MEC下基于模糊敏感度量的个性化轨迹隐私保护方法

蒋忠元[1,2]，房梦欣[1]，王启舟[3]，马建峰[1]，李兴华[1]
（1.西安电子科技大学网络与信息安全学院，陕西 西安 710126；2.紫金山实验室，江苏 南京 211111；
3.西安交通大学电信学部，陕西 西安 710049）

摘　要：针对现有轨迹隐私保护方法普遍缺乏对用户个性化隐私需求的考虑，且传统的加噪机制容易造成数据可用性下降的问题，提出了一种基于Laplace机制的个性化动态轨迹隐私保护方法。首先，利用模糊数学构建位置点敏感度量化模型，融合位置语义特征与用户隐私偏好，获得个性化的敏感度评估结果；随后，基于轨迹中位置点单元的隐私权重动态分配隐私预算，并使用Laplace机制实现动态轨迹扰动，从而在高敏感区域提供更强保护，在低敏感区域保持更高数据可用性。实验结果表明，与现有轨迹差分隐私保护方法相比，所提方法在隐私保护效果与轨迹数据可用性方面均具有显著优势。

关键词：轨迹隐私保护；模糊隶属度；差分隐私；Laplace机制
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026077

Personalized trajectory perturbation method based on fuzzy sensitivity quantification in MEC

Jiang Zhongyuan[1,2], Fang Mengxin[1], Wang Qizhou[3], Ma Jianfeng[1], Li Xinghua[1]
1. School of Cyber Engineering, Xidian University, Xi'an 710126, China
2. Purple Mountain Laboratories, Nanjing 211111, China
3. School of Telecommunication, Xi'an Jiaotong University, Xi'an 710049, China

Abstract: To address the limitations of existing trajectory privacy protection methods, which generally neglect users' personalized privacy requirements and suffer from utility degradation under traditional noise-injection mechanisms, a personalized dynamic privacy trajectory protection based on the Laplace mechanism was proposed. First, a fuzzy sensitivity quantification model was developed to characterize the semantic sensitivity of each location point by jointly considering spatial contextual features and individual privacy preferences, thereby enabling personalized sensitivity assessment. Then, a dynamic privacy budget allocation strategy was designed to distribute privacy budgets according to the sensitivity levels of trajectory points, upon which the Laplace mechanism was applied to generate adaptive perturbations. This enabled stronger protection for highly sensitive regions while maintaining higher data fidelity for low-sensitivity areas. Experimental results show that, compared with representative differential privacy-based trajectory perturbation methods, the proposed approach achieved superior privacy preservation performance and significantly enhanced the utility of perturbed trajectory data.

Keywords: trajectory privacy protection, fuzzy membership function, differential privacy, Laplace mechanism

收稿日期：2026–01–04；**修回日期：**2026–03–15
通信作者：房梦欣，mxfang1709@163.com
基金项目：陕西省杰出青年科学基金资助项目（No.2025JC-JCQN-085）；陕西省重点研发计划基金资助项目（No.2023-YBGY-270）
Foundation Items: Natural Science Basic Research Program of Shaanxi (No.2025JC-JCQN-085), The Key Research and Development Program of Shaanxi Province (No.2023-YBGY-270)

0　引言

随着卫星互联网、车联网以及基于位置的服务（location-based service, LBS）迅速发展[1-2]，位置感知应用已广泛应用于出行导航、路径规划和交通监测等场景，用户对位置信息的依赖不断增强。与此同时，智能终端与移动设备的普及使计算与通信规模持续扩大，网络中产生的时空数据呈指数级增长。移动边缘计算（mobile edge computing, MEC）作为一种分布式计算范式，将计算任务从云中心迁移至靠近用户的边缘节点，从而降低传输时延并提升服务响应能力，同时为大规模时空数据处理提供了重要技术支撑[3]。然而，由于MEC环境具有开放性与动态交互特征，轨迹数据在采集、传输与共享过程中极易遭受隐私泄露与安全攻击[4]。

近年来，多起轨迹数据泄露事件表明，即使移除显式身份标识，攻击者仍可利用少量轨迹数据结合外部信息实现身份重识别。例如，公开发布的纽约出租车轨迹数据曾被关联至社交媒体以推断用户出行信息。某运动应用发布的全球运动热力图也曾暴露部分海外军事基地位置。这些事件表明轨迹数据具有高度敏感性，涉及个人与公共安全，因此在MEC环境下开展轨迹隐私保护研究具有重要意义。

针对轨迹数据隐私泄露问题，已有研究主要包括基于轨迹扭曲、加密、匿名化[5]以及差分隐私（differential privacy, DP）[6]的扰动方法。然而，现有差分隐私轨迹保护方法仍存在一定局限：一方面，多数方法未充分考虑用户个性化隐私需求，难以适应多样化应用场景；另一方面，隐私预算通常采用静态或全局统一分配策略，容易破坏轨迹连续性并降低数据可用性。例如，PPBA方法[7]通过概率扰动增强个性化特征，但其隐私预算分配依赖固定距离比例，在多用户环境中难以动态调整，导致隐私预算利用率较低。Liu等[8]提出了语义感知在线轨迹共享框架，通过语义特征增强扰动策略，但其扰动强度主要由语义分布决定，难以反映用户个性化隐私需求，也缺乏对位置敏感度的自适应调节。因此，如何在满足个性化隐私需求的同时保持轨迹数据可用性，仍是当前研究的关键问题。

针对上述问题，本文提出了一种基于Laplace机制的个性化动态轨迹隐私保护（personalized dynamic privacy trajectory protection, PDPTP）方法。该方法在统一的差分隐私框架下，引入模糊敏感度量化模型与动态隐私预算分配机制，根据位置语义敏感度和用户隐私偏好自适应调整扰动强度，从而在高敏感区域增强隐私保护，在低敏感区域保持数据可用性。实验结果表明，PDPTP在不同隐私预算条件下能够实现隐私保护与数据可用性的较优平衡，通过精确合理量化隐私泄露风险，有效提高加噪轨迹数据的可用性和抑制潜在的轨迹推断行为，为MEC环境中的轨迹共享与位置服务提供了可行的隐私保护方案。

本文的主要工作如下。

1) 提出了一种基于模糊数学的位置信息敏感度量化方法，融合位置点单元的客观语义属性与用户的主观隐私偏好，构建隶属度函数，对位置点敏感度进行量化评估，为个性化隐私保护提供理论支撑。

2) 为兼顾轨迹数据的可用性与隐私保护，综合考虑位置点的隐私等级及其与邻近敏感位置点的空间关系，设计了敏感距离因子模型与隐私预算权重分配机制，并基于Laplace机制实现动态轨迹扰动，在保障隐私安全的同时提高轨迹数据可用性。

3) 从理论层面，证明所提方案满足差分隐私约束，并对其隐私保护性与效用性进行了严格分析与论证。通过仿真实验，对比不同轨迹扰动方法在轨迹误差、平均空间偏移距离及聚类一致性等多个方面的综合性能。实验结果表明，在相同隐私保护强度条件下，本文方案加噪后轨迹数据的可用性更高，且在高隐私预算条件下仍能有效保护敏感位置的隐私安全，验证了其优越性与实用价值。

1　相关工作

针对移动用户在基于位置服务中可能暴露的时空轨迹隐私问题，国内外学者已开展了大量研究。现有轨迹隐私保护方法主要包括以下几类。

1) 基于匿名化与泛化的轨迹隐私保护方法。该类方法通过位置泛化、聚类及扰动等技术，使每条轨迹与至少$(k-1)$条其他轨迹在空间与时间维度上不可区分。Abul等[9]提出了一种基于共定位的(k,δ)−匿名模型和NWA算法，通过聚类与离群点

剔除提高发布效率，并缓解由定位误差和不确定性导致的位置模糊性问题。Hu等[10]提出了一种基于划分时间间隔的轨迹隐私保护方法，通过构建隐私要求矩阵并利用曼哈顿距离构建*k*-匿名集。该类方法结构简单，可降低身份泄露风险，但在高维稀疏轨迹数据环境下易遭受外部数据关联攻击。

2) 基于抑制与假数据的轨迹隐私保护方法。该类方法通过删除轨迹中的敏感位置点或生成虚假轨迹来混淆真实轨迹，从而实现隐私保护。Benarous等[11]提出了一种面向车联网的位置隐私保护方案，利用协作、混淆与静默3种机制，降低信标的可关联性。Bindschaedler等[12]进一步提出了基于统计特征的假轨迹生成模型，通过捕捉真实轨迹的地理与语义特征，提取轨迹移动模式，生成高相似度的合成轨迹以提升轨迹数据可用性。该类方法能有效防止敏感信息泄露，但抑制会破坏轨迹的连续性，且假数据难以保持真实统计特性，计算代价较高，不易在大规模应用场景中推广。

3) 基于差分隐私的轨迹扰动方法。差分隐私以严格的数学定义为数据发布提供可量化的隐私保障，主要分为集中式和本地式两类。集中式差分隐私由可信服务端统一注入噪声并发布结果；本地式差分隐私则基于分布式架构在本地对数据进行隐私处理，避免第三方服务器介入造成隐私泄露。Jiang等[13]提出了基于指数机制加噪的SDD算法，利用移动对象的速度约束，在每个位置点选择下一位置的方向与距离。陈思等[6]提出了一种融合时空采样与双重差分隐私扰动的混合模型，增强对强背景知识攻击的鲁棒性。Sun等[14]提出了SPRT轨迹数据生成方法，将公开的地理结构信息融入差分隐私轨迹合成过程，以同时保留数据集的整体统计分布与个体移动模式。面向离线轨迹数据发布场景，Sun等[15]提出了UdpTrace方案，通过效用感知的差分隐私噪声分配提升轨迹发布后的查询可用性，并在扰动过程中引入区域聚合降低隐私损失。总体来看，差分隐私类方法在理论上能够提供严格的隐私保护，但多数方法采用静态或统一的隐私预算分配策略，忽视位置点敏感性与用户隐私偏好差异，易导致高敏感区域隐私保护不足或低敏感区域过度扰动，进而影响轨迹数据的可用性。

4) 融合位置语义与个性化的轨迹隐私保护方法。近年来，轨迹差分隐私研究在时间相关性建模、语义感知扰动与个性化隐私预算等方面取得了新的进展。文献[16]提出了一种个性化差分隐私发布机制，基于Hilbert曲线提取空间特征并对位置进行聚类，结合抽样和指数机制选取代表位置，实现个性化隐私预算分配。文献[17]提出了相关性Laplace机制，通过生成与原轨迹自相关一致的相关性噪声实现平滑扰动。Yang等[18]针对智能物流中的卡车轨迹隐私问题，提出了一种结合位置泛化与局部微分扰动的隐私保护方法。考虑车辆访问不同位置频率的差异性，Zhong等[19]提出了一种基于车辆移动规律性的个性化位置隐私保护方法。Cao等[20]提出了一种结合时间相关性建模的个性化差分隐私轨迹保护方法，其主要关注时间维度，利用连续访问点的时序依赖增强抗推断能力。Cao等[21]提出了TCPP机制，结合Hilbert曲线与地理同质性建模，实现了在轨迹关联约束下的差分隐私保护。Cao等[22]关注时间相关性下的个性化差分隐私轨迹保护，利用时序依赖构建隐私预算自适应调控机制，提高了在高关联轨迹场景中的鲁棒性。上述方法虽提升了轨迹隐私保护的灵活性与可用性，但多考虑单一因素，缺乏对敏感位置空间分布的动态适应能力，难以兼顾高敏感区域隐私安全与低敏感区数据可用性。

综上，现有方法虽然在匿名化、抑制、假轨迹生成以及差分隐私扰动等方面取得阶段性进展，但普遍存在个性化适应能力不足、隐私预算分配静态固化以及对高敏感区域隐私保护不充分等问题。鉴于上述不足，本文提出了一种基于差分隐私的个性化动态轨迹隐私保护方法，融合位置语义与用户隐私偏好，构建基于模糊数学的敏感度量化模型，实现自适应分配隐私预算和差异化Laplace加噪，在强化高敏感区域隐私保护的同时保持整体轨迹数据的可用性，从而实现隐私与效用的动态平衡。

2 系统模型

2.1 MEC系统架构

本文提出的个性化动态轨迹隐私保护方法适用于MEC环境下的LBS场景，其主要目标是在保障用户轨迹隐私安全的前提下，提高轨迹数据的可用性与服务响应效率。轨迹隐私保护系统由用户终端、边缘服务器和服务提供商3个核心实体组成，系统架构如图1所示。三者协同工作，共同完成轨

迹数据的采集、隐私保护与服务响应，构成完整的个性化动态轨迹隐私保护体系。在该架构下，用户轨迹数据在边缘侧完成隐私保护与动态扰动处理，而非直接上传至云端进行集中存储和分析。这种“边缘保护-云端服务”的协同架构在差分隐私机制的支撑下，能够有效防止攻击者通过轨迹数据重构推测用户的真实位置，实现对轨迹数据的强隐私保护与高可用性保障。

用户终端一般包括智能手机、可穿戴设备或车载导航系统等设备，具备高精度的定位感知与通信能力。当用户使用导航、社交或出行类应用时，终端会根据时间间隔或位移阈值采集用户的轨迹数据（GPS坐标和时间戳），并通过安全信道将该数据上传至边缘服务器。用户可通过终端发起基于位置的查询请求（如周边兴趣点或医院资源查询）或路径规划等服务。由于轨迹数据中包含用户的地理位置、时间信息和交互上下文，具有较高的敏感性，因此需在上传前进行加密与隐私标识处理，以降低在传输过程中面临的恶意窃取或关联分析风险。

边缘服务器部署在靠近用户的网络接入节点处，是实现轨迹隐私保护与语义增强的关键计算单元。首先，边缘服务器接收并预处理用户上传的原始轨迹数据，识别轨迹中的关键点并提取空间特征。随后，根据位置点所属区域的语义属性与敏感等级，计算其隐私权重，并依据模糊敏感度量化模型动态分配隐私预算。为进一步提升数据效用，边缘服务器引入位置语义映射机制，将轨迹点映射为语义特征向量$\overrightarrow{\text{Semi}}$，标注其语义类别（如教育机构、商业设施和医疗机构等功能区域），并依据Laplace机制生成加噪后的轨迹数据。最终，加噪处理后的轨迹数据被传递至服务提供商进行后续服务响应。

服务提供商通常为地理信息系统（geographic information system, GIS）或基于位置的服务平台，位于中心云端，负责数据存储、管理及服务响应。其主要任务是根据边缘服务器传输的加噪轨迹数据，执行用户请求的服务功能，如路径规划、兴趣点推荐或交通流量预测等。服务提供商不直接接触用户的原始轨迹数据，而是通过与边缘服务器的协同机制，在保障隐私安全的前提下提供高质量的位置服务响应。该机制可有效降低原始轨迹数据在中心云端聚集所带来的隐私泄露风险，提升系统的安全性、实用性和可扩展性。

在本文的MEC场景中，轨迹隐私保护机制部署于边缘节点侧，负责对用户按时间连续性划分的轨迹段进行本地预处理、敏感度评估和加噪处理，以避免高精度位置直接上传至中心云端，降低通信与隐私风险。该过程由产生轨迹的边缘节点独立完成，符合实际MEC系统基于地理位置或接入点调度任务的模式，可有效减少跨节点协同开销。考虑到实际MEC环境中的节点可能因负载、网络或设备故障发生动态加入或退出，导致局部拓扑与轨迹分布变化，本文进一步模拟了边缘节点随机失效情形，以评估PDPTP在拓扑扰动下的稳定性与适配性。

2.2　相关定义

本节介绍本文中涉及的基本概念及相关性质，所用符号如表1所示。

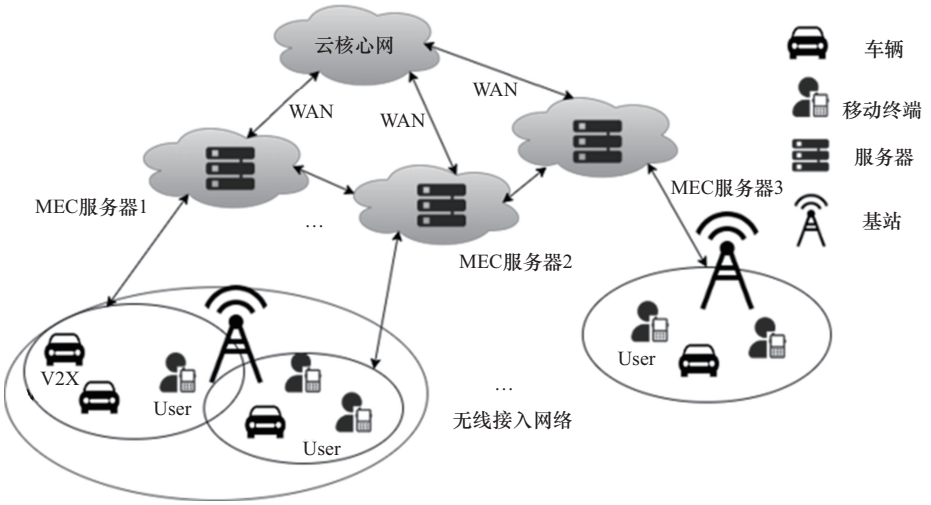

图1　MEC系统架构

表1 符号说明

符号	含义
D	若干条轨迹构成的轨迹数据集
D'	与D仅相差一条轨迹的邻近轨迹数据集
N	轨迹数据集包含的用户个数
m	用户轨迹拆分为若干个子轨迹段个数
n	轨迹序列中包含的轨迹点数
T	用户的原始轨迹
T'	用户的发布轨迹
p_i	轨迹数据集中第i个位置点的坐标及时间戳
x	用户对敏感位置点单元的隐私需求
$\mathrm{SL}_{\mathrm{obj}}$	位置点单元的客观敏感等级
$\mathrm{SL}_{\mathrm{user}}$	用户对于位置点单元的主观敏感等级
SL_k	敏感位置点单元k的综合语义敏感等级
pl_k	敏感位置点单元k的历史查询概率
S_k	敏感位置点单元k的综合敏感度
d_i	轨迹点p_i与最邻近敏感位置点单元k之间的距离
λ	敏感因子D_i受d_i影响的衰减系数
D_i	第i个轨迹点对应的敏感距离因子
ε	用户设定的轨迹总隐私预算
Δf	差分隐私全局敏感度

2.2.1 差分隐私

定义1 相邻数据集[23]。设有两个属性结构相同的数据集D和D'，其对称差数据集记为$D\Delta D'$，对称差数据集的个数记为$|D\Delta D'|$，若$|D\Delta D'|=1$，则称D和D'为相邻数据集。相邻数据集的定义用于描述数据库中仅包含单条记录差异的情况，是差分隐私理论的基础。

定义2 ε–差分隐私[23]。设D和D'为一对相邻数据集，M为随机化算法，且$\mathrm{Range}(M)$表示随机化算法M的输出范围。若随机化算法M在数据集D和D'上任意输出结果$O\in\mathrm{Range}(M)$满足式(1)，则随机化算法M满足ε–差分隐私。

$$\frac{\Pr\left(M(D)=O\right)}{\Pr\left(M(D')=O\right)}\leqslant\exp(\varepsilon) \tag{1}$$

其中，ε为隐私预算，用于衡量随机化算法M的隐私保护强度，ε越小，隐私保护强度越高，数据隐私性越好，但数据可用性相对降低；反之，ε越大，数据可用性越高。

定义3 全局敏感度[23]。在差分隐私机制中，全局敏感度用于度量某一查询函数对输入数据微小变动的敏感程度。设有函数$f: D\rightarrow R_d$，表示将数据库映射为d维实数向量，则其全局敏感度定义为

$$\Delta f=\max_{D,D'}\|f(D)-f(D')\|_1 \tag{2}$$

其中，D和D'表示任意一对相邻数据集，$\|\cdot\|_1$表示一阶范数距离。全局敏感度决定噪声注入强度，是差分隐私机制设计的关键参数。在轨迹隐私保护中，轨迹点通常表示为二维或多维空间中的位置坐标，其变化特性与距离度量方式密切相关。为适应MEC环境下的空间组织结构和差分隐私噪声机制，本文在轨迹扰动过程中采用一阶范数度量位置变化，相关依据将在后文进一步说明。

2.2.2 轨迹数据集

在轨迹隐私保护问题中，研究目标是在保证轨迹数据可用性的前提下，实现差分隐私保护。设轨迹数据集为$T=\{T_1,T_2,\cdots,T_N\}$，每个$T_{\mathrm{U}}=\{p_1,p_2,\cdots,p_n\}$表示用户U的轨迹序列。轨迹点$p_i$定义为三元组$p_i=(x_i,y_i,t_i)$，其中$(x_i,y_i)$为第$i$个轨迹点的经纬度坐标，$t_i$为时间戳。为实现个性化隐私保护，需构建隐私预算分配函数$B: p_i\rightarrow\varepsilon_i$，其中，$\varepsilon_i$表示分配给轨迹点$p_i$隐私预算，满足$\sum_{i=1}^{n}\varepsilon_i\leqslant\varepsilon$。

位置语义信息是指用于描述空间位置所具备功能属性的高层语义特征，通常与用户的行为模式及其所处地理空间中的功能区域密切相关。通过分析轨迹点位置对应的地理语义信息，能够推断用户在特定时间段内的活动意图和行为场景[24]。

本文通过将轨迹点的经纬度坐标(x_i,y_i)与GIS中预定义的功能区域进行空间匹配，确定其对应的位置语义类别，实现从几何空间到语义信息的映射。在此基础上，结合用户历史轨迹数据进行统计分析，提取用户频繁访问区域类型及行为偏好的语义特征，并将其作为后续敏感度量化与个性化隐私建模的重要输入。

假设轨迹数据库中每个位置点的空间位置为$d_i=(x_i,y_i)$，则该位置的语义表征可由特征向量$\overrightarrow{\mathrm{Semi}}=\{s_{i1},s_{i2},\cdots,s_{iq}\}$表示，其中$q$为关键语义特征数量。每个语义特征$\mathrm{s}_{ij}$为二值属性，当该位置具有特定语义属性时，$s_{ij}=1$；反之，$s_{ij}=0$。单个轨迹中所有位置点对应的特征向量构成的语义特征矩阵为

$$\boldsymbol{S}=\begin{bmatrix} s_{11} & s_{12} & \cdots & s_{1q} \\ s_{21} & s_{22} & \cdots & s_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m1} & s_{m2} & \cdots & s_{mq} \end{bmatrix} \tag{3}$$

其中，行表示位置点，列表示语义特征维度。

2.2.3　历史查询概率

历史查询概率用于度量轨迹数据库中给定位置点单元的访问频率，反映用户在特定区域内的历史访问行为模式，其计算方式为该位置点单元被访问次数与全部访问次数之比。设轨迹数据集为D，包括一系列用户访问的地理位置点单元。对于给定的敏感位置点单元s_j，其历史查询概率计算式为

$$\text{freq}_j=\frac{N_j}{\sum_{j=1}^{|\text{Geoset}|}N_j} \tag{4}$$

其中，N_j表示敏感位置点单元s_j的访问次数，|Geoset|表示区域内全部地理位置单元的集合规模，其大小相当于该区域轨迹数据集中访问的位置总数。

2.2.4　敏感距离因子

为更准确地描述轨迹点与高敏感位置的空间关联程度，本文定义敏感距离因子（sensitivity distance factor, SDF）。设位置点p_i到最近敏感位置点p_k的欧式距离$d_i=\|p_i-p_k\|_2$，则敏感距离因子可通过指数衰减函数计算，其计算式为

$$D_i=\exp\left[-\lambda\left(d_i-d_\theta\right)\right] \tag{5}$$

其中，$\lambda>0$为衰减系数，用于控制距离对敏感度的非线性影响，d_θ是设定的最小敏感距离，超出此值则忽略空间关联性。当d_i较小时，$D_i\approx 1$表示强敏感区域；当d_i较大时，D_i迅速衰减至接近0，表示低敏感区域。

3　基于Laplace机制的动态轨迹扰动算法

为满足MEC环境下用户个性化隐私保护需求，本文提出了一种基于位置语义敏感度量化与差分隐私扰动的动态轨迹隐私保护方案。该方案在差分隐私统一框架下实现了语义感知、动态预算分配与差异化扰动的有机结合，旨在保障隐私安全的同时提升轨迹数据的可用性与服务质量。PDPTP总体流程如图2所示，主要包括位置点敏感度量化与动态轨迹扰动两个阶段。其中，第一阶段构成敏感度建模子算法（算法1），用于对轨迹中各位置点进行多维度隐私敏感度评估；第二阶段构成动态轨迹扰动子算法（算法2），根据敏感度评估结果实现轨迹点级别的差异化差分隐私保护。

3.1　基于模糊数学的位置点单元敏感度量化算法

敏感度量化算法旨在通过融合位置语义属性与用户隐私偏好，计算轨迹中各位置点单元的综合敏感度，用于后续动态隐私预算分配。

3.1.1　敏感等级量化

在现实环境中，不同功能区域对用户隐私的重要性存在显著差异，如住宅区、医院等区域通常包含较高的隐私敏感信息，而公园、商圈等公共区域的隐私敏感度则相对较低。为量化不同区域的隐私敏感程度，本文定义位置点单元d_k所对应的语义类型为$C(d_k)$，其客观敏感等级SL_{obj}定义为

$$\text{SL}_{\text{obj}}=\text{Sem2Level}\left(C\left(d_k\right)\right) \tag{6}$$

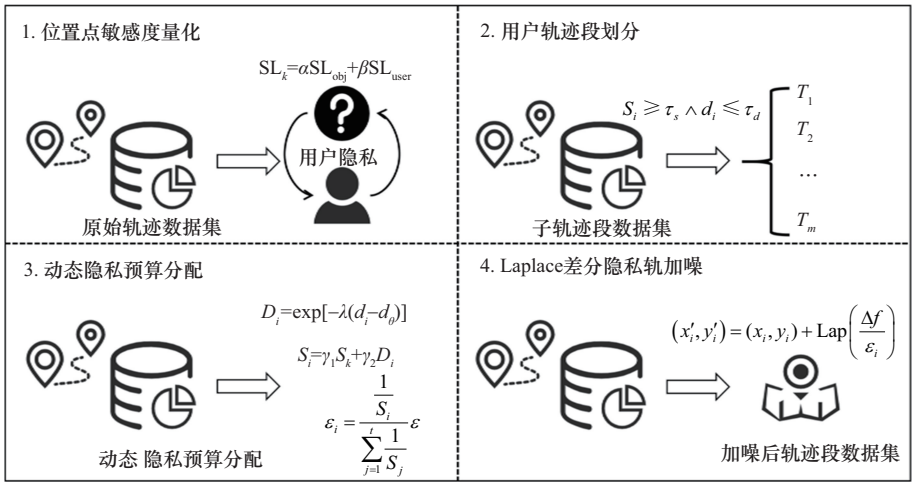

图2　PDPTP总体流程

其中，Sem2Level(·)为语义类型到敏感等级的映射函数，用于将位置点的语义类别转化为标准化的客观语义敏感等级值。

然而，仅依赖客观语义特征难以全面反映不同用户对同一语义区域的隐私感知差异，不同用户在隐私偏好上存在显著差异。为刻画用户主观隐私需求，本文引入模糊隶属度函数对用户隐私偏好进行量化建模，将用户对位置点单元的主观隐私判定映射为不同等级的隶属程度。相比线性归一化仅以单一变量表示偏好强度，以及分段函数的阈值映射方式，模糊隶属度函数能够描述用户隐私偏好在不同敏感等级之间的连续隶属关系，使主观敏感度随用户隐私偏好平滑变化，从而提升个性化隐私保护策略的表达能力与稳定性。设用户对位置点单元d_k的隐私敏感度判定值为$x \in [0,1]$，则其主观敏感等级$\mathrm{SL}_{\mathrm{user}}$通过模糊隶属度函数$F_{\mathrm{level}}(x)$进行计算。根据不同敏感级别（高、中、低）定义隶属度函数为

$$F_l(x)=\begin{cases}1, & 0\le x\le l\\ \dfrac{m-x}{m-l}, & l<x<m\\ 0, & m\le x\le 1\end{cases} \tag{7}$$

$$F_m(x)=\begin{cases}0, & 0\le x\le l\\ \dfrac{x-l}{m-l}, & l<x\le m\\ \dfrac{h-x}{h-m}, & m<x<h\\ 0, & h\le x\le 1\end{cases} \tag{8}$$

$$F_h(x)=\begin{cases}0, & 0\le x\le m\\ \dfrac{x-m}{h-m}, & m<x<h\\ 1, & h\le x\le 1\end{cases} \tag{9}$$

其中，$F_{\mathrm{level}}(x)\in[0,1]$，表示用户主观判断$x$与相应敏感级别之间的隶属程度。$h=0.7$，$m=0.5$，$l=0.2$。隶属度值越大，表明用户对该位置点单元的隐私关注程度越高。最终，取最大隶属度对应的敏感级别作为用户的主观敏感等级$\mathrm{SL}_{\mathrm{user}}$。

为保证映射的稳定性与可解释性，隶属度函数满足单调性与有界性约束，且各敏感等级之间保持连续过渡。在实际应用中，用户隐私偏好由终端侧隐私设置生成，并归一化至区间[0,1]后用于计算主观敏感等级。当用户未显式配置时，系统采用默认偏好初始化，从而在不依赖数据集标签的情况下实现个性化隐私保护。

通过上述定义，本文在统一的模糊数学框架下实现了用户主观隐私感知与客观语义敏感度的定量化建模，为后续的综合敏感度计算奠定基础。

3.1.2 综合敏感度计算

为实现位置点隐私敏感度的细粒度量化，本文构建了一种基于动态权重分配的双因素融合模型，在语义特征与用户隐私偏好之间实现协同计算，从而获得更具代表性和差异化的综合敏感等级。该模型主要由两个阶段组成：1) 语义与偏好的融合建模；2) 历史查询概率的修正加权。通过双层融合机制，模型能够在不同位置点之间形成更合理的敏感度刻画，为后续的个性化隐私预算分配提供更准确的量化依据。其中，综合语义敏感等级刻画语义与偏好融合后的等级结果，综合敏感度进一步融合历史访问特征用于后续个性化隐私预算分配，二者均不同于噪声校准所需的全局敏感度Δf。

设位置点单元的客观语义敏感度为$\mathrm{SL}_{\mathrm{obj}}\in[0,1]$，用户主观敏感等级为$\mathrm{SL}_{\mathrm{user}}\in[0,1]$，则其综合语义敏感等级$\mathrm{SL}_k$的计算式为

$$\mathrm{SL}_k=\alpha\mathrm{SL}_{\mathrm{obj}}+\beta\mathrm{SL}_{\mathrm{user}} \tag{10}$$

其中，α和β分别表示客观语义属性与主观隐私偏好的权重系数。为确保两者在不同敏感场景下的动态平衡，本文设计自适应权重分配函数为

$$\alpha=\frac{\mathrm{SL}_{\mathrm{obj}}}{\mathrm{SL}_{\mathrm{obj}}+\mathrm{SL}_{\mathrm{user}}},\beta=\frac{\mathrm{SL}_{\mathrm{user}}}{\mathrm{SL}_{\mathrm{obj}}+\mathrm{SL}_{\mathrm{user}}} \tag{11}$$

通过式(11)可实现语义与偏好的协同调节，当位置点语义敏感度较高时，提高α权重，强化对高敏感区域的隐私保护；反之，则增强用户个性化偏好的影响力。

若仅依赖位置点的敏感等级，仍可能存在潜在隐私泄露风险。在边缘服务器覆盖范围较大的服务场景中，若高敏感区域的访问频率显著低于部分低敏感区域，则攻击者可能利用非敏感区域的访问模式推断用户真实轨迹。为此，本文引入历史查询概率作为敏感度修正因子，以刻画位置点在用户历史行为中的相对暴露程度。该概率通过对历史轨迹中位置点访问频率的统计进行估计，计算开销较低，可在不显著增加系统负担的情况下补充语义敏感度信息。设pl_k为位置点单元i的历史查询概率，则该位置点单元的最终综合敏感度S_k定义为

$$S_k=w_1\mathrm{SL}_k+w_2\mathrm{pl}_k \tag{12}$$

其中，w_1和w_2分别表示综合语义敏感等级与历史查询概率的权重因子，两者的取值关系通过模糊矩阵$\boldsymbol{R}$确定。

模糊矩阵$\boldsymbol{R}=(r_{ij})_{n\times n}$用于表征敏感级别与历史查询概率之间的相对重要性。矩阵元素r_{ij}的取值依据系统需求定义为

$$r_{ij}=\begin{cases}0, & \text{pl更重要}\\ 0.5, & \text{两者重要性一致}\\ 1, & \text{SL更重要}\end{cases} \tag{13}$$

为避免主观赋值带来的不一致性，本文采用逻辑一致性变换，将模糊矩阵$\boldsymbol{R}$转换为一致矩阵$\boldsymbol{M}=(m_{ij})_{n\times n}$，其定义为

$$m_{ij}=\frac{m_i-m_j}{2n}+0.5 \tag{14}$$

其中，$m_i=\frac{1}{n}\sum_{j=1}^{n}r_{ij}$为矩阵$\boldsymbol{R}$第$i$行均值，$m_j=\frac{1}{n}\sum_{i=1}^{n}r_{ij}$为第$j$列均值。根据一致矩阵$\boldsymbol{M}$，权重系数$w_1$与$w_2$的计算式分别为

$$w_1=\frac{\sum_{j=1}^{n}m_{ij}-0.5}{\sum_{i=1}^{n}\left(\sum_{j=1}^{n}m_{ij}-0.5\right)} \tag{15}$$

$$w_2=\frac{\sum_{i=1}^{n}m_{ij}-0.5}{\sum_{j=1}^{n}\left(\sum_{i=1}^{n}m_{ij}-0.5\right)} \tag{16}$$

综合上述内容，基于模糊数学的位置点单元敏感度量化算法如算法1所示。

算法1　基于模糊数学的位置点单元敏感度量化

输入　i、$\mathbb{S}_{\mathrm{U}}$、x、pl_k

输出　位置点单元k的综合敏感度S_k

1) 用户U构建敏感位置语义集合：$\mathbb{S}_{\mathrm{U}}=\left\{(t_1,d_1),(t_2,d_2),\cdots,(t_s,d_s)\right\}$
2) 计算位置点单元客观敏感等级$\mathrm{SL}_{\mathrm{obj}}\leftarrow d_k$
3) 根据模糊函数分别计算$F_l(x)$、$F_m(x)$和$F_h(x)$
4) $F_i\leftarrow\max(\max(F_l(x),F_m(x)),F_h(x))$
5) switch$\left(F_{\mathrm{level}}\right)$
6) case $F_l(x)$
7)　　$\mathrm{SL}_{\mathrm{user}}\leftarrow l$
8)　　break
9) case $F_m(x)$
10)　$\mathrm{SL}_{\mathrm{user}}\leftarrow m$
11)　break
12) case $F_h(x)$
13)　　$\mathrm{SL}_{\mathrm{user}}\leftarrow h$
14)　　break
15) end switch
16) 计算权重系数α和β
17) $\mathrm{SL}_k\leftarrow\alpha\mathrm{SL}_{\mathrm{obj}}+\beta\mathrm{SL}_{\mathrm{user}}$
18) 建立模糊矩阵$\boldsymbol{R}$
19) 建立模糊一致矩阵$\boldsymbol{M}$
20) 计算得出权重因子和w_1和w_2
21) $S_k\leftarrow w_1\mathrm{SL}_k+w_2\mathrm{pl}_k$
22) return S_k

3.2　基于Laplace差分隐私的个性化轨迹扰动算法

本节介绍个性化轨迹隐私保护方法的实现步骤，包括轨迹段划分、动态隐私预算分配与Laplace加噪3个核心环节。该算法以Laplace机制为基础，结合位置语义敏感信息与用户个性化隐私偏好，实现对轨迹数据的差异化扰动，以在保证隐私安全的前提下最大化轨迹数据可用性。

性质1　串行组合[25]。数据集D上有一组差分隐私算法序列$A_1(D),A_2(D),\cdots,A_m(D)$，其中每个算法$A_i(D)$分别满足$\varepsilon_i$-差分隐私，且任意两个算法的随机过程相互独立，则组合算法满足$\sum\varepsilon_i$-差分隐私。该性质表明，当多个差分隐私算法顺序作用于同一数据集时，其整体隐私泄露水平等价于各阶段隐私预算的累积值。因此，在轨迹扰动过程中，对子轨迹段分配独立隐私预算可确保整体轨迹满足ε-差分隐私约束。

对任意轨迹段$T_j=\{p_1,p_2,\cdots,p_n\}$，需要加噪的轨迹点集合$Z_j$定义为

$$Z_j=\left\{p_i\,\middle|\,i\in[1,m],S_i\geqslant\tau_s\wedge d_i\leqslant\tau_d\right\} \tag{17}$$

其中，S_i为轨迹点p_i的隐私敏感度，基于其邻近敏感位置单元的敏感等级计算获得；$d_i=\min_k\|p_i-\mathrm{POI}_k\|_2$为轨迹点$p_i$与最邻近敏感位置点（如医院、住宅区）的欧氏距离；$\tau_s$与$\tau_d$分别为敏感度与距离阈值。当轨迹点的敏感度超过阈值且其距离接近敏

感区域时，将其标记为需加噪点。该策略能够有效识别高风险位置点，并对关键位置实施重点保护，从而抑制基于地理语义的轨迹反推攻击。

步骤1 轨迹段划分。为实现隐私预算在轨迹扰动过程中的合理分配，首先对原始轨迹T进行时空划分，将完整的轨迹序列分解为若干子轨迹段集合$\{T_1,T_2,\cdots,T_m\}$。划分过程中综合考虑时间约束、空间约束和轨迹查询长度约束3项条件，保证划分的合理性与一致性。设轨迹段$T_j=\{p_1,p_2,\cdots,p_n\}$，每个轨迹点$p_i$由经纬度坐标、时间戳及位置语义等信息组成，则轨迹段划分满足$\Delta t \leqslant t_\theta$，$\mathrm{Dist}(T_j) \leqslant d_\theta$，其中，$\Delta t$表示相邻轨迹点间的时间间隔，$\mathrm{Dist}(T_j)$表示轨迹段的空间跨度，$t_\theta$与$d_\theta$分别表示时间与空间阈值。该时空约束过程能够避免轨迹段内部出现明显的行为模式突变，从而符合轨迹时空连续性假设。同时，查询长度约束保证各子轨迹段的隐私预算分配满足串行组合定理。

步骤2 动态隐私预算分配。若对轨迹点采用统一加噪处理，虽能够提供一定的隐私保护，但其忽略了位置点的语义差异与空间关联特性，容易导致高敏感区域隐私保护不足或低敏感区域过度扰动，影响轨迹数据可用性。为此，本文在差分隐私框架下引入动态隐私预算分配机制，其核心思想是依据位置点的语义敏感度与空间距离因素自适应调整扰动强度。设用户在某一时间段内的轨迹为$T_j=\{p_1,p_2,\cdots,p_n\}$，每个轨迹点$p_i$对应的隐私敏感度$S_i$定义为

$$S_i=\gamma_1 S_k+\gamma_2 D_i \tag{18}$$

其中，S_k为轨迹点p_i最邻近敏感位置点单元k的综合敏感度（见3.1节定义），D_i为该轨迹点与最近敏感位置之间的敏感距离因子（见2.2节定义），γ_1和γ_2分别为控制两项影响程度的权重参数。

在传统的隐私分配模型中，隐私预算ε与隐私保护强度呈负相关关系。因此，为保证动态隐私预算分配方向与隐私保护目标一致，本文采用对敏感度的倒数进行加权分配，使高敏感轨迹点获得更小的隐私预算，从而在扰动阶段注入更强噪声。总隐私预算ε按敏感度进行加权分配的计算式为

$$\varepsilon_i=\frac{\frac{1}{S_i}}{\sum_{j=1}^{t}\frac{1}{S_j}}\varepsilon \tag{19}$$

其中，ε_i为轨迹点p_i分配的隐私预算，ε为轨迹段的总隐私预算。当S_i较大时，ε_i较小，轨迹点将获得更强的隐私保护；当S_i较小时，ε_i较大，以保证数据可用性。最后，需要对所有用户位置的隐私敏感度权重进行归一化，以满足$\sum_{i=1}^{n}\varepsilon_i \leqslant \varepsilon$的总隐私预算约束，确保生成的位置权重可以准确反映各种语义信息的相对重要性。

步骤3 Laplace加噪。

定理1 Laplace机制[26]。给定轨迹数据集D，对于任意查询函数$f: D \to R_d$，其全局度为Δf，若函数输出满足式(20)，则随机化算法M满足ε-差分隐私。

$$M(D)=f(D)+\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right) \tag{20}$$

其中，$\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon}\right)$表示服从均值为0、尺度为$\frac{\Delta f}{\varepsilon}$的Laplace分布随机噪声，其噪声大小与全局敏感度Δf成正比，与隐私预算ε成反比。

Laplace机制通过在查询结果中注入符合特定分布的随机噪声，使任意两个相邻数据集D与D'的输出概率分布差异受限，从而在统计上掩盖单个轨迹点对整体结果的影响，有效提升隐私保护强度。假设用户当前发起服务请求的位置点单元为i，其真实位置坐标为(x_i,y_i)。在保证轨迹数据可用性的前提下，利用差分隐私预算分配结果对轨迹点进行个性化加噪，扰动过程定义为

$$(x_i',y_i')=(x_i,y_i)+\mathrm{Lap}\left(\frac{\Delta f}{\varepsilon_i}\right) \tag{21}$$

其中，ε_i表示分配给第i个位置点的隐私预算，满足$\sum_{i=1}^{n}\varepsilon_i \leqslant \varepsilon$。由于$\varepsilon_i$已结合位置点的敏感度、历史查询概率及空间距离因子进行动态调整，噪声尺度$\frac{\Delta f}{\varepsilon}$可实现空间层与语义层的双重自适应。

当轨迹点位于高敏感区域时，ε_i较小，噪声强度增大，隐私保护增强；反之，当轨迹点位于低敏感区域时，ε_i相对较大，噪声幅度减弱，从而更好地保持轨迹空间连续性与服务响应效果，实现隐私性与可用性之间的平衡。此外，由于该扰动机制不涉及深度模型推断与迭代优化，其执行复杂度随查询长度线性增长，可在边缘节点实时完成隐私扰动

处理，提升MEC侧部署与响应效率。

考虑到MEC环境下的轨迹数据主要来自城市道路网络或规则化网格区域，其空间移动路径通常受到道路结构与路网拓扑的约束，位置变化在水平与垂直方向上呈现离散叠加特征。与欧式距离相比，曼哈顿距离能够更准确地刻画此类网格化空间中位置点之间的真实移动代价。因此，本文采用曼哈顿距离作为轨迹位置变化的衡量标准，并基于当前位置集合来描述全局敏感度Δf，其计算式为

$$\Delta f = \max_{1 \leqslant i,j \leqslant n} \left(\left| x_i - x_j \right| + \left| y_i - y_j \right| \right) \tag{22}$$

综上所述，基于Laplace差分隐私的轨迹扰动算法如算法2所示。

算法2　基于Laplace差分隐私的动态轨迹扰动

输入　ε、(x_i,y_i)、(x_k,y_k)

输出　扰动后的轨迹位置点单元(x_i',y_i')

1) 确定轨迹点对应最邻近敏感位置点单元k的综合敏感度S_k

2) 计算敏感距离因子D_i

3) 通过模糊矩阵数学模型求得权重因子γ_1和γ_2

4) 计算轨迹点i的隐私敏感度S_i

5) 为轨迹点i分配差分隐私预算ε_i

6) 获取历史位置数据集合$\mathbb{L}_i$

7) 计算全局敏感度Δf

8) $\left(x_i',y_i'\right) \leftarrow \left(x_i,y_i\right) + \mathrm{Lap}\left(0, \dfrac{\Delta f}{\varepsilon}\right)$

9) return (x_i',y_i')

4　隐私分析

4.1　差分隐私性质证明

证明1　本文提出的轨迹隐私保护方案满足ε-差分隐私。

设两个相邻数据集D与D'仅在一条轨迹T_{real}上存在差异，即$D' = D \cup \{T_{\mathrm{real}}\}$。算法$A(D)$表示对数据集中每条轨迹进行处理，对轨迹中的每个位置点$\left(x_i,y_i\right)$添加独立的Laplace噪声$\mathrm{Lap}(b)$，输出扰动后的轨迹数据集。其中，噪声尺度b与全局敏感度Δf及隐私预算ε_i的关系定义为$b = \dfrac{\Delta f}{\varepsilon}$。对于包含$n$个位置点的单条轨迹，算法根据每个位置点的敏感度动态分配隐私预算ε_i，同时满足隐私预算组合约束$\sum_{i=1}^{n} \varepsilon_i \leqslant \varepsilon$。

根据差分隐私定义，需证明对任意输出结果$T' \in \mathrm{Range}(A)$，输出概率密度比满足

$$\frac{\Pr\left[A(D) = T'\right]}{\Pr\left[A(D') = T'\right]} \leqslant e^{\varepsilon} \tag{23}$$

根据拉普拉斯概率密度函数

$$\Pr\left[\mathrm{Lap}(b) = x\right] = \frac{1}{2b} e^{-\frac{|x|}{b}} \tag{24}$$

相邻数据集D与D'的轨迹扰动后联合概率密度比表示为

$$\begin{aligned}
&\frac{\Pr\left[A(D) = T'\right]}{\Pr\left[A(D') = T'\right]} = \\
&\prod_{i=1}^{k} \frac{\Pr\left[f(D)_i + \mathrm{Lap}\left(\dfrac{\Delta f}{\varepsilon}\right) = T_i'\right]}{\Pr\left[f(D')_i + \mathrm{Lap}\left(\dfrac{\Delta f}{\varepsilon}\right) = T_i'\right]} = \\
&\prod_{i=1}^{k} \frac{e^{-\frac{\varepsilon}{\Delta f}|T_i' - f(D)_i|}}{e^{-\frac{\varepsilon}{\Delta f}|T_i' - f(D')_i|}} = \\
&\prod_{i=1}^{k} e^{\frac{\varepsilon}{\Delta f}\left(|T_i' - f(D')_i| - |T_i' - f(D)_i|\right)}
\end{aligned} \tag{25}$$

代入$b = \dfrac{\Delta f}{\varepsilon}$可得

$$\begin{aligned}
&\frac{\Pr\left[A(D)_i = T_i'\right]}{\Pr\left[A(D')_i = T_i'\right]} = \\
&\frac{e^{-\frac{\varepsilon}{\Delta f}|T_i' - f(D)_i|}}{e^{-\frac{\varepsilon}{\Delta f}|T_i' - f(D')_i|}} = e^{\frac{\varepsilon}{\Delta f}\left(|T_i' - f(D')_i| - |T_i' - f(D)_i|\right)}
\end{aligned} \tag{26}$$

由三角不等式$|T_i' - f(D')_i| - |T_i' - f(D)_i| \leqslant |f(D)_i - f\left(D'\right)_i|$进一步得

$$\begin{aligned}
&\frac{\Pr\left[A(D) = T'\right]}{\Pr\left[A(D') = T'\right]} \leqslant \\
&\prod_{i=1}^{k} e^{\frac{\varepsilon}{\Delta f}|f(D)_i - f(D')_i|} = e^{\frac{\varepsilon}{\Delta f}\sum_{i=1}^{k}|f(D)_i - f(D')_i|}
\end{aligned} \tag{27}$$

根据曼哈顿距离全局敏感度定义$\Delta f = \max\limits_{D,D'} \|f(D) - f(D')\|_1$，可得到$\sum\limits_{i=1}^{k}|f(D)_i - f(D')_i| \leqslant \Delta f$，最终得到

$$\frac{\Pr\left[A(D) = T'\right]}{\Pr\left[A(D') = T'\right]} \leqslant e^{\frac{\varepsilon}{\Delta f}\Delta f} = e^{\varepsilon} \tag{28}$$

因此，由ε-差分隐私定义可知，本文提出的轨迹加噪算法满足ε-差分隐私。

4.2 敏感位置隐私保护

为评估轨迹加噪算法在敏感区域的扰动效果，本文采用敏感位置附近轨迹点的平均空间偏移量作为经验性隐私指标，用于刻画加噪后轨迹的几何偏移程度。需要说明的是，平均空间偏移（average spatial displacement, ASD）并非差分隐私的形式化安全度量，其仅反映空间扰动强度。因此，ASD作为补充指标，与后续推理攻击的恢复精度联合用于评价隐私保护效果。ASD通过计算敏感位置单元周边轨迹点在加噪前后坐标的欧氏距离得到，平均偏移量越大，表示敏感区域空间不确定性越高，其计算式为

$$\mathrm{ASD}=\frac{1}{K}\sum_{j=1}^{K}\left(\frac{1}{n_j}\sum_{i=1}^{n_j}\sqrt{(x_{j,i}-x'_{j,i})^2+(y_{j,i}-y'_{j,i})^2}\right) \tag{29}$$

其中，K为敏感位置点的总数，n_j为第j个敏感位置点周边的轨迹点数量，$(x_{j,i},y_{j,i})$为第j个敏感点附近第i个轨迹点的原始坐标，$(x'_{j,i},y'_{j,i})$为其对应的加噪后坐标。

5 仿真实验

5.1 实验设置

为验证本文方法的有效性，基于真实轨迹数据开展了可用性与隐私保护性能评估。实验采用两个代表性轨迹数据集：T-drive数据集[27]和Geolife数据集[28]。T-drive数据集包含2008年2月北京市出租车的GPS轨迹数据。为提高数据质量并降低轨迹复杂度，实验对原始数据进行清洗与预处理，包括异常点剔除、重复点删除和等间隔采样处理，最终保留190 760个有效轨迹点作为实验样本。GeoLife数据集包含用户在步行、骑行和驾车等多种出行模式下的移动轨迹，属于用户多模态移动轨迹数据集，轨迹采样密度更高、运动形态更加多样。实验对GeoLife数据集进行60 s等间隔下采样，并随机筛选约1/3的用户，最终获得185 614个有效轨迹点作为实验样本。两个数据集在后续实验中均采用一致的数据清洗、轨迹切分和网格化映射流程，以保证实验结果的可比性。

为模拟MEC环境下的服务结构，实验将研究区域划分为若干矩形网格，并以网格中心点作为空间特征计算的基础，用于获取历史查询概率与敏感度权重等参数。实验在Python 3.9环境下进行，硬件平台配置为Intel Core i7-13700H处理器、16 GB内存。实验将本文方法与DP-SPTP、PPBA[7]和SEITP[8]进行对比。其中，DP-SPTP为平均隐私预算分配机制，简称DPTP。所有实验重复5次取平均值，以降低随机因素的干扰。评估指标包括轨迹误差、平均偏移量及聚类一致性等，用于综合衡量扰动后轨迹数据的性能表现。

为保证实验的可复现性，本文对关键参数进行统一设置：差分隐私预算参数ε用于控制隐私保护强度，取值范围设为$\varepsilon\in[0.5,5.0]$。模糊敏感度量化模型的隶属度函数参数通过预实验选定，并在所有实验中保持一致。轨迹划分相关参数则根据数据集采样频率与轨迹连续性特征配置。由于T-drive与GeoLife数据集不包含用户隐私偏好标注，实验中对所有用户统一采用$x=0.5$作为主观偏好输入，以模拟默认隐私偏好场景，实际系统中该偏好可由用户侧按语义类别个性化配置。

5.2 评估指标

5.2.1 空间偏移度量

为量化加噪与原始轨迹在空间结构上的偏离程度，本文采用平均绝对误差（mean absolute error, MAE）、均方误差（mean square error, MSE）和平均Hausdorff距离（average Hausdorff distance, AHD）3个指标进行评估。设原始轨迹点为(x_i,y_i)，加噪轨迹点为(x'_i,y'_i)，轨迹点数为n，MAE与MSE分别定义为

$$\mathrm{MAE}=\frac{1}{n}\sum_{i=1}^{n}\sqrt{(x_i-x'_i)^2+(y_i-y'_i)^2} \tag{30}$$

$$\mathrm{MSE}=\frac{1}{n}\sum_{i=1}^{n}\left[(x_i-x'_i)^2+(y_i-y'_i)^2\right] \tag{31}$$

其中，MAE用于刻画局部偏移，MSE对轨迹整体结构更敏感。AHD用于度量轨迹形态的整体相似性，其定义为

$$\mathrm{AHD}=\frac{1}{2}\left(\mathrm{hd}(T,T')+\mathrm{hd}(T',T)\right) \tag{32}$$

其中，定向Hausdorff距离定义为$\mathrm{hd}(T,T')=\max\limits_{p\in T}\min\limits_{p'\in T'}\|p-p'\|_2$。

5.2.2 聚类一致性度量

为分析轨迹扰动对聚类结构的影响，本文采用调整兰德指数（adjusted Rand index, ARI）与聚类标签匹配率（accuracy, Acc）作为一致性评价指标。ARI的计算基于兰德指数（Rand index, RI）和随机期望值。

$$\mathrm{ARI}=\frac{\mathrm{RI}-\mathrm{Expected\ RI}}{\max(\mathrm{RI})-\mathrm{Expected\ RI}} \tag{33}$$

其中，RI的计算式为

$$\mathrm{RI}=\frac{a+b}{C(n,2)} \tag{34}$$

其中，a表示同簇正确匹配对的数量，b表示异簇正确匹配对的数量，$C(n,2)$表示样本对总数。

聚类标签匹配率用于衡量扰动前后样本聚类标签的一致性，其定义为

$$\mathrm{Acc}=\frac{1}{n}\sum_{i=1}^{n}\delta\left(L_i,L_i'\right) \tag{35}$$

其中，当且仅当样本i扰动前后的聚类标签一致时，$\delta(L_i,L_i')=1$，否则为0。

5.3　可用性评估

为评估不同轨迹扰动算法在数据可用性方面的表现，本文在多组隐私预算ε下基于T-drive数据集比较4种算法在轨迹误差、平均空间偏移及聚类一致性上的表现，结果如图3所示。由图3可知，随着隐私预算增大,各算法的误差指标均呈明显下降趋势，轨迹扰动幅度逐步减弱，呈现典型的隐私-可用性权衡关系。当隐私预算ε较小时，各算法需引入较大的噪声以满足隐私约束，从而导致误差升高。当隐私预算ε较大时，扰动幅度降低，轨迹结构稳定性显著改善。

由图3可知，PDPTP在多数隐私预算条件下的MAE与MSE均低于DPTP与PPBA，说明其基于个性化敏感度建模与差异化隐私预算分配的扰动方法，在误差控制方面具有更高的稳定性。相比之下，DPTP与PPBA采用全局统一或粗粒度的扰动机制，未能充分考虑不同轨迹点的敏感度差异，因而在低隐私预算条件下误差显著增大，导致轨迹局部几何结构破坏程度较高。SEITP通过基于语义邻域的替换式扰动有效维持了整体轨迹结构，但其未引入敏感度差异与个性化需求建模，在敏感区域隐私保护方面存在不足。在结构一致性方面，随着隐私预算提升，各方法的ARI和Acc指标均呈上升趋势，表明噪声削弱后轨迹类别结构逐渐稳定。PDPTP在不同隐私预算下的ARI均保持在较高水平，尤其在低隐私预算场景中显著优于DPTP与PPBA，体现出其在强隐私约束下仍具备良好的轨迹结构保持能力。DPTP与PPBA在低隐私预算下全局统一扰动导致局部空间结构损失，聚类一致性明显下降。SEITP在结构一致性指标上的表现较好，但其在高敏感区域隐私保护能力有限，且难以满足用户个性化隐私需求。总体来看，PDPTP在误差控制与结构一致性之

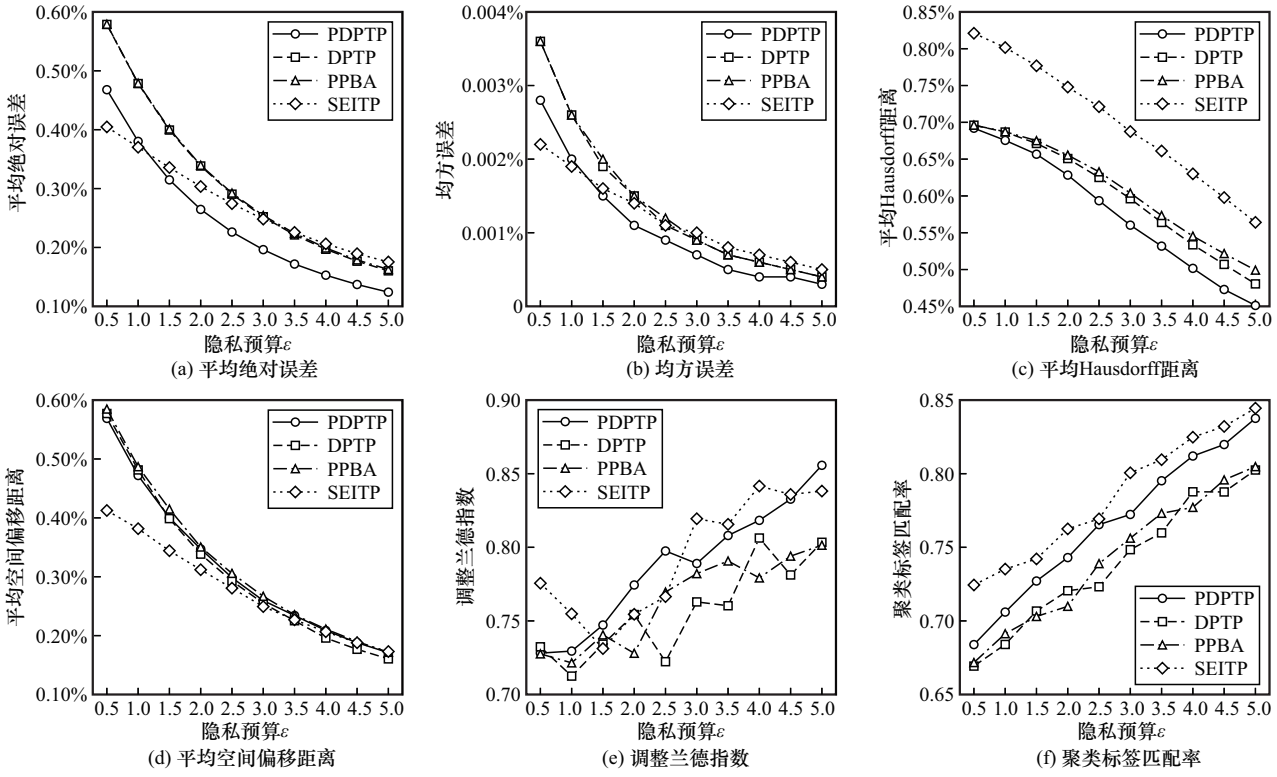

图3　T-drive数据集不同隐私预算下隐私保护性能对比

间取得了较为均衡的表现。在多组隐私预算下，其整体表现均优于DPTP与PPBA，且相较SEITP在敏感区域隐私保护和个性化需求满足方面更具优势。上述结果验证了PDPTP在兼顾可用性与隐私保护方面的有效性与鲁棒性。

在GeoLife数据集上，本文进一步评估了PDPTP在多模态、高采样频率轨迹场景下的隐私保护与数据可用性表现，实验结果如图4所示。整体来看，随着隐私预算ε增大，各方法的扰动幅度减弱、轨迹数据可用性提升，符合差分隐私机制的一般规律。DPTP与SEITP未引入位置敏感度建模，其在高敏感区域的扰动不足，且易受局部轨迹波动影响，导致轨迹数据可用性下降。相比之下，PPBA与PDPTP均通过动态预算分配强化高敏感区域的扰动，在隐私保护上优于前两种方法。然而，PPBA仅基于位置进行敏感度量化，无法细致刻画轨迹的语义差异与用户主观隐私偏好，易在低敏感区域产生过度扰动。相较而言，PDPTP在不同隐私预算ε条件下均保持较高的隐私保护强度，同时有效保留轨迹整体空间结构，表明其基于语义敏感度与主观偏好联合建模的隐私预算分配机制可在复杂轨迹结构下提供更稳定的扰动效果。综上，GeoLife数据集的实验结果进一步验证了PDPTP在多轨迹场景中的鲁棒性与泛化能力，可在多源运动模式下实现隐私保护与数据可用性的合理平衡。

为进一步分析查询长度对轨迹误差控制与聚类一致性的影响，本文在查询长度为5、10和20的条件下对4种算法进行了对比评估，实验结果如图5所示。从图5中可以看出，随着查询长度增加，各算法的MAE与MSE均呈上升趋势，表明较长轨迹对扰动更为敏感。在相同隐私预算下，较长轨迹包含更多位置点，隐私预算需要在更大范围内分配，导致关键位置的有效隐私预算减少，从而提升整体扰动强度并降低数据可用性。相比DPTP与PPBA，本文方法在不同查询长度下均获得更低的误差。SEITP采用基于语义相似性的替换式扰动，不依赖查询长度进行噪声分配，因此在不同查询长度条件下误差波动较小。随着查询长度的增加，各算法的ARI与Acc均呈下降趋势，说明扰动对轨迹类别结构的影响随查询长度变长而增强。在不同查询长度条件下，本文方法在ARI指标上均优于DPTP与PPBA，尤其在短轨迹场景中能够有效保持轨迹结构的稳定性，而传统统一扰动策略在该场景下的聚类一致性明显不足。

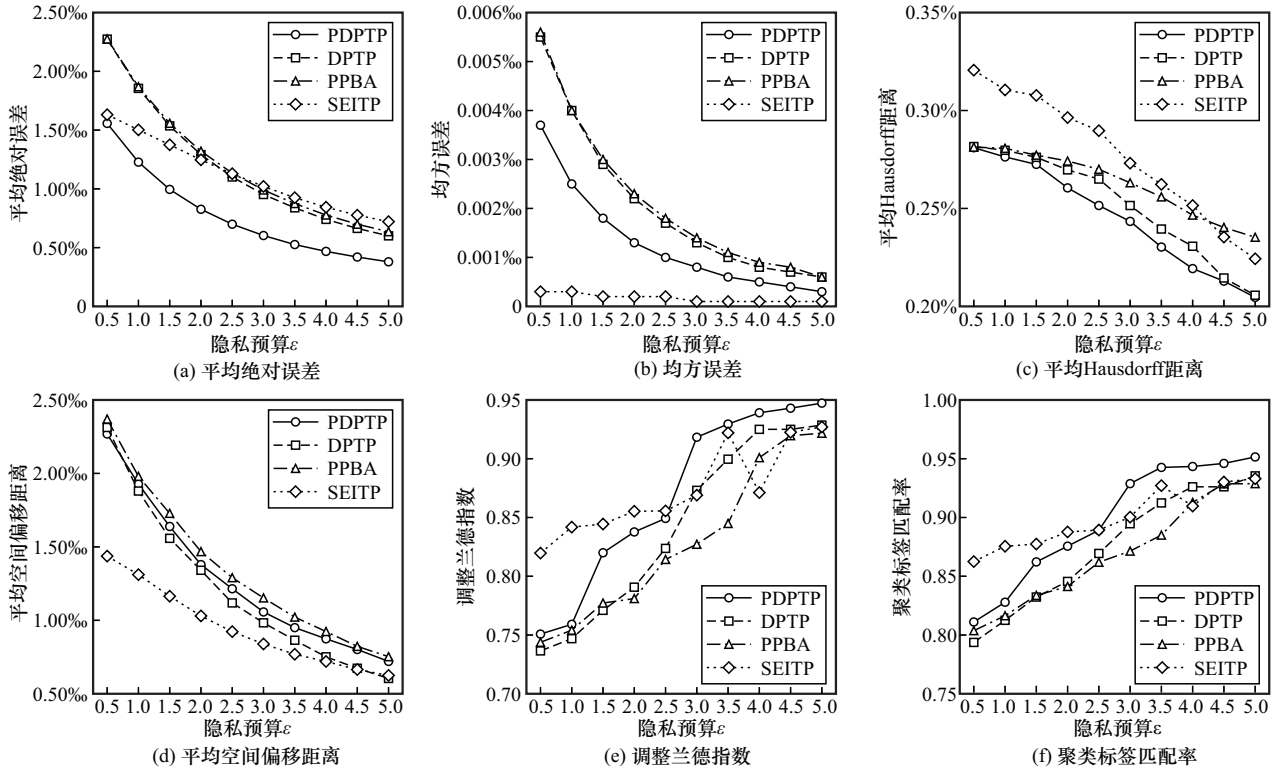

图4 Geolife数据集不同隐私预算下隐私保护性能对比

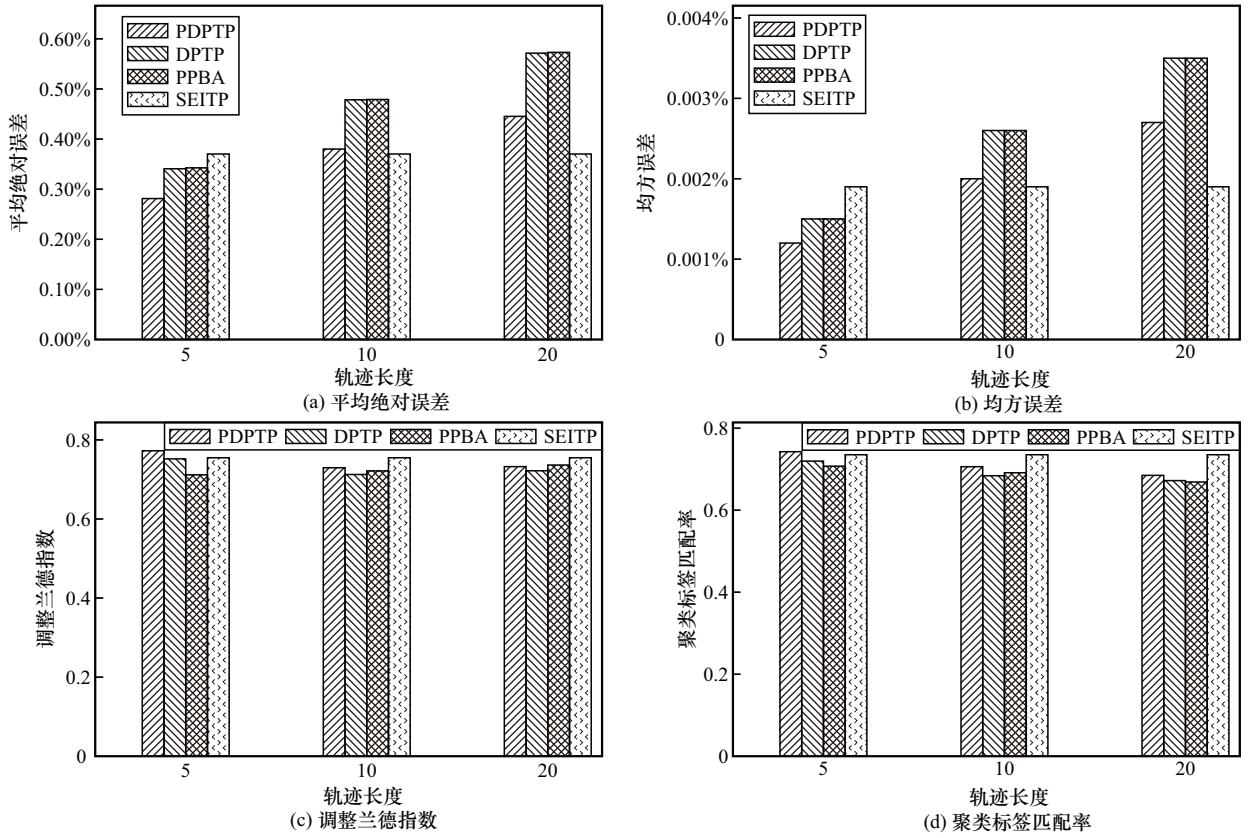

图5　查询长度对隐私保护性能的影响

在固定查询长度与隐私预算ε的条件下，本文进一步分析敏感距离因子中两个关键参数——最大敏感距离d_θ与距离变化斜率k对轨迹误差、隐私保护强度和结构一致性的影响。实验结果如图6所示。由图6(a)可知，随着d_θ增大，MAE与MSE持续上升，表明整体扰动强度随敏感区域范围扩大而增加。当d_θ增大时，更多轨迹点被纳入敏感区域，导致可分配至单点的隐私预算减少，从而使噪声幅度增大、轨迹偏移加剧。实验结果显示，d_θ从0.005增加至0.01时，平均偏移由0.393 8增加至0.523 9。较小的d_θ使隐私预算更集中于关键敏感点，有利于保持轨迹局部空间结构。较大的d_θ则导致隐私预算分布趋于均衡，削弱局部结构特征，聚类一致性下降。综合误差与结构保持性，本文选择$d_\theta = 0.007$作为推荐参数。由图6(b)可知，随着距离变化斜率k增大，轨迹扰动误差显著提升。例如，当k从30增至180时，MAE与MSE分别从0.069 1、0.000 3上升至0.380 1、0.00 2。较大的k

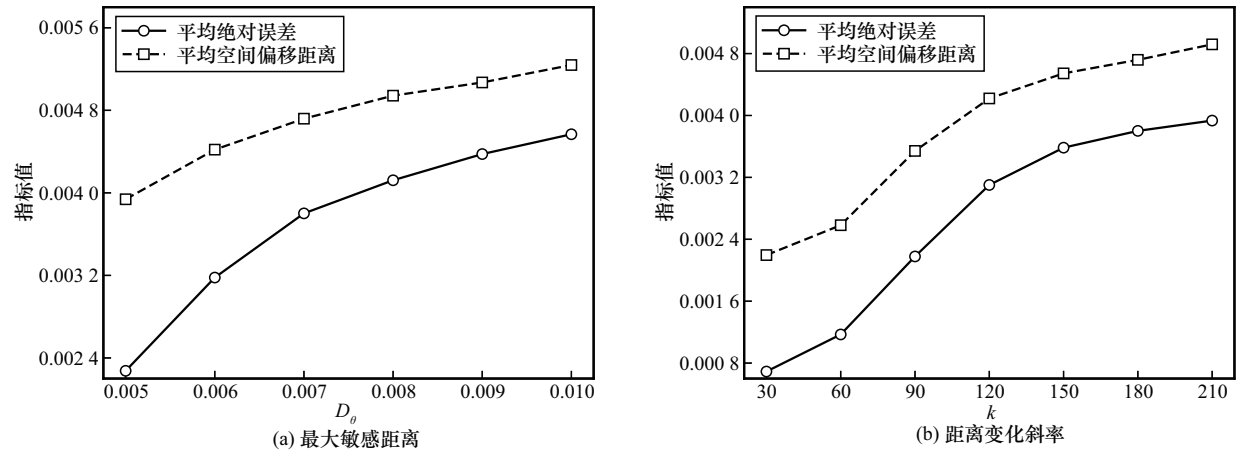

图6　参数d_θ和k对加噪轨迹数据可用性与安全性的影响

值使隐私预算高度集中在敏感点附近，导致远离敏感点处隐私预算不足、轨迹连续性下降。较小的k则可保持较均衡分配，但可能削弱对高敏感区域的隐私保护。综合隐私保护效果与数据可用性，本文选择$k = 180$，以兼顾敏感区域的强隐私保护与轨迹整体结构的稳定性。此外，本文在GeoLife数据集上进行了相同条件下的对照实验，其误差趋势、结构一致性变化及参数敏感性均与T-drive数据集呈现一致规律，验证了PDPTP在不同轨迹场景下的稳定性与泛化能力。

为评估边缘节点动态变化对本文方法的影响，本文设计了动态拓扑仿真实验。在基于网格划分的边缘节点部署基础上，随机选取部分网格节点作为失效节点，并设置10%与20%的节点退出比例，以模拟不同程度的拓扑扰动。对于被移除的网格节点，其包含的轨迹点依据空间邻近原则重新分配至最近邻节点，从而模拟边缘节点退出后轨迹向相邻节点迁移的情形。

由于边缘节点失效会引起局部轨迹密度、空间分布和敏感度结构的变化，隐私预算分配的稳定性可能受到影响，实验结果如图7所示。由图7可知，在不同拓扑扰动条件下，PDPTP的轨迹误差、平均空间偏移距离和可用性指标仅呈现有限波动，整体保持稳定趋势。随着节点退出比例增加，隐私保护强度有所降低而数据可用性相应提升，但变化幅度均处于可控范围内。这表明PDPTP基于局部敏感度建模与动态隐私预算分配的设计对固定拓扑结构依赖较弱，在边缘节点动态变化场景下仍具有良好的鲁棒性与适配性。

5.4 安全性评估

为评估本文方法的隐私保护性能，将PDPTP与DPTP、PPBA和SEITP这3种轨迹隐私保护方法进行对比，并以敏感区域轨迹点的平均空间偏移距离衡量隐私保护强度。不同隐私预算ε下的实验结果如图8所示。其中横轴为隐私预算ε，纵轴为对应敏感区域的平均空间偏移距离，偏移值越大表示隐私保护强度越高。由图8可观察到，随着ε增大，各算法的平均空间偏移距离均逐渐减小，表明隐私保护强度随隐私预算增加而减弱，该结果符合差分隐私噪声注入机制的理论特性。在相同隐私预算下，本文方法在不同ε值上的平均空间偏移距离整体高于DPTP和PPBA，且在中高隐私预算条件下

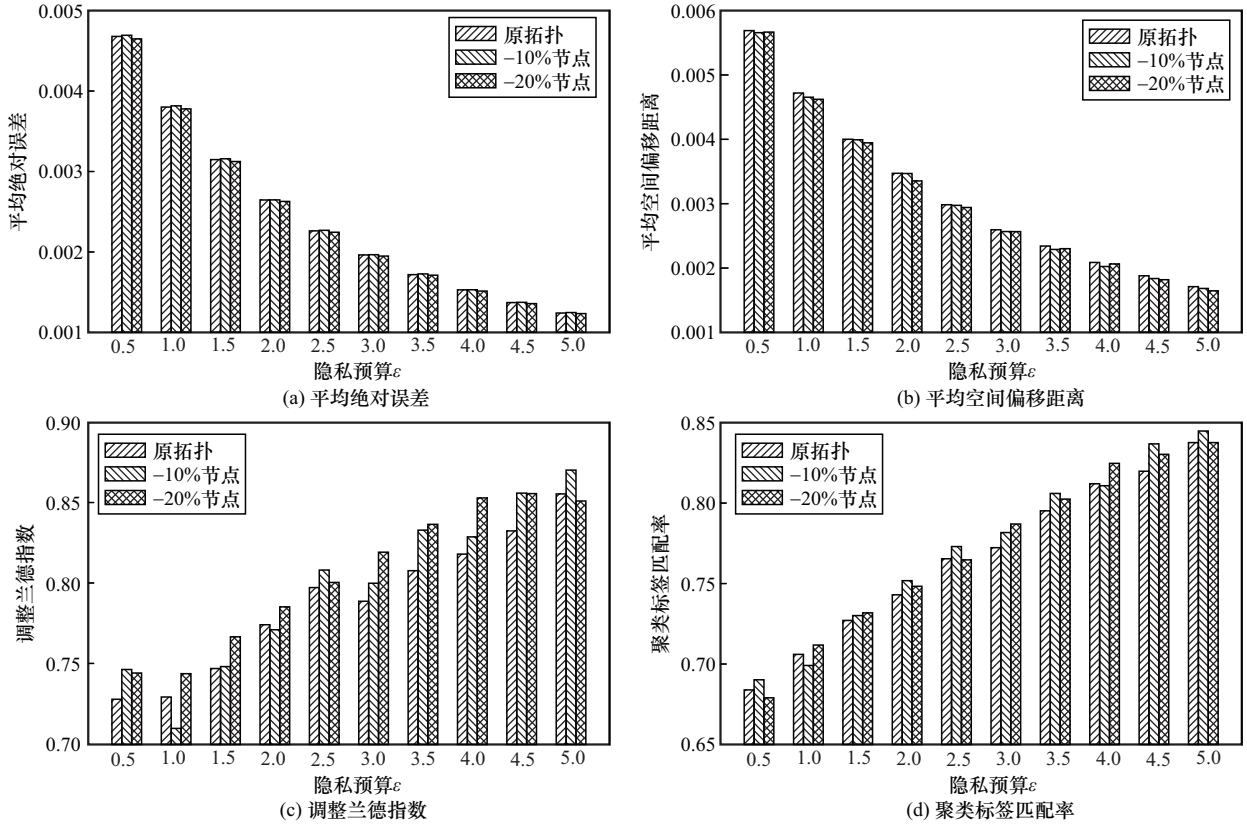

图7 动态拓扑下的隐私保护性能变化

仍保持较大的扰动幅度，说明其对敏感区域具有更强且更稳定的隐私保护能力。相比之下，DPTP和PPBA在高隐私预算区间的隐私保护强度下降明显，表明其在隐私预算放宽后保护能力减弱，存在较高隐私泄露风险。SEITP依赖语义邻域替换实现扰动，使轨迹点偏移至语义相近区域，在整体结构保持方面具有一定优势，其平均空间偏移距离相对稳定。但由于缺乏敏感度建模，其对高敏感区域的扰动幅度不足，难以在严格隐私约束下实现针对性隐私保护。综合分析可知，PDPTP在不同ε条件下均保持较高扰动强度，不仅在低隐私预算条件下有效阻断敏感信息泄露，在中高隐私预算条件下仍能兼顾轨迹数据可用性与整体稳定性，表现出良好的隐私保护鲁棒性。GeoLife数据集上获得相同结论，进一步验证PDPTP的有效性。

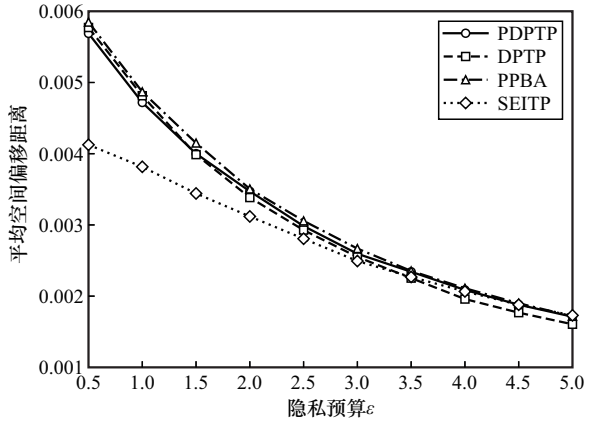

图8　不同隐私预算下各算法的隐私保护强度对比

为评估本文方法在推断攻击场景下的安全性，本节构建了基于马尔可夫链与Viterbi解码[29]的轨迹恢复攻击。攻击者首先利用背景用户学习状态转移概率$P\left(S_t|S_{t-1}\right)$，随后在扰动轨迹作为观测的条件下，通过动态规划推断最可能的隐状态序列并恢复轨迹路径。该攻击能够有效利用轨迹的时序相关性，是现有研究中常用的隐私评估手段。表2给出了4种扰动方法在该攻击下的恢复误差与命中率对比结果。实验显示，PDPTP、DPTP与PPBA在MAE/MSE上表现接近，说明在整体连续误差尺度上三者的抗推断性能相当。SEITP的误差显著更高，表明其以更大扰动换取更强的抗恢复能力。进一步观察Hit@100 m指标，各方法的命中率均处于较低水平（0.021 5~0.044 9），显示即便攻击者具备序列先验，恢复精度仍然有限。其中，PDPTP的命中率略高于DPTP和SEITP，但仍保持在较低范围，体现出其在个性化敏感点扰动策略下能够对推断攻击的有效抑制作用。整体而言，该攻击实验验证了PDPTP在保持可控误差的同时，能够限制攻击者的有效恢复能力。

表2　　轨迹推断攻击实验性能对比

方法	MAE	MSE	Hit@100 m
DPTP	0.462 9%	0.003 3%	0.024 6
SEITP	0.813 1%	0.012 1%	0.021 5
PPBA	0.463 5%	0.003 2%	0.044 9
PDPTP	0.461 9%	0.003 2%	0.044 5

5.5　用户隐私偏好分析

为验证本文方法在不同用户隐私偏好条件下的适应能力，本文在T-drive数据集上开展用户隐私偏好异质性实验。由于公开轨迹数据集中缺乏用户隐私偏好标注，为模拟真实应用场景中用户隐私需求的差异，本文构造三类典型用户群体：高隐私需求用户、中等隐私需求用户和低隐私需求用户。在实验中保持查询长度及其他算法参数一致，通过调整用户偏好参数x模拟不同隐私需求，并在相同隐私预算条件下比较轨迹误差、平均空间偏移距离和聚类匹配率，实验结果如图9所示。

由图9可以看出，不同隐私需求用户在各隐私预算条件下呈现明显的差异化表现。总体而言，高隐私需求用户的MAE与平均空间偏移距离均高于其他用户群体，而匹配准确率相对较低。相比之下，低隐私需求用户具有更小的轨迹误差和空间偏移，同时保持更高的匹配准确率。例如，在$\varepsilon = 3$时，高隐私需求用户的MAE为0.219 4，而低隐私需求用户为0.124 2，对应的平均空间偏移距离分别为0.294 6和0.190 6。该结果表明，当用户隐私需求较高时，算法会在敏感区域分配更高的扰动强度，从而增强对敏感位置的隐私保护能力。对于隐私需求较低的用户，算法避免过度扰动，从而保持较高的轨迹数据可用性。此外，随着隐私预算ε的增加，三类用户群体的轨迹误差与平均空间偏移距离均逐渐降低，而匹配准确率持续提升，这与差分隐私中隐私预算与数据可用性之间的理论关系一致。总体而言，PDPTP能够根据用户隐私偏好动态调节扰动强度，在高隐私需求场景下增强敏感区域隐私保

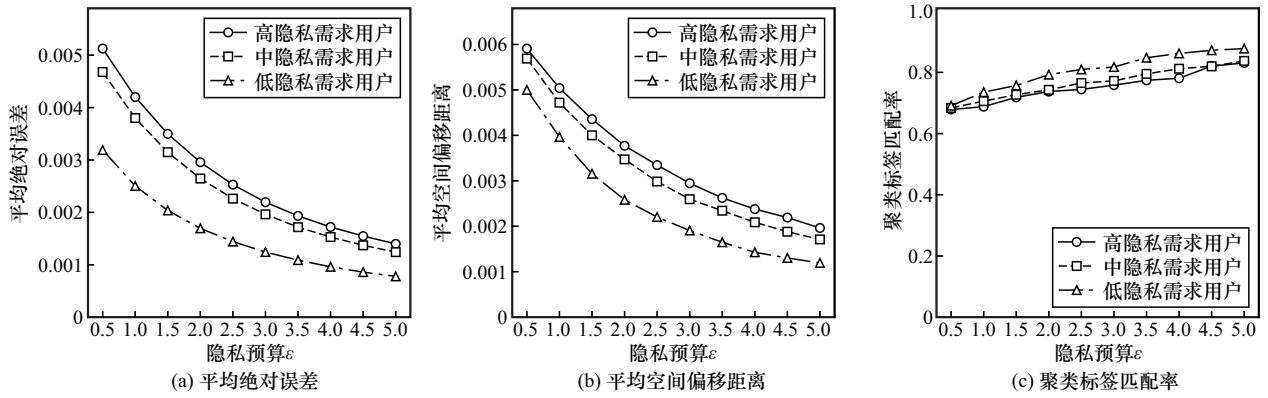

图9 不同隐私偏好用户在不同隐私预算条件下的性能比较

护，在低隐私需求场景下保持轨迹数据可用性，从而在隐私保护与数据可用性之间实现更灵活的权衡。

5.6 MEC性能分析

为评估本文方法在MEC环境中的计算开销，本文在一台具备中等算力配置的笔记本平台（Intel Core i7-13700H，16 GB RAM）上，基于T-drive数据集对4种轨迹扰动方法的执行时间、CPU使用率、内存占用、推理时延与功耗估算等指标进行了测试，结果如表3所示。

表3 边缘节点环境下各算法的运行开销比较

方法	执行时间/s	CPU使用率	内存占用/MB	推理时延/ms	功耗估算/W
DPTP	0.035 0	7.5%	18 173.7	0.70	11.5
SEITP	0.035 0	21.85%	19 654.5	0.76	14.4
PPBA	0.093 3	10.9%	18 175.5	1.87	12.2
PDPTP	0.104 0	12.8%	18 173.9	2.08	12.6

从表3可知，DPTP执行时间最低，平均执行时间为0.035 s，CPU使用率为7.5%，在4种方法中推理时延最小，功耗估算最低。SEITP在执行时间上与DPTP接近，但由于采用语义邻域搜索与替换式扰动，其CPU使用率和功耗估算相对较高。PPBA和PDPTP的执行时间和CPU使用率相对较高，但仍保持在毫秒级推理时延与可控CPU开销范围内。总体来看，尽管PDPTP在动态敏感度建模与隐私预算分配方面引入了额外计算，其资源消耗仍满足边缘节点对实时性和轻量级处理的要求，具备实际部署可行性。

6 结束语

本文针对MEC环境下的用户轨迹隐私保护问题，提出了一种基于Laplace机制的个性化动态轨迹扰动方法。该方法通过构建模糊敏感度量化模型，将位置语义特征与用户隐私偏好相结合，并设计动态隐私预算分配策略，对不同敏感等级位置点实施差异化扰动，从而在隐私保护与数据可用性之间取得平衡。实验结果表明，该方法在保证隐私保护强度的同时提升了加噪轨迹数据的可用性。未来将结合时序建模与联邦学习框架，构建跨边缘节点的分布式轨迹隐私保护机制。

参考文献：

[1] Jia D Y, Lu K J, Wang J P, et al. A survey on platoon-based vehicular cyber-physical systems[J]. IEEE Communications Surveys & Tutorials, 2016, 18(1): 263-284.

[2] Chen J, He K, Yuan Q, et al. Blind filtering at third parties: an efficient privacy-preserving framework for location-based services[J]. IEEE Transactions on Mobile Computing, 2018, 17(11): 2524-2535.

[3] 谢人超, 廉晓飞, 贾庆民, 等. 移动边缘计算卸载技术综述[J]. 通信学报, 2018, 39(11): 138-155.
Xie R C, Lian X F, Jia Q M, et al. Survey on computation offloading in mobile edge computing[J]. Journal on Communications, 2018, 39(11): 138-155.

[4] Ranaweera P, Jurcut A D, Liyanage M. Survey on multi-access edge computing security and privacy[J]. IEEE Communications Surveys & Tutorials, 2021, 23(2): 1078-1124.

[5] 袁健, 王迪, 高喜龙, 等. 基于差分隐私的匿名组LBS轨迹隐私保护模型[J]. 小型微型计算机系统, 2019, 40(2): 341-347.
Yuan J, Wang D, Gao X L, et al. Privacy protection model for anonymous group LBS trajectory based on differential privacy[J]. Journal of Chinese Computer Systems, 2019, 40(2): 341-347.

[6] 陈思, 付安民, 苏铠, 等. 基于差分隐私的轨迹隐私保护方案[J]. 通信学报, 2021, 42(9): 54-64.
Chen S, Fu A M, Su M, et al. Trajectory privacy protection scheme based on differential privacy[J]. Journal on Communications, 2021, 42 (9): 54-64.

[7] 徐川, 丁颖祎, 罗丽, 等. 车联网中基于位置服务的个性化位置隐私保护[J]. 软件学报, 2022, 33(2): 699-716.
Xu C, Ding Y Y, Luo L, et al. Personalized location privacy protection for location-based services in vehicular networks[J]. Journal of Soft-

ware, 2022, 33(2): 699-716.
[8] Zheng Z R, Li Z T, Jiang H B, et al. Semantic-aware privacy-preserving online location trajectory data sharing[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 2256-2271.
[9] Abul O, Bonchi F, Nanni M. Never walk alone: uncertainty for anonymity in moving objects databases[C]//Proceedings of the 2008 IEEE 24th International Conference on Data Engineering. Piscataway: IEEE Press, 2008: 376-385.
[10] Hu Z W, Yang J, Zhang J P. Trajectory privacy protection method based on the time interval divided[J]. Computers & Security, 2018, 77: 488-499.
[11] Benarous L, Kadri B. Obfuscation-based location privacy-preserving scheme in cloud-enabled Internet of vehicles[J]. Peer-to-Peer Networking and Applications, 2022, 15(1): 461-472.
[12] Bindschaedler V, Shokri R. Synthesizing plausible privacy-preserving location traces[C]//Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2016: 546-563.
[13] Jiang K F, Shao D X, Bressan S, et al. Publishing trajectories with differential privacy guarantees[C]//Proceedings of the 25th International Conference on Scientific and Statistical Database Management. New York: ACM Press, 2013: 1-12.
[14] Sun X Y, Ye Q Q, Hu H B, et al. Synthesizing realistic trajectory data with differential privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(5): 5502-5515.
[15] Sun W, Zhao K, Liang G, et al. UdpTrace: utility-enhanced differential privacy scheme for trajectory data publishing[J]. Neurocomputing, 2025, 649: 130785.
[16] 田丰, 吴振强, 鲁来凤, 等. 面向轨迹数据发布的个性化差分隐私保护机制[J]. 计算机学报, 2021, 44(4): 709-723.
Tian F, Wu Z Q, Lu L F, et al. A sample based personalized differential privacy mechanism for trajectory data publication[J]. Chinese Journal of Computers, 2021, 44(4): 709-723.
[17] 王豪, 徐正全, 熊礼治, 等. CLM: 面向轨迹发布的差分隐私保护方法[J]. 通信学报, 2017, 38(6): 85-96.
Wang H, Xu Z Q, Xiong L Z, et al. CLM: differential privacy protection method for trajectory publishing[J]. Journal on Communications, 2017, 38(6): 85-96.
[18] Yang Z G, Wang R Y, Wu D P, et al. Local trajectory privacy protection in 5G enabled industrial intelligent logistics[J]. IEEE Transactions on Industrial Informatics, 2022, 18(4): 2868-2876.
[19] Zhong H, Ni J Y, Cui J, et al. Personalized location privacy protection based on vehicle movement regularity in vehicular networks[J]. IEEE Systems Journal, 2022, 16(1): 755-766.
[20] Cao M G, Zhu H P, Min M H, et al. Protecting personalized trajectory with differential privacy under temporal correlations[C]//Proceedings of the 2024 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2024: 1-6.
[21] Cao M G, Zhu H P, Min M H, et al. Achieving privacy-preserving trajectory correlation with differential privacy[C]//Proceedings of the IEEE Wireless Communications and Networking Conference. Dubai: IEEE Press, 2024: 1-6.
[22] Cao M G, Zhu H P, Min M H, et al. Protecting personalized trajectory with differential privacy under temporal correlations[C]//Proceedings of the 2024 IEEE Wireless Communications and Networking Conference (WCNC). Piscataway: IEEE Press, 2024: 1-6.
[23] Zhu T Q, Li G, Zhou W L, et al. Differentially private data publishing and analysis: a survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2017, 29(8): 1619-1638.
[24] Wu L, Qin C Y, Xu Z H, et al. TCPP: achieving privacy-preserving trajectory correlation with differential privacy[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 4006-4020.
[25] Dwork C, McSherry F, Nissim K, et al. Calibrating noise to sensitivity in private data analysis[C]//Theory of Cryptography. Berlin: Springer, 2006: 265-284.
[26] Ye Q Q, Meng X F, Zhu M J, et al. Survey on local differential privacy[J]. Journal of Software, 2018, 29(7): 1981-2005.
[27] Yuan J, Zheng Y, Zhang C Y, et al. T-drive: driving directions based on taxi trajectories[C]//Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems. New York: ACM Press, 2010: 99-108.
[28] Bastani F, Xie X, Huang Y, et al. A greener transportation mode: flexible routes discovery from GPS trajectory data[C]//Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems. New York: ACM Press, 2011: 405-408.

[作者简介]

蒋忠元（1988– ），男，陕西榆林人，博士，西安电子科技大学教授、博士生导师，主要研究方向为空天地一体化网络、6G网络安全、数据与智能安全等。

房梦欣（2000– ），女，山东烟台人，西安电子科技大学硕士生，主要研究方向为数据安全与隐私保护、深度学习。

王启舟（1994– ），男，陕西汉中人，博士，西安交通大学助理研究员，主要研究方向为并行与分布式系统、海量存储、算法设计与分析等。

马建峰（1963– ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为无线网络安全、移动智能系统安全等。

李兴华（1978– ），男，河南南阳人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全、安全协议形式化等。