基于差分隐私的轨迹隐私保护方案

陈思[1,2]，付安民[1,3]，苏锴[1]，孙怀江[1]

（1. 南京理工大学计算机科学与工程学院，江苏 南京 210094；2. 南京理工大学后勤服务中心，江苏 南京 210094；
3. 中国科学院信息工程研究所，北京 100093）

摘 要：为了解决现有采样机制和数据混淆方法容易导致公开发布的轨迹数据可用性较低和隐私保护不足的问题，提出了一种基于差分隐私的轨迹隐私保护方案。该方案通过建立新的基于时间泛化和空间分割的高效采样模型，并利用 k-means 聚类算法进行抽样数据处理，同时借助差分隐私保护机制对轨迹数据进行双重扰动，有效解决了具有强大背景知识的攻击者窃取用户隐私的问题。同时，为适应轨迹数据查询范围的误差边界，设计了有效的数据发布预判机制，保证了发布的轨迹数据的精度。仿真结果表明，与现有的轨迹差分隐私保护方法相比，所提方案在处理效率、隐私保护强度和数据可用性等方面具有明显的优势。

关键词：差分隐私；轨迹隐私；数据采样；指数机制；数据发布

中图分类号：TP391

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021168

Trajectory privacy protection scheme based on differential privacy

CHEN Si[1,2], FU Anmin[1,3], SU Mang[1], SUN Huaijiang[1]

1. School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
2. Logistics Service Center, Nanjing University of Science and Technology, Nanjing 210094, China
3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract: To solve the problem that the current sampling mechanism and data obfuscation method may raise insufficient data availability and privacy protection, a trajectory privacy protection scheme based on differential privacy was proposed. A new efficient sampling model based on time generalization and spatial segmentation was presented, and a k-means clustering algorithm was designed to process sampling data. By employing the differential privacy mechanism, the trajectory data was disturbed to solve the user privacy leaking problem caused by the attacker with powerful background knowledge. Simultaneously, to respond to the error boundary of the query range of pandemic, an effective prediction mechanism was designed to ensure the availability of released public track data. Simulation results demonstrate that compared with the existing trajectory differential privacy protection methods, the proposed scheme has obvious advantages in terms of processing efficiency, privacy protection intensity, and data availability.

Keywords: differential privacy, trajectory privacy, data sampling, exponential mechanism, data publishing

---

收稿日期：2021−01−04；**修回日期**：2021−03−21

通信作者：付安民，fam_0522@163.com

基金项目：国家自然科学基金资助项目（No.62072239）；信息安全国家重点实验室开放基金资助项目（No.2021-MS-07）；中央高校基本科研业务费专项资金资助项目（No.30920021129）；中国高等教育学会“高等教育信息化研究”专项课题基金资助项目（No.2020XXHD06）

Foundation Items: The National Natural Science Foundation of China (No.62072239), Open Foundation of the State Key Laboratory of Information Security of China (No.2021-MS-07), The Fundamental Research Funds for the Central Universities (No.30920021129), Special Project of “Higher Education Informatization Research” of China Higher Education Association (No.2020XXHD06)

1　引言

随着物联网、智能穿戴设备和全球定位系统（GPS, global positioning system）定位技术的快速发展，基于位置服务技术得到广泛应用，如移动用户通过终端来租借共享单车、查询周边的美食、享受外卖与线上打车服务等，这些基于位置的服务能够使用户获取周边的实时信息，并为其提供高质量的生活方式。然而，轨迹数据具有隐私含义，因为它足够精确，敌手可能由此得到用户的住址、工作信息和个人生活习惯等隐私数据[1]。例如，一旦公共卫生机构公开发布用于流行病跟踪的轨迹统计数据，这些敏感数据可能会在用户不知情的情况下被保留或被攻击者用于其他目的[2]；公共卫生机构利用软件应用获取的位置数据进行病毒传播的追踪，有利于预防和阻止疾病大流行，但是轨迹数据的公开发布和使用却伴随着一系列伦理和隐私问题，难以预防一些网络攻击者重复利用并窃取用户隐私的事件发生[3]。因此，如何在保护用户隐私的情况下使用轨迹数据是一个关键挑战[4-5]。

目前，轨迹隐私保护的研究已经具有一定的积累，其中 *k*-匿名和差分隐私技术等被广泛应用在位置隐私保护领域[6]。*k*-匿名是最早被用于保护轨迹隐私的技术，操作简单。智能移动设备与用户绑定，例如，某些移动应用程序直接获取用户位置信息，而 *k*-匿名方法要求某一用户的位置记录至少与其他 *k*−1 个位置记录不可区分，采用匿名方法进行隐私保护，但是其需要基于一些特殊的攻击假设，会增加服务器的负载和网络传输开销，影响位置服务质量[7-8]。即使使用唯一标识符而不是名称，大多数用户行为仍可被轻而易举地追溯，因此差分隐私技术应运而生。差分隐私由 Dwork 等[9-10]提出，通过严格的数学定义对发布数据进行随机扰动，使在统计意义上攻击者即使拥有一定的背景知识（如用户的性别、邮政编码等），也无法识别一条记录（如 ID、姓名等）是否在原数据表中，从而达到隐私保护目的。该技术优点在于不需要特殊的攻击假设、不关心攻击者拥有的背景知识，同时给出了量化的分析来定义隐私泄露风险[11-13]。许多学者对差分隐私技术进行了大量的研究与探讨，根据不同场景下轨迹隐私保护需求提出众多隐私保护方法[14-21]。

然而，现有轨迹隐私保护工作存在以下困难。1) 个人用户精确的位置数据被利用在法律上是敏感的，那么机构如何构建高效采样机制来收集用户轨迹数据。2) 即使是群体聚合的轨迹数据也会有暴露隐私的风险，采用什么样的轨迹数据扰动混淆机制，可以有效抵抗具有背景知识的敌手攻击。3) 如何高效地提高轨迹数据发布的统计精度，增强公开发布的轨迹数据的可用性。总之，目前并没有克服上述所有困难的轨迹隐私保护方案。

因此，本文通过建立时间泛化和空间分割的轨迹数据处理模型，设计了一种基于差分隐私的轨迹隐私保护（TPPDP, trajectory privacy protection based on differential privacy）方案，不仅能够增强轨迹数据的可用性，量化轨迹数据的隐私保护程度，还能有效抵抗基于一定背景知识的攻击者的攻击。本文的主要贡献如下。

1) 现有轨迹隐私保护方案都是单独采用一种差分隐私机制，TPPDP 使用差分隐私的指数机制和 Laplace 机制进行双重数据随机扰动，适用于空间分割、轨迹发布的不同阶段，不仅可以量化隐私泄露的风险程度，在抵御具有一定背景知识的敌手攻击的同时，安全性也比单独使用一种机制大大提升。

2) 为了提高轨迹数据发布的查询精度，响应查询范围的误差边界，设计了一个有效的预判机制，减少异常轨迹数据发布的风险，在提高数据安全性的前提下，进一步保证发布的公共卫生轨迹数据的可用性。

3) 结合轨迹数据的敏感特征，充分考虑采样数据真正代表整个区域人口的可行性，设计了一个新的时间泛化和空间分割的高效采样模型，使用 k-means 聚类算法进行抽样数据处理，进而提高算法执行效率。

4) 理论上分析了 TPPDP 方案满足差分隐私，并使用微软公司发布的真实轨迹数据进行仿真测试。测试结果表明，TPPDP 方案在满足隐私保护的同时具有较高的数据效用，并表现出良好的性能。

2　相关工作

为了解决用户轨迹数据的泄露问题，学者们已进行了大量的研究与探讨。Chen 等[14]根据蒙特利尔地区公共交通机构发布的数据，在差分隐私模型下，提出了一种有效的数据依赖的隐私保护算法，在数据处理中利用前缀树的固有约束来进行约束推理，从而产生更好的效果，这是第一个差分隐私模型应用于发布大量轨迹数据的解决方案，缺点是

该算法依赖于严格的轨迹场景进行实现，在实施过程中有较大局限性。

随后，越来越多的学者着手设计轨迹隐私保护的框架模型。He 等[15]针对 GPS 设备可能导致的大量个人和人口流动的数据泄露，提出了一种基于个人原始 GPS 轨迹合成移动数据的框架，以差分隐私技术得到理想的隐私保护的效果，还提供了具体的建模方案，使用分层参考系统对原始轨迹进行离散化处理，使用方向加权抽样来提高效用。Cao 等[16]提出了一种灵活的“l-轨迹隐私保护”的安全模型，以确保每一段长度轨迹都受到隐私保护，利用分层设计思想来满足轨迹隐私，并基于 4 个真实数据集进行仿真实验，证明该算法是高效的。上述研究工作偏重于差分隐私的框架模型设计，主要是针对历史轨迹数据集进行处理，不能很好地适应轨迹数据的动态特征。

随着应用程序的发展，针对轨迹隐私的研究开始注重隐私保护系统的设计。Gursoy 等[17]将隐私保护和完整的位置跟踪进行合成，提供了一种综合隐私保护系统 Ada Trace。这是一个可扩展的系统，针对差分隐私和弹性位置攻击提供了一个效用感知的功能，Ada Trace 在 4 个阶段中执行特征提取、噪声注入和特征合成，部署在真实环境进行使用。Drakonakis 等[18]开发了 LPAuditor 系统，该系统是一个检查位置公开，衡量用户面临隐私风险信息的系统，并利用 Twitter 数据和公共应用程序接口（API, application programming interface）进行测试。LPAuditor 除了实现更高的粒度，还引入了一种集群方法，可以解决 GPS 读数或用户移动引起的空间位移问题。Yang 等[19]将位置隐私保护和区块链结合，确定了传统人群感知系统中可以披露的 3 种方式，并提出了一种新颖的区块链式隐私保护人群感应系统，该系统需要基于奖励的任务分配过程，使用区块链技术的匿名特征来隐藏用户的身份信息。上述隐私保护系统可以达到一定的隐私保护作用，但是在进行大量的位置泛化或匿名处理后再进行轨迹发布，会降低位置服务的有效性。

在基于差分隐私技术的轨迹隐私保护中，比较经典的方案是 Hua 等[20]和 Li 等[21]提出的方案。Hua 等[20]假设原始轨迹数据具有相同的时间戳，通过概率性统计合并相似节点形成新轨迹数据集，结合 Laplace 机制设计新轨迹发布算法 TSTDA（time-serial trajectory data algorithm），该算法既保持了比较高的数据效用，又可以应用到大规模轨迹隐私保护场景。Li 等[21]针对现有隐私保护算法使用随机和无限制的噪声导致用户隐私泄露的问题，提出了一种包含有界噪声约束和差分隐私技术结合的算法 NGTMA（noise generation and trajectory merging algorithm），实现了较高的数据可用性。但这些研究工作未考虑时间属性，且不允许所有用户在同一时间移动，没有建立时间和空间的关联性，不能很好地适应流行病环境下的轨迹隐私保护场景。

因此，针对上述问题，本文通过建立基于差分隐私的时间泛化和空间分割采样模型，借助差分隐私保护的思想，设计了一种新的轨迹隐私保护方案，在增强公共卫生数据的可用性的同时，能够高效抵抗基于背景知识的攻击者的攻击。

3 方案设计

本文提出的 TPPDP 方案适用于物联网背景下移动用户的轨迹隐私保护场景，核心思想是在保证用户隐私的同时，提高轨迹发布数据的有效性，同时具有较高的执行效率。

本文先给出 TPPDP 模型及流程设计，然后重点阐述 TPPDP 方案的 2 个核心子算法：轨迹处理子算法和数据发布子算法。表 1 给出了系统参数及其含义。

表 1 系统参数及其含义

参数	含义
t	时刻
l	簇心节点
T	轨迹
(x_i, y_i)	第 i 个查询位置坐标值
ln	Laplace 噪声
tc	真实轨迹数目
G	分区个数
P	候选分区
D	原始轨迹数据集
DG	位置泛化后的轨迹数据集
$\tilde{P}$	k-means 分区
nc	加噪之后的轨迹数目

3.1 模型及流程设计

为保护用户的动态轨迹隐私，TPPDP 进行时间属性处理，并建立时间和位置属性之间的关联模型。

TPPDP 模型如图 1 所示，包括时间泛化、空间分割、轨迹优化和轨迹发布 4 个步骤，其中时间泛化和空间分割构成轨迹处理子算法 TraPro，轨迹优化和轨迹发布构成轨迹发布子算法 TraRel。

首先，对原始轨迹数据集进行时间属性的泛化，相近时间节点的用户合并在同一区域，形成采样轨迹数据集。然后，在同一时间戳的用户通过聚类方法进行分组，利用差分隐私的指数机制计算该组的核心位置，该组内移动用户坐标被泛化成核心位置，对移动用户的轨迹有一定的隐私保护。接着，合并记录并删除异常轨迹数据。最后，在统计结果加入差分隐私的 Laplace 噪声，混淆统计数目的真实性进行发布。

3.2　轨迹处理子算法

轨迹处理子算法 TraPro 负责处理动态轨迹数据，联合时间和空间，有效消除连续的轨迹数据带来的隐私泄露风险。TraPro 由时间泛化和空间分割 2 个步骤组成。

3.2.1　时间泛化

与传统采集固定时间戳的静态轨迹数据不同，TraPro 通过对时间属性的泛化操作，处理动态轨迹数据集，并完成采样轨迹数据集的准备工作，具体实现过程如下。

1) k-means 聚类算法通过预先设定的 k 值及每个类别的初始质心对相似的数据点进行划分，将一天分成 k 个时间段，初始 k 个点是根据不同实验轨迹数据集特性进行选择的。为保证轨迹数据发布的精度，若用户的移动速度较快，较短时间内行动在不同区域，k 就需要取较大数值，反之亦然。通过划分后的均值迭代优化获得最优的聚类结果，选定 k 个中心的初值，针对不同时刻的 i 和 j，对应时间 t 之间的欧氏距离为

$$d\left(t_i,t_j\right)=\sqrt{\left(t_i-t_j\right)^{\mathrm{T}}\left(t_i-t_j\right)} \tag{1}$$

2) 将每个数据点归类到离它最近的那个中心点所代表的簇（cluster）中，计算时间 t 的质心为

$$u_i=\frac{1}{n}\sum_{j=1}^{n}d\left(t_i,t_j\right) \tag{2}$$

3) 计算每个 cluster 的新中心点，把距离质心最近的那些数据点分配给它，移动重心的位置到所有属于它的数据点的平均位置上。迭代直到最大的步数或者前后的距离值之差小于阈值为止，最终 cluster 质心会靠近目的地并停止移动，得到最接近的时间 cluster 集合，选取其质心作为该 cluster 的所有轨迹用户的时间戳。

4) 采用 k-means 聚类算法对时间属性进行泛

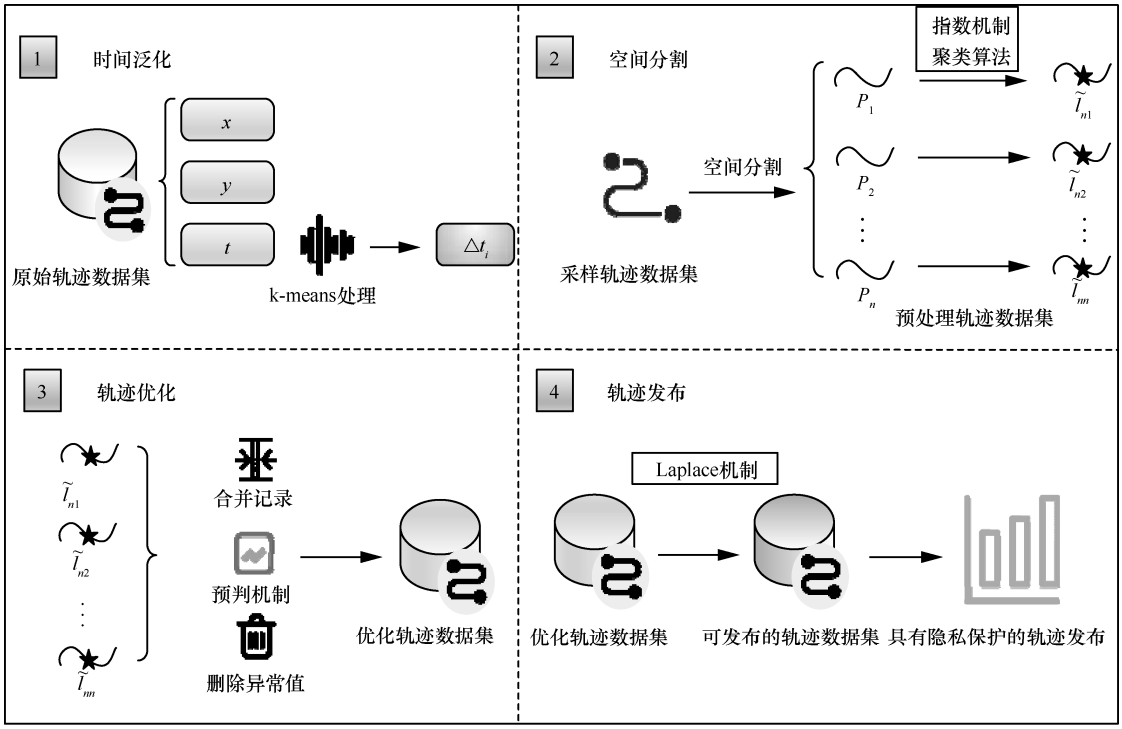


图 1　TPPDP 模型

化，将比较接近的时间合并为同一个时间段，即划分在一个固定的时间区域内。通过对时间属性泛化，将其分成 n 个固定的时间段 $\Delta t_i (i=1,2,\cdots,n)$，假设每条轨迹等长，同一时间段被认为具有相同的时间点。经时间泛化后的轨迹如图 2 所示。

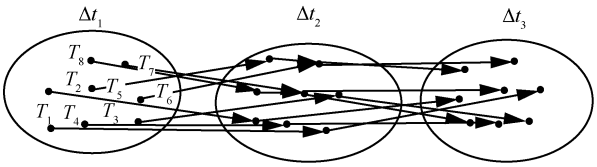


图 2 时间泛化后的轨迹

3.2.2 空间分割

目前，常见的空间划分的方法有网格单元法、二叉数、八叉树等空间分割方法[22]。

TPPDP 采用经典的指数机制和 k-means 聚类算法对采样数据集进行空间分割处理，使用满足特定分布的随机抽样来实现隐私保护，包括空间划分和分区选择两部分。

首先，在空间划分中，将相同时间戳 t 的位置数据进行分割，采用 k-means 聚类算法将该区域分成 k 个子区域，通过预先设定的 k 值及每个类别的初始质心对相似的数据点进行划分，初始 k 值根据不同实验轨迹数据集特性进行选择。然后，利用 k-means 聚类算法的处理结果，对具有更接近位置数据进行合并。最后，通过差分隐私的指数机制定义一个效用函数 U，U 对每一种输出方案计算出一个分值，选择分值最高的分区，也是最优分区方案。具体过程如下。

1) 使用经典的 k-means 方法对位置进行划分，在每个时间戳上根据它们的成对欧氏距离将原始位置数据划分为 N 组，而 k-means 的分区为 $\tilde{P}$。如果 N 的数目比较大，代表分配到很多区域，轨迹的精度损失也更少，计算代价会随之增加。

2) 在 t_i 时刻，所有的移动用户都被集中在区域 L 里，这时区域 L 可以被分割成 g 个候选分区簇，候选分区可以形成一个集合 τ。

3) TraPro 定义一个效用函数 U，对每一个候选的分区 $P \in \tau$ 都赋予一个效用值，选择效用值越高的分区。模型中，$\tilde{T}_i$ $(i=1,2,\cdots,g)$ 表示第 i 个分组的位置质点，其效用函数为

$$U(D,P)=\frac{\mathrm{MeanDist}(\tilde{P})}{\mathrm{MeanDist}(P)} \tag{3}$$

其中，

$$\mathrm{MeanDist}(P)=\frac{1}{g\left|D_{\mathrm{Ls}_P^k}\right|}\sum_{k=1}^{g}\sum_{T_i\in D_{\mathrm{Ls}_P^k}}\mathrm{Distance}\left(T_i,\tilde{T}_i\right) \tag{4}$$

其中，Ls_P^k 为一组按候选分区 P 划分为 k 组的位置集合，$D_{\mathrm{Ls}_P^k}$ 为通过 Ls_P^k 中位置的轨迹集合。

4) 针对第 i 个候选分区 $P_i \in \tau$，效用函数满足 ε-差分隐私的指数机制。根据分值选择分区方法，同时得到该分区的中心位置。

$$\frac{\exp\left(\frac{\varepsilon}{2\Delta u}U(D,P_i)\right)}{\sum_{P\in\tau}\exp\left(\frac{\varepsilon}{2\Delta u}U(D,P)\right)} \tag{5}$$

经过 TraPro 处理后，形成 m 个子簇，计算出每个子簇的簇心，最佳划分可以使轨迹数据点效用损失最小。TraPro 如算法 1 所示。

算法 1 TraPro

输入 D

输出 DG

1) if $D=\varnothing$, then
2) return $\perp$
3) end if
4) choose k center points
5) repeat
6) compute the Euclidean distance from all points
7) form k clusters
8) move the position of the center to the average position of all the points belonging to it
9) until the change of the center point is less than the threshold or reaches the maximum number
10) for each T in D
11) calculate the possible region partition cases $(P_1,P_2,\cdots,P_n)$
12) end for
13) for i=1 to n do
14) Compute $U(D,P_i)$
15) end for
16) select the max U
17) determine the partition $P_{\max}$
18) location partition
19) l←the centre of $P_{\max}$

20)　return DG

在已知的广义区域里，存在 m 个互不相关的移动用户，原始轨迹出现杂乱无章的状态。对原始轨迹数据集进行 TraPro 处理后，每个子簇都有对应的中心，如图 3 所示。

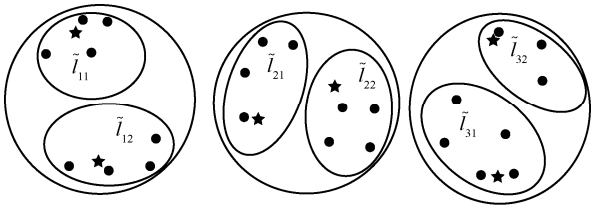


图 3　TraPro 处理后的轨迹

3.3　数据发布子算法

数据发布子算法 TraRel 负责提供轨迹数据发布前的优化操作，简单差分隐私处理会导致发布数据的可用性降低，而 TraRel 包含 2 个步骤：轨迹优化和轨迹发布，有效保证较高的可发布的轨迹数据效用。

3.3.1　轨迹优化

轨迹优化重点检查原始轨迹数据集在哪类新产生的数据集里存在，并运行预判机制，删除异常轨迹，降低发布空轨迹的风险性，增加轨迹发布的有效性。

假设 Ω 为广义的区域，针对同一 Δt_i，模型中假设 cluster 中所有移动用户的位置坐标被泛化为这个位置，在该时刻的所有位置数据点，都可以被认为是 32 个位置质点，那么，在 64 个固定的时间戳，会产生 32^{64} 条可能的轨迹数，这个数据覆盖了所有的轨迹发布的可能性，通过泛化的方法，保护了移动用户隐私，不过也会带来大量的资源消耗。

由于产生一些并不存在的异常假轨迹数据会降低 LBS 的可用性，轨迹优化算法将每个进行处理后的轨迹数据与真实轨迹数据进行对比，统计合并后的真实轨迹的记录数 Real，当发现 Real = 0 时，认为该条轨迹为异常流行病轨迹数据并删除，进一步减少发布空轨迹的风险性，增加轨迹发布的有效性。轨迹优化步骤增强了轨迹数据发布的可用性，1) 对原始数据集和产生的新的轨迹数据集进行对比合并，列举出真实存在流行病的轨迹的记录数；2) 如果监测到记录数为 0，说明新的轨迹数据为空轨迹，判断该条轨迹为异常数据，不进行发布，提高轨迹数据可用性，进一步加强公共卫生数据的服务质量。轨迹优化过程如表 2 所示。

表 2　　**轨迹优化过程**

产生新轨迹数据集	属于该条新轨迹的原始轨迹数据集	真实记录数统计	是否异常
$\tilde{l}_{11}\to\tilde{l}_{21}\to\tilde{l}_{31}$	T_2, T_5, T_8	3	否
$\tilde{l}_{12}\to\tilde{l}_{21}\to\tilde{l}_{31}$	null	0	是
$\tilde{l}_{11}\to\tilde{l}_{21}\to\tilde{l}_{32}$	null	0	是
$\tilde{l}_{12}\to\tilde{l}_{21}\to\tilde{l}_{32}$	T_6	1	否
$\tilde{l}_{11}\to\tilde{l}_{22}\to\tilde{l}_{31}$	T_7	1	否
$\tilde{l}_{12}\to\tilde{l}_{22}\to\tilde{l}_{31}$	T_1	1	否
$\tilde{l}_{11}\to\tilde{l}_{22}\to\tilde{l}_{32}$	null	0	是
$\tilde{l}_{12}\to\tilde{l}_{22}\to\tilde{l}_{32}$	T_3, T_4	2	否

3.3.2　轨迹发布

在轨迹优化处理后，考虑到如果直接发布这个统计数据，虽然已经达到一定隐私保护的目的，但是特别针对如某些统计数为 1 的轨迹，如果攻击方有一定的背景知识，很容易猜到用户归属从而造成隐私泄露。因此，在进行轨迹发布操作时，首先统计原始轨迹的数目，引入差分隐私的 Laplace 机制，添加 Laplace 噪声 $\mathrm{Lap}(S(F)/\varepsilon)$ 到每个真实数据中，可以抵制具有背景知识的攻击者由对数据发动的攻击。$\tilde{D}=\{\tilde{T}_1,\tilde{T}_2,\cdots,\tilde{T}_k\}$ 表示噪声计数排序的轨迹；C_i 表示 $\tilde{T}_i\in\tilde{D}$ 的噪声数，$C_1>C_2>\cdots>C_i$，具体过程如下。

1) 从集合 (C_2,C_1) 开始，根据 Laplace 机制计算 $\Omega-\tilde{D}$ 轨迹内噪声量位于 (C_{i+1},C_i) 的期望值 Num_i。$f(x,\varepsilon)$ 表示 Laplace 分布的概率密度函数。$\Omega-\tilde{D}$ 内每条轨迹的真实计数为 0。加上 $\mathrm{Lap}(S(F)/\varepsilon)$ 后，$\Omega-\tilde{D}$ 的一条轨迹含噪声量在 (C_{i+1},C_i) 区间内的概率为 $\int_{C_{i+1}}^{C_i} f(x,\varepsilon)\mathrm{d}x$，可得

$$\mathrm{Num}_i=\left|\Omega-\tilde{D}\right|\int_{C_{i+1}}^{C_i} f(x,\varepsilon)\mathrm{d}x \tag{6}$$

2) TPPDP 从 $\Omega-\tilde{D}$ 中随机选取不同轨迹的噪声量并将它们和 $\tilde{T}_i$ 一起包含在最终输出集中，噪声计数是这个区间内的随机值，当总计数达到原始数据集 D 的大小时，上述过程停止，并输出统计记录。

对记录数进行 Laplace 机制加噪后，形成的数据集包括轨迹数据集、加噪后记录数，这时只需将处理后的轨迹数据集发布。表 3 展示了轨迹发布过程。

表 3 轨迹发布过程

产生新轨迹数据集	真实记录数统计(不发布)	Laplace 加噪	是否发布
$\tilde{l}_{11}\to\tilde{l}_{21}\to\tilde{l}_{31}$	3	3.2	是
$\tilde{l}_{12}\to\tilde{l}_{21}\to\tilde{l}_{32}$	1	1.3	是
$\tilde{l}_{11}\to\tilde{l}_{22}\to\tilde{l}_{31}$	1	0.7	是
$\tilde{l}_{12}\to\tilde{l}_{22}\to\tilde{l}_{31}$	1	0.5	是
$\tilde{l}_{12}\to\tilde{l}_{22}\to\tilde{l}_{32}$	2	2.3	是

数据发布子算法 TraRel 如算法 2 所示。

算法 2 TraRel

输入 DG

输出 nc

1) if $D=\varnothing$, then
2) return $\perp$
3) end if
4) merging the same original trajectory
5) for different trajectory
6) count the real statistics tc
7) end for
8) for all $p,q\in[1,n_1]$
9) μ=ComputeAverage($\{\mathrm{tc}_p\}$)
10) $\Delta f=\max\limits_{p,q}\{|\mathrm{tc}_p-\mathrm{tc}_q|\}$
11) $b=\Delta f/\mu,\ \beta=2\mu$
12) $\mathrm{In}_i\leftarrow\mathrm{pdf}(x)$
13) end for
14) for each tc
15) if $\mathrm{tc}_i\neq 0$
16) $\mathrm{nc}_i\leftarrow\mathrm{tc}_i+\mathrm{In}_i$
17) end if
18) end for
19) for each nc_i
20) delete nc_i while $\mathrm{tc}_i=0$
21) end for
22) return $\{\mathrm{nc}_i|i=1,2,\cdots,N\}$

3.4 算法理论分析

TPPDP 包含 2 个子算法，在轨迹处理的过程中，子算法 TraPro 处理时间和空间数据，使用了聚类算法 k-means，选取适当的 k，将数据进行分类，时间复杂度为 $O(n^2)$，空间复杂度为 $O(n)$；子算法 TraRel 的时间复杂度为 $O(n)$，空间复杂度为 $O(n)$。本节将 TPPDP 与目前经典的 2 个算法 TSTDA[20] 和 NGTMA[21]进行对比，如表 4 所示。

表 4 时空复杂度分析

算法	时间复杂度	空间复杂度
TPPDP	$O(n^2)$	$O(n)$
TSTDA	$O(n^2\mathrm{lb}n)$	$O(n)$
NGTMA	$O(n^2)$	$O(n)$

如表 4 所示，TPPDP 时间复杂度比 TSTDA 低，体现了本文算法的性能优势。此外，TPPDP 与 NGTMA 时间复杂度相同，但是在数据发布前，TPPDP 在轨迹优化中增加了异常数据去除的步骤，后期不再进行异常数据处理，对比 NGTMA，TPPDP 在提高算法精度的同时，可以进一步节省算法实际运行时所消耗的时间。

4 隐私保护度分析

本节首先证明 TPPDP 各阶段满足 ε-差分隐私，进而根据差分隐私组合特性，证明方案满足差分隐私。

定理 1 TPPDP 在轨迹处理环节的子算法 TraPro 满足 ε-差分隐私。由于 TraPro 在进行原始轨迹处理时，在 k-means 聚类算法的处理结果上，采用效用函数进行空间划分的选择，对每一种分区方案计算实用性分值，设 q 是查询函数，u 是实用性效用函数，分值高的输出方案具有更大的概率进行发布。下面证明当使用查询函数 q 对子算法 TraPro 进行数据查询时，输出结果满足差分隐私。

证明 对任意的查询函数 q 和效用函数 u，定义 $\varepsilon_q^{\varepsilon}(d)$ 表示与 $\exp\big(\varepsilon q(T,r)\big)u(r)$ 成比例的概率选择 r。由 $\varepsilon_q^{\varepsilon}(d)$ 的定义可知，$\int_r\exp\big(\varepsilon q(T,r)\big)u(r)\mathrm{d}r$ 是有界的。根据定义，$\varepsilon_q^{\varepsilon}(d)$ 的概率密度为

$$\frac{\exp\big(\varepsilon q(T,r)\big)u(r)}{\int\exp\big(\varepsilon q(T,r)\big)u(r)\mathrm{d}r} \tag{7}$$

本文定义 Δq 为查询函数中最大可能的差异值。数据集 T 中单条记录变化最多可带来变化 Δq，有

$$\frac{\exp\big(\varepsilon q(T,r)\big)u(r)}{\int\exp\big(\varepsilon q(T,r)\big)u(r)\mathrm{d}r}\leqslant\frac{\exp(\varepsilon\Delta q)}{\exp(-\varepsilon\Delta q)}=\exp(2\varepsilon\Delta q) \tag{8}$$

因为一般选择 $\Delta q\leqslant 1$ 的查询函数为 q，$\varepsilon_q^{\varepsilon}(d)$ 满足 (2ε)-差分隐私，所以 $\varepsilon_q^{\varepsilon}(d)$ 满足 ε-差分隐私。

由此得证，子算法 TraPro 满足 ε-差分隐私。

定理 2 TPPDP 在数据发布环节的子算法

TraRel 满足 ε-差分隐私。假设函数集 F 具有 $S(F)$ 的敏感度，且 K 是将独立噪声添加到 F 中每个函数 f 的输出的算法，如果噪声服从参数值并且采用 $S(F)/\varepsilon$ 的 Laplace 分布，则算法 K 满足 ε-差分隐私，由于噪声在发布前进行添加，对于同一个查询，差分隐私算法输出结果必定相同，从而保证轨迹发布数据的安全性。

证明　在 TPPDP 中，利用条件概率函数，定义 t_i 为查询的数值，针对兄弟数据集 T_1 和 T_2，有

$$\frac{\Pr\left(K(T_1)=t\right)}{\Pr\left(K(T_2)=t\right)}=\Pi_i\frac{\Pr\left[K(T_1)=t_i\middle|t_1,\cdots,t_{i-1}\right]}{\Pr\left[K(T_2)=t_i\middle|t_1,\cdots,t_{i-1}\right]} \tag{9}$$

同时，根据条件分布算法可得

$$\Pi_i\frac{\Pr\left[K(T_1)=t_i\middle|t_1,\cdots,t_{i-1}\right]}{\Pr\left[K(T_2)=t_i\middle|t_1,\cdots,t_{i-1}\right]}\leqslant \Pi_i\exp\left(\frac{\left|f_t(T_1)_i-f_t(T_2)_i\right|}{\lambda}\right)= \exp\left(\frac{\left\|f_t(T_1)_i-f_t(T_2)_i\right\|}{\lambda}\right) \tag{10}$$

使用边界完成证明

$$S\left(F_t\right)\leqslant\lambda\varepsilon \tag{11}$$

因此，子算法 TraRel 满足 ε-差分隐私。

定理 3　TPPDP 满足 ε-差分隐私。

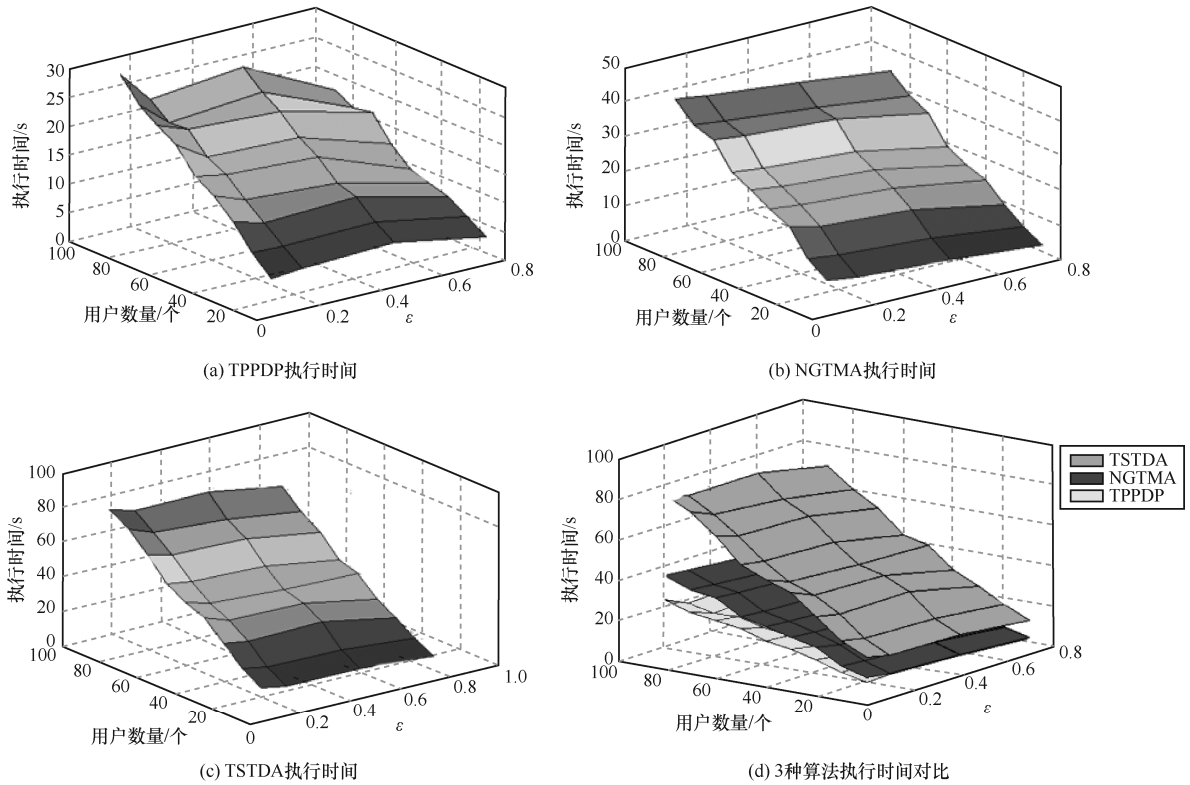
证明　由于差分隐私的组合特性，TPPDP 包含的 2 个子算法分别满足 ε-差分隐私。假设 TraPro 满足 ε_1-差分隐私，TraRel 满足 ε_2-差分隐私，则可推断 TPPDP 满足 ε-差分隐私，此时 $\varepsilon=\varepsilon_1+\varepsilon_2$ 。

5　性能分析

为验证所提 TPPDP 的有效性和数据可用性，本文基于微软的 Research's T-Drive 预研项目数据进行了相关实验[23-24]，其中包含 10 357 辆小车一周的轨迹数据，在这个数据库中的点的总数约为 1 500 万，轨迹的总距离达 9×10^6 km。本节通过 TPPDP 与 TSTDA[20]和 NGTMA[21]的实验对比展示 TPPDP 的高效性。

5.1　算法执行时间

本节将从隐私保护参数 ε 和轨迹数据集大小两方面来分析 TPPDP 的性能表现。将 TPPDP 执行时间与 TSTDA 和 NGTMA 进行对比，实验结果如图 4 所示。



(a) TPPDP执行时间　(b) NGTMA执行时间

(c) TSTDA执行时间　(d) 3种算法执行时间对比

图 4　随 ε 和轨迹数据集变化 3 种方案执行时间对比

由图 4 可以看出，一方面，当用户数量大小一定时，随着 ε 的增加，隐私保护能力逐渐降低，计算量降低，3 种算法的执行时间呈线性减少。另一方面，随着轨迹数据集的增大，计算量明显升高，算法执行时间呈线性增加。同时，由图 4(d)可知，TSTDA 和 NGTMA 的运算开销大于 TPPDP，时间代价高昂，导致运行速度较低，TPPDP 在执行效率上具有明显的优势。

5.2 轨迹合并时间

为了评估 TPPDP 在轨迹处理阶段的表现，在 ε=0.1 和 ε=0.5 这 2 种情况下进行仿真实验，分析随着用户数量的增加，平均轨迹合并时间的变化，实验结果如图 5 所示。

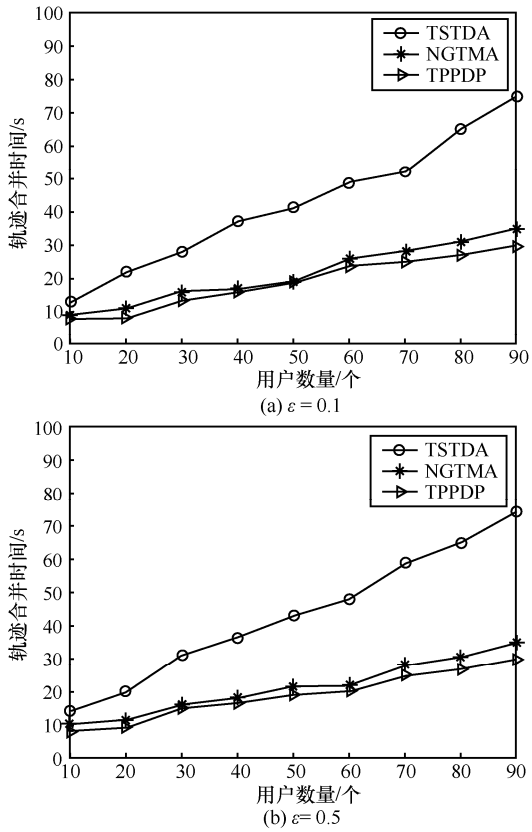


图 5 轨迹合并时间对比

从图 5 可以看出，随着用户数量的增加，3 种隐私保护方案的轨迹合并时间都呈上升趋势，轨迹合并阶段处理操作与隐私参数的选择并没有直接关系，与 TSTDA 和 NGTMA 相比，TPPDP 的轨迹合并时间较小，性能较优。

5.3 噪声产生时间

为了评估 TPPDP 在轨迹发布阶段的表现，取隐私参数 ε=0.1 和 ε=0.5，测试平均轨迹噪声产生时间随着用户数量的增加而产生的变化，对比结果如图 6 所示。实验结果表明，与 TSTDA 和 NGTMA 相比，TPPDP 的轨迹噪声产生时间较少，执行效率较高。

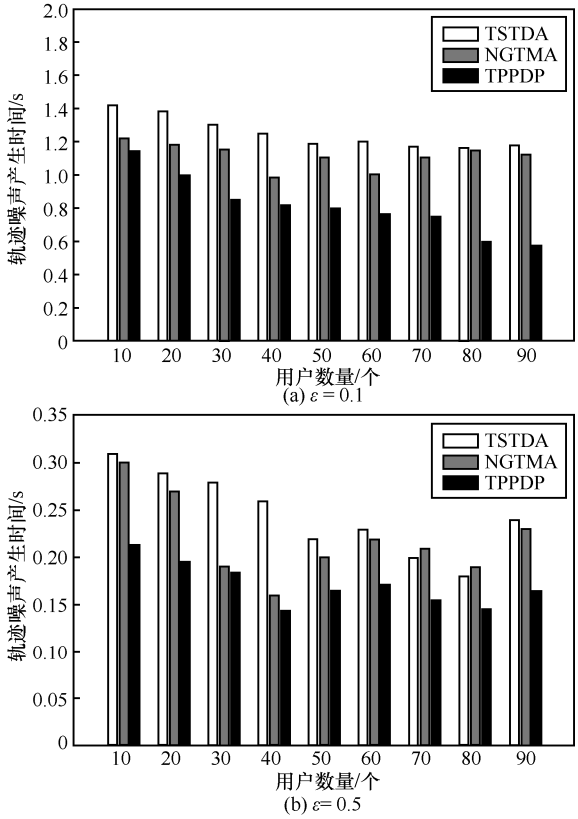


图 6 轨迹噪声产生时间对比

5.4 隐私保护强度

根据差分隐私模型定义，隐私参数 ε 用于衡量隐私保护强度，较小的 ε 提供较高的隐私保护强度。第 4 节从理论上证明了 TPPDP 满足 ε-差分隐私，说明算法可以满足用户轨迹隐私保护需求。本节进一步利用互信息（MI, mutual information）[25]来测试 TPPDP 的隐私保护强度。MI 是信息论里一种有用的信息度量，隐私作为一种信息，可以用信息熵进行量化，MI 用来测量 2 个集合之间的相互依赖关系，表现为猜中某特定用户的概率。

为了评估 TPPDP 在安全性能上的表现，实验取不同的隐私参数 ε=0.1 和 ε=0.5，分析 3 种方案互信息随着用户数量的变化情况，对比结果如图 7 所示。实验结果表明，与 TSTDA 和 NGTMA 相比，TPPDP 算法的互信息值较低，隐私损失度较低，安全性能较好。

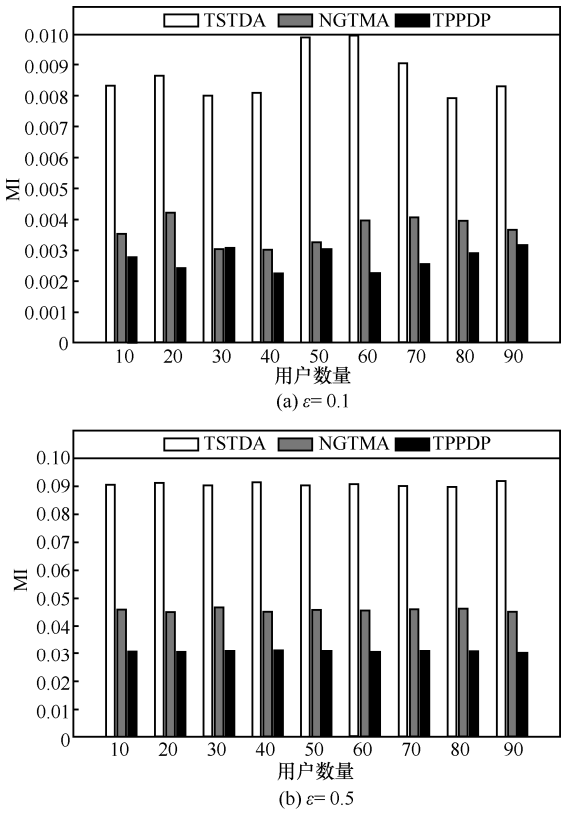


图 7　隐私保护强度对比

5.5　发布数据效用

TPPDP 采用差分隐私机制进行轨迹数据的隐私保护，会不可避免地影响轨迹数据效用。为了测试轨迹发布的数据效用，实验利用豪斯多夫距离（HD, Hausdorff distance）来评估 TPPDP 的轨迹数据效用[20]。HD 用来衡量 2 个点集间的距离，被广泛用于测量 2 个数据集的相似性。通过测试发布数据集和原始数据集之间的 HD 判断数据效用，距离值越小，代表 2 个数据越相似，数据可用性越高，反之亦然。

为了评估 TPPDP 方法在轨迹发布时的数据效用，计算合并轨迹前原始轨迹数据集的真实计数和 Laplace 加噪后计数之间的 HD。实验测量随着用户数量的增加，3 种方案 HD 的变化，实验结果如图 8 所示。实验结果表明，一方面，3 种方案随着 ε 的增加，HD 逐渐变小，隐私保护算法的数据效用增加。这是因为，隐私参数 ε 用于衡量隐私保护程度，ε 越大意味着发布数据集和原始数据集的概率密度函数相似度越低，隐私保护强度越弱，数据可用性越高。另一方面，与 TSTDA 和 NGTMA 相比，TPPDP 的 HD 更小，和原始数据集更相似，具有更高的数据效用。

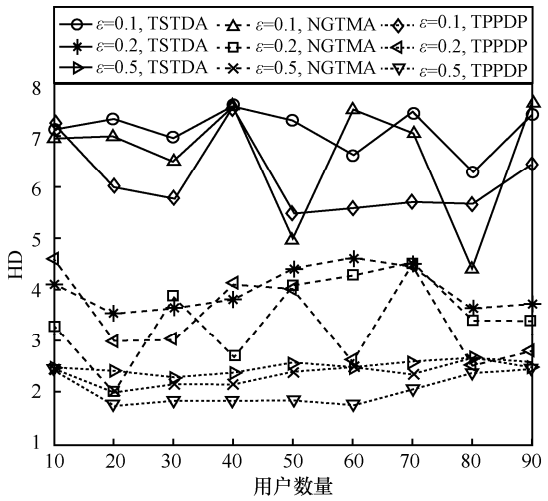


图 8　数据效用对比分析

从上述实验结果可以看出，与 TSTDA 和 NGTMA 相比，TPPDP 算法执行时间较少，隐私损失度较低，数据可用性较高，性能表现整体趋向平稳。

6　结束语

随着智能移动设备、无线通信及定位技术的发展，基于位置服务的技术得到了广泛的应用，给人们生活带来了巨大的便利，服务器根据用户的位置信息和服务需求，为其提供解决方案，因此用户提供位置信息越精确，服务器提供解决方案越理想。本文针对物联网背景下的智能移动设备场景，提出了一种时间泛化和空间分割相结合的差分隐私轨迹数据发布方案，不同于现有的方案，本文方案建立了精准高效的轨迹数据采样模型，通过 k-means 对轨迹数据进行聚合抽样，并且能够提供更强的隐私保护能力，同时引入提前预判机制，减少发布空轨迹的风险性，增加轨迹发布的有效性，保证更好的数据可用性。实验结果证明了 TPPDP 在隐私保护强度、轨迹数据效用和执行效率上具有较大的优势。

参考文献：

[1] 李家印, 郭文忠, 李小燕, 等. 基于智能交通的隐私保护道路状态实时监测方案[J]. 通信学报, 2020, 41(7): 73-83.
LI J Y, GUO W Z, LI X Y, et al. Privacy-preserving real-time road conditions monitoring scheme based on intelligent traffic[J]. Journal on Communications, 2020, 41(7): 73-83.

[2] 陈思, 付安民, 柯海峰, 等. MCDP: 基于神经网络的多集群分布式差分隐私数据发布方法[J]. 电子学报, 2020, 48(12): 2297-2303.
CHEN S, FU A M, KE H F, et al. MCDP: multi-cluster differential privacy data publishing method based on neural network[J]. Acta

Electronica Sinica, 2020, 48(12): 2297-2303.

[3] ZHOU C Y, FU A M, YU S, et al. Privacy-preserving federated learning in fog computing[J]. IEEE Internet of Things Journal, 2020, 7(11): 10782-10793.

[4] 叶阿勇, 孟玲玉, 赵子文, 等. 基于预测和滑动窗口的轨迹差分隐私保护机制[J]. 通信学报, 2020, 41(4): 123-133.
YE A Y, MENG L Y, ZHAO Z W, et al. Trajectory differential privacy protection mechanism based on prediction and sliding window[J]. Journal on Communications, 2020, 41(4): 123-133.

[5] CHEN S, FU A M, SHEN J, et al. RNN-DP: a new differential privacy scheme base on recurrent neural network for dynamic trajectory privacy protection [J]. Journal of Network and Computer Applications, 2020, 168: 102736.

[6] WU S, WANG X L, WANG S, et al. K-anonymity for crowdsourcing database[J]. IEEE Transactions on Knowledge and Data Engineering, 2014, 26(9): 2207-2221.

[7] HE X F, JIN R C, DAI H Y. Leveraging spatial diversity for privacy-aware location-based services in mobile networks[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(6): 1524-1534.

[8] 王洁, 王春茹, 马建峰, 等. 基于位置语义和查询概率的假位置选择算法[J]. 通信学报, 2020, 41(3): 53-61.
WANG J, WANG C R, MA J F, et al. Dummy location selection algorithm based on location semantics and query probability[J]. Journal on Communications, 2020, 41(3): 53-61.

[9] DWORK C, LEI J. Differential privacy and robust statistics[C]//Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 371-380.

[10] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis[C]//Conference on Theory of Cryptography. Berlin: Springer, 2006: 265-284.

[11] KE H F, FU A M, YU S, et al. AQ-DP: a new differential privacy scheme based on quasi-identifier classifying in big data[C]//2018 IEEE Global Communications Conference. Piscataway: IEEE Press, 2018: 1-6.

[12] WANG Y, YANG L, CHEN X Y, et al. Enhancing social network privacy with accumulated non-zero prior knowledge[J]. Information Sciences, 2018, 445/446: 6-21.

[13] 丁红发, 彭长根, 田有亮, 等. 基于演化博弈的隐私风险自适应访问控制模型[J]. 通信学报, 2019, 40(12): 9-20.
DING H F, PENG C G, TIAN Y L, et al. Privacy risk adaptive access control model via evolutionary game[J]. Journal on Communications, 2019, 40(12): 9-20.

[14] CHEN R, FUNG B C M, DESAI B C. Differentially private trajectory data publication[J]. arXiv Preprint, arXiv: 1112.2020, 2011.

[15] HE X, CORMODE G, MACHANAVAJJHALA A, et al. DPT: differentially private trajectory synthesis using hierarchical reference systems[C]//Proceedings of the VLDB Endowment. New York: ACM Press, 2015: 1154-1165.

[16] CAO Y, YOSHIKAWA M. Differentially private real-time data release over infinite trajectory streams[C]//2015 16th IEEE International Conference on Mobile Data Management. Piscataway: IEEE Press, 2015: 68-73.

[17] GURSOY M E, LIU L, TRUEX S, et al. Utility-aware synthesis of differentially private and attack-resilient location traces[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2018: 196-211.

[18] DRAKONAKIS K, ILIA P, IOANNIDIS S, et al. Please forget where I was last summer: the privacy risks of public location (meta)data[C]//Proceedings 2019 Network and Distributed System Security Symposium. VA: Internet Society, 2019: 1-17.

[19] YANG M M, ZHU T Q, LIANG K T, et al. A blockchain-based location privacy-preserving crowdsensing system[J]. Future Generation Computer Systems, 2019, 94: 408-418.

[20] HUA J Y, GAO Y, ZHONG S. Differentially private publication of general time-serial trajectory data[C]//2015 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2015: 549-557.

[21] LI M, ZHU L H, ZHANG Z J, et al. Achieving differential privacy of trajectory data publishing in participatory sensing[J]. Information Sciences, 2017, 400/401: 1-13.

[22] SHAN H M, ZHANG J P, KRUGER U. Learning linear representation of space partitioning trees based on unsupervised kernel dimension reduction[J]. IEEE Transactions on Cybernetics, 2016, 46(12): 3427-3438.

[23] YUAN J, ZHENG Y, XIE X, et al. Driving with knowledge from the physical world[C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2011: 316-324.

[24] 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.

[25] 彭长根, 丁红发, 朱义杰, 等. 隐私保护的信息熵模型及其度量方法[J]. 软件学报, 2016, 27(8): 1891-1903.
PENG C G, DING H F, ZHU Y J, et al. Information entropy models and privacy metrics methods for privacy protection[J]. Journal of Software, 2016, 27(8): 1891-1903.

[作者简介]

陈思（1987− ），女，湖北襄阳人，南京理工大学博士生，主要研究方向为大数据、隐私保护等。

付安民（1981− ）， 男，湖北咸宁人，博士，南京理工大学教授，主要研究方向为物联网安全、机器学习与隐私保护等。

苏铓（1987− ），女，内蒙古翁牛特旗人，博士，南京理工大学副教授，主要研究方向为云安全、访问控制与权限管理等。

孙怀江（1968− ），男，陕西西安人，博士，南京理工大学教授，主要研究方向为神经网络与机器学习等。