计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
62(11): 2843−2854, 2025

群智感知中基于个性化差分隐私的真值发现方法

王涛春[1,2,3] 强 勇[1] 许 诺[1] 陈付龙[1,2,3] 谢 冬[1,2,3] 赵传信[1,2,3]

[1](安徽师范大学计算机与信息学院 安徽芜湖 241002)

[2](安徽省医学大数据智能系统工程研究中心(安徽师范大学) 安徽芜湖 241002)

[3](工业智能数据安全安徽省重点实验室(安徽师范大学) 安徽芜湖 241002)

(wangtc@ahnu.edu.cn)

Personalized Differential Privacy-Based Truth Discovery Method in Crowdsensing

Wang Taochun[1,2,3], Qiang Yong[1], Xu Nuo[1], Chen Fulong[1,2,3], Xie Dong[1,2,3], and Zhao Chuanxin[1,2,3]

[1](*School of Computer and Information*, *Anhui Normal University*, *Wuhu*, *Anhui* 241002)

[2](*Anhui Engineering Research Center of Medical Big Data Intelligent System* (*Anhui Normal University*), *Wuhu*, *Anhui* 241002)

[3](*Anhui Provincial Key Laboratory of Industrial Intelligence Data Security* (*Anhui Normal University*), *Wuhu*, *Anhui* 241002)

Abstract In crowdsensing systems, users complete sensing tasks by providing data, but variations in sensor precision, user behavior, and environmental factors lead to significant differences in data quality. Truth discovery techniques mitigate the impact of low-quality data by aggregating multiple user inputs with weighted mechanisms. However, existing methods often overlook personalized privacy needs, exposing sensitive user information. Meanwhile, encryption-based privacy protection mechanisms, though secure, suffer from high computational and communication overhead, making them impractical for large-scale crowdsensing applications. To address these challenges, we propose personalized differential privacy truth discovery (PDPTD), a framework that integrates local differential privacy (LDP) with truth discovery, ensuring both strong privacy protection and high-quality data aggregation. Specifically, PDPTD employs a randomized response mechanism, enabling users to dynamically adjust their data perturbation levels based on personalized privacy budgets. This flexible approach balances privacy protection and data utility, allowing users to contribute valuable data while safeguarding sensitive information. On the server side, PDPTD incorporates a weighted aggregation strategy that compensates for information loss caused by perturbation, effectively improving inference accuracy. Additionally, PDPTD introduces a dynamic user weighting mechanism, which assigns weights based on data quality. This ensures that even if some users select higher perturbation levels, the system can still infer results closed to the true values, maintaining data reliability and consistency.Theoretical analysis and experimental results demonstrate that PDPTD complies with LDP principles while ensuring high accuracy in final inferred results. This makes it a practical and efficient solution for large-scale crowdsensing applications, where balancing privacy, data utility, and computational efficiency is crucial.

Key words privacy protectionc; crowdsensing; truth discovery; personalization; local differential privacy

摘 要 在群智感知系统中,用户通过提供感知数据完成感知任务.然而,由于传感设备精度、用户行为以及环境条件等因素的影响,不同用户提供的数据质量存在显著差异.真值发现技术能够有效地消除低质

收稿日期: 2024-10-10; **修回日期**: 2025-04-15

基金项目: 国家自然科学基金项目(62272006, 61972438); 安徽省科技重点研究与开发计划项目(2022a05020049); 安徽省自然科学基金项目(2108085MF219); 芜湖市重点研发与成果转化项目(2023yf110)

This work was supported by the National Natural Science Foundation of China (62272006, 61972438), the Key Research and Development Program of Anhui Province (2022a05020049), the Natural Science Foundation of Anhui Province (2108085MF219), and the Key Research and Development and Achievement Transformation Projects in Wuhu City (2023yf110).

量数据影响,从而能够更好地利用感知数据,但现有的真值发现方法往往忽略用户个性化隐私要求,且基于加密的隐私保护技术难以应用于大量用户参与的群智感知系统.基于此,提出一种个性化差分隐私真值发现(personalized differential privacy truth discovery, PDPTD)方法.PDPTD将本地差分隐私随机响应机制应用于隐私保护,使用户能够根据个人隐私需求自主调整感知数据的扰动幅度,平衡数据隐私与可用性.服务器在聚合数据时充分考虑扰动影响,并通过加权机制提升数据质量.与此同时,PDPTD依据数据质量动态分配用户权重,即使部分用户选择较高程度的扰动,系统仍能推断出接近真实值的结果,从而保证数据的可靠性.理论分析与实验结果表明,PDPTD方案符合本地差分隐私原则,同时确保最终推断结果具有较高的精确度.

关键词 隐私保护;群智感知;真值发现;个性化;本地差分隐私

中图法分类号 TP391

DOI: 10.7544/issn1000-1239.202440779 **CSTR:** 32373.14.issn1000-1239.202440779

智能手机等移动智能设备已成为人们日常生活必需品,这些设备内嵌多种传感器,如GPS、加速度和温度传感器等.随着这些设备的普及和智能云计算的发展[1-2],群智感知(crowdsensing)[3-6]得到了广泛的研究.在群智感知系统中,许多携带智能设备的用户参与感知任务并提供感知数据,服务器经过处理后提供相关服务,广泛应用于智能交通[7-8]、城市管理[9]、智慧医疗[10]和智能电网[11-12]等多个领域,具有高度的灵活性和低成本特点.在移动群智感知网络中,感知数据的来源涉及众多用户,由于用户因非专业性、操作不规范性和物理环境复杂性,使得获取的部分感知数据与真实数据存在较大偏差.此外,也存在恶意用户为获取更高奖励提交虚假信息,降低了感知数据质量.因此,为了从海量感知数据中提取真实有效的信息以保证数据质量,真值发现由于能够从多种数据源中获取真实数据受到了广泛研究.Du等人[13]针对群智感知场景下的数据冲突问题,将贝叶斯公式引入真值发现中,以捕获来自不同群体的数据细粒度可靠性,从而产生更精确的数据估计结果.Wang等人[14]将激励机制引入真值发现中,针对恶意用户上传的虚假数据,提出基于分裂聚合的真值发现机制,通过评估用户信任等级来抵御虚假数据从而提高数据质量.

同时,用户提交的信息中包含部分敏感信息从而面临隐私风险,保证用户敏感信息隐私是影响用户是否参与感知任务的关键因素.众多学者提出了基于加密技术的真值发现方法,Zhang等人[15]利用Paillier同态加密技术对感知数据进行加密,使用单向哈希链进行用户身份认证,利用超递增序列提高数据聚合效率,在提高数据精度的同时保护用户的隐私.但该方法需要参与感知任务的用户负责部分加密计算,计算开销大.Zheng等人[16]提出一种双服务器方法,将部分工作从用户端转移到服务器端,提高用户端效率,激励更多用户参与.然而,利用加密技术可能导致部分用户隐私保护不足、部分用户隐私保护过度,不能满足实现用户个性化隐私需求.

综上,本文设计了一种基于差分隐私的个性化隐私保护真值发现方法PDPTD(personalized differential privacy truth discovery),旨在平衡用户隐私保护的需求与数据质量.PDPTD中,用户将感知数据编码为二进制位,并通过随机响应机制对数据进行扰动,然后将扰动后的数据发送给服务器,服务器加权聚合计算得到最终真值.用户可根据自身隐私需求选择数据扰动程度,防止隐私保护不足或过度.此外,PDPTD设计了一种隐私预算分配算法,用于量化编码后每一位的隐私预算,使隐私预算分配更合理.用户只需将扰动后的数据上传云服务器即可,降低了用户与服务器之间的通信开销,提高系统服务效率.

本文主要贡献有3点:

1)提出了一种高效的隐私保护真值发现方法PDPTD,该方法通过随机响应机制对数据进行扰动,保证用户隐私.

2)用户能够自主选择数据扰动程度以支持个性化隐私需要,并设计了一种隐私预算分配算法,量化编码后每一位的隐私预算.

3)采集真实环境中的数据,并实验验证方法性能.结果表明,PDPTD在满足用户个性化隐私需求的同时准确计算出真值,保证最终结果的准确性.

1 相关工作

真值发现是能够从众多数据中获取真实数据以提高数据质量的有效方法,Yin等人[17]通过不同网站

信息的可靠性，提出了一种基于假设概率的真值发现方法. Shao 等人[18]基于多模态提取数据特征，提出一种无监督的真值发现机制，构建了具有多特征最大似然估计模型，用以提高数据正确性概率. 与平均或投票等简单聚合不同，真值发现根据用户提交的感知数据质量动态更新用户权值，并通过用户权值对感知数据进行加权聚合以获得更精确的结果. 加密技术和差分隐私技术常被用于保护数据隐私，防止真值发现过程中数据的隐私泄露.

在基于加密技术的真值发现中，Miao 等人[19]提出了 2 种真值发现隐私保护方法：通过门限 Paillier 密码系统对数据加密来保证用户隐私；通过 2 个非共谋云服务器实现，并降低了用户的计算开销. 为解决用户掉线问题，Xu 等人[20]通过 Shamir 秘密共享算法保证系统能在部分用户离线情况下仍能得到实际的聚合结果，该方法需要用户间提前通过 Diffie-Hellman 密钥交换协议协商公共密钥. Tang 等人[21]利用乱码电路技术实现了安全的真值发现方法，保证用户隐私. Zhang 等人[22]利用 Paillier 同态加密提出一种轻量级隐私保护真值发现方法. 为降低加密开销，Zhang 等人[23]利用矩阵乘法特性设计密钥，提高真值发现效率.

差分隐私[24-25]用于保护用户敏感信息，在隐私保护和效用损失间起到平衡作用，分为中心化差分隐私和本地化差分隐私. 中心化差分隐私将数据在可信的第三方进行扰动. 本地化差分隐私[26-27]表现为用户将数据扰动后传给服务器，服务器执行真值发现算法. Li 等人[28]提出了基于本地差分隐私的真值发现方法，用户通过对感知数据添加高斯噪声以保证用户隐私. Wang 等人[29]针对流数据提出了一种基于差分隐私的真值发现方法，该方法通过引入多个边缘服务器来解决单个服务器不可信的情况，同时还设计了基于可靠性的噪声扰动机制来提高真值发现的准确性. Xue 等人[30]为保护参与者的隐私，基于本地化差分隐私提出一种个性化的隐私保护方法. Chen 等人[31]提出了基于真值发现的隐私保护方法，该方法在数据上传至云服务器之前添加二项分布噪声，再通过用户的密钥对扰动后的数据进行加密，确保在没有可信第三方的情况下用户数据的隐私性和传输的可靠性. 然而，现有方法由于设置所有用户的隐私预算相同，可能造成部分数据过度保护而部分数据保护程度不足等问题.

2 预备知识

本节给出真值发现方法以及差分隐私技术，并对提出方法的系统模型和安全模型进行描述. 表 1 为本文使用的主要符号.

Table 1 Notations Used in Our Paper

表 1 本文使用的符号

符号	描述
I	用户数量
M	观测对象数量
x_m^i	用户 i 对观测对象 m 的感知数据
x_m^*	观测对象 m 的真值
B_m^i	x_m^i 的二进制编码
l	B_m^i 的长度
n	用户选择扰动的位数
$B_{m,1}^i$	B_m^i 中不需要扰动的前 $l-n$ 位
$B_{m,2}^i$	B_m^i 中需要扰动的后 n 位
$\tilde{B}_{m,2}^i$	扰动后的 $B_{m,2}^i$
ε_m^i	$B_{m,2}^i$ 总的隐私预算
$s_{m,k}^i$	$B_{m,2}^i$ 中每一比特位的敏感度
$\varepsilon_{m,k}^i$	$B_{m,2}^i$ 中第 k 位隐私预算
w_i	用户 i 的权值
$\tilde{x}_m^i$	扰动的 x_m^i
S_1^i	聚合 $\tilde{x}_m^i$ 与 x_m^* 之间的距离值
S_2	聚合的 S_1^i
S_w	聚合的 w_i
S_{Wd}^m	聚合所有用户对 o_m 的加权数据

2.1 真值发现

真值发现通过对用户提交的感知数据进行处理，迭代更新用户的权值和观测对象的真值，从而能够从多种数据源中获取真实数据. 真值发现方法从初始化真值开始，随后迭代地执行权值和真值更新，直到最终的结果满足收敛条件. 收敛的标准可以是预先设定的迭代次数，也可以是连续 2 次迭代真值之间的变化值小于设定的阈值.

1）权值更新阶段. 每个观测对象的真值 $\{x_m^*\}_{m=1}^M$ 固定不变，若用户 u_i 提供的感知数据 x_m^i 与观测对象 o_m 的真值更接近，则用户 u_i 将获得较高的权值，否则将获得较低的权值，如式（1）所示.

$$w_i = f\left(\sum_{m=1}^{M} d\left(x_m^i, x_m^*\right)\right), \tag{1}$$

其中 $f(\cdot)$ 是一个单调递减函数，$d(\cdot)$ 是计算用户 u_i 提交的感知数据 x_m^i 与观测对象 o_m 的真值之间的距离值. 本文将采取 CRH（conflict resolution on heterogeneous data）方法作为更新用户权值和观测对象真值的方法，权值计算如式（2）.

$$w_i = \ln\left(\sum_{i=1}^{I}\sum_{m=1}^{M} d\left(x_m^i, x_m^*\right) \Big/ \sum_{m=1}^{M} d\left(x_m^i, x_m^*\right)\right). \quad (2)$$

一般来说, 群智感知系统中有 2 种数据类型, 即连续数据和分类数据, 本文主要讨论连续数据下的群智感知应用场景, 距离值 $d\left(x_m^i, x_m^*\right) = \left(x_m^i - x_m^*\right)^2$.

2) 真值更新阶段. 给定用户权值 $\{w_i\}_{i=1}^{I}$ 不变, 观测对象 o_m 的真值 x_m^* 通过加权聚合可表示为式(3).

$$x_m^* = \sum_{i=1}^{I}\left(w_i \times x_m^i\right) \Big/ \sum_{i=1}^{I} w_i. \quad (3)$$

基于以上描述, 真值发现算法概括为算法 1.

算法 1. 真值发现算法.

输入: I 个用户 M 个物体的感知数据 $\{x_m^i\}_{i,m=1}^{I,M}$;

输出: M 个物体的估计真值 $\{x_m^*\}_{m=1}^{M}$.

① 初始化真值 $\{x_m^*\}_{m=1}^{M}$;

② repeat 迭代开始

③ for i=1 to I do

④ 更新权值 w_i;

⑤ end for

⑥ for m=1 to M do

⑦ 更新真值 x_m^*;

⑧ end for

⑨ until 满足收敛条件迭代结束;

⑩ return 真值 $\{x_m^*\}_{m=1}^{M}$.

2.2 本地差分隐私

差分隐私技术向原始数据中添加符合拉普拉斯分布的噪声来保护数据隐私技术, 具体见定义 1.

定义 1. ε-本地差分隐私. 假设 D 和 D' 是 2 个相邻的数据集且两者之间最多相差 1 条数据, M 为随机算法, *range*(M) 表示算法 M 的所有可能输出构成的集合, S 是 *range*(M) 的任一子集. 算法 M 满足

$$Pr[M(D) \in S] \leqslant \exp(\varepsilon) \times Pr[M(D') \in S], \quad (4)$$

其中 ε 表示隐私预算, 公开且非负. 其数值大小决定算法 M 的隐私保护程度. ε 值限定了 M 在任意一对值上输出相同结果的概率. ε 越小, 算法 M 隐私保护程度越高, 因为较小的 ε 值意味着对原始数据添加了更多的随机性或噪声, 但降低了数据可用性.

2.3 系统模型

PDPTD 主要由数据请求者、云服务器和用户 3 种不同类型的实体构成, 如图 1 所示.

1) 数据请求者. 通过向云服务器发送任务请求, 并接收云服务器返回的所需数据. 数据请求者是感知任务发起者, 并依赖用户的参与和提交的感知数据获得所需数据.

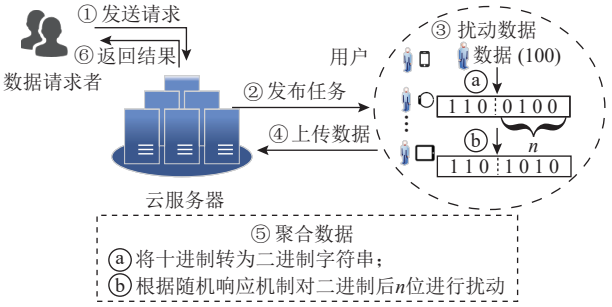


Fig. 1 PDPTD system model

图 1 PDPTD 系统模型

2) 云服务器. 负责接收真值发现任务请求并将其发布给用户, 接收用户发送的扰动数据, 再通过真值发现方法推导出真值, 最后将真值发送给数据请求者. PDPTD 为单服务器模型, 负责协调和处理用户的感知数据, 并提供准确的真值结果给数据请求者.

3) 用户. 用户可以根据云服务器发送的任务列表及报酬等相关信息选择任务参与, 根据参与任务需要, 通过感知设备采集相关感知数据. 同时, 用户对数据进行扰动后再发送给云服务器以保证数据的隐私性.

假设感知任务中有 M 个观测对象 O={o_1, o_2, ⋯, o_M}, I 个用户 U={u_1, u_2, ⋯, u_I}, 用户权值为 W={w_1, w_2, ⋯, w_I}, x_m^i 表示用户 u_i 对观测对象 o_m 生成的感知数据, x_m^* 表示观测对象 o_m 的实际值. 云服务器利用真值发现精确推算出用户上传的感知数据真值 $\{x_m^*\}_{m=1}^{M}$, 且保证感知数据隐私.

2.4 安全模型

PDPTD 中, 假设服务器和用户为半诚实模型, 即服务器和用户严格遵守并执行 PDPTD 协议, 但服务器可能保留获得的感知数据并试图推导出其他敏感信息. 同时, 用户可能根据已知信息推断出其他用户敏感信息, 但用户之间不共谋.

3 PDPTD 方法

本节首先对 PDPTD 进行概述, 再对各个阶段进行详细描述.

3.1 PDPTD 概述

PDPTD 执行过程主要包括数据扰动、权值更新和真值更新 3 个阶段, 如图 2 所示. 图 2 中括号中的数值 150、175、200 分别为 3 个用户的原始数据, 经过数据扰动后分别为 196、156、208, 实现了对用户数据的隐私保护.

数据扰动阶段包括数据编码、字符串分割、个

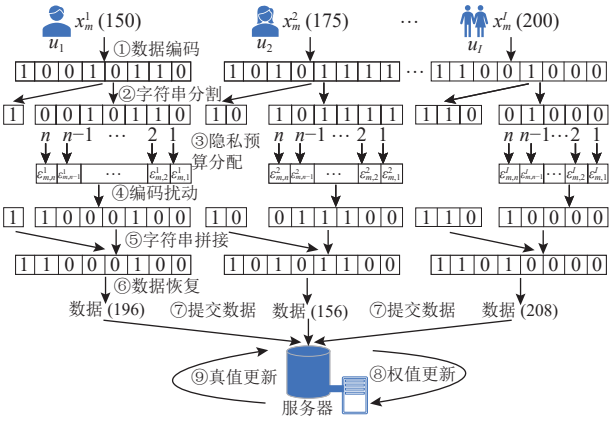


Fig. 2 The framework of PDPTD

图 2 PDPTD 框架

性化隐私预算分配、编码扰动、字符串拼接以及数据恢复过程. 用户 u_i 首先对感知数据 x_m^i 进行二进制编码，将感知数据 x_m^i 转换成长度为 $|l|$ 的二进制字符串 B_m^i. 其次，u_i 根据自身隐私保护需求将编码 B_m^i 拆分成前 $l-n$ 位 $B_{m,1}^i$ 不需要扰动和后 n 位 $B_{m,2}^i$ 需要扰动. 然后，u_i 根据 $B_{m,2}^i$ 内每比特位敏感度的高低对隐私预算 ε_m^i 进行个性化分配，设 $B_{m,2}^i$ 中高位比特位为高敏感度，低位比特位为低敏感度. 根据 $B_{m,2}^i$ 中每比特位所分配的隐私预算，对相应比特位进行扰动得到 $\tilde{B}_{m,2}^i$，并与 $B_{m,1}^i$ 拼接得到 $\tilde{B}_m^i$. 最后，u_i 将扰动后的二进制编码 $\tilde{B}_m^i$ 恢复成数据 $\tilde{x}_m^i$ 并提交给云服务器. 服务器根据 CRH 算法对扰动的数据聚合，迭代执行权值和真值更新，直到满足阈值要求，最后通过安全通道将真值返回给数据请求者.

3.2 数据扰动阶段

用户 u_i 将感知数据 x_m^i 进行扰动，并将扰动结果 $\tilde{x}_m^i$ 发送给云服务器，具体步骤如下：

1)用户 u_i 根据式(5)将感知数据 x_m^i 转换成二进制编码 $B_m^i=\{b_{m,0}^i,b_{m,1}^i,\cdots,b_{m,l-n-1}^i,b_{m,l-n}^i,\cdots,b_{m,l-1}^i\}$，$l$ 表示二进制编码位数，n 表示需要扰动的位数.

$$x_m^i \approx 2^{l-1}b_{m,0}^i+2^{l-2}b_{m,1}^i+\cdots+2^n b_{m,l-n-1}^i+2^{n-1}b_{m,l-n}^i+\cdots+2^0 b_{m,l-1}^i. \tag{5}$$

用户 u_i 将感知数据 x_m^i 编码为 B_m^i，并根据自身隐私保护需求，将 B_m^i 分割为 2 部分：前 $l-n$ 位 $B_{m,1}^i=\{b_{m,0}^i,b_{m,1}^i,\cdots,b_{m,l-n-1}^i\}$ 和后 n 位 $B_{m,2}^i=\{b_{m,l-n}^i,\cdots,b_{m,l-1}^i\}$.

2)用户 u_i 根据 $B_{m,2}^i$ 内每比特位的敏感度对隐私预算 ε_m^i 进行分配.

隐私预算越小则扰动程度越大，当用户隐私保护要求越高，则分配的隐私预算越低. 由于 $B_{m,2}^i$ 中高位比特位信息更敏感，所以高比特位信息分配较低的隐私预算，如图 3 所示.

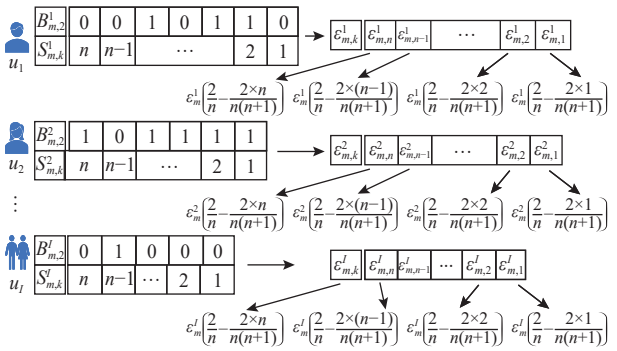


Fig. 3 Privacy budget allocation mechanism

图 3 隐私预算分配机制

假设 $B_{m,2}^i=\{b_{m,l-n}^i,\cdots,b_{m,l-1}^i\}$ 中 n 位比特位敏感度表示为 $s_m^i=\{n,n-1,\cdots,1\}$，n 表示 $B_{m,2}^i$ 中该位敏感度最高，1 表示该位敏感度最低. 用户 u_i 根据式(6)对 $B_{m,2}^i$ 中每个比特位 k 进行隐私预算分配.

$$\varepsilon_{m,k}^i = f_1(k), \tag{6}$$

其中 $f_1(\cdot)$ 为单调递减函数，k 越大则该位隐私保护越强，分配的隐私预算 $\varepsilon_{m,k}^i$ 越小. 同时，所有比特位所分配隐私预算 $\varepsilon_{m,k}^i$ 满足 $\sum_{k=1}^{n}\varepsilon_{m,k}^i=\varepsilon_m^i$，具体分配为式(7).

$$\varepsilon_{m,k}^i=\varepsilon_m^i\times\left(\frac{2}{n}-\frac{2k}{n\times(n+1)}\right),\ k\in\{1,2,\cdots,n\}. \tag{7}$$

3) $B_{m,2}^i$ 中每一比特位被分配隐私预算 $\{\varepsilon_{m,k}^i\}_{k=1}^n$ 后，用户 u_i 通过本地差分隐私随机响应机制对 $B_{m,2}^i$ 中每一位进行扰动得到 $\tilde{B}_{m,2}^i=\{\tilde{b}_{m,l-n}^i,\cdots,\tilde{b}_{m,l-1}^i\}$，扰动规则如式(8)所示.

$$\tilde{b}=\begin{cases}1, & \frac{1}{2}f,\\ b, & 1-f,\\ 0, & \frac{1}{2}f,\end{cases} \tag{8}$$

其中对 $B_{m,1}^i$ 中每一位扰动具体为算法 2.

算法 2. 二进制位扰动.

输入：$B_{m,2}^i=\{b_{m,l-n}^i,\cdots,b_{m,l-1}^i\}$，$\{\varepsilon_{m,k}^i\}_{k=1}^n$；

输出：$\tilde{B}_{m,2}^i=\{\tilde{b}_{m,l-n}^i,\cdots,\tilde{b}_{m,l-1}^i\}$.

① $f\leftarrow\dfrac{2}{\exp(\varepsilon_{m,k}^i)+1}$；

② for j from $l-n$ to $l-1$ do

③ 在 [0, 1) 中随机生成一个 r；

④ if $r<\dfrac{1}{2}f$ then

⑤ $\tilde{b}_{m,j}^i\leftarrow 1$；

⑥ else if $r<f$ and $r\geqslant\dfrac{1}{2}f$ then

⑦ $\tilde{b}_{m,j}^i\leftarrow 0$；

⑧ else $\tilde{b}_{m,j}^i\leftarrow b_{m,j}^i$；

⑨ end if

⑩ end for

⑪ return $\tilde{B}^i_{m,2}=\{\tilde{b}^i_{m,l-n},\cdots,\tilde{b}^i_{m,l-1}\}$.

4)用户 u_i 将 $B^i_{m,1}$ 与 $\tilde{B}^i_{m,2}$ 拼接得到 $\tilde{B}^i_m=\{b^i_{m,0},b^i_{m,1},\cdots,b^i_{m,l-n-1},\tilde{b}^i_{m,l-n},\cdots,\tilde{b}^i_{m,l-1}\}$, 并根据式(9)恢复出扰动后感知数据 $\tilde{x}^i_m$ 并发送给服务器.

$$\tilde{x}^i_m=2^{l-1}b^i_{m,0}+2^{l-2}b^i_{m,1}+\cdots+2^n b^i_{m,l-n-1}+2^{n-1}\tilde{b}^i_{m,l-n}+\cdots+2^0\tilde{b}^i_{m,l-1}. \tag{9}$$

3.3 权值更新阶段

云服务器根据用户上传的数据计算距离值并聚合得到 S^i_1, 并对所有用户所观测对象的感知数据进行聚合得到 S_2, 如式(10)所示.

$$\begin{aligned}S^i_1&=\sum_{m=1}^{M}(\tilde{x}^i_m-x^*_m)^2,\\ S_2&=\sum_{i=1}^{I}\sum_{m=1}^{M}(\tilde{x}^i_m-x^*_m)^2.\end{aligned} \tag{10}$$

根据 S^i_1 和 S_2, 云服务器计算每个用户权值 w_i, 如式(11)所示.

$$w_i=\frac{S_2}{S^i_1}=\ln\frac{\sum_{i=1}^{I}\sum_{m=1}^{M}(\tilde{x}^i_m-x^*_m)^2}{\sum_{m=1}^{M}(\tilde{x}^i_m-x^*_m)^2}. \tag{11}$$

3.4 真值更新阶段

云服务器根据权值对感知数据进行真值更新, 具体步骤如下:

1)云服务器对所有用户权值 $\{w_i\}_{i=1}^I$ 进行聚合, 得到:

$$S_w=\sum_{i=1}^{I}w_i. \tag{12}$$

2)云服务器根据用户权值 w_i 计算用户 u_i 对观测对象 o_m 的加权数据, 聚合加权数据得到所有用户对观测对象 o_m 加权数据的聚合值 S^m_{Wd}.

$$S^m_{Wd}=\sum_{i=1}^{I}w_i\times\tilde{x}^i_m. \tag{13}$$

3)云服务器通过 S_w 和 S^m_{Wd} 计算观测对象 o_m 的真值 x^*_m.

$$x^*_m=\frac{S^m_{Wd}}{S_w}=\frac{\sum_{i=1}^{I}w_i\times\tilde{x}^i_m}{\sum_{i=1}^{I}w_i}. \tag{14}$$

权值更新和真值更新为 1 轮迭代, 每轮迭代将计算出该轮迭代中观测对象 o_m 的真值 x^*_m, 云服务器判断真值 x^*_m 是否满足收敛条件, 若不满足, 则云服务器将该轮迭代的真值 $\{x^*_m\}_{m=1}^M$ 带入到下一轮迭代权值更新阶段中继续计算直至满足收敛条件为止, 并将最后的结果通过安全通道返回给数据请求者.

3.5 鲁棒性

在移动群智感知系统中, 由于用户的非专业性和环境复杂性使得部分数据不能正常提交至云服务器. 通过与基线 CRH 方法进行实验比较, 以验证 PDPTD 方法的鲁棒性.

设系统中有 200 位用户采集多个观测对象的感知数据, 随机选取 1 个观测对象进行结果验证, 并给出不同数据丢失率情况下真值计算的结果. 扰动位数设置为 n=5, 隐私预算分别设置为 ε=0.2, ε=0.3, ε=0.4, 结果如图 4(a)(b)所示. 由结果可知, 数据扰动程度最大时(ε=0.2), PDPTD 计算的经纬度真值结果与真实结果之间最大误差绝对值分别为 7.9E−6°, 1.13E−5°, 对应距离实际为 1.39 m. 因此, 在保证位置隐私情况下, PDPTD 方法仍保持较高的定位精度.

同时, 通过对不同方法实验以进一步分析误差情况. 由图 4(c)(d)可知, PDPTD 方法在计算结果与实际值之间误差波动幅度远小于 PPTD(personalized privacy in trajectory data)方法[32], 在数据丢失率较高情况下表现更突出. 综上, PDPTD 在不同数据丢失率下都保持了较高的准确性, 具有较强的抗数据丢失能力. 因为 PDPTD 方法对真值进行二进制编码, 并基于比特位的高低为其定义不同的敏感度, 再根据敏感度为其分配不同的隐私预算, 所以 PDPTD 方法不仅能够保证数据隐私, 还能具有较高的准确性、可靠性和鲁棒性.

4 隐私分析

本节对 PDPTD 方法隐私性进行分析, 在数据扰动阶段, 用户 u_i 根据 $B^i_{m,2}$ 中每个比特位分配的隐私预算对其进行扰动.

定理 1. $\tilde{B}^i_{m,2}$ 中每个比特位 k 满足 $\varepsilon^i_{m,k}$-差分隐私, $\{\varepsilon^i_{m,k}\}_{k=1}^n$ 是 $B^i_{m,2}$ 中第 k 比特位的隐私预算.

证明. 令 $f\leftarrow\frac{2}{\exp(\varepsilon^i_{m,k})+1}$, 根据差分隐私定义可得:

① $Pr(\tilde{b}=0|b=0)=1-f+\frac{1}{2}f=1-\frac{1}{2}f$;

② $Pr(\tilde{b}=1|b=0)=\frac{1}{2}f$;

③ $Pr(\tilde{b}=0|b=1)=\frac{1}{2}f$;

④ $Pr(\tilde{b}=1|b=1)=1-f+\frac{1}{2}f=1-\frac{1}{2}f$.

由于 $0<f<1$, 所以满足:

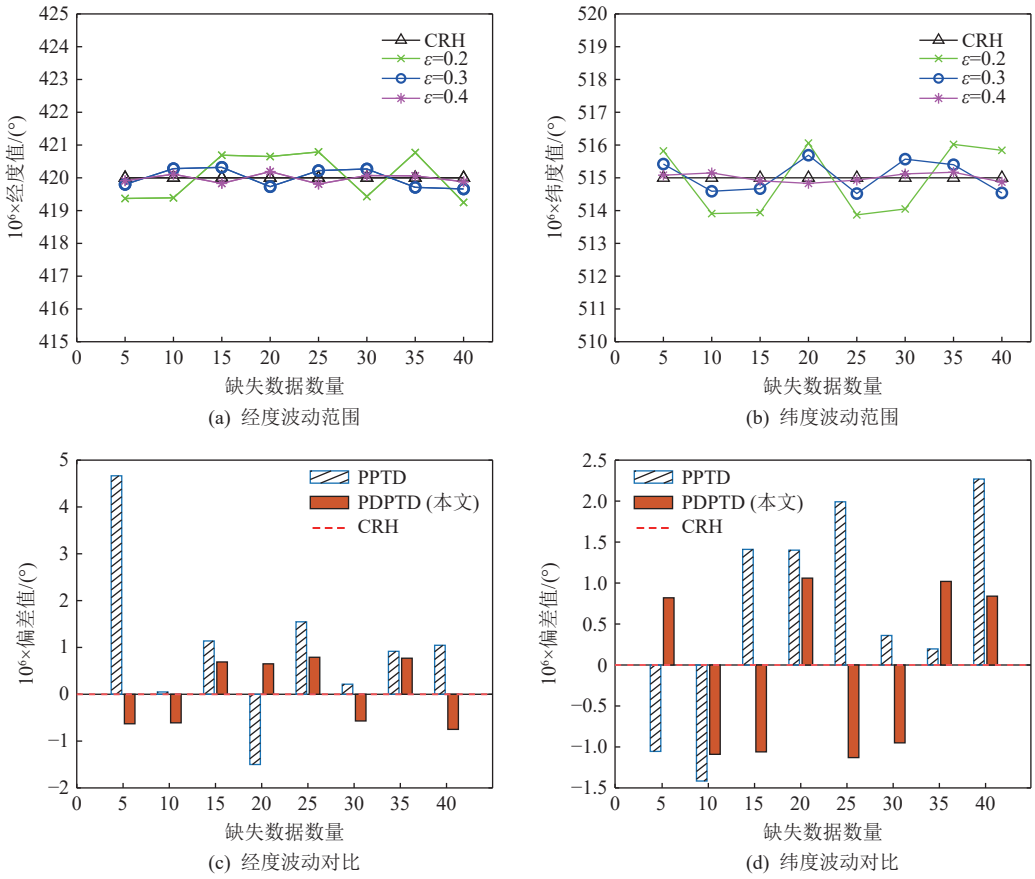


Fig. 4 Sensing value under various data loss

图 4 不同数据丢失量感知值

$$\frac{Pr(\tilde{b}=b''|b=b')}{Pr(\tilde{b}=b''|b=1-b')}\leqslant\frac{1-\frac{1}{2}f}{\frac{1}{2}f}\leqslant\exp(\varepsilon_{m,k}^{i}). \tag{15}$$

因此每个比特位 k 满足 $\varepsilon_{m,k}^{i}$-差分隐私. 证毕.

定理 2. 扰动后的数据 $\tilde{x}_m^i$ 满足 ε_m^i-差分隐私.

证明. 根据差分隐私定义:

①由于 B_m^i 中前 $l-n$ 位 $B_{m,1}^i=\{b_{m,0}^i,b_{m,1}^i,\cdots,b_{m,l-n-1}^i\}$ 不需要扰动, 由此可得

$$\frac{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i'})}{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i''})}=\prod_{j=1}^{l-n}1=1. \tag{16}$$

②由于 B_m^i 中后 n 位 $B_{m,2}^i=\{b_{m,l-n}^i,\cdots,b_{m,l-1}^i\}$ 需要扰动, 由此可得

$$\frac{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i'})}{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i''})}=\prod_{j=1}^{n}\frac{Pr(\tilde{b}_{m,l-j}^i=b_{m,l-j}^{i'''}|b_{m,l-j}^i=b_{m,l-j}^{i'})}{Pr(\tilde{b}_{m,l-j}^i=b_{m,l-j}^{i'''}|b_{m,l-j}^i=b_{m,l-j}^{i''})}. \tag{17}$$

根据定理 1 得

$$\frac{Pr(\tilde{b}_{m,b}^i=b_{m,b}^{i'''}|b_{m,b}^i=b_{m,b}^{i'})}{Pr(\tilde{b}_{m,b}^i=b_{m,b}^{i'''}|b_{m,b}^i=b_{m,b}^{i''})}\leqslant\frac{1-\frac{1}{2}f}{\frac{1}{2}f}\leqslant\exp(\varepsilon_{m,b}^{i}). \tag{18}$$

将式(18)代入式(17), 得

$$\frac{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i'})}{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i''})}=\prod_{j=1}^{n}\frac{Pr(\tilde{b}_{m,l-j}^i=b_{m,l-j}^{i'''}|b_{m,l-j}^i=b_{m,l-j}^{i'})}{Pr(\tilde{b}_{m,l-j}^i=b_{m,l-j}^{i'''}|b_{m,l-j}^i=b_{m,l-j}^{i''})}\leqslant\prod_{j=1}^{n}\exp(\varepsilon_{m,j}^{i}). \tag{19}$$

综上:

$$\begin{aligned}\frac{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i'})}{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i''})}&=\prod_{j=1}^{n}\frac{Pr(\tilde{b}_{m,l-j}^i=b_{m,l-j}^{i'''}|b_{m,l-j}^i=b_{m,l-j}^{i'})}{Pr(\tilde{b}_{m,l-j}^i=b_{m,l-j}^{i'''}|b_{m,l-j}^i=b_{m,l-j}^{i''})}\leqslant\\&1^{l-n}\times\exp(\varepsilon_{m,n}^{i})\times\cdots\times\exp(\varepsilon_{m,1}^{i})=\\&\exp\left(\sum_{k=1}^{n}\varepsilon_{m,k}^{i}\right)=\exp(\varepsilon_m^i).\end{aligned} \tag{20}$$

由此可得 $\frac{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i'})}{Pr(\tilde{x}_m^i=x_m^{i'''}|x_m^i=x_m^{i''})}\leqslant\exp(\varepsilon_m^i)$, 所以, 扰动后的数据 $\tilde{x}_m^i$ 满足 ε_m^i-差分隐私. 证毕.

现在隐私保护方法中, 位置信息扰动通常在服务器端完成, 需要第三方服务器完全可信. PDPTD 采用本地差分隐私技术, 用户在本地对位置信息进行扰动, 再将扰动后的数据发送到服务器, 不再依赖可信的第三方, 从而更有效地保护数据隐私.

5 实 验

本节从收敛性、准确性和计算开销等方面对PDPTD的性能进行实验验证. 实验环境为: 操作系统Win10, CPU2.5 GHz Inter Core i5, 内存8 GB, 编程语言Python. 数据集分别为MySensing, T-drive, San Francisco, 其中MySensing是本文采集的真实数据集. 数据集MySensing采集了1 237个目标物体的经度、纬度等. 数据集San Francisco包含旧金山湾区30天内采集的位置信息, 数据集T-drive记录了北京10 357辆出租车的近1 500万个轨迹点. 为了提高实验效率, PDPTD保留位置信息数据小数点后3~5位的数据, 且从San Francisco数据集中提取了旧金山主城区附近(经度−122.38°~−122.43°, 纬度37.77°~37.80°)的轨迹, 从T-drive数据集中提取了北京主城区附近经度116.23°~116.53°, 纬度39.8°~40.03°的轨迹.

1)收敛性. 方法收敛性为迭代误差小于阈值的轮数. 经纬度分别设置5个不同的初始化真值进行验证, 设置用户数量I=200, 阈值σ=0.001, 隐私预算ε_m^i=0.3. 图5的实验结果分别验证了扰动位数n=3, 4, 5情况下PDPTD方法的收敛性. 由实验结果可知, 在不同的初始化真值下, PDPTD收敛速度快, 2次迭代后都能得到相对平稳的真值, 且不同初始化真值对PDPTD的真值发现结果影响可忽略不计.

2)准确性. 通过计算绝对误差平均数(mean absolute error, *MAE*)来衡量PDPTD方法的准确性, 计算公式为

$$MAE=\frac{\sum_{i=1}^{I}\sum_{m=1}^{M}(x_m^*-x_m^i)}{I\times M}. \tag{21}$$

如图6所示, 随着隐私预算ε的增加, *MAE*值显著下降, 表明隐私预算和真值准确性呈负相关, 即隐私预算越大, 数据扰动强度越低, 真值的准确性越高. 因此, 用户通过动态设置隐私预算能够满足个性化需求. 当用户需要高准确性真值时, 则为高比特位分配较高的隐私预算, 为低比特位分配较低的隐私预算, 在保护数据隐私的同时满足用户真值准确性要求.

图7给出了用户数量I=200时, 3种数据集MySensing, T-drive, San Francisco下*MAE*的变化情况. 由实验结果可知, 不同扰动位数以及不同隐私预算情况下, PDPTD方法的*MAE*值变化基本稳定在一个较低的范围内, 从而表明在不同隐私预算设置下, PDPTD方法具有较强的鲁棒性和稳定性.

Gauss机制是一种经典的差分隐私保护方法[33],

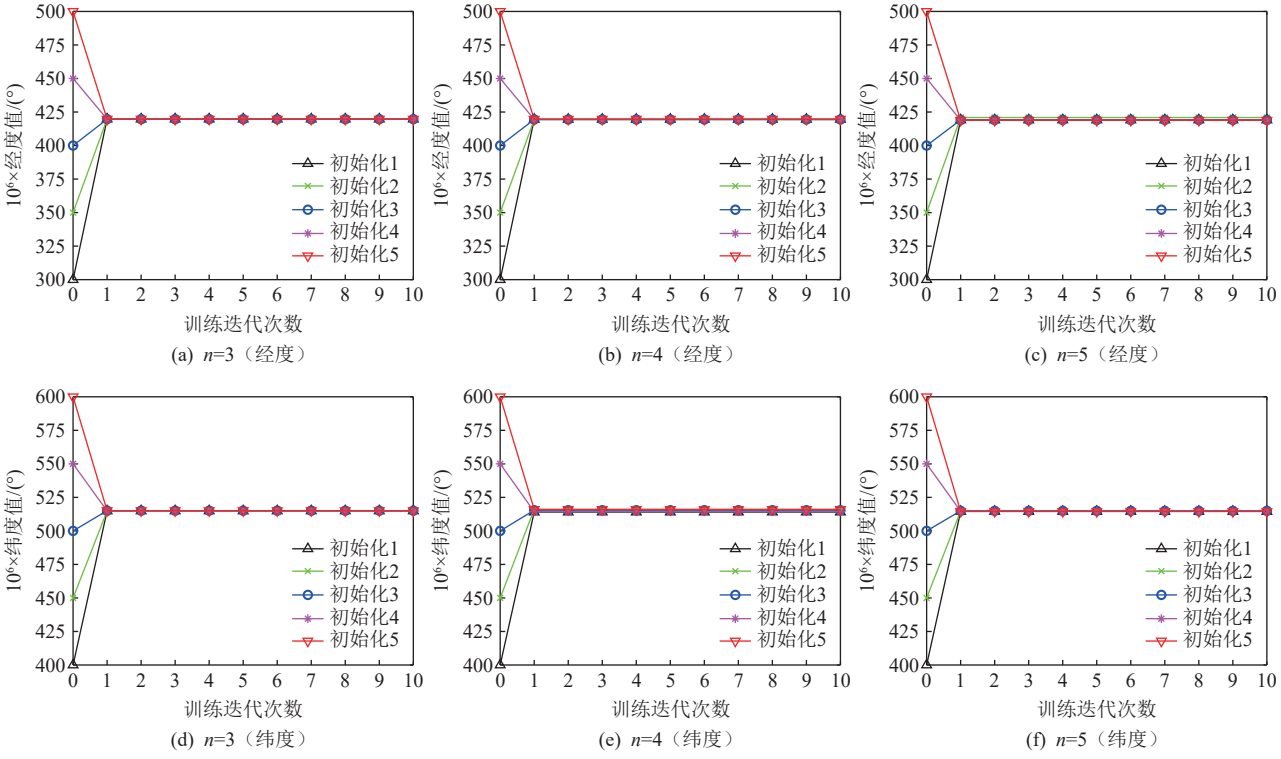
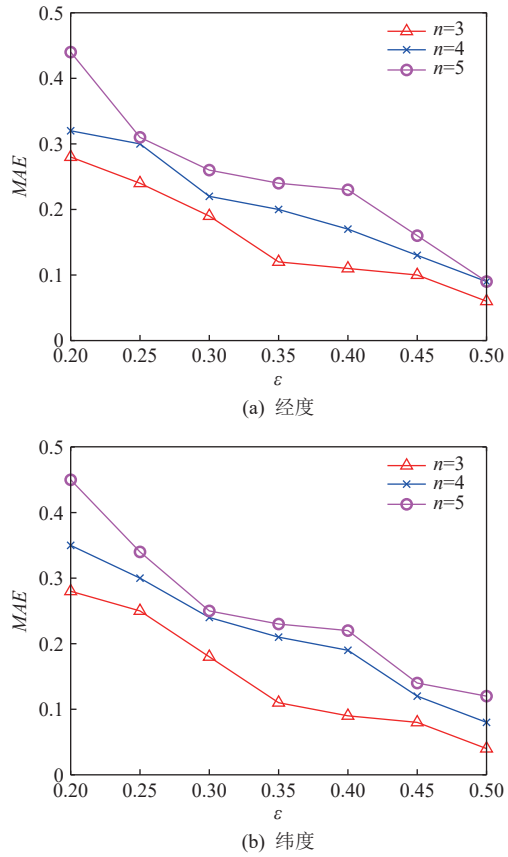


Fig. 5 Comparison of convergence

图5 收敛性比较



(a) 经度

(b) 纬度

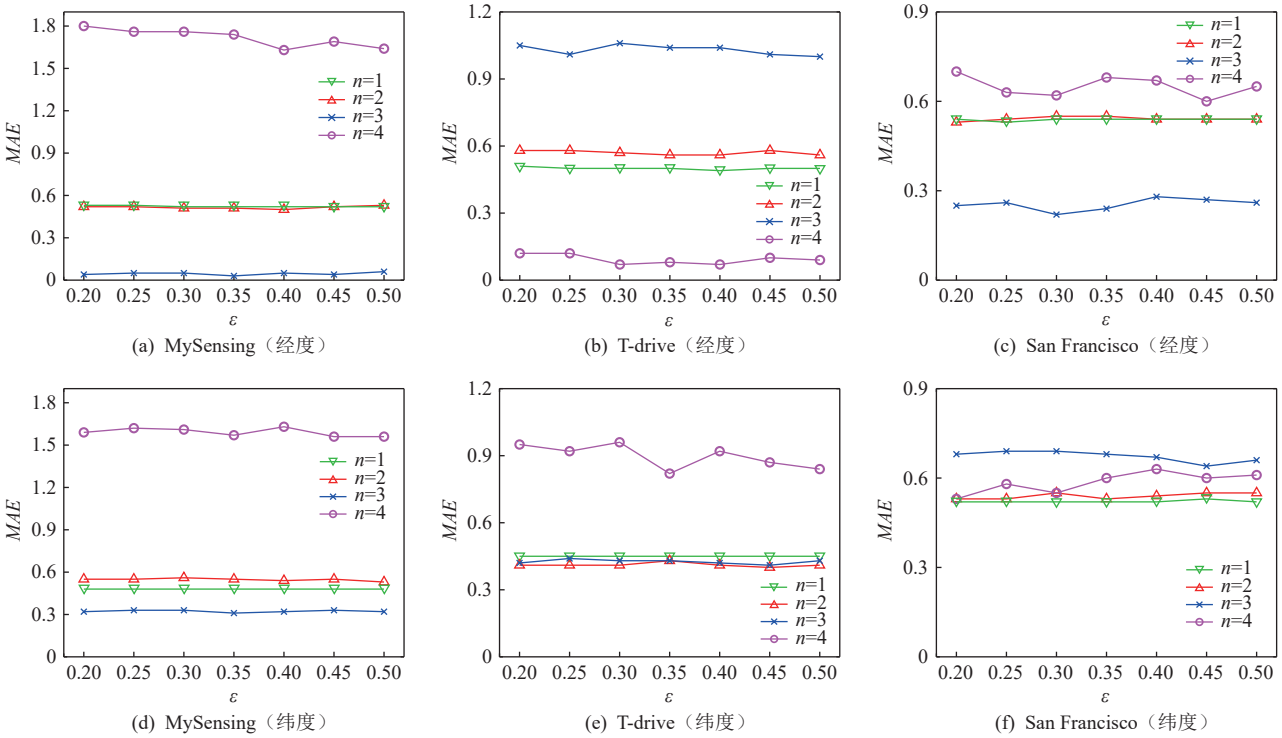
Fig. 6 Comparison of *MAE* under different privacy budgets

图 6 不同隐私预算下 *MAE* 对比

通过向查询结果中添加服从高斯分布的随机噪声实现隐私保护，具有计算效率高、适用范围广的特点. 图 8 给出了在不同数据集和不同扰动机制下，PDPTD 和 Gauss 这 2 种隐私保护方法的 *MAE*. 由于高斯噪声变化幅度不能根据任务特性和数据分布进行自适应调整，所以降低了真值发现结果的准确性. 实验结果表明 PDPTD 的准确度高于 Gauss 机制，当隐私预算较大时，*MAE* 降低幅度更大.

3)计算开销. 在相同的软硬件环境下，对比不同数量用户提交的感知数据执行真值发现方法所需时间来评估不同方法的计算开销，其中 L^2-PPTD[34] 和 InPPTD[35] 这 2 种方法通过加密实现隐私保护，其密钥大小设置为 1 024 b. 由于加解密计算开销较大，随着用户数量或观测对象数量增加，加解密计算开销随之增加，而基于差分隐私的真值发现隐私保护增长幅度极低，计算开销具有明显优势，如图 9 所示.

同时，为了进一步验证方法的计算开销，测试不同扰动位数和不同参与人数情况下 PDPTD 的计算开销，如图 10 所示. 当参与人数较少时(如 25 人)，云服务器所需聚合数据量较低，计算开销小. 随着参与人数的增加(如 200 人)，云服务器所需聚合数据量较高，使得计算开销较大. 此外，随着扰动位数的增加，计算开销随之增加，且扰动位数越大，计算开销增长幅度越大.



(a) MySensing（经度） (b) T-drive（经度） (c) San Francisco（经度）

(d) MySensing（纬度） (e) T-drive（纬度） (f) San Francisco（纬度）

Fig. 7 Comparison of *MAE* under different data sets

图 7 不同数据集下 *MAE* 对比

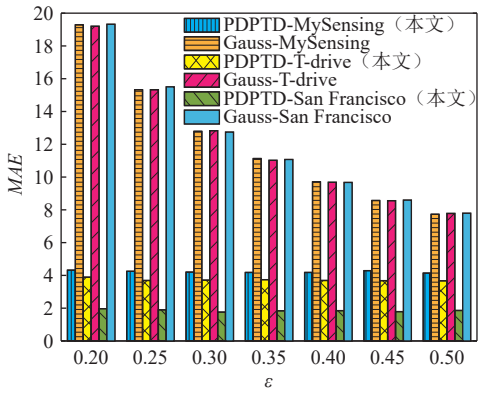


Fig. 8 Comparison of *MAE* under different encryption methods

图 8 不同加密方法下 *MAE* 对比

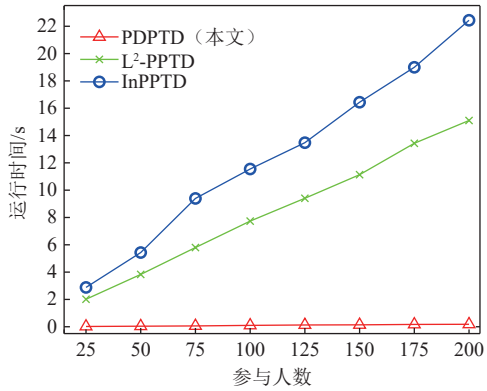


Fig. 9 Runtime of different methods under different numbers of user participation

图 9 不同用户数量参与下各方法运行时间

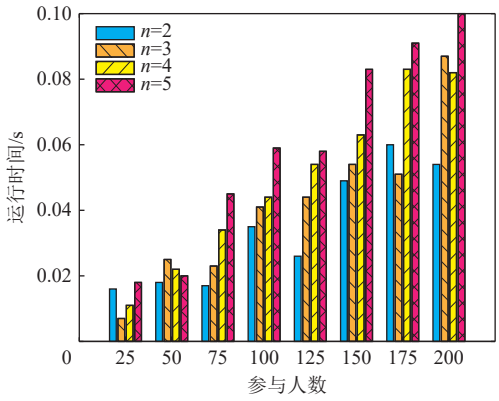


Fig. 10 Time overhead under different numbers of perturbation bits

图 10 不同扰动位数下的时间开销

4)平衡性. 为了验证真值结果的准确性 *MAE* 和隐私性(privacy, *PRI*)之间的关系, 图 11 给出 2 种数据集 MySensing, T-Drive 上 PDPTD 在不同隐私预期情况下真值结果的 *MAE* 和 *PRI* 的变化趋势, 其中 *PRI* 的计算公式为

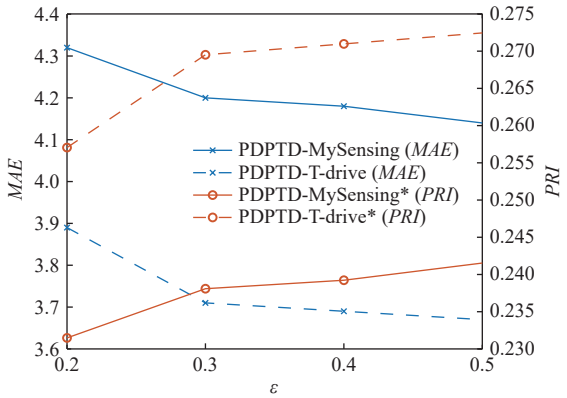


Fig. 11 Comparison of *MAE* and *PRI* under different privacy budgets

图 11 不同隐私预算下 *MAE* 和 *PRI* 对比

$$PRI=\frac{I\times M}{\sum_{i=1}^{I}\sum_{m=1}^{M}(x_m^*-x_m^i)}. \tag{22}$$

由图 11 可知, 随着隐私预算ε的增加, *MAE* 随之下降, 而 *PRI* 呈现上升的趋势. 因此, 较大的隐私预算使得隐私保护度较低, 而过小的隐私预算降低了结果的 *MAE*, 通过设置隐私预算能较好地平衡 *MAE* 和 *PRI*, 满足个性化要求.

6 总 结

针对移动群智感知真值发现方法面临用户个性化隐私保护要求的问题, 提出了一种基于差分隐私的个性化隐私保护真值发现方法 PDPTD. PDPTD 中用户利用随机响应机制对感知数据进行扰动以保护数据隐私, 且通过设置感知数据扰动位数, 实现不同程度的隐私保护以满足个性化隐私要求. 同时, PDPTD 设计了一种隐私预算分配方法, 用于量化编码后的每一位的隐私预算来提高隐私保护效能. 实验结果表明, PDPTD 具有较好的性能, 不仅满足用户的个性化隐私需求, 且数据聚合结果具有较高的准确性. 同时, 实验验证了隐私预算对聚焦结果的准确性和数据隐私性的影响.

作者贡献声明: 王涛春提出了算法思路, 完成论文撰写与修改; 强勇和许诺完成实验并撰写论文; 陈付龙和谢冬提出指导意见并修改论文; 赵传信进行了实验指导.

参 考 文 献

[1] Zhang Zhan, Zhang Xianqi, Zuo Decheng, et al. Research on target

tracking application deployment strategy for edge computing[J]. Journal of Software, 2020, 31(9): 2691−2708 (in Chinese)
(张展, 张宪琦, 左德承, 等. 面向边缘计算的目标追踪应用部署策略研究[J]. 软件学报, 2020, 31(9): 2691−2708)

[2] Wu Yulin, Wang Xuan, Willy S, et al. Efficient server-aided secure two-party computation in heterogeneous mobile cloud computing[J]. IEEE Transactions on Dependable and Securev Computing, 2021, 18(6): 2820−2834

[3] Wang Liang, Yu Zhiwen, Wu Kaishun, et al. Towards robust task assignment in mobile crowdsensing systems[J]. IEEE Transactions on Mobile Computing, 2023, 22(7): 4297−4313

[4] Hu Jiahui, Wang Zhibo, Wei Jian, et al. Towards demand-driven dynamic incentive for mobile crowdsensing systems[J]. IEEE Transactions on Wireless Communications, 2020, 19(7): 4907−4918

[5] Deng Qingyong, Zuo Qinghua, Li Zhetao, et al. Privacy-preserving bilateral reputation evaluation in blockchain based crowdsensing[J]. Journal of Computer Research and Development, 2024, 61(11): 2681−2692 (in Chinese)
(邓清勇, 左清华, 李哲涛, 等. 基于区块链的群智感知双向信誉评估隐私保护[J]. 计算机研究与发展, 2024, 61(11): 2681−2692)

[6] Zhang Qiong, Wang Taochun, Tao Yuan, et al. Location privacy protection method based on differential privacy in crowdsensing task allocation[J]. Ad Hoc Networks, 2024, 158: 103464

[7] Huang Hongji, Yang Jie, Huang Hao, et al. Deep learning for super-resolution channel estimation and DOA estimation based massive MIMO system[J]. IEEE Transactions on Vehicular Technology, 2018, 67(9): 8549−8560

[8] Wang Zhenning, Cao Yue, Jiang Kai, et al. Incentive-driven vehicle selection and scheduling method in vehicular crowdsensing[J]. Journal of Computer Research and Development, 2024, 61(9): 2213−2228 (in Chinese)
(王振宁, 曹越, 江恺, 等. 车辆群智感知中激励驱动的车辆选择与调度方法[J]. 计算机研究与发展, 2024, 61(9): 2213−2228)

[9] Sawafi Y A, Touzene A, Day K, et al. Context-aware RPL-based mobile crowd sensing and routing protocol for smart city networks[C]//Proc of the 16th Int Wireless Communications and Mobile Computing (IWCMC). Piscataway, NJ: IEEE, 2020: 1830−1835

[10] Wang Taochun, Wu Qingshan, Chen Jian, et al. Health data security sharing method based on hybrid blockchain[J]. Future Generation Computer Systems, 2024, 153: 251−261

[11] Li Beibei, Zhu Ziqing, Zhang Linghao, et al. EPPSQ: Achieving efficient and privacy-preserving statistics queries over encrypted data in smart grids[J]. Future Generation Computer Systems, 2023, 149: 265−279

[12] Zhao Shuai, Li Fenghua, Li Hongwei, et al. Smart and practical privacy-preserving data aggregation for fog-based smart grids[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 521−536

[13] Du Yang, Sun Y E, Huang He, et al. Bayesian co-clustering truth discovery for mobile crowd sensing systems[J]. IEEE Transactions on Industrial Informatics, 2019, 16(2): 1045−1057

[14] Wang Ping, Li Zhetao, Guo Bin, et al. A UAV-assisted truth discovery approach with incentive mechanism design in mobile crowd sensing[J]. IEEE/ACM Transactions on Networking, 2024, 32(2): 1738−1752

[15] Zhang Chuan, Zhu Liehuang, Xu Chang, et al. Reliable and privacy-preserving truth discovery for mobile crowdsensing systems[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1245−1260

[16] Zheng Yifeng, Duan Huayi, Yuan Xingliang, et al. Privacy-aware and efficient mobile crowdsensing with truth discovery[J]. IEEE Transactions on Dependable and Secure Computing, 2017, 17(1): 121−133

[17] Yin Xiaoxin, Han Jiawei, Yu Philip S. Truth discovery with multiple conflicting information providers on the web[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(6): 796−808

[18] Shao Huajie, Sun Dachun, Yao Shuochao, et al. Truth discovery with multi-modal data in social sensing[J]. IEEE Transactions on Computers, 2020, 70(9): 1325−1337

[19] Miao Chenglin, Jiang Wenjun, Su Lu, et al. Cloud-enabled privacy-preserving truth discovery in crowd sensing systems[C]//Proc of the 13th ACM Conf on Embedded Networked Sensor Systems. New York: ACM, 2015: 183−196

[20] Xu Guowen, Li Hongwei, Liu Sen, et al. Efficient and privacy-preserving truth discovery in mobile crowd sensing systems[J]. IEEE Transactions on Vehicular Technology, 2019, 68(4): 3854−3865

[21] Tang Xiaoting, Wang Cong, Yuan Xingliang, et al. Non-interactive privacy-preserving truth discovery in crowd sensing applications[C]// Proc of the 37th IEEE Conf on Computer Communications (INFOCOM). Piscataway, NJ: IEEE, 2018: 1988−1996

[22] Zhang Chuan, Zhu Liehuang, Xu Chang, et al. LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT[J]. Future Generation Computer Systems, 2019, 90: 175−184

[23] Zhang Chuan, Zhao Mingyang, Zhu Liehuang, et al. Enabling efficient and strong privacy-preserving truth discovery in mobile crowdsensing[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3569−3581

[24] Cynthia D. Differential privacy: A survey of results[C]//Proc of the 5th Int Conf on Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1−19

[25] Wang Xiujun, Mo Lei, Zheng Xiao, et al. Sampling based fast publishing algorithm with differential privacy for data stream[J]. Journal of Computer Research and Development, 2024, 61(10): 2433−2447 (in Chinese)
(王修君, 莫磊, 郑啸, 等. 基于采样的数据流差分隐私快速发布算法[J]. 计算机研究与发展, 2024, 61(10): 2433−2447)

[26] Michele G, Emanuele U, Stefano C. Encrypted data aggregation in mobile crowdsensing based on differential privacy[C]//Proc of the 20th IEEE Int Conf on Pervasive Computing and Communications Workshops and Other Affiliated Events (PerCom Workshops). Piscataway, NJ: IEEE, 2022: 22−25

[27] Jin Wenqiang, Xiao Mingyan, Guo Linke, et al. ULPT: A user-centric location privacy trading framework for mobile crowd sensing[J]. IEEE Transactions on Mobile Computing, 2021, 21(10): 3789−3806

[28] Li Yaliang, Xiao Houping, Qin Zhan, et al. Towards differentially private truth discovery for crowd sensing systems[C]//Proc of the 40th Int Conf on Distributed Computing Systems (ICDCS). Piscataway, NJ: IEEE, 2020: 1156−1166

[29] Wang Dan, Ren Ju, Wang Zhibo, et al. Privacy-preserving streaming truth discovery in crowdsourcing with differential privacy[J]. IEEE Transactions on Mobile Computing, 2022, 21(10): 3757−3772

[30] Xue Qiao, Zhu Youwen, Wang Jian. Mean estimation over numeric data with personalized local differential privacy[J]. Frontiers of Computer Science, 2022, 16(3): 163806

[31] Chen Jingxue, Liu Yining, Xiang Yong, et al. RPPTD: Robust privacy-preserving truth discovery scheme[J]. IEEE Systems Journal, 2022, 16(3): 4525−4531

[32] Komishani E G, Abadi M, Deldar F. PPTD: Preserving personalized privacy in trajectory data publishing by sensitive attribute generalization and trajectory local suppression[J]. Knowledge-Based Systems, 2016, 94: 43−59

[33] Dwork C, Roth A. The algorithmic foundations of differential privacy[J]. Foundations and Trends in Theoretical Computer Science, 2014, 9(3/4): 211−407

[34] Miao Chenglin, Su Lu, Jiang Wenjun, et al. A lightweight privacy-preserving truth discovery framework for mobile crowd sensing systems[C]//Proc of the 36th IEEE Conf on Computer Communications(INFOCOM). Piscataway, NJ: IEEE, 2017: 1−9

[35] Xue Kaiping, Zhu Bin, Yang Qingyou, et al. InPPTD: A lightweight incentive-based privacy-preserving truth discovery for crowdsensing systems[J]. IEEE Internet of Things Journal, 2020, 8(6): 4305−4316



Wang Taochun, born in 1979. PhD, professor, PhD supervisor. Member of CCF. His main research interests include privacy preservation, crowdsensing, and wireless sensor networks.

王涛春, 1979 年生. 博士, 教授, 博士生导师. CCF 会员. 主要研究方向为隐私保护、群智感知、无线传感器网络.



Qiang Yong, born in 1997. Master. Student member of CCF. His main research interests include crowdsensing and privacy protection.

强　勇, 1997 年生. 硕士. CCF 学生会员. 主要研究方向为群智感知、隐私保护.



Xu Nuo, born in 1999. Master. His main research interests include mobile crowdsensing and privacy protection.

许　诺, 1999 年生. 硕士. 主要研究方向为移动群智感知、隐私保护.



Chen Fulong, born in 1978. PhD, professor, PhD supervisor. His main research interests include embedded computing, pervasive computing, and high-performance computer architecture.

陈付龙, 1978 年生. 博士, 教授, 博士生导师. CCF 高级会员. 主要研究方向为嵌入式计算、普适计算、高性能计算机体系结构.



Xie Dong, born in 1987. PhD, associate professor. Member of CCF. His main research interests include cryptography and information security, and image security and applications.

谢　冬, 1987 年生. 博士, 副教授. CCF 会员. 主要研究方向为密码学与信息安全、图像安全与应用.



Zhao Chuanxin, born in 1978. PhD, professor, PhD supervisor. Member of CCF. His main research interests include Internet of things and intelligent information processing.

赵传信, 1978 年生. 博士, 教授、博士生导师, 教授. CCF 会员. 主要研究方向为物联网、智能信息处理.