Therefore, providing personalized privacy protection for 3D spatiotemporal trajectory remains an urgent challenge that needs to be addressed.

In this paper, we propose a personalized 3D spatiotemporal trajectory privacy protection mechanism, named 3DSTPM, to protect the user's trajectory privacy in 3D space. To achieve this, we generate a transfer probability matrix based on the user's historical behavior and data, quantifying the spatiotemporal correlation between trajectory locations, thereby resisting attackers who can analyze spatiotemporal characteristics. Furthermore, we combine the complementary properties of 3D-GI [22] and distortion privacy (i.e., expected inference error) [24]. 3D-GI can limit the posterior information obtained by an attacker, but cannot completely defend against an attacker with prior knowledge, while distortion privacy ensures that the attacker's inference error remains above the threshold, but does not limit the exposure of a posteriori information. By combining the two, we improve the robustness of our mechanisms against attackers with knowledge of spatiotemporal information, while meeting the individual needs of our users. In addition, we dynamically adjust the privacy budget according to the user's personalized needs, and provide corresponding privacy protection for locations with different sensitivities, enabling more flexible privacy protection tailored to user-specific contexts.

The sliding window mechanism can effectively group continuous queries within a specified time interval [10], thereby limiting cumulative privacy leakage. Building upon this, we introduce the Window-based Adaptive Privacy Budget Allocation (W-APBA) algorithm to mitigate privacy leakage from continuous queries in 3D space. Specifically, the algorithm dynamically allocates privacy budgets to different locations based on their sensitivity at various times, meeting users' fluctuating privacy protection needs. Additionally, the sliding window mechanism constrains the total privacy budget within each window, further reducing cumulative leakage from consecutive queries along the trajectory.

Furthermore, building upon the PF (Permute-and-Flip) mechanism proposed in our previous work [23], we perturb the real locations at different timestamps along the trajectory. Additionally, we theoretically demonstrate that the distance between the real and perturbed locations generated by the PF mechanism is constrained by a controllable upper bound. This enhancement further strengthens the theoretical foundation of the PF mechanism in balancing user privacy protection requirements with QoS. Simulation results demonstrate that 3DSTPM provides personalized trajectory privacy protection, and offers superior privacy protection compared to P3DLPPM [23], 2DPTPPM [17] and 3DPIM. The main contributions of our work include:

- We propose a personalized 3D spatiotemporal trajectory privacy protection mechanism, named 3DSTPM, to protect users' trajectory privacy in 3D space. This mechanism effectively tackles the challenges posed by the high dimensionality of 3D space, expanding its applicability. Besides, it considers the spatiotemporal correlations between locations on the trajectory, and integrates the complementary characteristics of 3D-GI and distorted privacy, enhancing the overall robustness of the protection.
- We propose a W-APBA algorithm to meet the user's dynamically changing privacy protection needs. Specifically, the algorithm adapts to temporal variations in location sensitivity, thereby enabling more flexible privacy protection. It also incorporates a sliding window mechanism to limit the cumulative privacy leakage caused by continuous queries, ensuring robust privacy protection. Based on the allocated privacy budget, the perturbed

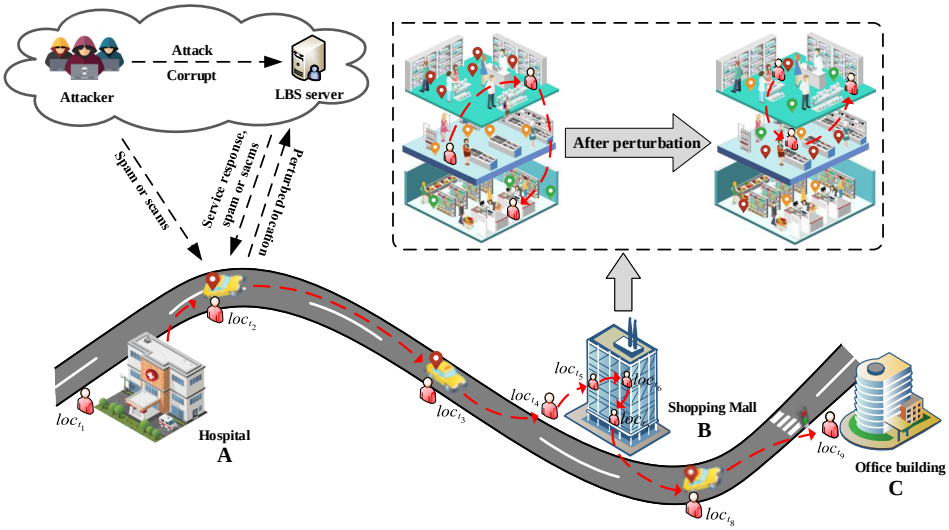


Fig. 1. Illustration of 3D spatiotemporal trajectory privacy protection, the user moves between three large buildings and requests LBS services in both indoor and outdoor scenarios. To prevent attackers from obtaining the user's personal information from the obtained trajectory data, the user uploads perturbed locations to the LBS server to obtain the corresponding service.

location is generated using the PF mechanism, effectively balancing privacy protection and QoS.

- We conduct simulations to study the effects of key privacy parameters, including privacy budget, expected inference error bound, and window size, on trajectory privacy and QoS loss. In addition, we compare and analyze the overall performance of 3DSTPM against benchmarks to demonstrate the advantage of our proposed mechanism.

The remainder of this paper is organized as follows. Section II reviews the related work. Section III presents the system model and we present the trajectory privacy protection statement in Section IV. A 3DSTPM framework is proposed in Section V. The evaluation results are provided in Section VI. Finally, we conclude this work in Section VII.

II. Related Work

Existing research on privacy protection in 3D space primarily focuses on individual location protection [25]–[28], such as anonymity [29], location perturbation [30], and generalization [31]. A mechanism based on anonymity, 3D Clique Cloak, was proposed in [32], to safeguard users' location privacy in 3D space. Nonetheless, such k-anonymity-based privacy protection mechanisms [33] rely heavily on trusted third parties, which introduce potential privacy leakage in the event of server failures or malicious attacks. To address this limitation, a 3D spatial personalized location privacy protection mechanism based on differential privacy, P3DLPPM, was proposed in [23], integrating the complementary characteristics of 3D-GI and distortion privacy to enhance the mechanism's robustness. However, these methods were designed specifically for location privacy protection and overlook spatiotemporal correlations between different locations. When directly applied to trajectory privacy protection, they cannot defend against attackers who exploit such correlations, increasing the risk of privacy leakage.

Spatiotemporal trajectory exhibits spatiotemporal correlations between locations, possibly exposing users' behavioral patterns. Once attackers exploit these correlations, they can accurately infer sensitive personal information [9], [34]. A PIM mechanism was proposed in [16] to protect trajectory privacy, considering the temporal correlations between locations on the trajectory. It hides the real location within a set of possible locations filtered based on prior knowledge, thereby reducing the accuracy of attackers' inferences. Nonetheless, this mechanism overlooks the spatial correlations between locations on the trajectory. On this basis, the concept of spatiotemporal event privacy was introduced in [35], which considers both temporal and spatial correlations between locations on the trajectory simultaneously and provides a quantifiable privacy metric. However, the above mechanisms do not consider the height information of the trajectory and are only suitable for 2D space. If directly applied to 3D spatiotemporal trajectory privacy protection, they will be unable to effectively defend against attackers who possess height information, leading to significant privacy leakage risks.

The sensitivity of different locations on a trajectory varies, and even the sensitivity of the same location may change over time. Applying uniform protection across all locations on the trajectory can not address personalized privacy protection needs of users [17], [36]. By incorporating the temporal correlation of locations, personalized privacy protection for different locations on the trajectory based on user needs is provided in [17]. However, this mechanism only analyzes the impact of privacy parameters on the degree of personalized privacy protection using simplified models, without fully accounting for the factors that influence trajectory sensitivity. To address its limitations, a false location generation mechanism

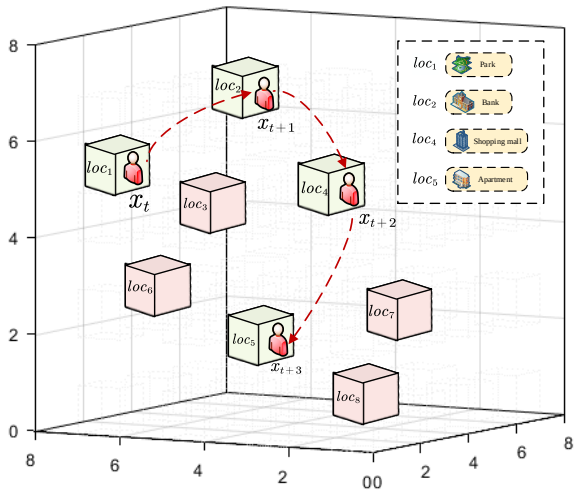


Fig. 2. User 3D spatiotemporal trajectory coordinate mapping and coordinate status.

TABLE I: List of Notations.

Symbol	Description
$\mathcal{A}$	User map
$D(\Phi_t)$	Diameter of Φ_t
E_m	Expected inference error bound
loc_i	Location i
$LS_{i,t}$	Location sensitivity of loc_i at time t
$LP_{i,t}$	Location predictability of loc_i at time t
$\mathbf{M}$	Location transition probability matrix
$\mathbf{p}_t^-/\mathbf{p}_t^+$	prior/posterior probability at time t
w	Size of sliding window
$\boldsymbol{x}_t/\boldsymbol{x}_t^{'}/\hat{\boldsymbol{x}}_t$	Real/perturbed/inferred location at time t
ϵ_w	Total privacy budget of sliding window
δ	Probability thresholds, $0 < \delta < 1$
$\Delta\chi_t$	Possible location set at time t
Φ_t	Protection location set (PLS) at time t

based on a semantic tree was proposed in [36] for personalized privacy protection, comprehensively considering the factors influencing location sensitivity. However, this mechanism does not account for the fact that the sensitivity of different locations on the trajectory may change over time, making it unable to adapt to the evolving privacy protection needs of users.

III. System Model

We consider an LBS system that consists of mobile users equipped with location enabled devices in 3D space (including both outdoor scenarios and indoor buildings), and an untrusted LBS server, as shown in Fig. 1. For outdoor scenarios, users share their location data with the LBS server to obtain services, such as vehicle users' navigation for live traffic information. For indoor scenarios, users can access LBS in high-rise indoor buildings for indoor navigation. Fig. 1 depicts the user's movement trajectory, with points A, B, and C representing three large buildings. The differently colored markers represent the potential locations of users across various floors in a building. Each floor offers distinct services and experiences tailored to the user's needs, similar to that in [23]. The user, travelling by vehicle from one building to another, generates trajectory points denoted as $loc_{t_1}, loc_{t_2}, \ldots, loc_{t_9}$. Attackers may corrupt untrusted LBS servers to infer the user's personal information from the obtained trajectory data, risking spam or fraud. To protect users' trajectory privacy, the user uploads perturbed locations, thereby reducing the risk of exposure to their actual trajectory. Important symbols are summarized in Table I.

A. User Model

We represent the user's trajectory in 3D space as $Tr =< \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t, \ldots, \boldsymbol{x}_T >$, where $\boldsymbol{x}_t$ denotes the user's 3D location at time t, and T indicates the total length of the trajectory. The space encompassing all locations along the user's trajectory is divided into multiple subspaces, each corresponding to a unique 3D coordinate that represents a possible user location. The set of all possible locations of the user within the region is denoted as $\mathcal{A}$, where $\mathcal{A} = \{loc_1, loc_2, \ldots, loc_N\}$, N represents the total number of locations. As shown in Fig. 2, $\mathcal{A} = \{loc_1, loc_2, \ldots, loc_9\}$, and the user's location at time t is given by $\boldsymbol{x}_t = loc_1 = [2, 6, 5]$.

To protect privacy, the user applies a location perturbation mechanism, which transforms the actual location $\boldsymbol{x}_t$ from the original location set O_1 into a fake location $\boldsymbol{x}_t^{'}$ drawn from the perturbed location set O_2. The probability distribution for location perturbation, denoted as f, 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 define $\mathbf{p}_t$ as the user's location state at time t, and $\mathbf{p}_t[i] = \Pr(\boldsymbol{x}_t = loc_i)$, where $\boldsymbol{x}_t$ is the real location of the user at time t, loc_i is the i_{th} location of all possible locations of the user, $\mathbf{p}_t[i]$ is the probability that the user is located loc_i at time t. Assuming that the user has an equal probability of being at any given location, the set of locations $\mathcal{A} = \{loc_1, loc_2, loc_6, loc_8\}$, and the probability distribution of user locations is given by $\mathbf{p}_t = [0.25, 0.25, 0, 0, 0, 0.25, 0, 0.25, \cdots, 0]$. The prior and posterior probabilities of the user, denoted as $\mathbf{p}_t^-$ and $\mathbf{p}_t^+$, represent the probabilities before and after observing the released perturbed location $\boldsymbol{x}_t^{'}$, respectively.

B. Attack Model

Attackers can be either untrusted LBS servers or external entities attempting to compromise or attack local service system servers. We assume that attackers possess knowledge of spatiotemporal correlations [17]. In addition to the prior probability distribution of user locations $\mathbf{p}_t^-$, and the probability distribution of perturbed locations $f(\boldsymbol{x}_t'|\boldsymbol{x}_t)$, which are typically known to traditional attackers, they can also derive the user's location transition probability matrix $\mathbf{M}$ based on their historical behavior [16]. By leveraging this additional

information, attackers can significantly enhance their ability to infer the user's real trajectory. The specific process by which attackers infer the user's real trajectory is as follows:

After observing the perturbed location posted by the user, the attacker can compute the posterior probability distribution based on the existing prior knowledge, i.e:

$$\mathbf{p}_t^+ = \Pr\left(\boldsymbol{x}_t|\boldsymbol{x}_t'\right) = \frac{\Pr\left(\boldsymbol{x}_t\right) f\left(\boldsymbol{x}_t'|\boldsymbol{x}_t\right)}{\sum_{\boldsymbol{x}_t\in\mathcal{A}} \Pr\left(\boldsymbol{x}_t\right) f\left(\boldsymbol{x}_t'|\boldsymbol{x}_t\right)}. \tag{2}$$

A Bayesian attacker can employ an optimal inference attack, i.e., inferring the real location by minimizing the expected inference error of the posterior distribution that depends on the perturbed location [24]. Thus, the inferred location can be expressed as

$$\hat{\boldsymbol{x}}_t = \arg\min_{\hat{\boldsymbol{x}}_t\in\mathcal{A}} \sum_{\boldsymbol{x}_t\in\mathcal{A}} \Pr\left(\boldsymbol{x}_t|\boldsymbol{x}_t^{'}\right) d_3\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right), \tag{3}$$

where $d_3\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right)$ denotes the Euclidean distance between the attacker's inferred location and the user's real location in 3D space at time t.

The prior knowledge of an attacker who has knowledge of the spatiotemporal correlation between different locations on the user's trajectory is not static, and it can be constantly updated with the prior distribution probability of the user's location at the next time as

$$\mathbf{p}_{t+1}^- = \mathbf{p}_t^+\mathbf{M}. \tag{4}$$

The attacker updates the prior probability to compute the posterior probability for the next time step and derives the inferred location at time $t+1$ according to (4). By iteratively performing optimal inference on the user's location at each time step, the attacker can reconstruct the user's entire trajectory, thereby compromising their trajectory information.

IV. Trajectory Privacy Notions and Problem Statement

In this section, we first list the trajectory features and mainly used trajectory privacy notions. Then, we present this paper's problem statement.

A. 3D Spatiotemporal Trajectory

The 3D spatiotemporal trajectory extends the traditional 2D trajectory model by incorporating additional height dimension, such as altitude or floor level, to more precisely represent a user's movement patterns over both space and time. Here, we provide the definition of a 3D spatiotemporal trajectory.

Definition 1. (3D Spatiotemporal Trajectory) *A 3D spatiotemporal trajectory is defined as an ordered sequence of points that represent the movement of an object within a specific time interval in 3D space. It can be mathematically expressed as*

$$Tr = < \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t, \ldots, \boldsymbol{x}_T >, \tag{5}$$

where $\boldsymbol{x}_t$ denotes the user's 3D location at time t, and T represents the total length of trajectory. Consequently, the trajectory Tr can also be formulated as

$$Tr = \{\boldsymbol{x}_t \mid t \in \{1, 2, \ldots, T\}\}. \tag{6}$$

The locations at adjacent moments in the trajectory are spatially and temporally correlated [10], [37]. Specifically, the likelihood of a user appearing at a particular location at time t is influenced by the location at the previous time step, and, in turn, affects the probability of the user being at a specific location at $t+1$. Moreover, two locations that are not geographically accessible to each other cannot appear consecutively at adjacent time steps. This limitation arises from the inherent spatial constraints, which restrict the feasibility of transitions between locations.

B. Location Transition Probability Matrix

The location transition probability matrix $\mathbf{M}$ represents the probability of a user transferring between two locations, which we assume that it remains constant over time. The element in the ith row and jth column of matrix $\mathbf{M}$ is m_{ij}, and $m_{ij} = \frac{n_{ij}}{\sum_j n_{ij}}$, where m_{ij} denotes the probability of a user transferring from loc_i to loc_i, n_{ij} is an element in the location transfer matrix $\mathbf{N}$, which denotes the number of times the user has traveled from loc_i to loc_j.

The matrix $\mathbf{M}$ can reflect the spatiotemporal correlation between the locations on the trajectory, and the prior probability distribution $\mathbf{p}_t^-$ of the user at time t can be computed from the posterior probability distribution $\mathbf{p}_{t-1}^+$ at time $t-1$ and the matrix $\mathbf{M}$. Moreover, when the two locations are not geographically spatially reachable $m_{ij} = 0$.

C. Differential Geo-Perturbation in 3D Space

3D geo-indistinguishability (3D-GI) is a privacy concept proposed in [22], which extends geo-indistinguishability to 3D space. It ensures that the perturbed locations generated for any two locations within a sphere of radius r have similar probability distributions, making it geographically indistinguishable to an attacker for all locations within it. In the sequel, we define the sphere as a protected area, and all locations within it constitute protected location sets (PLS). Expanding on this notion, we enhance the initial 3D-GI, originally tailored for singular locations, to encompass trajectories spanning multiple timestamps. Next, we present a refined definition of 3D-GI at each timestamp along the trajectory.

Definition 2. (3D Geo-Indistinguishability, 3D-GI) *For a user's possible location set $D_t \in \mathbb{R}^3$ at time t, and any given locations $\boldsymbol{x}_t$ and $\boldsymbol{y}_t$, where $t \in [1, 2, \ldots, T]$, the perturbation mechanism $\mathcal{M}_t$ satisfies 3D-GI if and only if the following inequality holds:*

$$\Pr[\mathcal{M}_t(\boldsymbol{x}_t'|\boldsymbol{x}_t)] \leq e^{\epsilon d_3(\boldsymbol{x}_t, \boldsymbol{y}_t)} \Pr[\mathcal{M}_t(\boldsymbol{x}_t'|\boldsymbol{y}_t)]. \tag{7}$$

By defining $\epsilon_t = \epsilon d_3(\boldsymbol{x}_t, \boldsymbol{y}_t)$, where $d_3(\boldsymbol{x}_t, \boldsymbol{y}_t)$ denotes the Euclidean distance between $\boldsymbol{x}_t$ and $\boldsymbol{y}_t$ in 3D space, we establish that the mechanism $\mathcal{M}_t$ satisfies ϵ_t-differential

privacy, as stated in (7). This ensures that the probability distributions of the perturbed locations corresponding to the real locations $\boldsymbol{x}_t$ and $\boldsymbol{y}_t$ remain similar, thereby limiting an attacker's ability to accurately infer the user's real location based solely on the observed perturbed data. The degree of similarity between the perturbed and real locations is governed by the parameter ϵ_t, where a smaller ϵ_t value indicates a higher level of privacy protection for the user's location information.

According to (7) we derive

$$\Pr(\boldsymbol{x}_t|\boldsymbol{x}_t') \leq e^{\epsilon_t} \frac{\Pr(\boldsymbol{x}_t)}{\sum_{\boldsymbol{y}_t \in D_t} \Pr(\boldsymbol{y}_t)}. \tag{8}$$

This result indicates that, regardless of the prior knowledge an attacker possesses, 3D-GI bounds the multiplicative distance between posterior and prior probabilities within ϵ_t, effectively limiting the attacker's ability to infer posterior information.

D. Distortion Geo-Perturbation (Expected Inference Error)

The expected inference error [24] is one of the key methods for quantifying the effectiveness of trajectory privacy protection. It measures the effectiveness of privacy protection by evaluating the level of error an attacker might incur when attempting to infer the user's real location. The definition is described as follows:

Definition 3. (Expected Inference Error) *An expected inference error can be categorized into the conditional expected inference error and unconditional expected inference error. The conditional expected inference error refers to the expected error incurred by an attacker with prior knowledge attempting to infer the real location of the user at time t. In contrast, the unconditional inference expected error represents the average error of an attacker who lacks prior knowledge and attempts to infer the user's location at time t in all scenarios.*

We assume that the attacker who has the knowledge of spatiotemporal correlation can observe all perturbed locations posted at previous moments. Under such conditions, the conditional expected inference error is defined as

$$ExpEr\left(\boldsymbol{x}_t^{'}\right) = \min_{\hat{\boldsymbol{x}}_t \in \mathcal{A}} \sum_{\boldsymbol{x}_t \in \mathcal{A}} \Pr\left(\boldsymbol{x}_t|\boldsymbol{x}_t^{'}\right) d_3\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right). \tag{9}$$

When the attacker possesses sufficient prior knowledge, their inferred location is constrained to include the user's real location within the PLS, minimizing the inference error and maximizing the user's privacy protection level [23]. The inference error is then given by

$$\begin{aligned} &\min_{\hat{\boldsymbol{x}}_t \in \mathcal{A}} \sum_{\boldsymbol{x}_t \in \Phi_t} \frac{\Pr\left(\boldsymbol{x}_t|\boldsymbol{x}_t'\right)}{\sum_{\boldsymbol{y}_t \in \Phi_t} \Pr\left(\boldsymbol{y}_t|\boldsymbol{x}_t'\right)} d\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right) \\ &\geq e^{-\epsilon} \min_{\hat{\boldsymbol{x}}_t \in \Phi_t} \sum_{\boldsymbol{x}_t \in \Phi_t} \frac{\Pr\left(\boldsymbol{x}_t\right)}{\sum_{\boldsymbol{y}_t \in \Phi_t} \Pr\left(\boldsymbol{y}_t\right)} d\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right). \end{aligned} \tag{10}$$

E. δ-Location Set

To enhance the protection of locations frequently visited by users, the δ-location set is introduced, as proposed in [16]. This set represents the collection of locations where the user is most likely to appear at time t, and we denote it as $\Delta\chi_t$. Specifically, the δ-location set $\Delta\chi_t$ is defined as a set containing the minimum number of locations at time t with a prior probability sum not less than $1-\delta$, where $0 < \delta < 1$. Formally, it is defined as

$$\Delta\chi_t = \min\left\{ loc_i | \sum_{loc_i} \mathbf{p}_t^- [i] \geq 1 - \delta \right\}. \tag{11}$$

Since the δ-location set includes locations with a high probability of user presence at time t, there exists a small probability that the user's real location $\boldsymbol{x}_t$ of the user be excluded. In such a case, we substitute the closest location $\tilde{\boldsymbol{x}}_t$ for the real location $\boldsymbol{x}_t$, given by

$$\tilde{\boldsymbol{x}}_t = \underset{\tilde{\boldsymbol{x}}_t \in \Delta\boldsymbol{\chi}_t}{\arg\min}\ d\left(\tilde{\boldsymbol{x}}_t, \boldsymbol{x}_t\right). \tag{12}$$

In this framework, it is considered protected if the user's real location $\boldsymbol{x}_t$ belongs to the δ-location set (i.e., $\boldsymbol{x}_t \in \Delta\chi_t$). Otherwise, the closest location $\tilde{\boldsymbol{x}}_t$ serves as the protected location to mitigate potential location inference risks.

F. Concepts Related To Privacy Budget Allocation

To more comprehensively and flexibly meet the personalized privacy protection needs of users at different times and locations, we consider multiple factors that influence the sensitivity of users' trajectories during the privacy budget allocation process. Based on this, we define several key concepts closely related to privacy budget allocation.

Definition 4. (w-Trajectory Sequence Differential Privacy) *Consider a user's trajectory denoted as $Tr = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \ldots, \boldsymbol{x}_T\}$. For any continuous sequence of w timestamped location subsets $\{\boldsymbol{x}_{i-w+1}, \boldsymbol{x}_{i-w+2}, \ldots, \boldsymbol{x}_i\}$, if the cumulative privacy budget for this sequence satisfies (13), then the user's trajectory privacy is said to satisfy the w-trajectory sequence differential privacy, which is given by*

$$\forall i \in [n], \sum_{k=i-w+1}^{i} \epsilon_k \leqslant \epsilon, \tag{13}$$

where $\boldsymbol{x}_t$ represents the user's real location, which is perturbed to $\boldsymbol{x}_t'$ by the privacy-preserving mechanism $\mathcal{M}_i$, which satisfies ϵ_i-differential privacy.

Definition 5. (Location Predictability) *Location predictability $LP_{i,t}$ quantifies the predictability of the user's real location at time t, given by*

$$LP_{i,t} = \frac{1}{1 + \sum_{j=1}^{n} \mathrm{p}_t^-\left(loc_i\right) \mathrm{p}_t^-\left(loc_j\right) d_3\left(loc_i, loc_j\right)}, \tag{14}$$

where $\mathrm{p}_t^-\left(loc_i\right)$ and $\mathrm{p}_t^-\left(loc_j\right)$ denote the probabilities that, at time t, the user's real location is loc_i and the attacker's inferred location is loc_j, respectively. $d_3\left(loc_i, loc_j\right)$ denotes the Euclidean distance between loc_i and loc_j in 3D space.

Definition 6. (Location Sensitivity) *Location sensitivity $LS_{i,t}$ represents the sensitivity of loc_i, taking into account the*

user's sojourn time, visit frequency of loc_i, and the semantic sensitivity of loc_i, given by

$$LS_{i,t} = \gamma_t T_i + \gamma_f F_i + \gamma_s Sen_i \cdot (1 + \lambda I_{\text{user}}), \tag{15}$$

where T_i and F_i denote the user's sojourn time and visit frequency at loc_i, respectively. These values can be derived from the user's historical trajectory data. Sen_i denotes the semantic sensitivity of loc_i to the user, which can be configured based on the potential risk of privacy exposure with the semantic context of the location. Furthermore, individual privacy protection requirements can vary even within the same location, depending on user-specific attributes. For instance, the sensitivity attributed to a hospital location is typically lower for a physician compared to a patient. The characteristic adjustment coefficient, I_{user}, is introduced to account for such distinctions. For instance, in the scenario where a patient visits a hospital, $I_{user} = 0.8$; conversely, for a doctor visiting the same hospital, $I_{user} = 0.1$. The parameter λ represents the weight of I_{user}, determining the extent of its impact.

The coefficients γ_t, γ_f, and γ_s indicate the respective weights assigned to sojourn time, visit frequency, and location semantic sensitivity in the calculation of location sensitivity, which satisfy

$$\gamma_t + \gamma_f + \gamma_s = 1. \tag{16}$$

This allows the users to adjust the weighting parameters according to their specific needs. For example, for a patient, although the sojourn time and visit frequency at the hospital may be short, the hospital itself could still reveal sensitive health information, leading to a higher semantic sensitivity for the patient. Consequently, lower values can be assigned to γ_t and γ_f, while a higher value is assigned to γ_s.

G. Problem Statement

Compared to 2D space, incorporating height information in 3D space leads to a larger data scale and richer semantic content [23]. This increases data processing complexity and poses challenges in establishing location sensitivity. In addition, unlike protecting singular locations' privacy, neglecting spatiotemporal correlations makes it easier for attackers to exploit this knowledge to infer users' sensitive information [17], heightening privacy breach risks. Thus, 3D spatiotemporal trajectory privacy protection must account for the dynamic changes in prior distributions across different trajectory locations due to spatiotemporal correlations. Directly applying existing mechanisms to 3D spatiotemporal trajectory privacy cannot handle 3D spatiotemporal trajectory data. Therefore, we focus on protecting the privacy of 3D spatiotemporal trajectory in this work.

Significant spatiotemporal correlations often exist between locations on a trajectory, which attackers can exploit to enhance inference accuracy by updating their prior knowledge [18]. For example, by utilizing a known user location at a given time and the transition probability matrix between locations, an attacker can infer the user's potential locations at subsequent time steps, posing a greater threat to user privacy. Furthermore, the sensitivity of different locations along a trajectory varies, and users' privacy protection needs change accordingly. Even for the same location, the sensitivity may fluctuate due to contextual changes. In addition, as continuous location-based queries are made along the trajectory, privacy accumulation issues may arise [38]. Continuous queries gradually expose the user's behavior patterns, significantly increasing the risk of privacy leakage.

Algorithm 1: Personalized 3D spatiotemporal trajectory privacy protection mechanism (3DSTPM)

Input: $\mathbf{p}_{t-1}^{+}$, δ, E_m, $Tr = [\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_T]$, ϵ_s, $\Delta\epsilon$, $\mathbf{M}$, and w
Output: $\mathbf{p}_t^{+}$, $\boldsymbol{x}_t^{'}$

$\mathbf{p}_t^{-}$=$\mathbf{p}_{t-1}^{+}\mathbf{M}$;
$\epsilon_{i,t} = \mathbf{Algorithm1}(\epsilon_s, \Delta\epsilon, \mathbf{M}, w)$;
Determine $\Delta\chi_t$ from $\mathbf{p}_t^{-}$, δ;
if $\boldsymbol{x}_t \notin \Delta\chi_t$ **then**
  $\boldsymbol{x}_t = \tilde{x}_t$ via (11);
for $loc_i \in \Delta\chi_t$, $i = 1$ **to** *size of* $\Delta\chi_t$ **do**
  Find PLS Φ_t via Multiple rotated 3D Hilbert curve [23];
  Release perturbed locations $\boldsymbol{x}_t^{'}$ by PF mechanism;
Update $\mathbf{p}_t^{+}$ via (2);
Go to next timestamp;

To resolve this issue, we incorporate spatiotemporal correlation into our privacy protection strategy. By dynamically updating the prior probabilities of the user's potential locations at different times, we construct a possible location set $\Delta\chi_t$ for the user based on these probabilities and a predefined probability threshold. All locations within $\Delta\chi_t$ are subsequently protected. We leverage the complementary properties of 3D-GI and distortion privacy, employing a minimum distance search algorithm based on the 3D Hilbert curve to determine the protected location set Φ_t for each time step in the trajectory. Additionally, we adjust the privacy parameters E_m and ϵ to cater to users' personalized privacy requirements, which is influenced by factors such as sojourn time, visit frequency, and location semantic sensitivity. To more flexibly meet users' personalized needs while addressing the privacy accumulation issue caused by continuous queries along the trajectory, we propose a W-APBA algorithm, which effectively considers location sensitivity attributes. Moreover, to protect privacy while meeting users' QoS requirements, we apply the PF mechanism [23] to perturb the real locations.

V. Personalized Trajectory Privacy Protection Mechanism

A. Overview

In this section, we propose a personalized 3D spatiotemporal trajectory privacy protection mechanism, named 3DSTPM, as illustrated in Fig. 3. This mechanism is designed to protect the trajectory privacy of objects moving in 3D space, which also remains applicable to 2D space by setting the height coordinate to zero. To build this mechanism, we consider the spatiotemporal correlations between different locations

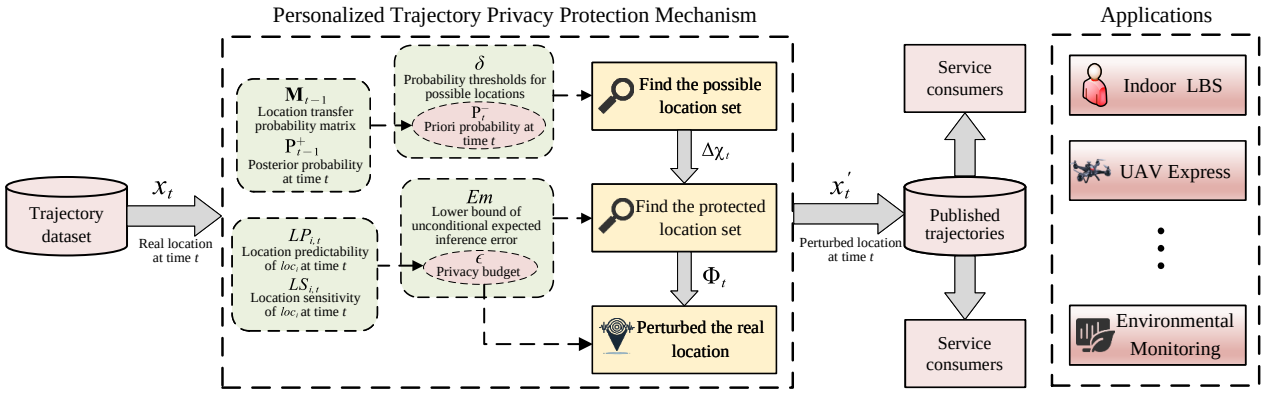


Fig. 3. The framework of 3DSTPM. 3DSTPM provides personalized trajectory privacy protection and is applicable to various scenarios. It operates in three stages: finding the possible location set, finding the protected location set, and perturbing the real location based on the privacy budget allocated according to the user's location sensitivity at different times.

in a 3D spatiotemporal trajectory and provide personalized trajectory privacy protection for users by integrating 3D-GI with expected inference error. Specifically, we first extract the location transition probability matrix from the user's historical trajectory dataset, and then, by combining the prior probability of each location with the probability threshold for possible locations, determine the possible location set. Next, by integrating the complementary characteristics of 3D-GI and distorted privacy, we identify a PLS for all locations within the possible location set, thereby enhancing the robustness of the mechanism while meeting users' personalized privacy needs. To enhance user QoS, we utilize a multiple-rotated 3D Hilbert curve to find the PLS with the smallest diameter. Additionally, we employ PF mechanism [23] to generate a perturbed location $\boldsymbol{x}_t^{'}$ for each location in the PLS, achieving a balance between trajectory privacy protection and QoS. The process of the 3DSTPM is summarized in Algorithm 1.

Furthermore, the sensitivity of different locations along a trajectory varies and may change dynamically over time, resulting in varying privacy protection requirements for users across different times and locations. In addition, continuous location-based queries along the trajectory lead to the gradual accumulation of privacy leakage, significantly increasing privacy risks. To overcome these challenges, we propose a novel privacy budget allocation algorithm, fully considering the sensitivity variations of locations over time and limiting the cumulative privacy leakage caused by continuous queries.

B. Determine $\Delta\chi_t$ at Continuous Times

To determine the possible location set $\Delta\chi_t$ at time t, we first eliminate all impossible locations where $\mathbf{p}_t^-$ is minimal or equal to zero, following the criteria specified in (11). This ensures that frequently visited locations of users are effectively protected, thereby enhancing privacy protection. If the real location at time t is removed, it is replaced with $\tilde{\boldsymbol{x}}_t$ to mitigate potential location inference risks.

Next, the posterior probability $\mathbf{p}_t^+$ is calculated according to (2), considering the spatiotemporal correlations between locations along the trajectory to enhance robustness against attackers who exploit such correlations. Using this posterior probability, the prior probability $\mathbf{p}_{t+1}^-$ for the next time step is then updated based on (4). From the updated $\mathbf{p}_{t+1}^-$ we derive $\Delta\chi_{t+1}$. The size of $\Delta\chi_{t+1}$ is determined by setting the value of δ, which can be adjusted based on the user's privacy protection needs. This process is iteratively applied to obtain $\Delta\chi_t$ for consecutive time steps.

C. Determine Protection Location Set

After obtaining $\Delta\chi_t$ of the user at the current moment, we provide protection for all locations within $\Delta\chi_t$ by finding a PLS Φ_t for each possible location. 3D-GI can effectively limit attackers from further inferring users' personal information by observing perturbed locations released at different times. However, it cannot restrict the attacker's expected inference error. On the other hand, the distortion privacy can limit the attacker's inference accuracy, but its effectiveness depends heavily on the attacker's prior knowledge. To leverage the advantages of both approaches, we integrate them to enhance the robustness against attackers with knowledge of spatiotemporal correlation information, constraining the attacker's inference error while independent of prior knowledge.

For any observed perturbed location, the conditional expectation error is formulated as [23]:

$$E\left(\Phi_t\right) = \min_{\hat{\boldsymbol{x}}_t \in \mathcal{A}} \sum_{\boldsymbol{x}_t \in \Phi_t} \frac{\Pr\left(\boldsymbol{x}_t\right)}{\sum_{\boldsymbol{y}_t \in \Phi_t} \Pr\left(\boldsymbol{y}_t\right)} d_3\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right). \quad (17)$$

In the worst case, the attacker's inferred location is narrowed down to an arbitrary location within the PLS containing the user's real location, the specific formula is given by [23]

$$E\left(\Phi_t\right) = \min_{\hat{\boldsymbol{x}}_t \in \mathcal{A}} \sum_{\boldsymbol{x}_t \in \Phi_t} \frac{\Pr\left(\boldsymbol{x}_t\right)}{\sum_{\boldsymbol{y}_t \in \Phi_t} \Pr\left(\boldsymbol{y}_t\right)} d_3\left(\hat{\boldsymbol{x}}_t, \boldsymbol{x}_t\right). \quad (18)$$

From (7), we obtain

$$ExpEr(\boldsymbol{x}_t') \geq e^{-\epsilon} E(\Phi_t). \quad (19)$$

Here, we introduce the privacy parameter E_m, which allows users to determine the unconditional expectation error lower

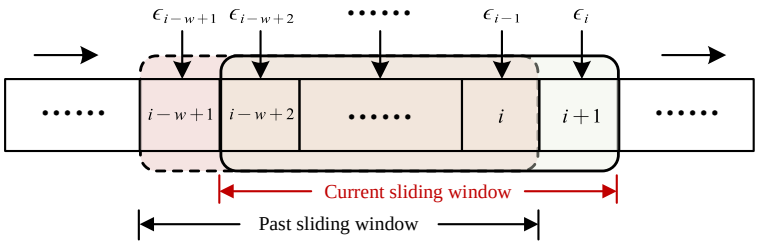


Fig. 4. w-sliding window.

term, i.e. $e^{-\epsilon}E(\Phi_t) \geqslant E_m$, according to their privacy preserving needs. To ensure this constraint is satisfied, we impose the following condition:

$$E(\Phi_t) \geqslant e^{\epsilon}E_m. \tag{20}$$

The locations within the PLS Φ_t can satisfy the condition:

$$ExpEr(\boldsymbol{x}_t') \geq e^{-\epsilon}E(\Phi_t), \tag{21}$$

indicating that a larger PLS generally provides stronger privacy protection. However, increasing the size of the PLS also results in greater QoS loss. To better balance trajectory privacy protection and QoS, we build upon the multi-rotation 3D Hilbert curves proposed in [23], and integrate the prior probability distribution that dynamically varies over time into the search process, so as to construct minimum-diameter PLS for all possible locations on the trajectory that better align with its spatiotemporal correlation characteristics. For the $\boldsymbol{x}_t$ in $\Delta\chi_t$, along the multi-rotation 3D Hilbert curve direction traverses all possible locations of the user and selects the sphere with the smallest diameter as the location protection set PLS Φ_t.

Furthermore, let $D(\Phi_t)$ denote diameter within the PLS, which is defined as the maximum distance between any two locations within the PLS at time t, i.e., $D(\Phi_t) \geqslant d(\boldsymbol{x}_t, \hat{\boldsymbol{x}}_t)$. Under this definition, we derive the following bound:

$$e^{\epsilon}E_m \leq E(\Phi_t) \leq \min_{\hat{\boldsymbol{x}}_t \in \Phi_t} \sum_{\boldsymbol{x}_t \in \Phi_t} \frac{\Pr(\boldsymbol{x}_t)}{\sum_{\boldsymbol{y}_t \in \Phi_t} \Pr(\boldsymbol{y}_t)} \mathrm{D}(\Phi_t) = \mathrm{D}(\Phi_t). \tag{22}$$

Thus, the diameter of the PLS must be no smaller than $e^{\epsilon}E_m$.

D. Privacy Budget Allocation Mechanism

To address the dynamic variation in location sensitivity so as to meet users' personalized requirements and reduce cumulative privacy leakage arising from continuous location-based queries, we introduce the W-APBA algorithm, which dynamically allocates privacy budgets to different locations along the trajectory. The w-sliding window refers to the sequence of locations with timestamps of length w that are continuously queried by the user, as illustrated in Fig. 4.

We aim to protect all complete trajectories that contain the user's possible locations. To achieve this, the user first sets the sliding window size w and the total privacy budget ϵ_s for all possible locations within the sliding window, based on their privacy protection needs. To ensure the practical usability of the method, the value of w should be smaller than the length of the trajectory. On this basis, we assign an initial privacy budget $\epsilon_r = \frac{\epsilon_s}{w \cdot n}$ to each possible location within w window, where n denotes the number of possible locations of the user for each timestamp. Additionally, we define $\epsilon_w = \frac{\epsilon_s}{n}$ as the total privacy budget allocated to w sliding window for a single specific trajectory.

The attacker gradually grasps the spatiotemporal correlation between different locations in the trajectory by continuously accumulating data on the user's behavioral patterns, travel habits, and other contextual information. This iterative update enhances the attacker's prior knowledge, leading to dynamic variations in the predictability of different locations over time. Moreover, the location sensitive fluctuates depending on temporal and environmental contexts, resulting in users' varying privacy protection requirements for different locations within the trajectory at different moments.

To accommodate these dynamically changing privacy requirements, we introduce the privacy increment $\Delta\epsilon$ and the privacy budget control coefficient λ, which enable the system to dynamically allocate privacy budgets to potential locations within the trajectory at different moments. This approach provides more precise control over privacy protection strength. Based on this framework, we define the privacy budget for location i at time t as

$$\epsilon_{i,t} = \epsilon_r - \lambda_{i,t}\Delta\epsilon, \tag{23}$$

where $\Delta\epsilon = \frac{\epsilon_s}{2}$, and $\lambda_{i,t}$ is determined by location predictability and location sensitivity, and we define $\lambda_{i,t}$ as

$$\lambda_{i,t} = \alpha_1 LP_{i,t} + \alpha_2 LS_{i,t}. \tag{24}$$

Here, $LP_{i,t}$ is the predictability of the user's real location $\boldsymbol{x}_t$, with higher predictability requiring stronger privacy protection. However, predictability alone does not fully capture user's privacy preferences. Even when two locations exhibit the same predictability, users may have different privacy needs. To better accommodate users' personalized preferences, we also incorporate location sensitivity $LS_{i,t}$, which quantifies the sensitivity of loc_i. The coefficients α_1 and α_2 represent the weights of $LP_{i,t}$ and $LS_{i,t}$, respectively, and can be adjusted by users based on their individual privacy preferences.

To further address the cumulative privacy leakage caused by continuous queries along the trajectory, the sliding window mechanism dynamically limits the total privacy budget that can be allocated at a given time. Specifically, the maximum privacy budget available for the current location is defined as

$$\epsilon_{\max,t} = \epsilon_w - \sum_{k=i-w+1}^{i-1} \epsilon_k, \tag{25}$$

Algorithm 2: Window-based Adaptive Privacy Budget Allocation (W-APBA)

Input: ϵ_s, $\Delta\epsilon$, $\mathbf{M}$, and w
Output: privacy budget: $\epsilon_{i,t}$

for *location* loc_i, $i = 1$ **to** n **do**
  $\mathbf{p}_t^- = \mathbf{p}_{t-1}^+ \mathbf{M}$;
  for *Inferred locaion* x_j, $j = 1$ **to** n **do**
    Calculate $d_3(loc_i, loc_j)$;
    Location predictability LP_i^t via (13);
    Location Sensitivity LS_i^t via (14);
    $\lambda_{i,t} = \alpha_1 LP_i^t + \alpha_2 LS_i^t$;
    Calculate maximum privacy budget $\epsilon_{\max,t}$ via (22);
    $\epsilon_t = \min(\epsilon_t, \epsilon_{\max,t})$;
    $\epsilon_r = \frac{\epsilon_t}{n}$;
    $\epsilon_{i,t} = \epsilon_r - \lambda_{i,t}\Delta\epsilon$;

RETURN $\epsilon_{i,t}$

where ϵ_k represents the privacy budget allocated to the user's real location at time k.

Given the constraint of $\epsilon_{\max,t}$, the privacy budget assigned to the current location is

$$\epsilon_{i,t} = \min\left(\epsilon_r - \lambda_{i,t}\Delta\epsilon, \epsilon_{\max,t}\right). \tag{26}$$

W-APBA not only ensures that the trajectory satisfies the w-trajectory sequence differential privacy, but also allocates different privacy budgets to different locations based on location predictability and location sensitivity, which fully meets the personalized needs of users.

As illustrated in Algorithm 2, the overall process of the proposed W-APBA algorithm is summarized. The computational complexity of the algorithm is $O(n^3)$, determined by the number of locations n in the user's trajectory. This relatively low complexity enables the algorithm to perform privacy protection computations efficiently on large-scale trajectory datasets, thereby reducing computational overhead and improving processing efficiency.

E. Differentially Private Mechanism in Protection Location Set

Based on the allocated privacy budget, we apply the PF mechanism proposed in [23] to perturb all the real locations along the trajectory. Furthermore, we demonstrate that the distance between the real and perturbed locations generated by the PF mechanism is constrained by a controllable upper bound, indicated in the following Theorem. Additionally, the algorithmic complexity of PF is $O(n^2)$, influenced by the number of possible user locations at different times along the trajectory [23]. This relatively low complexity enables PF to efficiently process large-scale trajectory data while maintaining privacy protection.

Theorem 1. *The distance between the user's real location $\boldsymbol{x}_t$ and the perturbed location $\boldsymbol{x}_t'$ sampled from the possible location set $\Delta\chi_t$ by the PF mechanism, with probability at least $1-\psi, (0 \le \psi \le 1)$ satisfies the following inequality:*

$$d_3(\boldsymbol{x}_t, \boldsymbol{x}_t') \le \frac{2D(\Phi_t)}{\epsilon}\left[\ln|\Delta\chi_t| - \frac{\epsilon}{2} - \ln|\Phi_t| - \ln\psi - \max d_3(\boldsymbol{x}_t, \boldsymbol{x}_t')\right] \quad (0 \le \psi \le 1). \tag{27}$$

Proof. The probability of a location being selected from $\Delta\chi_t$ is given by [17]

$$w_{\boldsymbol{x}} \exp\left(\frac{-\epsilon\left(d_3\left(\boldsymbol{x}_t, \boldsymbol{x}_t{}'\right) - \max d_3\left(\boldsymbol{x}_t, \boldsymbol{x}_t{}'\right)\right)}{2D(\Phi_t)}\right), \tag{28}$$

where $w_{\boldsymbol{x}}$ is the probability distribution normalization factor. Based on (28), we derive an upper bound on the total probability of the output perturbed locations that satisfy $d_3\left(\boldsymbol{x}_t, \boldsymbol{x}_t{}'\right) \geqslant a, (a \geqslant 0)$ within $\Delta\chi_t$, i.e.,

$$w_{\boldsymbol{x}}|\Delta\chi_t| \exp\left(\frac{-\epsilon\left(a - \max d_3\left(\boldsymbol{x}_t, \boldsymbol{x}_t{}'\right)\right)}{2D(\Phi_t)}\right). \tag{29}$$

According to [23], for any $\boldsymbol{x}_t'$, $w_{\boldsymbol{x}} \leqslant \frac{e^{\frac{-\epsilon}{2}}}{|\Phi_t|}$. Thus, the above equation becomes

$$\le \frac{|\Delta\chi_t| e^{-\frac{\epsilon}{2}}}{|\Phi_t|} \exp\left(\frac{-\epsilon a - max d_3\left(\boldsymbol{x}_t, \boldsymbol{x}_t{}'\right)}{2D(\Phi)}\right). \tag{30}$$

Let the right-hand side be ψ, we have:

$$a = \frac{2D(\Phi)}{\epsilon}\left[\left(\ln|\Delta\chi_t| - \ln\psi - \ln|\Phi_t| - \frac{\epsilon}{2}\right) - \max d_3\left(\boldsymbol{x}_t, \boldsymbol{x}_t{}'\right)\right]. \tag{31}$$

Therefore, for any $\boldsymbol{x}_t'$ sampled from $\Delta\chi_t$ by the PF mechanism, with probability at least $1-\psi$, we have (27). □

Remark 1. *The PF mechanism achieves a great balance between trajectory privacy and QoS by bounding the maximum perturbation distance from the real location. As demonstrated in (27), this upper bound is jointly determined by ϵ and E_m, which affect the diameter of the PLS. Therefore, by adjusting the values of ϵ and E_m, the mechanism exhibits flexibly to users' personalized privacy needs while maintaining QoS.*

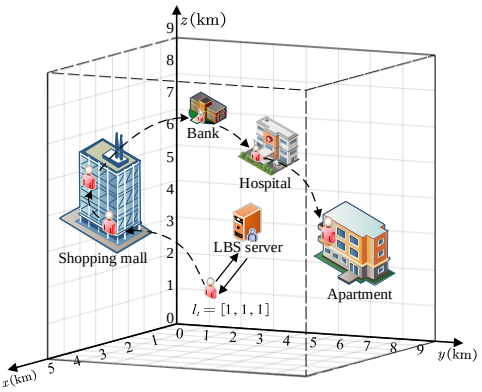
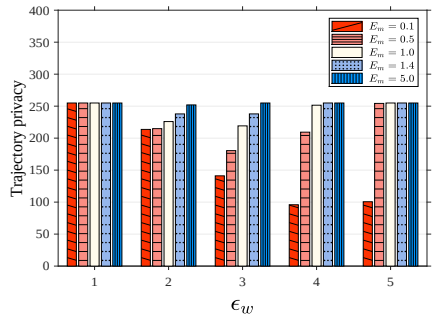


Fig. 5. Simulation setting of the trajectory of a user.

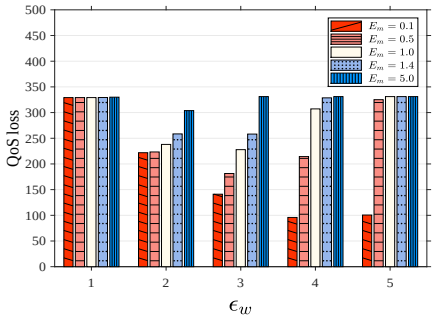
VI. Simulations Results

A. Simulation Setup

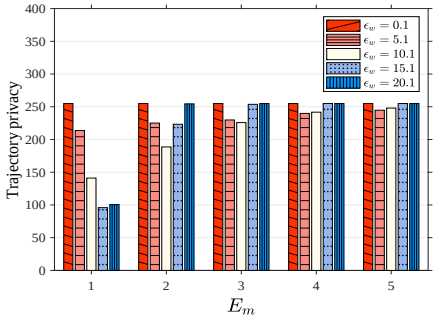
In this section, we analyze the impact of privacy parameters on the performance of our proposed mechanism 3DSTPM.



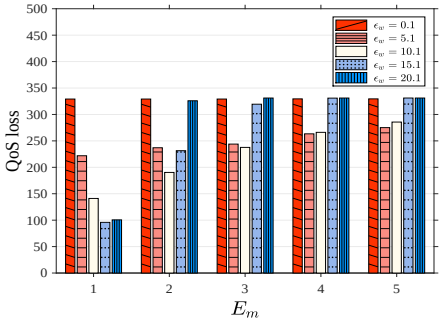
(a) Trajectory privacy v.s. ϵ_w under same E_m



(b) QoS loss v.s. ϵ_w under same E_m



(c) Trajectory privacy v.s. E_m under same ϵ_w



(d) QoS loss v.s. E_m under same ϵ_w

Fig. 6. Impact of ϵ_w and E_m on personalized trajectory privacy protection.

Additionally, we compare the trajectory privacy and QoS loss performance of 3DSTPM with P3DLPPM [23] and 2DPTPPM [17] under attacks from attackers possessing spatiotemporal correlation knowledge. Moreover, the PIM mechanism in [16] is also modified and applied in the 3D space, named 3DPIM, as a benchmark.

For the simulation, we divide a 10m × 10m × 10m 3D space into 512 cells, with each cell representing a potential 3D location of the user. We then randomly select 50 of these cells as the user's real locations, and the probability of the user reaching each of these locations is treated as the attacker's prior distribution. This setup simulates the attacker's initial knowledge of the user's location. Fig. 5 depicts the trajectory of the user at five sequential moments.

The trajectory privacy p and QoS loss q are evaluated according to the metrics described in our previous work [23], which are given by

$$p = \sum_{\boldsymbol{x}_t, \boldsymbol{x}'_t, \hat{\boldsymbol{x}}_t \in \mathcal{A}} \Pr(\boldsymbol{x}_t)\, f(\boldsymbol{x}'_t \mid \boldsymbol{x}_t)\, h(\hat{\boldsymbol{x}}_t \mid \boldsymbol{x}'_t)\, d(\boldsymbol{x}_t, \hat{\boldsymbol{x}}_t), \tag{32}$$

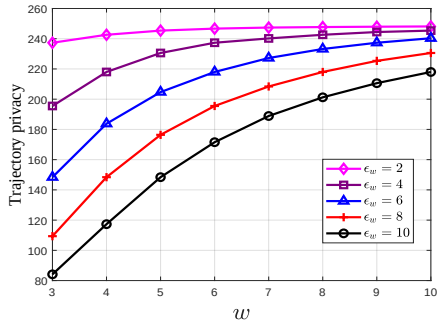
$$q = \sum_{\boldsymbol{x}_t, \boldsymbol{x}'_t \in \mathcal{A}} \Pr(\boldsymbol{x}_t)\, f(\boldsymbol{x}'_t \mid \boldsymbol{x}_t)\, d(\boldsymbol{x}_t, \boldsymbol{x}'_t). \tag{33}$$

B. Impact of Privacy Parameters on Personalized Trajectory Privacy Protection

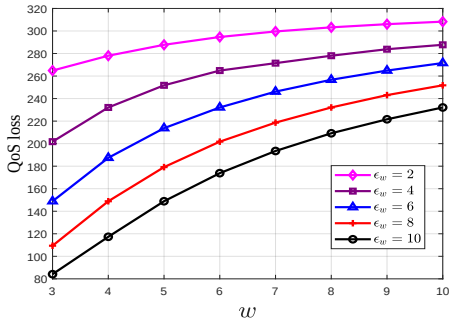
By setting different privacy budgets ϵ and inference error thresholds E_m, we evaluate the impact of various privacy parameters on the privacy protection performance of 3DSTPM. As illustrated in Fig. 6, it can be seen that the two privacy parameters ϵ, E_m have a significant impact on both trajectory privacy and QoS loss.

Specifically, from $e^{\epsilon} E_m \leq \mathrm{D}(\Phi_t)$, it can be seen that the impact of ϵ on $\mathrm{D}(\Phi_t)$ exhibits exponential growth, while the impact of E_m on $\mathrm{D}(\Phi_t)$ is linear. As shown in Figs. 6(a) and 6(b), when E_m is fixed and ϵ_w is small, increasing ϵ_w leads to a decrease in $D(\Phi_t)/\epsilon_w$, which, in turn, reduces the distance between the real location and the perturbed location. Consequently, both trajectory privacy and QoS loss gradually decrease. Moreover, as the value of E_m increases, the trajectory privacy and QoS loss also increase. With a further increase in ϵ_w, the diameter of the protection region increases sharply, causing $D(\Phi_t)/\epsilon_w$ to increase, which results in a larger distance between the real and perturbed locations. This effect varies depending on the settings of E_m. Nonetheless, in practical scenarios, the diameter of the protection region cannot increase indefinitely, so both trajectory privacy and QoS loss will eventually converge to an upper limit.

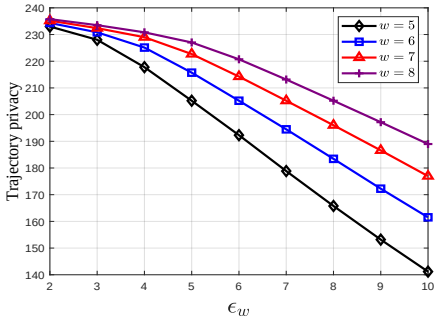
Figs. 6(c) and 6(d) illustrate the impact of E_m on trajectory privacy and QoS loss under different values of ϵ_w. Given a specific ϵ_w, as E_m increases, the diameter of the protection region increases, leading to higher trajectory privacy and QoS loss. However, when ϵ_w is sufficiently large, its effect on $\mathrm{D}(\Phi_t)$ is far greater than that of E_m. Thus, when $\epsilon_w = 2.5$, an increase in E_m causes a significant change in the diameter of the protection region, the distance between the user's real location and the perturbed location increases, resulting in a steep increase in trajectory privacy and QoS loss, making the curve steep. In practical applications, however, the diameter of



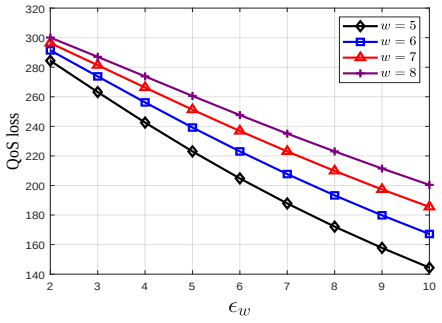
(a) Trajectory privacy v.s. w under same ϵ_w



(b) QoS loss v.s. w under same ϵ_w



(c) Trajectory privacy v.s. w under same w



(d) QoS loss v.s. w under same w

Fig. 7. Impact of W-APBA parameters on personalized trajectory privacy protection.

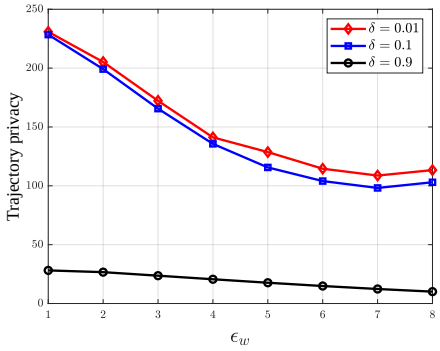


Fig. 8. Impact of probability thresholds δ on personalized trajectory privacy protection.

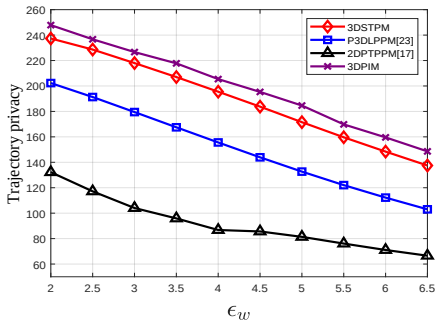
the protection region is limited, so trajectory privacy and QoS loss will converge to a finite value. Additionally, an excessively small privacy budget allocation is insufficient to ensure an acceptable level of QoS loss. Therefore, regardless of the E_m setting, when $\epsilon_w = 0.1$, trajectory privacy and QoS loss reach their maximum values.

In Fig. 7, we explore the impact of the window size w on trajectory privacy and QoS loss. As shown in Figs. 7(a) and 7(b), when ϵ_w is fixed, the privacy budget allocated to each window decreases as w increases. This leads to an increase in $D(\Phi_t)/\epsilon_w$, as shown in (27) in Theorem 1, the distance between the user's real location and the perturbed location increases, leading to an increase in trajectory privacy. For instance, when $\epsilon_w = 8$, the trajectory privacy protection value is 176.41 with $w = 5$, representing an 18.87% increase compared to the value at $w = 4$. Furthermore, the increase in the distance between the real location and the perturbed location also leads to a higher QoS loss. For example, the QoS loss value when $w = 5$ is 20.34% higher than the QoS loss value at $w = 4$. Similarly, Figs. 7(c) and 7(d) demonstrate that when w is fixed, the privacy budget allocated to each window increases as ϵ_w increases. This leads to a larger range of perturbed locations, gradually increasing the distance between the real location and the perturbed location, thereby reducing trajectory privacy while decreasing QoS loss.

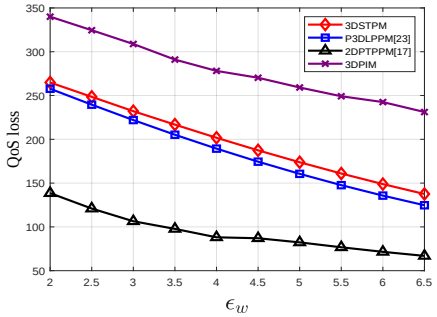
Fig. 8 illustrates the impact of the probability threshold δ on trajectory privacy p. As depicted in Fig. 8, trajectory privacy q decreases as δ increases. When δ continues to rise towards 1, trajectory privacy experiences a significant decline, and the user's privacy can no longer be effectively protected. This occurs because, as δ increases, the number of possible user locations decreases, boosting the success rate of the attacker's inference. Consequently, trajectory privacy diminishes. When δ nears 1, the number of possible user locations can drop to just one, causing the attacker's inference success rate to soar, and the user's trajectory privacy is almost entirely lost, making it impossible to ensure adequate protection.

C. Performance of Different Trajectory Privacy Protection Mechanisms

Next, we quantitatively compare 3DSTPM with P3DLPPM, 3DPIM and 2DPTPPM in terms of trajectory privacy and QoS



(a) Comparison of different mechanisms performance on Trajectory privacy.



(b) Comparison of different mechanisms performance on QoS loss.

Fig. 9. Comparison of the performance of different mechanisms.

loss to verify its advantages.

As illustrated in Fig. 9, 3DSTPM exhibits significant advantages over 2DPTPPM. When facing the same attacker with spatiotemporal correlation knowledge, 2DPTPPM demonstrates lower QoS loss but significantly falls short in trajectory privacy value compared to 3DSTPM, making it inadequate to meet the trajectory privacy protection requirements in 3D space. For instance, when $\epsilon_w = 4.0$, the trajectory privacy value of 3DSTPM is approximately 2.3 times higher than 2DPTPPM. This disparity arises because 2DPTPPM perturbs only the horizontal coordinates of trajectory locations, overlooking height information, which can also pose a risk of privacy leakage. In contrast, 3DSTPM not only safeguards the horizontal trajectory but also protects the height data, which offers a higher level of privacy protection.

Fig. 9 also shows that under similar QoS levels, 3DSTPM demonstrates a more significant advantage in trajectory privacy compared to P3DLPPM and 3DPIM. For the same ϵ_w, the QoS loss of 3DSTPM is slightly higher than that of P3DLPPM, but the improvement in trajectory privacy significantly outweighs the increase in QoS loss. For instance, when $\epsilon_w = 4.5$, the privacy level of 3DSTPM improves by 21.68% compared to P3DLPPM, while the QoS loss increases by only 6.91%. This advantage arises because P3DLPPM does not account for the spatiotemporal correlation between locations on the trajectory, instead offering protection solely for individual locations along the trajectory. In contrast, 3DSTPM enhances privacy protection by incorporating spatiotemporal correlations between trajectory locations and dynamically updating the prior probability of a user's location using the location transition probability matrix. Additionally, although the privacy level of 3DSTPM is slightly lower than that of 3DPIM, its QoS loss is significantly reduced. For instance, when $\epsilon_w = 4.5$, the trajectory privacy of 3DSTPM is 6.30% lower than that of 3DPIM, while the QoS loss is reduced by 30.66%. The reason is that 3DSTPM employs the PF mechanism to perturb different locations along the trajectory, providing a smaller perturbation distance while guaranteeing privacy needs. As a result, it ensures trajectory privacy while minimizing QoS loss.

VII. Conclusion

In this paper, we have proposed a personalized 3D spatiotemporal trajectory privacy protection mechanism 3DSTPM. This paper has two novel contributions. First, we overcome the challenges posed by the high dimensionality of 3D space, consider the spatiotemporal correlations between locations on the trajectory, and combine the complementary characteristics of 3D-GI and expected error, expanding the applicability of the mechanism while enhancing its robustness. Second, we have proposed a W-APBA, which dynamically adjusts the privacy budget to provide more flexible privacy protection for users. We have also demonstrated that the distance between the real and perturbed locations generated by PF is constrained by a controllable upper bound, further reinforcing the theoretical foundation of the PF mechanism. Simulation results demonstrate that 3DSTPM significantly outperforms benchmarks in defending against spatiotemporally correlated attackers. For instance, when $\epsilon_w = 5.0$, 3DSTPM achieves a privacy level that is 2.1 times higher than 2DPTPPM and 29% higher than P3DLPPM, with only an 8% increase in QoS loss compared to P3DLPPM. Moreover, although 3DSTPM has a 7.08% lower privacy level than 3DPIM, its QoS loss is reduced by 32.94%.

References

[1] Y. Mekdad, A. Aris, L. Babun, A. El Fergougui, M. Conti, R. Lo Cigno, and A. S. Uluagac, "A survey on security and privacy issues of UAVs," *Comp. Networks.*, vol. 224, Apr. 2023.

[2] A. Lagorio, R. Pinto, and R. Golini, "Research in urban logistics: a systematic literature review," *Int. J. Phys. Distrib. Logist. Manag.*, vol. 46, no. 10, pp. 908–931, Nov. 2016.

[3] Q. Guo, Y. Wang, and X. Dong, "Effects of smart city construction on energy saving and CO2 emission reduction: Evidence from china," *Appl. Energy.*, vol. 313, no. 118879, May. 2022.

[4] H. Huang, J. Su, and W. Feiyue, "The potential of low-altitude airspace: The future of urban air transportation," *IEEE Trans. Intell. Veh.*, vol. 9, no. 8, pp. 5250–5254, Aug. 2024.

[5] Y. Ren, X. Li, Y. Miao, R. H. Deng, J. Weng, S. Ma, and J. Ma, "Distpreserv: Maintaining user distribution for privacy-preserving location-based services," *IEEE Trans. Mobile Comput.*, vol. 22, no. 6, pp. 3287–3302, Jun. 2023.

[6] X. Chen, C. Wang, Q. Yang, H. Teng, and C. Jiang, "Privacy passport: Privacy-preserving cross-domain data sharing," *IEEE Trans. Inf. Forensics Security.*, vol. 20, pp. 636–650, Dec. 2024.

[7] S. Cai, X. Lyu, X. Li, D. Ban, and T. Zeng, "A trajectory released scheme for the internet of vehicles based on differential privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 16534–16547, Sep. 2022.

[8] H. Jiang, J. Li, P. Zhao, F. Zeng, Z. Xiao, and A. Iyengar, "Location privacy-preserving mechanisms in location-based services: A comprehensive survey," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–36, Jan. 2021.

[9] R. Gui, X. Zhang, X. Gui, and J. Han, "A location correlation differential privacy extension scheme based on user spatiotemporal characteristics," *IEEE Internet Things J.*, vol. 11, no. 24, pp. 41151–41165, Dec. 2024.

[10] S. Qiu, D. Pi, Y. Wang, and Y. Liu, "Novel trajectory privacy protection method against prediction attacks," *Expert Syst. Appl.*, vol. 213, no. 118870, Mar. 2023.

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

[12] W. Zhang, Z. Xie, A. M. Vera Venkata Sai, Q. Zia, Z. He, and G. Yin, "A local differential privacy trajectory protection method based on temporal and spatial restrictions for staying detection," *Tsinghua Sci. Technol.*, vol. 29, no. 2, pp. 617–633, Sep. 2024.

[13] F. Jin, W. Hua, L. Li, B. Ruan, and X. Zhou, "Efficient frequency-based randomization for spatial trajectories under differential privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 36, no. 6, pp. 2430–2444, Oct. 2024.

[14] P. Liu, D. Wu, Z. Shen, H. Wang, and K. Liu, "Personalized trajectory privacy data publishing scheme based on differential privacy," *IoT*, vol. 25, Apr. 2024.

[15] L. Yao, Z. Chen, H. Hu, G. Wu, and B. Wu, "Privacy preservation for trajectory publication based on differential privacy," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 3, pp. 1 – 21, Apr. 2022.

[16] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Oct. 2015.

[17] M. Cao, H. Zhu, M. Min, Y. Li, S. Li, H. Zhang, and Z. Han, "Protecting personalized trajectory with differential privacy under temporal correlations," in *Proc. IEEE Wirel. Commun. Netw. Conf.*, Dubai, UAE, Apr. 2024.

[18] J. Xi, M. Shi, W. Zhang, Z. Xu, and Y. Liu, "Trajectory privacy-protection mechanism based on multidimensional spatial–temporal prediction," *Symmetry*, vol. 16, no. 9, p. 1248, Sep. 2024.

[19] J. Li and G. Chen, "A personalized trajectory privacy protection method," *Comput. Secur.*, vol. 108, no. 102323, Sep. 2021.

[20] Z. Zheng, Z. Li, H. Jiang, L. Y. Zhang, and D. Tu, "Semantic-aware privacy-preserving online location trajectory data sharing," *IEEE Trans. Inf. Forensics Security.*, vol. 17, pp. 2256–2271, Jun. 2022.

[21] C. Dwork, "Differential privacy," in *Proc. Int. Colloq. Automata Lang. Program.*, Springer, Berlin, Heidelberg, July. 2006.

[22] 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. Wireless Commun.*, vol. 21, no. 7, pp. 4682–4694, July. 2022.

[23] M. Min, H. Zhu, J. Ding, S. Li, L. Xiao, M. Pan, and Z. Han, "Personalized 3D location privacy protection with differential and distortion geo-perturbation," *IEEE Trans. Depend. Secure Comput.*, vol. 21, pp. 3629 – 3643, Nov. 2023.

[24] 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.

[25] H. Yuan, L. Wu, L. Xu, L. Ban, H. Wang, Y. Su, and W. Meng, "SCTP: Achieving semantic correlation trajectory privacy-preserving with differential privacy," *IEEE Trans. Veh. Technol.*, pp. 1–14, Nov. 2024.

[26] C. Qiu, A. Squicciarini, C. Pang, N. Wang, and B. Wu, "Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability," *IEEE Trans. Mobile Comput.*, vol. 21, no. 7, pp. 2436–2450, Nov. 2020.

[27] R. Hu, Y. Guo, and Y. Gong, "Federated learning with sparsified model perturbation: Improving accuracy under client-level differential privacy," *IEEE Trans. Mobile Comput.*, vol. 23, no. 8, pp. 8242–8255, Dec. 2023.

[28] Y. Zhu, Y. Hong, Q. Xue, X. Lan, Y. Zhang, and Y. Xiang, "LDGI: Location-discriminative geo-indistinguishability for location privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 37, no. 3, pp. 1282–1293, Mar. 2025.

[29] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Trans. Mobile Comput.*, vol. 7, no. 1, Jan. 2008.

[30] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, "On the privacy preserving properties of random data perturbation techniques," in *Proc. IEEE Int. Conf. Data Mining (ICDM)*, Melbourne, FL, Nov. 2003.

[31] M. Gramaglia, M. Fiore, A. Furno, and R. Stanica, "GLOVE: towards privacy-preserving publishing of record-level-truthful mobile phone trajectories," vol. 2, pp. 1–36, ACM New York, NY, Sep. 2021.

[32] A. Liu, Z. Huang, M. Li, Y. Wan, W. Li, T. X. Han, C. Liu, R. Du, D. K. P. Tan, J. Lu, Y. Shen, F. Colone, and K. Chetty, "A survey on fundamental limits of integrated sensing and communication," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 994–1034, Feb. 2022.

[33] S. De Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati, "k-anonymity: From theory to applications," *Trans. Data Priv.*, vol. 16, no. 1, pp. 25–49, Apr. 2023.

[34] Z. Shen, Y. Zhang, H. Wang, P. Liu, K. Liu, and Y. Shen, "Bigru-dp: Improved differential privacy protection method for trajectory data publishing," *Expert Syst. Appl.*, vol. 252, Oct. 2024.

[35] Y. Cao, Y. Xiao, L. Xiong, L. Bai, and M. Yoshikawa, "Protecting spatiotemporal event privacy in continuous location-based services," *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 8, pp. 3141–3154, Aug. 2021.

[36] G. Qiu, D. Guo, Y. Shen, G. Tang, and S. Chen, "Mobile semantic-aware trajectory for personalized location privacy preservation," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 16165–16180, Aug. 2020.

[37] H. Liu, X. Li, H. Li, J. Ma, and X. Ma, "Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Atlanta, GA, May. 2017.

[38] C. Zhang, Y. Wang, W. Wang, H. Zhang, Z. Liu, X. Tong, and Z. Cai, "A personalized location privacy protection system in mobile crowdsourcing," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9995–10006, Oct. 2023.