

基于关键路径的动态本地化差分隐私位置保护方法

晏燕, 刘坤, 张艳莉, 冯涛

(兰州理工大学计算机与人工智能学院, 甘肃 兰州 730050)

摘要: 位置信息作为数字时代重要的个人数据资产, 在提供便利服务的同时面临着严重的隐私泄露风险。本地化差分隐私模型无须依赖可信的第三方, 近年来受到广泛关注。然而, 现有本地化差分隐私位置保护方法普遍面临两大挑战: 一是空间分割结构难以适应位置分布的复杂特性; 二是用户与服务器端的通信与计算开销制约了系统效率。针对上述挑战, 提出一种基于关键路径的动态本地化差分隐私位置保护方法。该方法首先通过非均匀四叉树空间分割与 Hilbert 曲线遍历, 构建适配于用户分布密度的空间索引, 有效提升了数据可用性。继而由服务器运行提出的关键路径编码机制, 将复杂的分割结构压缩为简洁的路径信息, 减少了下发参数时的通信开销。用户端根据本地化差分隐私模型对自身所处区域的 Hilbert 索引编码进行随机响应扰动, 实现原始位置的隐私保护。服务器端则根据收集到的用户扰动位置编码进行聚合分析, 并依据位置分布的时空连续性执行所提出的空间分割结构动态调整策略, 以极低的计算成本高效适应用户分布的动态变化。在实际位置数据集上的实验证明, 所提方法能够在实现用户位置本地化差分隐私保护的基础上, 提高数据可用性和算法运行效率。

关键词: 位置隐私; 本地化差分隐私; 空间分割与索引; 关键路径; 分割结构动态调整

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025061

Dynamic local differential privacy location protection method based on critical path

YAN Yan, LIU Kun, ZHANG Yanli, FENG Tao

School of Computer Science and Artificial Intelligence, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: Location information was recognized as a critical personal data asset in the digital age, offering convenient services while simultaneously posing significant risks of privacy breaches. Local differential privacy models, which do not rely on trusted third parties, had garnered widespread attention. However, significant challenges were identified in existing location protection methods, including the difficulty of adapting spatial partitioning to complex location distributions, along with high communication and computational overhead that limited system efficiency. To address these challenges, a dynamic local differential privacy location protection method based on a criti-

收稿日期: 2025-05-22; 修回日期: 2025-07-18

基金项目: 国家自然科学基金 (62361036)

Foundation Item: The National Natural Science Foundation of China (62361036)

引用格式: 晏燕, 刘坤, 张艳莉, 等. 基于关键路径的动态本地化差分隐私位置保护方法[J]. 网络与信息安全学报, 2025, 11(5): 68-87.

Citation Format: YAN Y, LIU K, ZHANG Y L, et al. Dynamic local differential privacy location protection method based on critical path[J]. Chinese Journal of Network and Information Security, 2025, 11(5): 68-87.

cal path was proposed. A spatial index adapted to user distribution density was constructed through non-uniform quadtree spatial partitioning and Hilbert curve traversal, which effectively improved data usability. Subsequently, the proposed critical path encoding mechanism was executed on the server side to compress the complex partition structure into concise path information, thereby reducing communication overhead during parameter transmission. On the user side, the Hilbert index encoding of the user's region was perturbed using a randomized response mechanism under the local differential privacy model to protect the privacy of the original location. On the server side, the collected perturbed location encodings from users were aggregated and analyzed. Based on the spatiotemporal continuity of location distribution, the proposed spatial partition structure dynamic adjustment strategy was then implemented to efficiently adapt to dynamic changes in user distribution at an extremely low computational cost. Experiments conducted on real-world location datasets demonstrate that the proposed method provides improved location data availability and algorithm runtime efficiency while achieving local differential privacy protection for user locations.

Keywords: location privacy, local differential privacy, spatial partition and index, critical path, partition structure dynamic adjustment

0 引言

随着移动互联网、物联网与定位技术的发展,位置信息已成为数字时代非常重要的个人数据资产之一。基于位置的服务(location-based services, LBS)被广泛应用于地图导航、兴趣点推荐、社交网络和共享出行等领域^[1-4],显著提升了社会运行效率和用户体验。与此同时,智慧交通、公共安全、商业智能等领域也高度依赖位置数据的分析与应用,以优化资源配置和辅助科学决策^[5-7]。然而,位置数据因其时空唯一性和强语义关联性,也带来了突出的隐私泄露风险。攻击者通过分析用户轨迹,能够精准推断出用户的身份信息、住址、工作单位、日常行为模式,乃至健康状况等深层敏感信息。此类信息一旦泄露,可能导致用户面临精准诈骗、跟踪骚扰、歧视对待等威胁。因此,在充分发挥位置数据价值的同时,如何有效保障用户隐私安全,已成为一个兼具重要理论意义与紧迫现实需求的关键课题。

本地化差分隐私(local differential privacy, LDP)^[8-9]作为一种无须可信第三方的强隐私保护模型,近年来备受关注。该模型允许用户在本地对位置数据进行扰动处理,再将结果提交给服务器,从而避免对任何第三方的信任依赖,从源头上消除了服务器端数据泄露所带来的隐私风险。同时,LDP提供严格且可量化的隐私保护,能够抵御具有任意背景知识的攻击者发起的攻击。即使攻击者获取了除目标用户外的所有其他

用户的数据,也无法准确推断出目标用户的真实位置信息。此外,LDP赋予用户对自身位置数据隐私保护的自主控制权,允许用户根据自身的隐私偏好和应用场景灵活选择不同的隐私保护级别。

尽管LDP在位置隐私保护领域具有显著优势,但现有相关保护方法仍存在多方面不足,难以满足实际场景的需求。首先,大多数方法采用均匀化空间分割与索引策略(如均匀网格划分^[10-11]、四叉树划分^[12]),该类策略未考虑用户位置分布的异质性特征,直接导致“两极化”问题。在用户分布稀疏区域,过度分割会大幅增加位置编码的复杂度,使得扰动后位置的可用性严重下降;而在用户分布密集区域,均匀分割的粒度又过于粗糙,无法为用户提供足够强度的隐私保护,最终存在位置隐私泄露的风险。其次,为降低用户端的计算复杂度,许多LDP位置隐私保护方法采用“服务器端集中处理+全量下发”的模式(即由服务器端预先完成全部空间结构划分与位置编码生成,并将完整数据下发至用户端)^[11,13]。这种模式会产生巨大的通信开销,难以支持大规模用户场景。最后,静态的空间结构划分无法适配位置数据的动态变化特性(如早晚高峰时段的人流迁移、节假日期间景点的游客聚集等),按照固定时间间隔下发新的空间结构划分与位置编码信息虽然可以实现对位置数据分布的动态跟踪^[14],但由于位置数据存在时空动态关联性,频繁的重复分割与编码更新会产生大量

冗余计算, 严重消耗系统资源。综上, 现有主流 LDP 位置隐私保护方法在处理大规模、动态变化的用户位置数据时, 主要面临三大核心挑战: 空间分割和索引策略难以匹配位置数据分布的异质性; 用户端与服务器之间的通信开销导致产生可扩展性瓶颈; 重复的空间分割操作产生的大量冗余计算严重影响系统运行效率。

针对上述挑战, 本文提出基于关键路径的动态本地化差分隐私位置隐私保护 (dynamic local differential privacy location protection based on critical path, DLDP-CP) 方法。该方法实现了 3 个层面的目标: 首先, 设计了合理的空间分割与索引机制, 确保空间分割结构能够精确适配异质的用户位置分布; 其次, 建立了一套高效的位置编码下发与重构方案, 解决了复杂位置编码导致的通信开销问题; 最后, 提出了空间分割结构动态调整策略, 避免了位置数据动态变化过程中重复的空间分割操作。上述 3 个层面的创新设计使得 LBS 系统较好地兼顾了隐私保护需求、数据可用性与系统运行效率。本文的主要贡献如下。

1) 针对位置数据空间分布异质性问题, 引入非均匀四叉树分割方法进行空间分割, 并设计了相应的 Hilbert 曲线遍历算法对空间分割结果进行索引。该方法能够根据用户分布密度自适应调整空间分割粒度, 在保证高密度区域隐私保护强度的同时, 兼顾稀疏区域的数据可用性。

2) 为减少 LBS 中用户端与服务器之间的通信开销, 提出一种基于关键路径的位置编码算法, 并设计了相应的服务器端下发和用户端重构机制, 该机制将复杂的空间分割索引结果转化为简洁的关键路径编码, 有效减少了用户端与服务器交互过程中的数据传输量。

3) 考虑到位置数据的时空动态关联特性, 提出一种空间分割结构动态调整策略。该策略充分利用相邻时段位置数据分布的时空相关性, 实现对空间分割结构的自适应调整, 避免重复的空间分割操作, 提高系统运行效率。

1 相关工作

在 LBS 场景中, 基于 LDP 模型对用户位置进行本地化隐私保护是近年来位置隐私保护领域的主流方法。在对位置数据的空间分割与索引方

面, 张啸剑等^[10]将地理空间分为相同大小的网格, 并引入四叉树结构建立空间索引, 在用户端应用层次随机采样和优化随机响应机制实现位置隐私保护; 晏燕等^[11]提出了基于 Hilbert 编码的 LDP 位置保护方法, 利用均匀网格结构划分二维平面空间, 通过 Hilbert 编码实现位置数据的降维, 并采用随机响应机制进行扰动。上述基于均匀网格的空间分割方法实现简单, 但往往忽略了位置数据分布的异质性, 导致空间分割粒度与隐私保护强度相互制约, 容易产生数据稀疏区域“过度保护”或者数据密集区域“保护不足”问题。霍峥等^[15]提出一种用于位置数据收集的众包方法, 该方法通过构建 Voronoi 图对路网空间进行划分, 但是其范围查询的准确性较低。树结构在 LDP 位置隐私保护中也得到了广泛应用。晏燕等^[13]提出基于二叉树分割索引结构和 Huffman 编码机制的 LDP 位置隐私保护方法, 允许用户自定义隐私保护范围, 通过保持空间聚类特性来减少扰动带来的位置服务质量损失, 同时提高数据可用性与处理效率。Zhang 等^[16]针对范围查询问题, 提出了基于二叉堆树和前缀编码的高效方案, 用户仅需上传 w 比特信息即可高效响应任意范围查询。Ju 等^[17]设计了结合优化一元编码与 B+ 树安全分层算法的 LDP 范围查询方案, 在保护用户隐私的同时提升了服务器端的查询效率。Wang 等^[18]将分层树结构与分段线性函数相结合, 用分段线性函数代替传统的均匀分布假设来模拟树节点内的数据分布, 从而提高了 LDP 下的范围查询准确性。总体而言, 树结构通常具有较好的灵活性, 能够针对查询类型利用层次结构提升查询效率。但是, 树结构的构建和维护过程相对复杂, 且多数方法仍基于均匀分布假设, 难以在编码复杂度与查询效率之间取得理想平衡。

在实现 LDP 模型的具体方法上, 沃纳随机响应 (Warner's randomized response, W-RR)^[19]、广义随机响应 (generalized randomized response, GRR)^[20]、优化一元编码 (optimized unary encoding, OUE)^[21]、随机可聚合保护隐私的有序响应 (randomized aggregatable privacy-preserving ordinal response, RAPPOR)^[22]等随机响应机制被

相继提出, 这些机制可用于对用户位置或编码进行扰动, 实现对真实位置的LDP保护。为了更好地适应位置数据的特殊性并提升扰动后位置的可用性, 研究者提出了多种改进方案。Wang等^[12]利用Hilbert线映射技术将用户在地图上的位置映射为一维编码, 随后对该编码添加拉普拉斯噪声, 从而保护用户的位置隐私。Yan等^[23]结合位置Hilbert编码中0/1比特的分布情况, 提出了优化随机响应的位置编码扰动方法, 有效减少了LBS的质量损失。随后, 他们利用该方法解决三维空间位置隐私保护问题, 提出了基于三维Hilbert编码和优化随机响应的LDP保护方法^[24]。杨宏宇等^[25]针对ADS-B报文中的三维定位数据隐私泄露问题, 提出先将三维位置进行降维编码, 再采用阶段式等差随机响应方法实施扰动, 在保护隐私的同时有效地保证了数据的可用性。Acharya等^[26]设计了基于Hadamard矩阵随机响应方法, Zhao等^[27]提出了一种灵活的Hadamard响应机制, 在通信成本、计算复杂度与估计准确性之间实现了更好的平衡。Varma等^[28]使用RAPPOR和Hadamard随机响应扩展了一种结合随机采样与假数据的策略, 并在实验涉及的部分隐私预算设定下, 提升了频率估计的性能。Hong等^[29]提出一种旨在最小化位置扰动误差的平方机制, 并设计了基于凸优化的后置处理算法, 用于从收集到的扰动后数据中更准确地估计原始空间频率分布, 从而在保护用户位置隐私的同时提高收集数据的可用性和频率估计准确性。Feng等^[30]结合混合空间结构, 利用几何级数设定非均匀扰动概率, 将更多的隐私预算分配给用户真实位置邻近区域, 从而提高LDP框架下的空间范围查询效率。Li等^[31]针对时间序列数据提出了模式感知的自适应采样和有界扰动机制, 以寻求更有效的隐私与效用平衡。为解决传统LDP机制可能破坏位置轨迹语义导致效率低的问题, Sun等^[32]提出了语义约束的LDP模型, 在实现位置隐私保护的同时保留了轨迹的语义信息。总体来看, 上述研究多聚焦于随机响应策略的改进, 而在空间分割结构与位置编码机制方面的优化较为有限。多数方法采用服务器端预编码、客户端选择性扰动的基本架构, 虽然减轻了用户端的计算负担,

但仍面临通信开销较大、对动态位置分布适应能力差等共性问题。

从整体发展趋势来看, 当前LDP位置隐私保护领域仍存在一些尚未妥善解决的技术挑战。例如, 如何将隐私保护的有效范围从二维地理坐标扩展至三维空间乃至融合语义信息的多维时空数据; 如何针对不同LBS应用场景特点和用户个体差异, 设计出真正个性化的自适应隐私保护策略; 如何在联邦学习等新兴的分布式范式下, 构建高效且可信的位置隐私保护框架。这些问题的探索不仅代表了该领域的前沿发展方向, 也为本文所提方法的进一步拓展与深化提供了重要的理论支撑和技术路径。

2 基础知识

在传统的中心化差分隐私 (centralized differential privacy, CDP) 模型中, 可信第三方负责对集中收集的数据添加满足特定约束的噪声。该方法在保留数据原有统计特性的同时, 能够确保无法识别出特定用户的个体信息, 从而实现隐私保护。然而, 该可信第三方存在无法自证清白的问题, 其可能面临的内部操作失误或外部恶意攻击, 极易导致用户隐私的直接泄露。为应对由潜在不可信第三方所带来的隐私泄露风险, LDP提供了一种更加严谨的解决方案。LDP将隐私保护机制前置至用户端, 通过对用户数据在本地进行扰动处理, 使得数据在离开用户设备时即具备隐私保护能力。因此, 即使数据收集方或第三方服务器遭受攻击或发生数据泄露, 也不会直接暴露用户的原始数据, 从而有效避免了更严重的隐私安全风险。

定义1 本地化差分隐私^[8-9]。对于定义域和值域分别为 $\text{Dom}(B)$ 和 $\text{Rang}(B)$ 的隐私保护算法 B , 若其定义域内任意两个数据 $t, t' \in \text{Dom}(B)$ 得到相同输出结果 $t^* \in \text{Rang}(B)$ 的概率满足以下不等式, 则称隐私保护算法 B 满足本地化差分隐私。

$$\Pr[B(t) = t^*] \leq e^\epsilon \times \Pr[B(t') = t^*] \quad (1)$$

定义1中的参数 ϵ 称为隐私预算, 其值越小, 两个数据 t, t' 得到相同输出结果的概率越小, 隐私保护算法 B 所提供的隐私保护强度越高。由此可见, 本地化差分隐私模型通过控制任意两个输

入数据在输出分布上的相似性,实现隐私保护的目标。将该模型应用于位置隐私保护场景中时,即使攻击者已掌握目标用户的背景知识,也无法通过观察或截获 LBS 的某一输出结果准确推断出用户的真实位置信息。

定理 1 串行组合特性^[33]。给定数据集 T 和 n 个隐私保护算法 $\{B_1, \dots, B_n\}$, 若 $B_i (1 \leq i \leq n)$ 满足对数据集 T 的 ϵ_i -本地化差分隐私, 则该组隐私保护算法 $\{B_1, \dots, B_n\}$ 能够对数据集 T 实现 $\sum_{i=1}^n \epsilon_i$ -本地化差分隐私。

定理 2 并行组合特性^[33]。若数据集 T 包含 n 个互不相交的子集 $T = \{T_1, \dots, T_n\}$, 由 n 个隐私保护算法 $\{B_1, \dots, B_n\}$ 分别作用于数据子集 $T = \{T_1, \dots, T_n\}$, 且 $B_i (1 \leq i \leq n)$ 满足对数据子集 T_i 的 ϵ_i -本地化差分隐私, 则该组隐私保护算法 $\{B_1, \dots, B_n\}$ 能够实现对数据集 T 的 $\max\{\epsilon_i\}$ -本地化差分隐私。

3 所提方法

为解决现有基于 LDP 的位置隐私保护方法在处理复杂位置分布时难以兼顾数据可用性与隐私保护强度, 且在高精度要求下会产生高昂的通信开销的问题, 本文提出基于关键路径的动态 LDP 位置隐私保护方法。

本文提出的方法的交互流程包含以下 4 个核心阶段, 如图 1 所示。

1) 空间分割与索引阶段: LBS 服务器根据用户位置数据的聚合结果, 对二维平面进行非均匀二叉树分割, 并采用 Hilbert 曲线遍历算法对生成的空间单元进行索引编码。

2) 关键路径下发与重构阶段: 服务器依据本文设计的关键路径编码机制, 将复杂的空间分割结构压缩为少量参数并下发给用户端, 从而大幅减少通信开销。

3) 本地化扰动阶段: 用户端根据接收到的参数重构出空间分割结构, 结合自身精确位置判定所处区域及计算 Hilbert 索引编码, 继而利用随机响应机制对该编码进行本地化扰动, 并将扰动后的结果提交给 LBS 服务器。

4) 空间分割结构动态调整阶段: LBS 服务器

聚合分析所有用户提交的扰动后位置编码, 并据此对空间分割结构进行增量式更新。该过程以极低的计算成本实现空间分割结构的动态优化, 从而高效适应用户分布的动态变化。

3.1 位置空间分割与索引编码

传统的均匀分割策略通常预先固定位置空间的划分粒度, 在处理空间分布动态变化的位置数据时表现出明显的局限性。在用户位置分布密集区域, 过粗的分割粒度可能导致位置服务精度下降; 而在用户位置分布稀疏区域, 过细的分割粒度则容易造成计算资源的浪费。相比之下, 非均匀二叉树结构能够依据局部数据密度自适应调整空间分割粒度, 从而更精准地匹配位置数据的实际分布特征。因此, 本文在位置空间分割过程中引入了非均匀二叉树结构^[34], 以位置数据的分布均匀性及其他阈值条件作为空间分割依据, 实现对二维空间的自适应迭代划分, 生成大小不一、密度各异的子区域。图 2 展示了采用非均匀二叉树对 Yellow_tripdata 数据集进行空间分割的过程。

定义 2 区域均匀性^[34]。给定二维平面内的矩形区域, 按照垂直、水平、左右对角线等对称轴可以将其平均分割为两个面积相等的子区域, 分别用 $C_1, C_2, \dots, C_n$ 表示上述多个方向平均分割后各个子区域内位置数据的统计值, 若式(2)成立, 则认为该矩形区域是分布均匀的。

$$\frac{\sum_{i=1}^n |C_i - \bar{C}|}{\sum_{i=1}^n C_i} \leq \theta \quad (2)$$

其中, $\bar{C} = \frac{\sum_{i=1}^n C_i}{n}$ 为各个子区域的位置数据统计平均值, n 为多个方向分割后的子区域数量, θ 为设定的阈值。

为进一步优化位置数据的存储效率和查询性能, LBS 服务器采用 Hilbert 曲线对非均匀二叉树空间分割结构进行遍历和编码, 从而将二维空间中的位置坐标映射为一维编码。Hilbert 曲线的空间聚集特性确保了在二维空间中相邻的位置, 其对应的一维编码也保持相邻, 有效维持了位置数据的空间邻近关系。

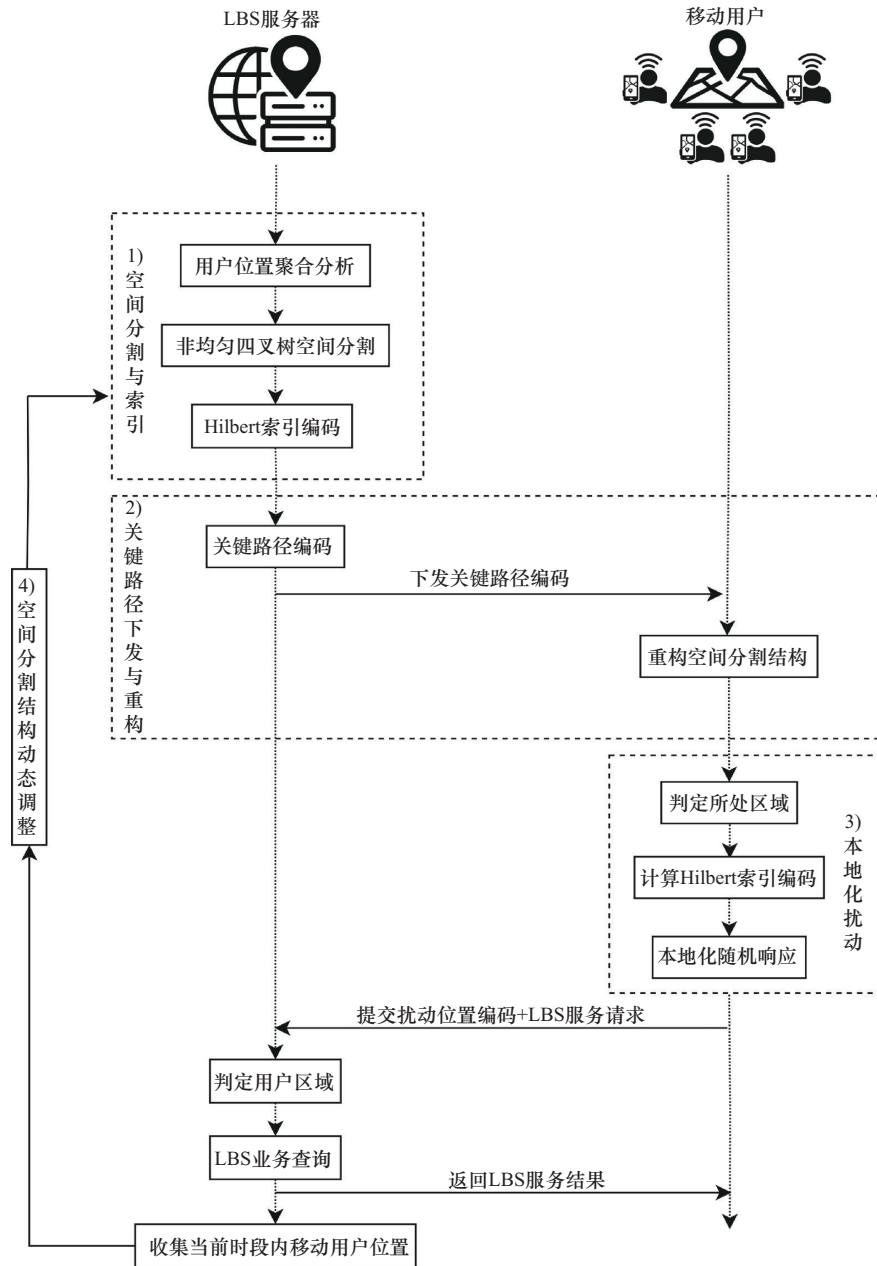


图1 所提方法的交互流程

Figure 1 Interaction flow of the proposed method

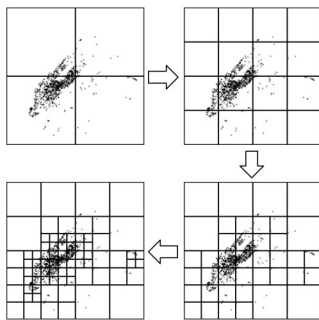


图2 基于非均匀四叉树的空间分割示例

Figure 2 Example of spatial partition based on non-uniform quadtree

定义3 Hilbert 索引编码。给定二维空间分割结构中的某个区域及其 Hilbert 划分象限编号 $U_i \in \{0,1,2,3\}$ ，则该区域在当前划分阶数中对应的 Hilbert 索引编码如式(3)所示。

$$Z_i = \begin{cases} 00, & U_i = 0 \\ 01, & U_i = 1 \\ 10, & U_i = 2 \\ 11, & U_i = 3 \end{cases} \quad (3)$$

图3展示了非均匀四叉树空间分割后的 Hil-

bert 索引生成过程, 按照 Hilbert 曲线的遍历顺序为每个区域赋予唯一的索引编号作为其标识符。

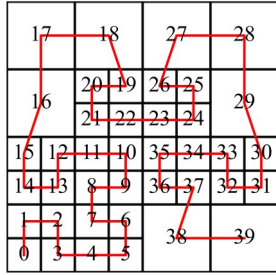


图3 基于非均匀四叉树的 Hilbert 索引示例

Figure 3 Example of Hilbert index based on non-uniform quadtree

算法 1 描述了非均匀四叉树空间分割与 Hilbert 索引编码的过程。在非均匀四叉树递归分割过程中, 每个子区域进一步被划分为 4 个更小的子区域, 分别对应 Hilbert 曲线划分的 4 个象限。以图 3 中位于索引编号 17 区域的用户为例, 其 Hilbert 索引编码生成过程为: 在一阶非均匀四叉树分割时, 该区域位于第 1 象限, 所以其第一阶 Hilbert 索引编码为“01”; 在二阶非均匀四叉树分割时, 该区域位于第 3 象限, 所以其第二阶 Hilbert 索引编码为“11”; 在三阶非均匀四叉树分割时, 该区域位于第 1 象限, 所以其第三阶 Hilbert 索引编码为“01”; 最终得到完整的 Hilbert 索引编码为{011101}。对于位于索引编号 24 区域的用户, 其编码过程为: 在一阶非均匀四叉树分割时, 该区域位于第 2 象限, 所以其第一阶 Hilbert 索引编码为“10”; 在二阶非均匀四叉树分割时, 该区域位于第 1 象限, 所以其第二阶 Hilbert 索引编码为“01”。为确保所有用户的位置编码长度一致, 以便于后续处理, 低阶区域的编码需要在末尾补零。因此, 最终得到该用户所处区域的 Hilbert 索引编码为{100100}。

算法 1 非均匀四叉树空间分割与 Hilbert 索引编码算法

输入 位置数据集 D 、二维平面的值域 G_R 、均匀性阈值 θ 、区域统计阈值 δ 、LBS 最小服务范围 γ

输出 空间分割结构 T 、空间分割结构对应的 Hilbert 索引编码 Z

1) 将二维平面的值域 G_R 初始化为根节点

root, $Z = \phi$

2) 空间分割结构 $T \leftarrow \{\text{root}\}$

3) 将位置数据集 D 映射到二维平面的值域 G_R

4) 初始化待处理队列 $Q \leftarrow \{\text{root}\}$

5) **while** $Q \neq \phi$ **do**

6) 从 Q 中取出当前节点 R

7) **if** R 的统计值 $\leq \delta$ **or** R 的覆盖范围 $\leq \gamma$ **then**

8) 标记 R 为叶子节点 //满足统计或范围阈值, 停止分割

9) **else**

10) 按照 Hilbert 曲线索引顺序将 R 分割为 $\{R_0, R_1, R_2, R_3\}$

11) 计算每个子节点 R_i 的均匀性指标 $U(R_i)$

12) **for** 每个子节点 R_i **do**

13) **if** $U(R_i) \leq \theta$ **then**

14) 标记 R_i 为叶子节点 //满足均匀性条件, 停止分割

15) **else**

16) 将 R_i 加入待处理队列 Q //继续分割

17) **end if**

18) **end for**

19) **end if**

20) **end while**

21) 计算最大编码长度, 为所有叶子节点生成补零后的 Hilbert 编码并加入 Z

22) **return** T, Z

算法 1 的时间复杂度分析: 在初始化阶段, 将 m 个空间位置点映射到初始空间范围的时间复杂度为 $O(m)$ 。在空间分割阶段, 算法 1 根据位置数据的分布特性进行自适应非均匀四叉树分割。在最坏的情况下, 非均匀四叉树最多可生成 $O(4^h)$ 个节点, 其中 h 表示最大分割深度。然而, 在实际运行过程中, 大量区域因满足终止条件而提前停止分割, 使得实际参与处理的有效节点数 $t \ll 4^h$ (t 表示空间分割结构中的节点总数), 从而将该阶段的实际时间复杂度优化为 $O(t)$ 。在编码生成阶段, 需要为 r 个叶子节点 ($r < t$) 生成固定长度的 Hilbert 编码, 由于每个编码操作的时间复杂度为 $O(h)$, 因此该阶段的总时间复杂度为 $O(r \cdot h)$ 。综上所述, 算法 1 的整体时间复杂度为 $O(m + r \cdot h)$ 。

3.2 关键路径编码与重构机制

若LBS服务器直接将完整的空间分割结构和Hilbert索引编码下发给每个移动用户,则会产生巨大的通信开销。在用户密集、空间分割层数较多、区域单元数量庞大的场景下,这一问题尤为突出,不仅限制了系统对大规模用户的支持能力,也严重影响了系统的整体性能与用户体验。为简化LBS服务器与用户端之间的通信流程,本文提出一种基于关键路径编码的高效下发与重构机制。该机制的核心思想在于摒弃对完整空间分割结构进行冗余编码,仅对分割结构中决策骨架的“关键路径”进行编码,从而实现结构信息的无损压缩。服务器仅需向用户端发送从根节点到关键节点的路径编码,即可在避免传输冗余信息的同时,确保用户端能够准确重构出完整的空间分割结构。这种以关键路径代替完整空间分割结构的策略,能够实现通信开销的数量级减少,显著提升LBS系统在大规模用户场景下的实用性与可扩展性。

定义4 关键节点。在基于非均匀四叉树的空间分割结构中,如果一个非叶子节点的4个子节点均为叶子节点(不可再分割的区域),那么该节点被定义为关键节点。

定义5 关键路径。在基于非均匀四叉树的空间分割结构中,关键路径被定义为一条从根节点出发、随分割阶数递增依次选择各阶某一子区域,直至到达某一关键节点所形成的路径。关键路径完整记录了空间由粗到细逐层分割的决策过程,可视为空间分割过程中的决策路径。

LBS服务器采用深度优先策略遍历整个非均匀四叉树空间分割结构,记录从根节点到关键节点的路径作为关键路径。每条关键路径采用一组唯一的二进制编码表示,该编码由路径编码和前缀编码两部分构成。

定义6 路径编码。用 $Q \in \{00,01,10,11\}$ 表示四叉树叶子节点的二进制编码集合,对应Hilbert曲线的遍历顺序为 $\{0,1,2,3\}$ 。对于空间分割深度为 d 的某个节点 v ,其路径编码 $P(v)$ 表示为:

$$P(v) = q_1 q_2 \cdots q_d, q_i \in Q, 1 \leq i \leq d \quad (4)$$

其中, q_i 表示从根节点到达节点 v 的关键路径上第 i 层的分支选择。

定义7 前缀编码。路径编码 $P(v)$ 的长度 $|P(v)|$ 的二进制表示定义为前缀编码,记为:

$$\text{Prefix}(P(v)) = \text{Binary}(|P(v)|) \quad (5)$$

其中, $\text{Binary}(\cdot)$ 为将路径编码长度 $|P(v)|$ 补齐成定长的二进制表示。用 h 代表空间分割的最大深度,则前缀编码的位数为:

$$L_{\text{prefix}} = \lceil \log_2(2h-1) \rceil \quad (6)$$

结合定义6和定义7,完整的关键路径编码 $K(v)$ 可以表示为:

$$K(v) = \text{Binary}(|P(v)|) \cdot P(v) \quad (7)$$

其中, $\text{Binary}(|P(v)|)$ 为前缀编码, $P(v)$ 表示路径编码, $\cdot$ 表示位串连接操作。

图4给出了一个分割深度 $h=3$ 的关键路径示例。算法2描述了关键路径编码的具体过程。根据式(6)可知前缀编码的位数为 $L_{\text{prefix}} = \lceil \log_2(2 \times 3 - 1) \rceil = 3$ 。节点 v_1 和 v_2 均为关键节点,从根节点到达至 v_1 和 v_2 的路径都构成关键路径。对于关键节点 v_1 ,路径编码 $P(v_1) = 00$ 、前缀编码 $\text{Binary}(|P(v_1)|) = 010$,因此其关键路径编码 $K(v_1) = \text{Binary}(|P(v_1)|) \cdot P(v_1) = 01000$ 。对于关键节点 v_2 ,路径编码 $P(v_2) = 1000$ 、前缀编码 $\text{Binary}(|P(v_2)|) = 100$,因此其关键路径编码 $K(v_2) = \text{Binary}(|P(v_2)|) \cdot P(v_2) = 1001000$ 。

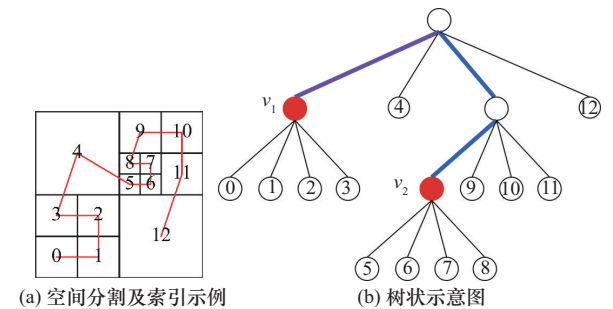


图4 关键路径示例($h=3$)
Figure 4 Example of critical path($h=3$)

算法2 关键路径编码算法

输入 空间分割结构 T

输出 所有关键路径编码集合 E 、最大分割深度 h

1) 对空间分割结构 T 进行深度优先遍历,得

到最大分割深度 h

- 2) 初始化关键路径编码集合 $E \leftarrow \phi$
- 3) 从根节点开始, 递归处理每个节点 node , 记录 path 和 depth
- 4) **if** node 是叶子节点 **then**
- 5) **continue** //已达叶子节点, 停止处理
- 6) **else if** node 有且仅有 4 个子节点, 且子节点均为叶子节点 **then**
- 7) $\text{len} \leftarrow |\text{path}|$ //路径编码长度
- 8) $L_{\text{prefix}} \leftarrow \lceil \log_2(2h - 1) \rceil$ //前缀编码的位数
- 9) $\text{prefix} \leftarrow \text{Binary}(\text{len})$ //补齐为 L_{prefix} 位
- 10) $K \leftarrow \text{prefix} \cdot \text{path}$ //拼接为完整编码
- 11) $E \leftarrow E \cup \{K\}$ //添加到编码集合
- 12) **else if** node 的子节点中存在非叶子节点 **then**
- 13) **for** i in 所有子节点 **do**
- 14) 递归处理 $\text{node.child}[i]$, 令 $\text{path} \leftarrow \text{path} \cdot i$, $\text{depth} \leftarrow \text{depth} + 1$
- 15) **end for**
- 16) **end if**
- 17) **return** E, h

算法 2 的时间复杂度分析: 算法 2 包含两个处理阶段。第一阶段通过深度优先遍历空间分割结构确定最大分割深度 h , 即从根节点至任意叶子节点的最大路径长度。由于遍历过程中每个节点仅被访问一次, 该阶段的时间复杂度为 $O(t)$, 其中 t 表示空间分割结构中的节点总数。第二阶段在已知最大分割深度 h 的基础上, 递归遍历整棵树以识别关键节点并生成其对应的关键路径编码。每个关键节点的编码由路径编码和前缀编码两部分构成, 其中路径编码的长度不超过最大深度 $2h$, 前缀编码的长度为 $\lceil \log_2(2h - 1) \rceil$, 则时间复杂度为 $O(l)$ 。因此, 该阶段的时间复杂度同样为 $O(t)$ 。综上所述, 算法 2 整体的时间复杂度为 $O(t)$ 。

为减少通信开销, LBS 服务器仅向用户下发关键路径编码, 用户端通过解析关键路径可以重构出空间分割结构。每条关键路径编码由“前缀编码+路径编码”两部分组成, 前缀编码表示路径编码的有效长度, 而路径编码则表征了从根节

点出发的象限遍历路径。用户端根据前缀编码确定路径长度后, 将路径编码按两位一组划分为象限序列, 依次构建相应的内部节点, 并在到达路径终止节点时, 为其添加 4 个叶子节点, 完成一个关键节点及其子区域的还原。

图 5 展示了用户端接收到两条关键路径编码“01000”和“1001000”后的重构过程。

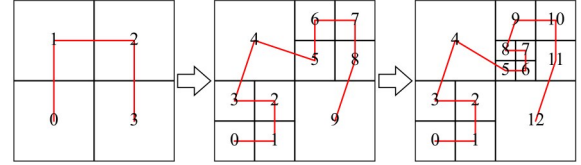


图 5 根据关键路径重构空间分割结构

Figure 5 Reconstructing spatial partition structure based on critical path

对于关键路径编码“01000”: 前 3 位“010”是前缀编码, 对应十进制数 2, 表示路径编码长度为 2 位; 后两位“00”是路径编码, 转化为十进制数 0, 表示从根节点出发选择第 0 象限。由于该节点为关键节点, 用户端为其创建 4 个叶子节点, 对应区域索引编号为 0、1、2、3。

对于关键路径编码“1001000”: 前 3 位“100”是前缀编码, 对应十进制数 4, 表示路径编码长度为 4 位; 后 4 位“1000”是路径编码, 按两位一组划分为“10”和“00”, 分别对应十进制数 2 和 0, 因此路径为“第 2 象限”→“第 0 象限”。依次构建该路径上的内部节点, 最终定位到关键节点并为其生成 4 个子节点, 对应区域索引编号为 5、6、7、8。

用户端根据接收到的关键路径编码重构出空间分割结构后, 可以结合自身真实位置判断所处的节点区域, 并进一步获得该区域的 Hilbert 索引编码。当用户发起 LBS 请求时, 为避免潜在攻击者通过监听/截获通信数据包获得用户真实位置, 可以对所在区域的 Hilbert 索引编码进行随机响应扰动后再提交给 LBS 服务器, 以实现位置编码的 LDP 保护。本文对于用户所处区域的 Hilbert 索引编码 Z , 随机选择其中的某一位, 按照式(8)所示的概率函数进行 W-RR^[19]随机响应扰动。

$$\Pr[Z'[i] = 1] = \begin{cases} \frac{e^c}{e^c + 1}, & Z[i] = 1 \\ \frac{1}{e^c + 1}, & Z[i] = 0 \end{cases} \quad (8)$$

3.3 空间分割结构动态调整策略

用户位置信息具有动态变化特性，其空间分布密度可能随时间推移发生明显变化。若采用周期性完全重构四叉树的方法适应此类变化，不仅会产生高昂的计算成本，更重要的是忽略了实际位置变迁中普遍存在的时间局部性规律（即相邻时间段内用户分布模式虽存在变化，但其宏观空间结构通常保持较高连续性），仅少数情况下会发生剧烈的全局性突变。为使空间分割结构能够持续适应用户位置分布的变化，LBS服务器端需要定期对收集到的用户扰动位置数据进行聚合分析，并据此对下一时段的空间分割结构进行动态调整。本文提出的空间分割结构动态调整策略如算法3所示。

算法3 空间分割结构动态调整算法

输入 下一时段的空间分割结构 T 、用户扰动位置编码集合 S 、均匀性阈值 θ 、区域统计阈值 δ 、LBS 最小服务范围 γ

输出 动态调整后的空间分割结构 T^*

1) 将用户扰动位置编码集合 S 映射到空间分割结构 T ，统计每个区域的用户数量

2) **for** 每个区域 $R \in T$ **do**

3) **if** R 为叶子节点 **then**

4) **if** (R 的覆盖范围 $> \gamma$ 且 R 的统计值 $> \delta$ 且不满足均匀性条件 θ) **then**

5) 将 R 分割为 4 个子区域 // 3 个条件均满足时要求进一步细化，继续分割

6) **end if** // 否则满足分割终止条件，停止分割

7) **else if** (R 的子区域数量 = 4 且均为叶子节点) **then**

8) 计算 R 的均匀性指标 $U(R)$ // 使用式(2)判断是否合并

9) **if** 不满足均匀性条件 θ **then**

10) 计算 4 个子区域合并后的统计值 C

11) **if** $C < \delta$ **then**

12) 合并 4 个子区域为 R ，设为叶子节点 // 区域合并操作，停止分割

13) **end if** // 否则不满足合并条件，继续分割

14) **end if** // 否则满足均匀性条件，停止分割

15) **else if** R 的子区域数量 $\neq 4$ **then**

16) **continue**

17) **end if**

18) **end for**

19) **return** T^*

算法3主要包含以下两个核心操作。

1) 区域合并。针对当前区域首先判断其是否包含子区域，若当前区域不包含子区域（即当前区域为叶子节点），则保持其结构不变。若当前区域包含子区域，则进一步判断其子区域的数量和分布情况。若子区域数量不是 4，则保持当前结构不变。若包含完整的 4 个相邻子区域（均为叶子节点），则进行均匀性判断。若不满足区域均匀性条件（式(2)），则计算 4 个子区域合并后的统计值。若合并后的统计值达到预设的阈值 δ ，则保持当前结构不变；否则将 4 个子区域合并为一个区域。

2) 区域细化。针对当前区域首先判断其是否为叶子节点，若不是叶子节点，则保持当前结构不变；若是叶子节点，则进一步判断该区域的统计情况。若区域覆盖范围大于 LBS 服务的最小范围 γ 、区域统计值超过预设的阈值 δ 且不满足均匀性条件（式(2)），则将该区域进一步分割为 4 个子区域。若区域覆盖范围小于 LBS 服务的最小范围 γ ，或者区域统计值未超过预设的阈值 δ ，或者该区域满足均匀性条件（式(2)），则保持当前结构不变。

上述动态调整策略采用分层决策机制，以确保空间分割结构能够适应用户位置分布的变化。首先，在区域合并操作中，遵循自底向上的处理顺序，将“4 个子区域均为叶节点”作为区域合并的前提条件，从而确保合并操作从树结构的末端逐层向上推进。该机制能够有效应对因历史位置密集而被过度细分、当前却趋于稀疏的区域，逆转此前不必要的空间分割，同时避免因误合并包含复杂分布的节点而造成信息损失。其次，通过引入均匀性判定来确保合并操作的合理性。直观上，若父节点区域分布均匀，则其分割得到的子节点区域也必然均匀；相应地，当所有子节点区域均满足均匀性条件时，合并后形成的父节点区域也具备分布均匀性。均匀性判定机制能够有效避免对用户分布不均匀的区域进行错误合并，

从而保障位置聚合统计结果的可用性和后续 LBS 的准确性。最后，区域合并后的统计值必须小于预设阈值 δ ，防止生成用户过度集中的“热点区域”，确保空间分割的粒度与用户实际分布密度相匹配。

区域细化操作首先判定“当前区域是否为叶节点”，确保操作仅在叶子节点层面执行，避免破坏已有的空间分割结构。其次，判断当前区域的覆盖范围是否大于 LBS 最小服务范围 γ ，保证细化后的子区域仍具有实际服务意义，防止过度细分导致区域碎片化。此外，该操作还受到区域内统计值超过阈值 δ 且不满足均匀性条件的双重约束，从而确保细化仅针对那些用户密度高、分布不均匀、需要更精细管理的区域，避免对分布已趋稳定的区域进行不必要的再分割。

算法 3 的时间复杂度分析：算法 3 首先将 m 个扰动位置编码映射到空间分割结构中。由于映射路径的最大深度为 h ，因此该阶段的时间复杂度为 $O(m \cdot h)$ 。随后，算法 3 依次判断空间分割结构中的 t 个节点是否满足细化或合并条件。每个节点的判断与更新操作的时间复杂度为 $O(1)$ ，因此该部分的整体复杂度为 $O(t)$ 。综上，算法 3 的总时间复杂度为 $O(m \cdot h + t)$ 。

3.4 安全性分析

本节将证明所提 DLDP-CP 方法能够为用户位置提供严格的 ε -本地化差分隐私保护，并基于不同攻击场景分析其安全性。

证明：在 DLDP-CP 方法中，用户的隐私信息为其真实位置所对应的 Hilbert 编码 Z ，服务器最终接收到的是在用户端经过随机扰动后生成的 Hilbert 编码 Z' 。该机制所提供的隐私保护核心源于用户端所执行的随机响应过程，其形式化定义如式(8)所示。

假设 $Z(b_i)$ 和 $Z'(b'_i)$ 分别为原始编码和扰动编码的第 i 位。根据 LDP 的并行组合特性（定理 2），有以下等式成立。

$$\Pr[Z'|Z] = \Pr[Z'(b'_i) = 1|Z(b_i)] \quad (9)$$

同理，对于另一个位置编码 Z^* ，有以下等式成立。

$$\Pr[Z'|Z^*] = \Pr[Z'(b'_i) = 1|Z^*(b_i)] \quad (10)$$

则有

$$\begin{aligned} \frac{\Pr[Z'|Z]}{\Pr[Z'|Z^*]} &= \frac{\Pr[Z'(b'_i) = 1|Z(b_i)]}{\Pr[Z'(b'_i) = 1|Z^*(b_i)]} \leq \\ &= \frac{\max \Pr[Z'(b'_i) = 1|Z(b_i)]}{\min \Pr[Z'(b'_i) = 1|Z^*(b_i)]} = \\ &= \frac{\Pr[Z'(b'_i) = 1|Z(b_i) = 1]}{\Pr[Z'(b'_i) = 1|Z^*(b_i) = 0]} = \\ &= \frac{e^\varepsilon / (e^\varepsilon + 1)}{1 / (e^\varepsilon + 1)} = e^\varepsilon \end{aligned} \quad (11)$$

因此，本文所提方法严格满足 ε -本地化差分隐私的定义，能够为用户真实位置提供相应的隐私保护。在此机制下，即使攻击者获得扰动位置编码 Z' ，也无法有效推断出用户的真实原始位置。同时，该方法的隐私保护强度与隐私预算 ε 的取值直接相关。 ε 越小，所提供的隐私保护强度越大。

假设攻击者具备监听所有通信信道的能力，结合图 1 所示的交互流程，针对以下 3 种情形对本方法的安全性进行评估。

1) 攻击者截获服务器下发的关键路径编码。在 DLDP-CP 中，服务器向所有用户下发的是关键路径编码集合 E 和最大深度 h 。这些信息描述的是服务器端对整个地理空间的公开划分规则，不包含任何特定用户的个人信息。即使攻击者截获这些参数，最多能重构出空间网格的划分方式，但无法从中推断出用户的真实位置，该威胁在模型的隐私保障范围内。

2) 攻击者截获用户提交的扰动位置编码。该场景为 LDP 模型的核心防御目标。在 DLDP-CP 中，用户仅向服务器提交在本地端完成扰动的 Hilbert 编码 Z' ，其真实编码 Z 从未离开用户设备。鉴于扰动过程采用了满足 ε -本地化差分隐私的随机响应机制，攻击者即使截获了 Z' ，由于随机化过程的不可逆性，也无法确切地反推出原始编码 Z 。攻击者的任何推断能力均被隐私预算 ε 严格限制，因此用户的真实位置得到了有效保护。

3) 攻击者截获服务器返回的服务结果。用户

提交扰动位置后，服务器基于该扰动位置提供服务。攻击者如果截获了服务结果，最多只能反推出服务是基于哪个位置发起的。因此，用户隐私在这种场景下同样得到了保护。

在此场景中，用户向服务器提交的是经过扰动的位置编码 Z' ，而服务器返回的服务结果也是基于该扰动位置编码生成的。攻击者即便截获服务结果，至多只能推断出该服务响应所对应的扰动位置编码。由于 Z' 本身就是经过隐私保护的、非真实的位置编码，攻击者依然无法触及用户的真实位置编码 Z ，因此用户的真实位置隐私在此场景下依然得到有效保护。

4 实验与结果分析

为全面评估本文所提出的DLDP-CP位置保护方法，本文分别从用户端扰动位置的数据可用性、服务器端位置聚合的准确度、位置编码算法的运行效率及空间分割结构动态调整效率等维度，将本文方法与现有LDP位置保护方法进行对比分析。所选取的对比方法如下。

1) DPL-HC (differential privacy location protection scheme based on Hilbert curve) 方法^[12]：采用四叉树空间划分结合Hilbert曲线索引与Laplace加噪机制。

2) GT-R (grid-based quadtree range query) 方法^[10]：基于均匀四叉树分割结构与空间索引的范围查询方法。

3) LDPHE (local differential privacy location protection method using Hilbert encoding) 方法^[11]：采用均匀四叉树分割和Hilbert曲线编码索引的LDP位置保护方法。

4) LDPORR (local differential privacy location protection method based on optimized random response) 方法^[23]：基于均匀四叉树分割、Hilbert曲线编码和优化随机响应的LDP位置保护方法。

5) LDPHC (local differential privacy location protection for mobile terminals based on Huffman coding) 方法^[13]：采用二叉树分割索引和Huffman编码的LDP位置保护方法。

实验平台配置为：AMD Ryzen7 4700U处理器（8核，2.00 GHz）、16 GB内存、Windows 11

操作系统。所有算法均基于Python 3.7环境实现。

实验选用纽约出租车管理委员会提供的Yellow_tripdata数据集和北京出租车数据集进行验证，数据集的属性如表1所示。

表1 数据集属性
Table 1 Dataset attributes

数据集	位置范围	位置数据量
Yellow_tripdata	40.54°N~41.02°N, -74.3°W~-73.52°W	160 805
北京出租车数据集	39.6°N~40.2°N, 116.1°E~116.7°E	218 874

4.1 实验设置与评估指标

为全面评估本文所提方法（DLDP-CP）的性能，本文实验将从数据可用性、聚合准确度、运行效率及动态调整效率4个维度，将本文方法与多种主流的LDP位置保护方法进行对比。

在数据可用性方面，为从用户体验层面评估扰动位置的可用性，本文采用扰动位置与真实位置之间的平均距离误差（average distance error, ADE）作为评价指标，用来衡量隐私保护机制引入的位置服务质量损失。该指标能够有效反映隐私保护强度与服务质量之间的平衡关系，其具体计算方式如式(12)所示。

$$ADE = \frac{1}{m} \times \sum_{i=1}^m \text{dis}(x_i, x'_i) \quad (12)$$

其中， m 表示实验数据集中的总数据量， x_i 和 x'_i 分别表示第 i 个真实位置和扰动位置， $\text{dis}(\cdot)$ 函数用于计算两个位置之间的欧几里得距离。

在聚合准确度方面，KLD (Kullback-Leibler divergence) 可用于衡量两个概率分布的差异。用于评估平面位置分布时，KLD可以反映所有用户的原始位置概率分布与隐私保护后位置概率分布之间的差异。其数值越小，说明经过隐私保护处理后的位置概率分布与原始位置概率分布越接近，也说明服务器端聚合统计的位置结果更接近原始情况。该指标将用于两个场景的评估：一是在静态环境下比较不同LDP方法的聚合准确度；二是在动态环境中验证本文所提动态调整策略的适应性与可用性。KLD的具体定义如式(13)

所示。

$$\text{KLD}(I_{\Omega}|J_{\Omega}) = \sum_{l \in \Omega} I(l) \log \left(\frac{I(l)}{J(l)} \right) \quad (13)$$

其中, I_{Ω} 和 J_{Ω} 分别表示空间范围区域 Ω 中全部用户的原始位置概率分布和经算法扰动后的位置概率分布。 $I(l)$ 和 $J(l)$ 分别表示第 l 个区域的原始位置和扰动位置的概率分布。

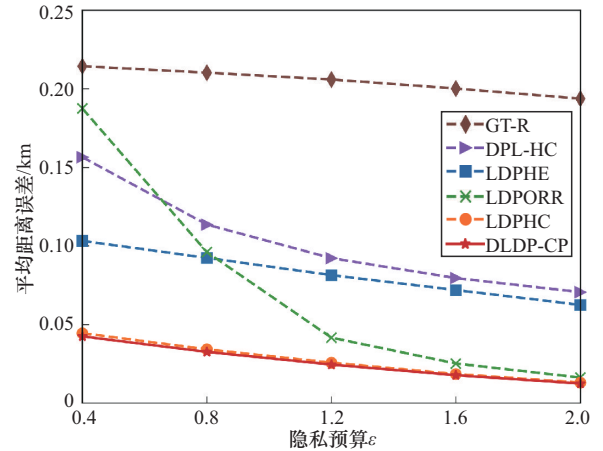
为评估算法的运行效率, 本文将对分析各方法的时间复杂度、编码排序效率、通信开销。

为评估本文所提动态调整策略的效率, 实验采用平均调整时间与累积调整时间作为指标, 二者分别反映服务器在连续时间段内执行空间结构调整或完整重构所需的计算开销, 从而验证该策略在适应数据分布动态变化时所具备的效率优势。

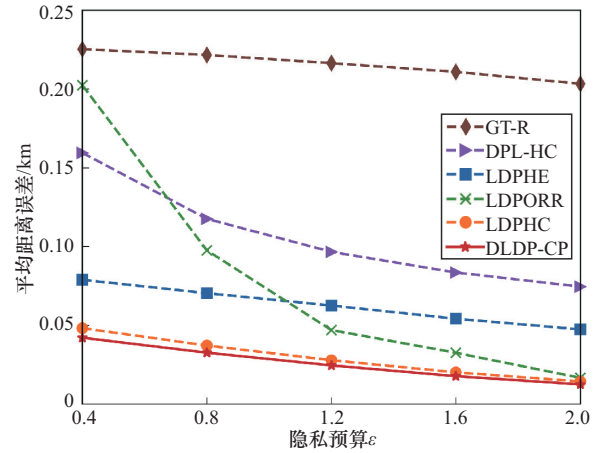
为确保实验的公平性与结果的可靠性, 所有对比方法均设置相同的空间分割深度 ($h = 7$), 每种方法进行 500 次实验后取平均值作为最终结果。该深度参数的设定旨在平衡方法性能差异的显著性与实验计算效率。若空间分割深度过小, 则区域划分过于粗略, 每个区域面积过大, 难以体现不同方法在细粒度位置处理上的差异; 反之, 若空间分割深度过大, 将显著增加不必要的计算负担, 影响运行效率。

4.2 用户端扰动位置的可用性

图 6 分别展示了不同方法在不同数据集上的平均距离误差随隐私预算 ϵ 变化的情况。结果表明, 随着隐私预算 ϵ 的增大, 所有方法的平均距离误差均呈下降趋势。这是由于较大的隐私预算 ϵ 值意味着引入的随机噪声更少, 从而使扰动位置更接近真实位置。在相同数据集与隐私预算 ϵ 设置下, 各方法性能存在显著差异, 尤其在低 ϵ 区间 (即隐私保护要求更为严格时), 不同方法在隐私与可用性之间的权衡能力差异更为突出。具体来看, GT-R 方法的平均距离误差最大, 而 LDPORR 方法在多数场景下优于 DPL-HC 与 LDPHE 方法。LDPHC 方法凭借其二叉树邻近节点扰动机制, 整体表现较好。本文提出的 DLDP-CP 在所有测试中略优于 LDPHC 方法, 在保持相同隐私保护级别的情况下, 进一步减少了位置扰动引入的误差。



(a) Yellow_tripdata 数据集实验结果



(b) 北京出租车数据集实验结果

图 6 平均距离误差对比

Figure 6 Comparison of average distance error

上述性能差异主要源于各方法的内在机制。GT-R 方法基于四叉树分割, 用户随机选择树的某一层并对该层的所有节点应用随机响应机制。若所选层级靠近根节点, 扰动位置可能与真实位置产生显著偏差; 同时, 对每位编码独立进行扰动进一步增大了偏离程度。DPL-HC 方法通过 Hilbert 曲线对空间网格进行遍历编码, 并对区域索引施加拉普拉斯噪声。在隐私预算 ϵ 较小时, 噪声幅度较大, 容易导致扰动位置严重偏离实际位置。LDPHE 方法依据用户在 Hilbert 象限中的位置生成二进制编码, 并随机选取部分编码位进行随机响应扰动, 因而在多数情况下产生相对较小的平均距离误差。LDPORR 方法在 LDPHE 方法的基础上, 根据编码中 0/1 比特的分布调整扰动方式, 显著提高了扰动后位置仍位于原始位置附近的概率, 从而进一步减小

了平均距离误差。LDPHC方法则通过将相邻区域映射到二叉树的左右节点,有效实现了对二叉树邻近节点的扰动,从机制上约束了位置偏离程度,降低了服务质量损失。本文提出的DLDP-CP方法能够取得最优性能,关键在于其对现实世界中复杂位置分布的自适应能力。该算法在数据稀疏区域实施粗粒度分割,在密集区域则实施细粒度分割,并能够根据空间均匀性动态调整分割策略。相较于传统的固定分割方法,基于数据分布均匀性的动态调整方法能够更好地适应真实世界位置数据的复杂分布特性,因此在同等隐私保护强度下实现了更小的位置扰动误差。

4.3 服务器端位置聚合的准确度

图7展示了不同方法在两个数据集上的KLD随隐私预算 ϵ 变化的情况。可以观察到,所有方法的KLD均随隐私预算 ϵ 的增大而呈下降趋势。这是由于随着隐私预算 ϵ 的增大,各方法引入的扰动幅度相应减小,造成扰动后位置的概率分布更接近原始位置的概率分布。在相同隐私预算条件下,本文所提DLDP-CP方法的KLD始终低于其他对比方法。较低的KLD表明,经DLDP-CP处理后的整体数据分布更好地保留了原始位置数据的统计特征。这一特性对于服务器端进行宏观统计分析具有重要意义。更小的平均距离误差也证明了本文方法能够保证扰动后的用户位置概率分布更接近真实位置概率分布,从而在服务器端

聚合统计的位置结果更接近原始位置分布情况,数据的可用性更高。

4.4 位置编码方法的运行效率

位置隐私保护方法的运行效率直接决定了用户终端的计算开销和通信成本,尤其对于资源受限的移动设备和大规模位置服务系统而言,高效的编码方案至关重要。为验证本文所提DLDP-CP方法的运行效率,本节从时间复杂度、编码排序效率、通信开销3个维度,将本文方法与现有典型方法进行对比。

表2对各种方法的时间复杂度进行了对比。从表中数据来看,GT-R方法和DPL-HC方法的时间复杂度随空间分割粒度 N 的增加呈平方级增长;LDPHE与LDPORR方法的时间复杂度略低于平方级;LDPHC方法的时间复杂度最高,接近立方级;本文提出的DLDP-CP方法采用非均匀空间分割策略,能够根据用户分布密度动态调整结构,因此在处理数据分布不均的大规模位置数据时,实际运行效率更高。这种自适应机制使DLDP-CP在保持理论复杂度优势的同时,在实际应用场景中也展现出更优的计算性能。

编码排序效率直接关系到用户终端的计算开销和数据处理速度。DLDP-CP方法和LDPHE方法都使用Hilbert曲线进行空间索引编码。本文对上述两种算法的编码排序效率开展了实验对比。为消除单次结果的随机性影响,每种方法在每个数据集上各进行500次独立实验,取平均值作为

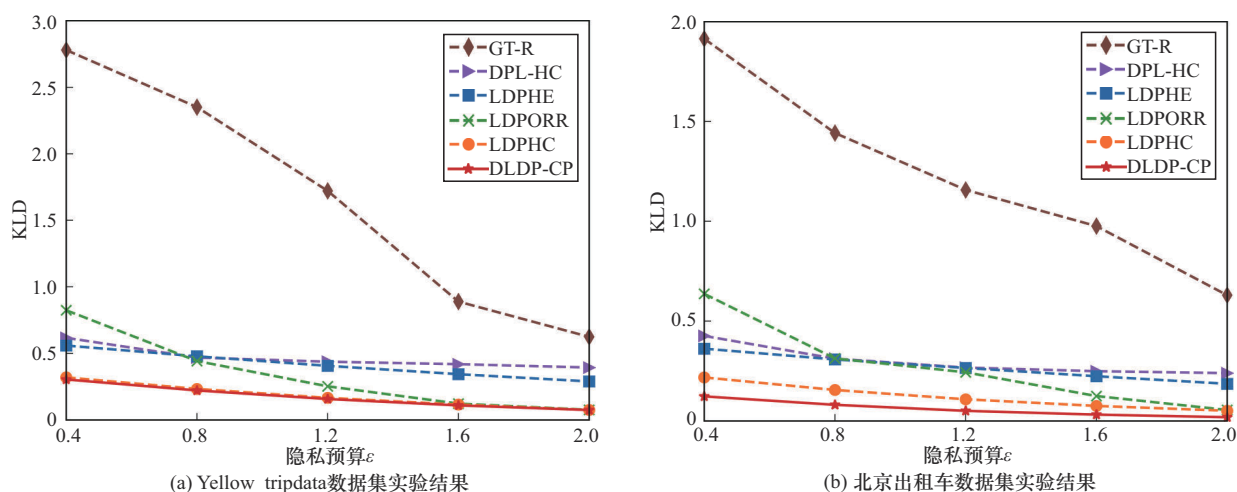


图7 位置聚合结果的KLD对比
Figure 7 Comparison of KLD of location aggregation results

实验结果。实验结果如表 3 所示,从表中数据可以看出,DLDP-CP 方法在编码排序效率方面展现出显著优势,在两个数据集上平均比 LDPHE 方法快约 1.36 倍。该性能提升主要得益于 DLDP-CP 方法采用的非均匀四叉树分割策略。该策略能够根据用户分布密度动态调整区域划分粒度,在数据稀疏区域采用粗粒度划分,有效减少了需要编码排序的区域单元数量。这一特点使 DLDP-CP 在处理大规模位置数据时能够显著减少计算开销,提升整体处理效率。

表 2 各方法时间复杂度对比
Table 2 Comparison of time complexity
for each method

方法	时间复杂度
GT-R	$O(N^2)$
DPL-HC	$O(N^2)$
LDPHE	$O(N \log N)$
LDPORR	$O(N \log N)$
LDPHC	$O(N^2 \log N)$
DLDP-CP	$O(m + r \cdot h)$

表 3 编码排序效率对比
Table 3 Comparison of coding sorting efficiency

数据集	编码排序耗时/s	
	LDPHE	DLDP-CP
Yellow_tripdata	4.723 620 891 571 0	3.471 866 965 293 8
北京出租车数据集	5.848 973 424 434 6	4.287 522 525 787 3

表 4 对各种方法的上/下行数据量进行了比较。

表 4 各方法上/下行数据量比较
Table 4 Comparison of upstream and downstream
data volume for each method

方法	上行数据量	下行数据量
GT-R	$2\lceil \log_2 N \rceil + 1$	$2\lceil \log_2 N \rceil + 1$
DPL-HC	$2\lceil \log_2 N \rceil$	$\lceil \log_2 N \rceil$
LDPHE	$2\lceil \log_2 N \rceil$	$N^2 \cdot 2\lceil \log_2 N \rceil$
LDPORR	$2\lceil \log_2 N \rceil$	$N^2 \cdot 2\lceil \log_2 N \rceil$
LDPHC	$2\lceil \log_2 N \rceil$	$N^2 \cdot 2\lceil \log_2 N \rceil$
DLDP-CP	$2\lceil \log_2 N \rceil$	$k \cdot 2\lceil \log_2 N \rceil$

在上行数据量方面,GT-R 方法在最坏的情况下需要选择叶子层的节点进行扰动,此时需要上传的数据量为 $2\lceil \log_2 N \rceil + 1$ 。DPL-HC、LDPHE 和 LDPORR 方法上传的数据量取决于 Hilbert 曲线的分割阶数,其长度为 $2\lceil \log_2 N \rceil$ 。Hilbert 曲线阶数每增加一阶,编码长度将增加 2 bit。LDPHC 算法的编码长度也是 $2\lceil \log_2 N \rceil$,但分割深度每增加一层,对应的 Huffman 编码长度增加 1 bit。在相同的分割粒度下,本文提出的 DLDP-CP 方法在保持相同编码长度 $2\lceil \log_2 N \rceil$ 的前提下,在稀疏区域减少冗余分割以压缩数据量,在密集区域则通过局部细化提升精度,避免了固定分割粒度产生的冗余数据传输,在复杂场景下能够实现更高效的空间编码和通信性能。

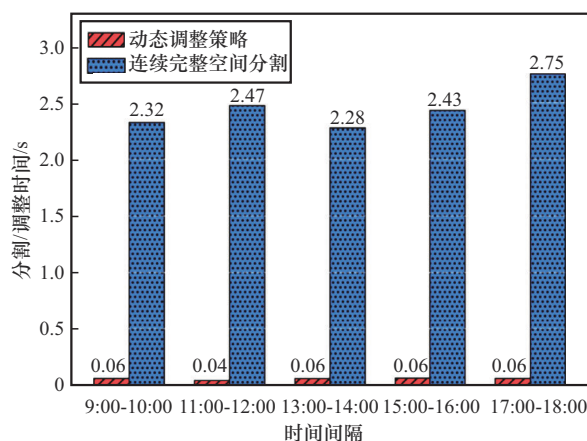
在下行数据量方面,GT-R 方法需要根据二维平面的分割粒度 ($N \times N$) 构建一个叶子节点为 N^2 的完全四叉树,服务器需要向用户传输整个四叉树结构,其下行数据量为 $2\lceil \log_2 N \rceil + 1$ 。DPL-HC 方法只需传输分割深度,下行数据量为 $\lceil \log_2 N \rceil$,通信效率最高。LDPHE 和 LDPORR 方法不仅需要传输分割深度,还要预先计算并传输所有区域 (N^2 个) 的 Hilbert 编码,每个编码的长度为 $2\lceil \log_2 N \rceil$,LDPHC 的编码长度也为 $2\lceil \log_2 N \rceil$,因此这 3 种方法的下行数据总量均为 $N^2 \cdot 2\lceil \log_2 N \rceil$ 。本文提出的 DLDP-CP 方法通过关键路径编码机制显著优化了下行数据传输。每条关键路径包含 $\lceil \log_2(2h-1) \rceil$ 位前缀编码和 $2d$ 位路径编码。其下行数据量为 $k \cdot 2\lceil \log_2 N \rceil$,其中 k 为关键路径数量。DLDP-CP 方法采用非均匀空间分割策略, k 值通常远小于 N^2 ,因此显著减少了下行通信开销。

为更直观地体现本文所提关键路径机制在降低通信成本方面的实际效果,本文在最大分割深度 ($h=7, N=128$) 条件下对各算法的下行数据量进行了量化测算,结果如表 5 所示。其中, DPL-HC 方法只需下发空间分割的深度 ($h=7$),其下行数据量为 3 bit,是所有方法中最少的。然而,该方法的分割机制建立在数据均匀分布的假设之上,这种理想化的分布假设无法适应真实场景

中位置数据分布的异质性, 导致所生成扰动位置的可用性显著下降。图6与图7中的实验结果印证了该局限性。相比之下, GT-R方法需要下发树结构中叶子节点的信息, $h=7$ 时共有16 384个叶子节点, 下行数据量为32 769 bit。LDPHE、LDPORR和LDPHC方法则需要传输全部空间单元(共16 384个)的完整编码信息, 下行数据量为229 376 bit。在同等实验条件下, 本文提出的DLDP-CP方法在两个数据集上的下行数据量分别为4 736 bit与6 192 bit。与LDPHE、LDPORR、LDPHC方法相比, DLDP-CP方法的下行数据量降幅超过97%; 相较于GT-R方法, DLDP-CP方法的下行数据量降幅超过80%。这一结果充分证明, 关键路径机制能够有效缓解传统LDP方法中普遍存在的通信瓶颈问题, 在保持对异质数据分布适应能力的同时, 显著降低了通信开销, 从而提升系统在大规模用户场景下的可扩展性与运行效率。

表5 $h=7$ 时各方法的下行数据量
Table 5 Downstream data volume for each method ($h=7$)

方法	Yellow_tripdata数据集 数据量/bit	北京出租车数据集 数据量/bit
GT-R	32 769	32 769
DPL-HC	3	3
LDPHE	229 376	229 376
LDPORR	229 376	229 376
LDPHC	229 376	229 376
DLDP-CP	4 736	6 192

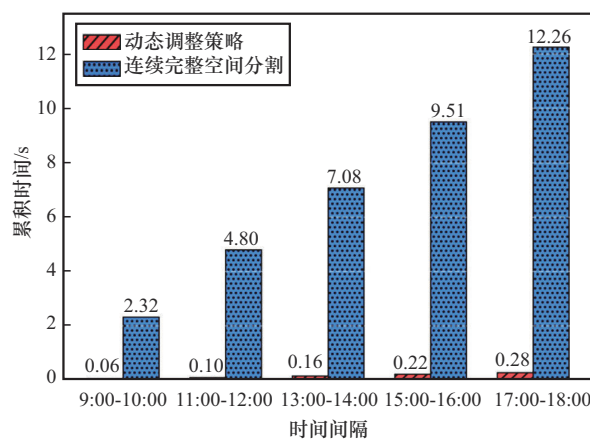


(a) 单次执行时间对比

4.5 空间分割结构的调整效率与适应性

为验证本文提出的空间分割结构动态调整策略在提升系统效率与维持数据可用性方面的效果, 模拟用户位置分布随时间动态变化的场景, 将其与在每个时段均执行完整空间分割的基线方法展开对比实验。实验重点考察两类指标: 一是完成空间结构重建所需的平均时间与累积时间, 用于衡量计算效率; 二是两种方法所得分割结构与真实位置分布之间的KLD, 用于评估数据可用性。为保证可用性比较的公平性, 所有KLD的计算均在统一的隐私预算($\epsilon=1$)下进行。实验过程中将数据集按照时间顺序分割为6个连续的时段(6:00—8:00、9:00—10:00、11:00—12:00、13:00—14:00、15:00—16:00、17:00—18:00)。动态调整策略在初始时段(6:00—8:00)执行一次完整的非均匀二叉树分割; 后续时段则基于前一阶段的用户位置分布, 仅对发生显著变化的区域进行局部调整, 并复用其余未明显变动区域的历史分割结构。作为对比, 基线方法在每个时段均基于当前用户位置分布重新执行完整的非均匀二叉树构建操作。

图8和图9分别展示了两种方法在空间分割结构调整效率方面的对比结果。实验结果显示, 空间分割结构动态调整策略在各时段均保持较短的执行时间, 而连续完整空间分割方法的执行时间显著更长。在Yellow_tripdata数据集上, 两种方法的执行时间均较为平稳; 在北京出租车数据集上, 连续完整空间分割方法在高峰时段(15:00—16:00)执行时间达到峰值。总体来看, 在不同



(b) 累积时间对比

图8 Yellow_tripdata数据集空间分割结构调整效率

Figure 8 Efficiency of spatial partition structure adjustment on Yellow_tripdata dataset

数据集上, 动态调整策略相比连续完整空间分割方法节省超过95%的时间。究其原因, 连续完整空间分割方法需要在每个时段重新分析全量用户分布并构建完整的非均匀二叉树, 其计算开销随数据规模与分布复杂度的上升而显著增加, 尤其在高峰时段更加明显。相比之下, 动态调整策略充分利用位置数据时空连续性和上一时段的空间分割信息, 仅对发生显著变化的区域进行局部调整, 从而大幅减少重复计算, 实现了效率提升。累积时间对比进一步突显了两种方法的效率差距。动态调整策略的累积时间始终维持在极低水平, 仅为连续完整空间分割方法的2%左右。这表明该策略不仅在单次调整中具有更高效率, 更在长期运行中具有显著的累积性能优势, 对需要持续处理大规模动态位置数据的LBS系统具有重要的实用价值, 能够有效减少服务器计算资源消耗, 并提高系统的响应速度。

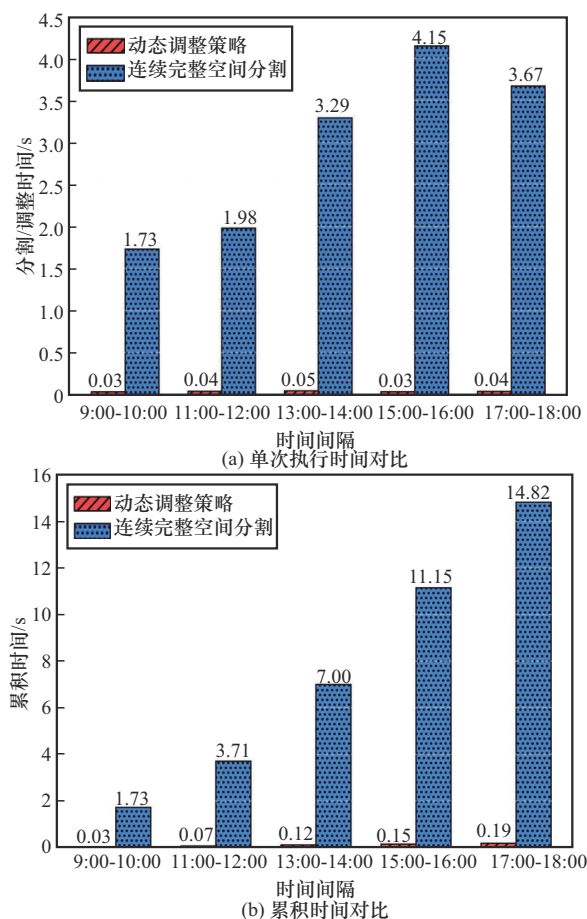


图9 北京出租车数据集空间分割结构调整效率

Figure 9 Efficiency of spatial partition structure adjustment on Beijing Taxi dataset

图 10 对比了各时段内两种方法所得空间分割结构与真实位置分布结构之间的KLD。可以看出, 本文提出的动态调整策略在不同数据集、不同时段内均能保持较低的KLD, 说明其生成的空间结构更贴近真实位置分布, 具有更优的数据可用性。这一效果主要得益于动态调整策略的双重机制: 一方面, 该策略继承了上一时段的有效结构信息, 保持了分割边界的稳定性; 另一方面, 它对发生显著变化的局部区域进行针对性微调, 实现按需调整。该机制充分利用了位置数据在时空维度上的连续性特征, 有效避免了细微波动导致的边界频繁抖动, 从而能够持续、精准地拟合动态变化的用户位置分布。

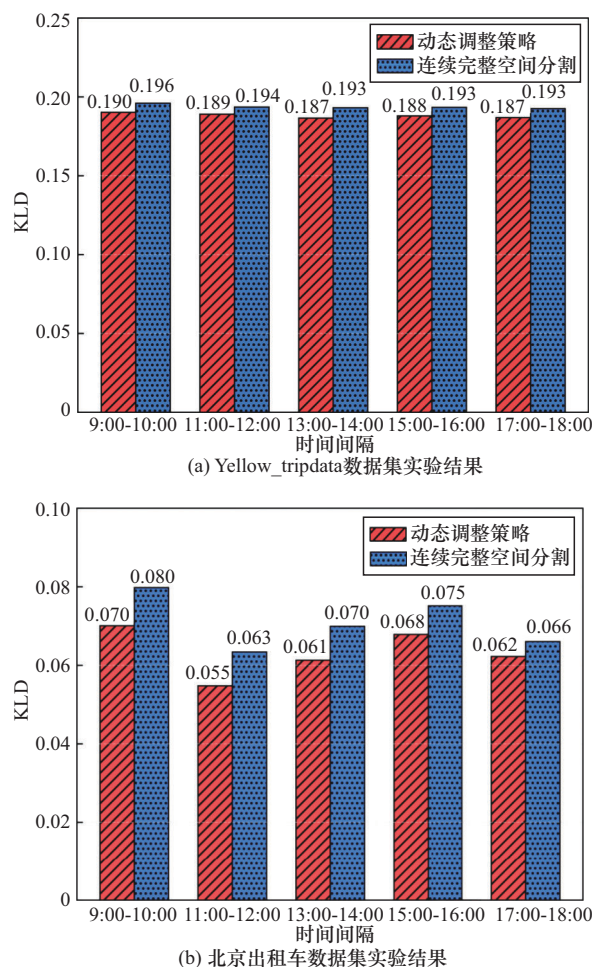


图 10 动态调整策略与连续完整空间分割方法的KLD散度比较
Figure 10 Comparison of KLD for dynamical adjusting strategy and continuous complete space partitioning method

结合图 8 与图 9 的调整效率分析, 以及图 10 的数据可用性结果可知, 本文提出的空间分割结

构动态调整策略在实现计算效率数量级提升的同时,保持了较优的数据可用性,证明了该策略在真实动态LBS系统中能够高效地平衡适应性与优化效果,具备较高的应用价值。

5 结束语

随着LBS的广泛普及,位置隐私保护已成为一项关键挑战。如何在有效保护用户位置隐私的同时,提高数据的高可用性,成为当前隐私保护研究中的重要课题。传统的位置隐私保护方法往往难以在隐私保护强度与数据可用性之间实现良好平衡,存在一定的局限性。为此,本文提出一种基于关键路径的动态LDP位置保护方法。该方法依据用户位置的实际分布密度,采用非均匀四叉树空间分割与Hilbert曲线索引,显著减少了位置编码过程中的冗余计算;通过设计关键路径编码机制,进一步减少了服务器与用户端之间的数据传输开销,优化了系统通信效率;引入了空间分割结构动态调整策略,在保障算法高效运行的同时,有效维持了空间分割结构对动态位置分布的适应性。

本文提出的DLDP-CP方法适用于用户分布呈现显著时空不均匀性的大规模LBS系统,在智慧交通管理、共享出行调度、外卖配送优化等场景中具有应用潜力。该方法在用户分布高度不均匀时性能优势尤为突出。实际部署时,需要结合具体场景合理设置隐私预算与动态调整周期等关键参数。此外,该方法的有效实施需要服务器端具备一定的计算能力和用户分布监控能力,且在初始化阶段需要积累足够的历史数据以构建有效的初始空间分割结构。

当然,本文所提方法也存在一些局限性。首先,空间分割结构动态调整策略的有效性依赖于位置数据在时空维度上的连续性假设。该策略在处理具有周期性或渐变特征的数据时表现良好,但在面对大型集会、紧急疏散等突发事件导致的瞬时性、剧烈且无规律的用户分布变化时,可能出现一定的“调整滞后”。未来的工作可探索引入短期预测模型(如基于时序分析或图神经网络的流量预测方法),以增强系统对突发分布变化的前瞻性适应能力。其次,随着LBS需求的不断变化,移动终端的动态特性对隐私保护策略

的灵活性提出了更高的要求。未来可进一步探索动态隐私预算分配机制,使隐私保护强度能够随用户移动模式与环境上下文自适应调整,从而更好地适应复杂多变的移动场景。此外,本文实验主要基于有限的时间切片对动态调整策略的瞬时效率进行了验证。下一步将通过长周期的连续实验,评估系统在包含复杂周期性模式与突发性事件场景下的真实性能与稳定性。最后,本文所采用的本地化随机响应机制较为简单,未来可结合LBS需求,设计更加合理或个性化的扰动方式,以进一步提升扰动后位置数据的可用性与服务价值。

参考文献:

- [1] XIAO Z R, LI P S, LIU C, et al. MACNS: a generic graph neural network integrated deep reinforcement learning based multi-agent collaborative navigation system for dynamic trajectory planning[J]. Information Fusion, 2024, 105: 102250.
- [2] ZHOU W, FU C, SANG C Y, et al. Next PoI recommendation based on graph convolutional networks and multiple context-awareness[J]. IEEE Transactions on Services Computing, 2025, 18(1): 302-313.
- [3] VAGHEFI M S, NAZARETH D L, NERUR S P, et al. Self-disclosure in online social networks: an empirical study of location-based check-ins and impression management[J]. Information & Management, 2024, 61(7): 104017.
- [4] QIU G Y, TANG G M, LI C D, et al. Differentiated location privacy protection in mobile communication services: a survey from the semantic perception perspective[J]. ACM Computing Surveys, 2024, 56(3): 1-36.
- [5] ZHOU X K, YANG Q Y, LIU Q, et al. Spatial-temporal federated transfer learning with multi-sensor data fusion for cooperative positioning[J]. Information Fusion, 2024, 105: 102182.
- [6] TANG L L, HE M X, XIONG L, et al. An efficient and privacy-preserving query scheme in intelligent transportation systems[J]. Information Sciences, 2023, 647: 119448.
- [7] LI Z J, MA J F, MIAO Y B, et al. Enabling efficient privacy-preserving spatiotemporal location-based services for smart cities[J]. IEEE Internet of Things Journal, 2024, 11(3): 5288-5300.
- [8] KASIVISWANATHAN S P, LEE H K, NISSIM K, et al. What can we learn privately? [J]. SIAM Journal on Computing, 2011, 40(3): 793-826.
- [9] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Local privacy and statistical minimax rates[C]//Proceedings of the 2013 51st Annual Allerton Conference on Communication, Control and Computing (Allerton). Piscataway: IEEE Press, 2013.
- [10] 张啸剑, 付楠, 孟小峰. 基于本地差分隐私的空间范围查询方法[J].

- 计算机研究与发展, 2020, 57(4): 847-858.
- ZHANG X J, FU N, MENG X F. Towards spatial range queries under local differential privacy[J]. *Journal of Computer Research and Development*, 2020, 57(4): 847-858.
- [11] 晏燕, 董卓越, 徐飞, 等. 一种 Hilbert 编码的本地化位置隐私保护方法[J]. *西安电子科技大学学报*, 2023, 50(2): 147-160.
- YAN Y, DONG Z Y, XU F, et al. Localized location privacy protection method using the Hilbert encoding[J]. *Journal of Xidian University*, 2023, 50(2): 147-160.
- [12] WANG J, WANG F, LI H T. Differential privacy location protection scheme based on Hilbert curve[J]. *Security and Communication Networks*, 2021, 2021(1): 5574415.
- [13] 晏燕, 吕雅琴, 李飞飞. 基于 Huffman 编码的移动终端本地差分隐私位置保护[J]. *计算机科学与探索*, 2025, 19(3): 802-817.
- YAN Y, LYU Y Q, LI F F. Local differential privacy location protection for mobile terminals based on huffman coding[J]. *Journal of Frontiers of Computer Science and Technology*, 2025, 19(3): 802-817.
- [14] 晏燕, 丛一鸣, MAHMOOD A, 等. 基于深度学习的位置大数据统计发布与隐私保护方法[J]. *通信学报*, 2022, 43(1): 203-216.
- YAN Y, CONG Y M, MAHMOOD A, et al. Statistics release and privacy protection method of location big data based on deep learning[J]. *Journal on Communications*, 2022, 43(1): 203-216.
- [15] 霍峥, 张坤, 贺萍, 等. 满足本地化差分隐私的众包位置数据采集[J]. *计算机应用*, 2019, 39(3): 763-768.
- HUO Z, ZHANG K, HE P, et al. Crowdsourcing location data collection for local differential privacy[J]. *Journal of Computer Applications*, 2019, 39(3): 763-768.
- [16] ZHANG E Z, GUAN Y G, LU R X, et al. An efficient heap tree-based range query scheme under local differential privacy[J]. *IEEE Internet of Things Journal*, 2024, 11(11): 20648-20659.
- [17] JU Z C, LI Y C. Local differential privacy-based privacy-preserving data range query scheme for electric vehicle charging[J]. *IEEE Transactions on Network Science and Engineering*, 2024, 11(1): 673-684.
- [18] WANG L X, YE Q Q, HU H B, et al. PriPL-tree: accurate range query for arbitrary distribution under local differential privacy[J]. *Proceedings of the VLDB Endowment*, 2024, 17(11): 3031-3044.
- [19] WARNER S L. Randomized response: a survey technique for eliminating evasive answer bias[J]. *Journal of the American Statistical Association*, 1965, 60(309): 63-69.
- [20] KAIROUZ P, BONAWITZ K A, RAMAGE D. Discrete distribution estimation under local privacy[C]//*Proceedings of the 33rd International Conference on Machine Learning*. 2016: 2436-2444.
- [21] WANG T H, BLOCKI J, LI N H, et al. Locally differentially private protocols for frequency estimation[C]//*Proceedings of the USENIX Security Symposium*. Berkeley: USENIX Association, 2017: 729-745.
- [22] ERLINGSSON Ú, PIHUR V, KOROLOVA A. RAPPOR: randomized aggregatable privacy-preserving ordinal response[C]//*Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. New York: ACM, 2014: 1054-1067.
- [23] YAN Y, CHEN J Z, MAHMOOD A, et al. LDPORR: a localized location privacy protection method based on optimized random response[J]. *Journal of King Saud University - Computer and Information Sciences*, 2023, 35(8): 101713.
- [24] YAN Y, YAN P B, MAHMOOD A, et al. Achieving local differential location privacy protection in 3D space via Hilbert encoding and optimized random response[J]. *Journal of King Saud University - Computer and Information Sciences*, 2024, 36(6): 102085.
- [25] 杨宏宇, 张恒鸣, 朱友文, 等. 面向 LBS 的 ADS-B 报文定位数据本地化差分隐私保护方法[J]. *网络与信息安全学报*, 2025, 11(4): 32-49.
- YANG H Y, ZHANG H M, ZHU Y W, et al. Differential privacy protection method for localization of ADS-B message positioning data oriented to LBS[J]. *Chinese Journal of Network and Information Security*, 2025, 11(4): 32-49.
- [26] ACHARYA J, SUN Z T, ZHANG H Y. Hadamard response: estimating distributions privately, efficiently, and with little communication[C]//*Proceedings of the 22nd International Conference on Artificial Intelligence and Statistics*. New York: PMLR, 2018: 1120-1129.
- [27] ZHAO D, CHEN H, ZHAO S Y, et al. FLDP: flexible strategy for local differential privacy[C]//*Proceedings of the 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Piscataway: IEEE Press, 2022: 2974-2978.
- [28] VARMA G, CHAUHAN R, SINGH D. Sarve: synthetic data and local differential privacy for private frequency estimation[J]. *Cybersecurity*, 2022, 5(1): 26.
- [29] HONG D, JUNG W, SHIM K. Collecting geospatial data under local differential privacy with improving frequency estimation[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2023, 35(7): 6739-6751.
- [30] FENG G H, WANG G J, PENG T. Toward answering federated spatial range queries under local differential privacy[J]. *International Journal of Intelligent Systems*, 2024, 2024(1): 2408270.
- [31] LI Z T, ZENG X Y, XIAO Y, et al. Pattern-sensitive local differential privacy for finite-range time-series data in mobile crowdsensing[J]. *IEEE Transactions on Mobile Computing*, 2025, 24(1): 1-14.
- [32] SUN X Y, YE Q Q, HU H B, et al. Generating location traces with semantic-constrained local differential privacy[J]. *IEEE Transactions on Information Forensics and Security*, 2024, 19: 9850-9865.
- [33] 叶青青, 孟小峰, 朱敏杰, 等. 本地化差分隐私研究综述[J]. *软件学报*, 2018, 29(7): 1981-2005.
- 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.
- [34] YAN Y, GAO X, MAHMOOD A, et al. Differential private spatial decomposition and location publishing based on unbalanced quadtree partition algorithm[J]. *IEEE Access*, 2020, 8: 104775-104787.

[作者简介]



晏燕（1980—），女，甘肃兰州人，兰州理工大学教授、博士生导师，主要研究方向为大数据隐私保护、时空位置数据采集与隐私保护、机器学习与隐私保护、区块链隐私保护等。



张艳莉（2000—），女，山西大同人，兰州理工大学硕士生，主要研究方向为隐私保护、个性化本地差分隐私。



刘坤（2001—），男，陕西咸阳人，兰州理工大学硕士生，主要研究方向为隐私保护、本地化差分隐私。



冯涛（1970—），男，甘肃临洮人，兰州理工大学研究员、博士生导师，主要研究方向为网络与信息安全。