基于差分隐私模型的位置轨迹发布技术研究

冯登国*①② 张 敏①② 叶宇桐①

①(中国科学院软件研究所可信计算与保障实验室 北京 100190)

②(中国科学院软件研究所计算机科学国家重点实验室 北京 100190)

摘 要：位置轨迹大数据的安全分享、发布需求离不开位置轨迹隐私保护技术支持。在差分隐私出现之前，K-匿名及其衍生模型为位置轨迹隐私保护提供了一种量化评估的手段，但其安全性严重依赖于攻击者所掌握的背景知识，当有新的攻击出现时模型无法提供完善的隐私保护。差分隐私技术的出现有效地弥补了上述问题，越来越多地应用于轨迹数据隐私发布领域中。该文对基于差分隐私理论的轨迹隐私保护技术进行了研究与分析，重点介绍了差分隐私模型下位置直方图、轨迹直方图等空间统计数据发布方法，差分隐私模型下轨迹数据集发布方法，以及连续轨迹实时发布隐私保护模型。与此同时，在对现有方法对比分析的基础上，提出了未来的重点发展方向。

关键词：隐私保护；差分隐私；位置大数据；轨迹大数据；数据发布

中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2020)01-0074-15

DOI: 10.11999/JEIT190632

Research on Differentially Private Trajectory Data Publishing

FENG Dengguo①② ZHANG Min①② YE Yutong①

①(*Trusted Computing and Information Assurance Laboratory*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)

②(*State Key Laboratory of Computer Science*, *Institute of Software*, *Chinese Academy of Sciences*, *Beijing* 100190, *China*)

Abstract: Securely sharing and publishing location trajectory data relies on support of location privacy protection technology. Prior to the advent of differential privacy, K-anonymity and its derived models provide a means of quantitative assessment of location-trajectory privacy protection. However, its security relies heavily on the background knowledge of the attacker, and the model can not provide perfect privacy protection when a new attack occurs. Differential privacy effectively compensates for the above problems, and it proves the level of privacy protection based on rigorous mathematical theory and is increasingly used in the field of trajectory data privacy publishing. Therefore, the trajectory privacy protection technology based on differential privacy theory is studied and analyzed, and the methods of spatial statistical data publishing are introduced such as location histogram and trajectory histogram, the method of trajectory data set publishing and the model of continuous real-time location release privacy protection. At the same time, the existing methods are compared and analyzed, the key development directions are put forward in the future.

Key words: Privacy preserving; Differential privacy; Location big data; Trajectory big data; Data publishing

1 引言

移动互联网的快速发展将人类带入位置大数据时代。越来越多基于位置的服务(Location Based Services, LBS)融入人们的日常生活，提供诸如兴趣点查询、社交网络实时位置共享、路线规划与导航等服务，为人们提供了极大的便利。与此同时，各类LBS服务汇聚了数以亿计的位置信息，为企业挖掘有价值的商业信息提供了基础数据。通过位置轨迹大数据分析，企业与政府部门能更准确地预测城市交通动态、预先采取措施缓解交通拥堵压力、进行道路规划[1]；也可以为用户构建画像并提供更为精准的个性化服务[2]。

但是，如果缺乏足够的位置轨迹隐私保护，那么数据发布必然导致大量用户隐私泄露。例如，2014

收稿日期：2019-08-26；改回日期：2019-11-30；网络出版：2019-12-05

*通信作者： 冯登国 feng@is.iscas.ac.cn

基金项目：国家自然科学基金(U1636216)

Foundation Item: The National Natural Science Foundation of China (U1636216)

年数据科学家Tocher[3]曾根据公开数据以及乘坐出租车的公开新闻照片识别出了纽约名人搭乘出租车的起点、目的地与乘车费用等；2017年风靡欧美的运动Strava[4]发布了世界用户活动“热图”，被网友挖掘出军事基地的位置、训练时间以及个人用户家庭住址和真实身份等。目前轨迹发布面临最为突出的风险是轨迹去匿名化，即匿名轨迹属主的身份被重新识别出来。在个体位置被持续记录的场景下，轨迹如同指纹一般可以唯一标识出用户。不仅轨迹中特征位置容易暴露匿名轨迹用户身份，而且轨迹中的时序特征、位置分布特征都隐藏着轨迹与现实用户之间的关联。例如，目前基于HMM模型的轨迹去匿名化方法可以识别出Gowalla数据集中近90%的匿名用户[5]。除可能暴露用户身份隐私以外，轨迹还可能泄露大量用户敏感信息。例如，观察到用户出现在医院可以推测出其本人或家庭成员的健康状况；根据用户对某类兴趣点的访问频率，可以推测出用户偏好及经济水平；结合轨迹的产生时段以及起始、结束地点信息，容易推测出用户家庭住址，等等。因此，如何实现位置轨迹数据的安全分享与发布，保护用户身份隐私、敏感属性隐私不被泄露，已成为当前IT产业界与学术界共同关注的重要问题。

在差分隐私出现之前，轨迹匿名与隐私保护大多采用以K-匿名为代表的基于等价类的方法。K-匿名理论假设攻击者能力有限，仅能将攻击目标缩小到一定的等价类范围内，无法唯一地准确识别攻击目标。研究者通过轨迹分割、子轨迹聚类、泛化与扰动等处理，实现至少K个用户轨迹之间不可区分。经典的代表是Abul等人[6]提出的(K,δ)匿名模型，基于欧氏距离对轨迹进行聚类，组内轨迹数目至少为K，组内轨迹间距离小于阈值δ，发布内容为组内均值轨迹，或真实位置点重构轨迹。此后，研究者提出了基于轨迹分割[7]、基于位置点扰动[8]等方法进一步减少位置轨迹片段中的用户特征序列，以满足K-匿名模型或改进的L-diversity模型要求。此外，也有研究者提出了基于路网Mix-zone的假名轨迹集分割、基于伪随机加密的可逆位置泛化等多种改进方法[9]，降低匿名轨迹的重识别风险，增强数据可用性。K-匿名理论面临的最大问题是，一旦攻击者能力超过了预先的假设，就能够进一步区分等价类内的不同记录，实现去匿名化。例如攻击者可通过链接攻击、位置同质性攻击、位置关联依赖攻击等破坏位置或轨迹的K-匿名安全性。总体来说，虽然K-匿名模型及其衍生模型提供了一种量化评估的手段，使得不同类型的方案之间具有可比性，但无法提供严格数学证明，安全性依赖于攻击者所掌握的背景知识。当有新的攻击出现时，原有保护机制可能完全或部分失效，模型无法提供完善的隐私保护。

差分隐私技术的出现有效地弥补了上述问题。一方面，差分隐私模型对攻击者的能力做了最大假定，并不依赖于攻击者所掌握的背景知识；另一方面，差分隐私模型建立于坚实的数学基础之上，对隐私保护进行了严格定义，并提供了量化评估方法，使得不同方法提供的隐私保护水平具有可比性。正因为如此，差分隐私[10]自2006年被提出以来，就受到众多隐私保护领域研究者的关注，广泛应用于支持隐私保护的数据挖掘与数据发布领域[11]。近年来，差分隐私理论与轨迹隐私保护融合研究方面涌现出了一批新成果，本文重点来综述和分析这方面的最新研究成果，并在对比分析的基础上提出未来的重点发展方向。

2　差分隐私模型

2.1　基本定义

差分隐私[10]是基于数据失真的隐私保护技术，通过注入噪声，使得增加或删除一条数据记录的操作对输出的影响不可区分，保证数据集中个体的隐私。其基本概念和定义如下。

定义1(ε-差分隐私，简称ε-DP)[10]　对于一个支持随机机制的查询算法f:$D\rightarrow R^d$，其输入为一个数据集，输出为d维实数向量。若对任意数据集D及其相邻数据集D'，算法f对任意输出$S\subseteq \mathrm{Range}(f)$都满足下列式(1)，则称算法$f$满足$\varepsilon$-差分隐私。

$$\frac{\Pr[f(D)\in S]}{\Pr[f(D')\in S]}\leq \mathrm{e}^{\varepsilon} \tag{1}$$

其中，参数ε被称为隐私预算。定义1表明，ε越小，则差分隐私算法作用在一对相邻数据集上所产生查询结果的概率分布越相似，攻击者更难以判断某元素是否存在于数据集中，因而隐私保护程度更高。

定义2 (全局敏感度)[12]　对于函数f: $D\rightarrow R^d$，定义$\Delta f=\max_{D,D'}\|f(D)-f(D')\|_1$，称为函数$f$的全局敏感度。

全局敏感度是特定查询函数f在所有可能的相邻数据集D和D'上查询时输出值变化的最大范围，其度量值为两者之间的$L1$距离。它与数据集D无关，由查询函数f自身决定。全局敏感度直接影响添加噪声的多少。f的全局敏感度越大，则在ε相同条件下需要注入的噪声越多。在特殊场景下被较小的局部敏感度取代。

复杂的隐私保护问题通常由多个处理步骤组成，需要确定在每个组成算法满足差分隐私的前提下，

设定合理的整体隐私预算。McSherry等人[12,13]提出了两个重要的差分隐私算法组合性质，称为序列组合性和并行组合性。

定义3(序列组合性)[12] 序列组合性是指，给定数据库D与n个随机算法$\{A_1, A_2, \cdots, A_n\}$，若每个算法$A_i$作用在数据集$D$上都满足$\varepsilon_i$-DP，则$\{A_1, A_2, \cdots, A_n\}$在$D$上的顺序序列组合满足$\left(\sum_i^n \varepsilon_i\right)$–DP。

序列组合性表明多个算法序列同时作用在一个数据集上时，最终的隐私预算是各个算法隐私预算之和。

定义4(并行组合性)[13] 将一个数据库D分成n个互不相交的集合$\{D_1, D_2, \cdots, D_n\}$，在每个集合上分别作用一个随机算法$\{A_1, A_2, \cdots, A_n\}$，并且$A_i$满足$\varepsilon_i$-DP。则$\{A_1, A_2, \cdots, A_n\}$在$D$上的并行序列组合满足$(\max\ \varepsilon_i)$–DP。

并行组合性说明若多个算法作用于一个数据集的不相交子集上，则最终的隐私预算是各个算法隐私预算中的最大值。

差分隐私组合性会带来累加噪声，因此复杂函数的隐私预算将随着子查询函数个数的增加而大幅增长，导致数据可用性降低。对于某些场景下，ε-DP显得过于严格，相对松弛的模型可减少所添加的噪声。

定义5((ε,δ)-差分隐私，简称(ε,δ)–DP)[13] 对任意$0<\delta<1$，若随机算法f在数据集合D及其任意相邻数据集D'上，对任意输出$S \subseteq \mathrm{Range}(f)$都满足式(2)，则称$f$满足$(\varepsilon,\delta)$-差分隐私。

$$\Pr[f(D) \in S] \le \mathrm{e}^{\varepsilon} \cdot \Pr[f(D') \in S] + \delta \tag{2}$$

该定义提供了一定自由度，可以理解为使算法f以(1–δ)的概率满足ε-DP。(ε,δ)-DP也称为近似差分隐私。

ε-DP和(ε,δ)-DP的前提假设是数据集中的内容无关联[10,14]。Kifer等人[15]已指出，若该条件不被满足，那么即使加噪数据集满足差分隐私要求，攻击者仍可以利用该关联提升对真实数据的猜测概率[15,16]，并提出了一种较差分隐私更为普适性的隐私定义：PufferFish隐私。

定义6(ε-PufferFish隐私)[17] 给定一个支持随机机制的查询算法$f: D \to R^d$以及一个隐私框架(S, Q, Θ)，其中S为秘密数据集合，$Q \subseteq S \times S$为秘密数据对集合，Θ为数据分布集合。若对于任何分布$\theta \in \Theta$，任何数据对$(s_i, s_j) \in Q$ $(\Pr(s_i|\theta) \ne 0, \Pr(s_j|\theta) \ne 0)$，以及任何输出$w \in \mathrm{Range}(f)$，$f$都满足式(3)，则称$f$在框架$(S, Q, \Theta)$下满足$\varepsilon$-PufferFish隐私。

$$\mathrm{e}^{-\varepsilon} \le \frac{\Pr[f(X) = w|s_i, \theta]}{\Pr[f(X) = w|s_j, \theta]} \le \mathrm{e}^{\varepsilon} \tag{3}$$

θ分布既是数据相关性描述，也是攻击者能掌握的最大能力。式(3)表明，ε-PufferFish隐私仅限定集合Q中的任何数据对s_i, s_j对输出结果概率的影响无显著差别，要求不如ε-DP严格。当Θ为所有可能的数据分布集合，S为全体数据集，Q为集合S上的笛卡尔积时，ε-DP可以看做ε-PufferFish隐私的一个特例。

2.2 噪声机制

Laplace机制、指数机制是实现差分隐私保护最基础的两种噪声机制。其中拉普拉斯机制向返回结果中加入服从拉普拉斯分布的随机噪声，使结果满足ε-差分隐私，适用于数值型数据保护；而指数机制基于打分函数控制各候选项的输出概率，适用于离散型数据保护。

差分隐私的算法所需噪音大小与全局敏感性密切相关，Laplace机制通过拉普拉斯分布产生的噪音扰动真实输出值来实现差分隐私保护。

定理1[18] 对任意一个函数f: $D \to R$，若随机化算法A的输出结果满足式(4)，则称算法A满足ε-DP。

$$A(D) = f(D) + \mathrm{Lap}(\Delta f/\varepsilon) \tag{4}$$

其中，$\mathrm{Lap}(\Delta f/\varepsilon)$是添加的Laplace噪声。噪声变量与全局敏感度成正比，与ε成反比。

指数机制的关键在于设计打分函数$u(D, r)$ $(r \in O)$，其中r表示从输出域O中选择的输出项目。

定理2[18] 给定一个对于数据库D的打分函数u:$(D \times O) \to R$，若算法A满足式(5)，则A满足ε-DP。

$$A(D, u) = \{r : \Pr[r \in O] \propto \exp\left(\frac{\varepsilon u(D, r)}{2\Delta u}\right) \tag{5}$$

其中，Δu是打分函数的最大输出差值，即全局敏感度。打分越高，被选择输出的概率越大。

3 主要研究方向

差分隐私模型所下保护的位置轨迹数据形式复杂多样。其中，统计类数据包括位置直方图、轨迹直方图、地理位置熵等，可满足计数类查询应用需求。除了严格的差分隐私模型外，相对更为宽松的隐私保护需求，如(ε,δ)-DP[14], PufferFish隐私[17]等也被采用以降低所添加的噪声，提高数据在实际应用场景中的可用性。

3.1 差分隐私模型下空间统计数据发布

频度直方图是数据发布经典形式之一。它可以直观地表示数据分布情况，并响应关于数据统计值的查询。在差分隐私模型下对直方图注入随机噪

声，发布加噪后的直方图，可以抵抗攻击者对于数据集是否包含某用户的猜测攻击。由于直方图结构能够降低查询敏感度($\Delta f \approx 1$)，是差分隐私保护中的常用结构之一。

一个朴素的空间直方图把底层的空间分解成网格单元，每个单元记录位置或轨迹片段数量，可以提供单元级别的空间信息查询。由于经典的空间位置大多为2维数据，所以空间位置发布多为2维直方图。空间数据频度直方图可用于空间信息聚集查询，如查询某个区域的用户或者轨迹数量，统计通过一个路段的所有车辆总数，或者一个城市中任意街区的智能手机的使用者数量等。典型的空间直方图包括空间位置直方图与轨迹直方图，分别用于支持空间位置计数查询与空间轨迹计数查询。

3.1.1 位置直方图隐私发布

在差分隐私模型下，一种直观的噪音注入方式是对构成空间直方图的每个单元网格添加独立同分布的拉普拉斯噪声[19]，但在大多数实际应用中，网格粒度的选择面临两难困境：若网格粒度过大，则查询结果精确度难以满足应用需求；而网格粒度过细时，会带来两个严重问题：其一是大多数网格的数据稀疏，其二是误差累加效应明显，覆盖面积较大的查询结果精度急剧降低，且该问题在高维直方图发布中表现尤为突出。以我国地图为例，若采用10 m×10 m的精度表示，则由近10^{11}个网格构成。一个包含千万级位置信息的数据集分散在该地图上时，绝大多数网格被命中的次数为0或者非常小的数值。此时，若为了满足查询ε-差分隐私要求而采用Laplace机制注入噪声干扰，在每个网格单元上应添加Lap($1/\varepsilon$)噪声，方差为σ^2。当查询Q覆盖相当于北京市面积的数据时，查询带来噪声叠加效应将包含10^8个区域的误差，查询结果的方差可达$10^8\sigma^2$。即查询范围愈大，结果失真愈严重。虽然文献[20]中分别给出了一种统一规划的UG方案，以及一种适应性调整AG方案，通过网格粒度优化机制部分改善了该问题，但无法从根本上解决该矛盾。

为了对任何范围查询都提供高精度查询结果，更为普遍的做法是借鉴空间索引的设计思想，实现支持空间计数查询的层次化直方图结构[21,22]。采用不同层次节点表示不同面积的网格，取代统一粒度的网格对外提供直方图查询服务。最常见的是基于四叉树结构的发布方法。

四叉树(QuadTree，又称四分树或四元树)是一种经典空间网格划分方法，可以为划分后的网格提供空间索引服务。当树中每个节点中记录该节点区域所包含的位置点个数时，四叉树可用于响应针对任意区域内所包含位置点的计数查询。由于四叉树结构与数据的相关度较小，因而其所对应的差分隐私保护方法较其他索引更为简单，应用更为广泛。早期的方法采用完全四叉树[21]，树结构本身是完全公开的，只有每个节点所代表的本区域范围位置数目涉及用户隐私，因此其噪声注入方法比较简单，仅涉及对节点计数添加拉普拉斯噪声。因为增加或者删除某个位置，将改变由该位置所在的叶子节点到根节点路径上所有中间节点的计数，所以按照差分隐私的序列组合性(定义3)，总体隐私预算为路径上各个节点的隐私预算之和，且与树的高度密切相关。假定四叉树高度为h，则第i层的树节点的计数注入数量为Lap($1/\varepsilon_i$)的Laplace噪音，当对于各层的隐私预算配额采用平均分配策略时，各层的隐私预算相同，均为$\varepsilon_i = \varepsilon/h$。其和满足总体隐私预算：$\sum_{i=0}^{h} \varepsilon_i = \varepsilon$。

由于各个节点所添加的随机噪声规模相同，因此父节点计数所含噪声期望小于所有子节点随机噪声期望值之和。在响应用户的计数查询时，应采用类似索引树的查询模式，自上而下在四叉树中搜索匹配该查询的节点或节点集合，并根据节点加噪计数进行回答，以最小化结果误差。此外，上述方案还可以从多个角度进行优化：

(1) 各层的隐私预算配额改用几何分配策略，降低总体节点方差；

(2) 可以采用最小二乘法对所有节点的加噪计数进行后置处理，当父子节点之间计数满足一致性约束时，可得到无偏最佳估计值。该处理步骤需要完成自上而下、自下而上、再自上而下的3次树遍历，以提高处理复杂度为代价提升查询结果准确度。

文献[22]提出一种基于不完全四叉树的位置发布方法PrivTree，如图1所示，对高维空间位置数据进行更为合理的划分，摆脱了对树高h的参数依赖，并采用局部敏感度和引入近似误差δ降低噪声误差。较文献[21]方法在Gowalla数据集上的准确率提升近20%。

虽然完全四叉树易于实现差分隐私分析，但它同时也带来很大弊端。尤其是当位置点数据分布极端不均衡时，基于完全四叉树的方法将增加树的高度并形成大量空节点，导致总体注入过多噪声。此时若能采用某种形式的平衡树，更为均衡地实现空间划分，则可以有效降低层次树的高度。单维直方图数据发布中的经典方法之一是为数据集构建K叉平均树[23]，划分使得直方图各个区间数目较为均衡，再通过最优线性无偏估计对其进行一致性修正，降低中间节点所代表的区间查询噪声误差。类

似地，在2维及多维直方图数据发布时，可以采用KD-树索引，每次选择一个中位数所代表的超平面对空间进行均衡划分。由于KD树索引中位置点分布影响树结构，所以隐私预算不仅包括为节点计数注入噪声的配额ε_i^c，还包括用于树结构的随机化的配额ε_i^m。总体隐私预算为：$\sum_{i=0}^{h}\varepsilon_i^c+\sum_{i=0}^{h}\varepsilon_i^m=\varepsilon$

节点计数可以直接添加拉普拉斯噪音，此处不再赘述。而树结构的随机化主要是指中位数选取的随机化。文献[21]给出了多种中位数噪声方法。例如：

(1)添加拉普拉斯噪声方法：计算出每个区间的敏感度σ_s(median)，并在区间中位数基础上添加Lap($2\sigma_s$(median)$/\varepsilon$)噪声。为提高可用性，采用基于局部敏感度包络的平滑敏感度(smooth-sensitivity)替代全局敏感度，使之满足(ε,δ)–近似差分隐私；

(2)采用指数机制加噪。设置rank$(\cdot)$函数返回所有数据排序后的序号。越接近中位数的点其打分函数分值越高，被选择的概率也越大。由于排序函数的敏感度为1，所以某个位置x被选中作为加噪中位数的概率可表示为

$$\Pr\left[\mathrm{EM}\left(c\right)=x\right]\propto\exp\left(-\frac{\varepsilon}{2}\left|\mathrm{rank}\left(x\right)-\mathrm{rank}\left(x_m\right)\right|\right) \tag{6}$$

此外文献[24]中提出的启发式KD树划分方法可供参考。需要指出的是，由于KD索引树是二叉树，其扇出小于四叉树中节点扇出(fanout为4)，导致树高相差近1倍。所以，若不做特殊处理则其误差反而会大于四叉树。只有通过扁平化处理，提升KD树中索引节点的扇出，才能真正达到其设计目的。

3.1.2 轨迹直方图隐私发布

一个朴素的空间轨迹直方图把底层的空间分解成网格单元，每个单元记录轨迹片段数量，可以提供单元级别的空间轨迹查询。但由于各单元之间彼此独立无关，轨迹在多个单元中的子轨迹会被重复计数，导致大范围轨迹聚集查询误差较大。因而EH(Euler Histograms)模型及其变种DEH(Distributed Euler Histogram)模型[25]，以及层次化改进模型EHT(Euler Histograms Tree)模型[26]等作为其改进模型，都可以在某种程度上降低子轨迹重复技术带来的误差，更好地支持矩形空间聚集查询。以EH模型为例，每个单元内的子轨迹数量被记录为面计数(称为Face或F)，同时，穿过单元4个边界的轨迹数目被记录为边记录(称为Edge或E)。当需要准确计算出指定区域内的轨迹数目时，将其拆分为针对面计数F和边计数E的两个子查询，然后计算两者返回值之间的差值，即：$q(H)=q_F(F)-q_E(E)$。

图2为一个说明性示例。在图2(a)中，由16个网格组成的地图包含有4条轨迹。该轨迹集的EH模型表示包括16个面计数以及24个边计数，具体内容如图2(b)所示。当需要查询q所代表空间范围内的轨迹个数时，先分别计算出$q_F(F)$=0+2+2+1+1+2+1+0=9以及$q_E(E)$=0+2+1+0+2+1+0+1+0+0=7，然后可得$q(H)$=9–7=2。

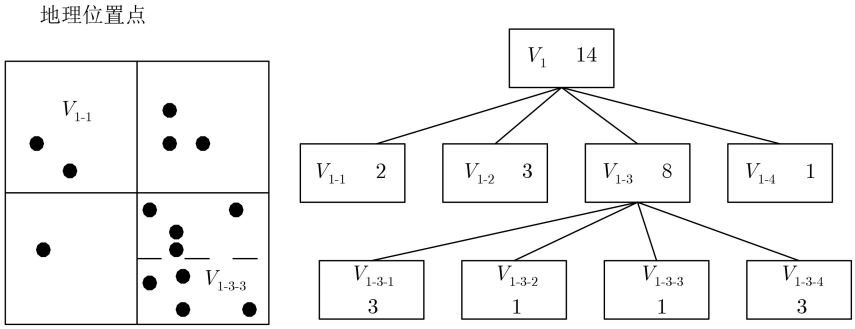
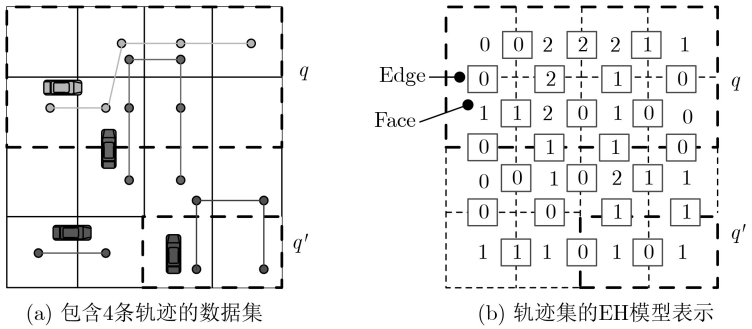


图 1 基于四叉树的差分隐私位置计数查询方法



(a) 包含4条轨迹的数据集　　(b) 轨迹集的EH模型表示

图 2 EH模型功能示意图

因为仅涉及计数，轨迹直方图将轨迹上添加噪声的顺序过程变成了一个并行过程。前者需要满足序列组合性(定义3)，每个节点分配到的隐私预算较小；而后者仅需要满足并行组合性(定义4)，可以保持每个节点的隐私预算不变。因此，上述数据结构可以降低误差，提高发布数据的可用性。且轨迹越长时其优势越明显。

但是，对面计数与边计数分别独立添加噪声将破坏它们之间的关联，影响查询结果的可用性。privSH机制[27]提供了一种满足差分隐私约束的EH模型生成方法，定义了依赖性约束，规定面计数(Face)中的子轨迹数目一定大于等于其相邻的边计数(Edge)。

定义6(依赖性约束dependency consistent)　若直方图$H=\{F,E\}$中的任意边$e\in E$，以及边e的两个相邻的面$f_e,f_e^{'}\in F$，都满足：$c(e)\le\min\left\{c(f_e),c\left(f_e^{'}\right)\right\}$。则称直方图$H$满足依赖性约束。

privSH机制借鉴了一种普遍应用于1维直方图差分隐私的“乘法权重指数机制”(MWEM)[28]，方法基本原理是从一个初始直方图H_0(包括面计数(Face)与边计数(Edge)，且初始为均匀分布)开始，进行I轮迭代运算，不断更新直方图。每次从查询集合Q中随机选择一个查询q，计算q在直方图H_i上的计算结果$q(H_i)$与真实值$q(D)$之间的误差，并根据该误差调整生成新一轮的直方图H_{i+1}。每轮迭代具体步骤如下：

(1) 采用指数机制，以隐私预算$\varepsilon/2I$从查询集合Q中随机选择一个查询wq_i；

(2) 计算该查询在当前直方图的返回值，并以隐私预算$\varepsilon/2I$添加拉普拉斯噪声。$\mathrm{na}_i=\mathrm{wq}_i(H)+\mathrm{Lap}(2I/\varepsilon)$；

(3) 令$\mathrm{qerror}=\mathrm{na}_i-\mathrm{wq}_i(H)$，并对于直方图中的每个元素$x$如式(7)进行更新

$$H_i[x]=H_{i-1}[x]\cdot e^{\mathrm{wq}[x]\cdot\mathrm{qerror}/2n} \tag{7}$$

(4) 对直方图$H_i[x]$中的面计数与边计数进行调整，将面计数设定为4个相邻边计数中的最大值，$c(f_e)=\max\{c(e1),c(e2),c(e3),c(e4)\}$，以满足依赖性约束。

privSH机制通过逐步逼近可生成满足ε-DP的轨迹直方图，保持了EH数据结构一致性，可提供有效的轨迹查询服务。但是作者也指出，方案中的一致性调整方法对原有的MWEM机制性能有一定影响，仍有待改进。

3.1.3　位置熵直方图隐私发布

除了位置与轨迹计数信息以外，位置相关统计信息还包括位置熵(Location Entropy, LE)[29]。它以熵的形式衡量地理位置的受用户欢迎程度，不仅反映了位置被访问的热度，同时兼顾了用户参与的多样化程度，定义如下。

定义7(位置熵LE)　若某个地理位置l曾经被$|U_l|$个用户所访问，并且每个用户访问的次数分别表示为$C_{l,U1},C_{l,U2},\cdots,C_{l,|Ul|}$，则该位置的熵表示为

$$H(l)=-\sum_{u\in U_l}p_{l,u}\lg p_{l,u} \tag{8}$$

其中，U_l为所有访问过位置l的用户集合，$p_{l,u}=c_{lu}/c_l$表示用户u对位置l的贡献度，C_l表示对位置l的所有访问次数，c_{lu}表示该用户u对位置l的访问次数。某个位置的位置熵值越大，说明该地理位置越受用户欢迎。

显然，为了对发布的位置熵直方图进行差分隐私保护，防止攻击者能感知到某个用户数据是否对发布的位置熵有贡献，可以采用拉普拉斯机制对其进行噪声处理，注入噪声的规模取决于全局敏感度。由于删除某个用户时，将同时删除该用户所访问的所有位置，及其对每个位置的访问次数，因此全局敏感度取决于两个因素：一个是用户所允许访问的位置数目，用$M_{\max}$表示；另一个是用户对每个位置的最大访问次数C，其对熵值的影响可以表示为：$\Delta H=\max\{\lg 2,\lg C-\lg(\lg C)-1\}$。因此总体添加的噪声规模为$\mathrm{Lap}(M_{\max}\Delta H/\varepsilon)$。

对于参数$M_{\max}$, C的取值可能导致全局敏感度与噪声过大的问题，既可以通过限制参数的取值范围解决，也可以采用本地敏感度或本地敏感度函数的上确界——平滑敏感度函数替代全局敏感度的方式解决[29]。由于本地敏感度、平滑敏感度均与数据相关，存在一定隐私泄露风险，因此只能满足$(\varepsilon,\delta)-\mathrm{DP}$，其中$\delta<1/\#\mathrm{users}$。但这些方法通过引入少量的近似误差显著地减少了扰动误差，提升了发布的位置熵数据的可用性。

3.2　差分隐私模型下轨迹数据集发布

用户轨迹中不仅反映了位置分布特征，还蕴含了丰富的时序特征。但显然这些时序信息在空间直方图发布过程中都被丢弃了。空间直方图的主要缺陷就在于它无法满足数据使用者进行序列分析等深层次需求。与之相比，直接发布轨迹数据可以最大程度保留轨迹特征。在差分模型下，轨迹发布的目标是如何对轨迹数据集进行净化处理，保证相邻轨迹数据库的输出概率不可区分，确保用户轨迹隐私不被泄露。目前已有基于树重构、基于位置聚类等多种差分隐私轨迹发布方法。尽管它们仍对发布轨迹集特征有较多限制，如限制轨迹最大长度、位置

集合规模等，但是这些方法最大程度地保留了轨迹的序列特性，可以应用于频繁子序列发现等轨迹分析处理。

3.2.1 基于树重构的差分隐私轨迹发布

首先考虑最为简化的情形，一条轨迹可以抽象表示为一个位置序列，所有位置来源于一个已知位置集合。表1是一个轨迹数据集样例[30]。基于树重构生成净化轨迹数据集方法，顾名思义，先将待发布的轨迹数据集表示为“树”的形式，再基于差分隐私模型对该树的结构及节点内容进行调整，最后基于重构后的轨迹树生成净化轨迹数据集。所采用的树结构包括前缀树[30]、搜索树[31]、以及预测后缀树(PST[22])等。

表 1 轨迹序列数据集

序号	路径
1	$L1\rightarrow L2\rightarrow L3$
2	$L1\rightarrow L2$
3	$L3\rightarrow L2\rightarrow L1$
4	$L1\rightarrow L2\rightarrow L4$
5	$L1\rightarrow L2\rightarrow L3$
6	$L3\rightarrow L2$
7	$L1\rightarrow L2\rightarrow L4\rightarrow L1$
8	$L3\rightarrow L1$

最为典型的树结构为前缀树。前缀树是一种紧凑的序列表达方式，通过前缀树的深度优先遍历，可以无损恢复位置序列，因而前缀树可更为节省空间地存储序列。如图3所示。

在一种基于前缀树的轨迹差分隐私保护方法[30]中，通过两个核心步骤实现树重构：(1)构造加噪前缀树；(2)为加噪前缀树中每个节点计数注入噪声。需要注意以下问题：首先，对于一个给定的轨迹序列集合D，可以为其构造前缀树PT，同时记录每个节点的重复出现次数。但加噪前缀树与之不同，为了满足后续差分隐私处理需求，在树PT节点生成过程中，除了对应于真实轨迹中存在的子节点以外，其他所有位置也都被设置为当前节点的子节点，其计数为零。因此每个节点都有大量零计数子节点。其次，步骤(2)中隐私预算可采用均一化分配策略，树的高度为h，因此每个节点的隐私预算为$\bar{\varepsilon}=\varepsilon/h$，意味着为PT中的每个节点$n$计数添加Lap$(1/\bar{\varepsilon})$拉普拉斯噪声。

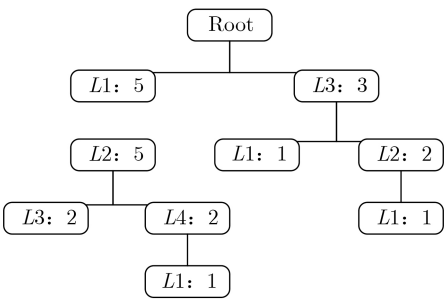


图 3 轨迹序列的前缀树表示

考虑到存储效率因素，上述两个步骤可以采用反复迭代模式进行，即：先对当前节点计数添加Lap$(1/\bar{\varepsilon})$拉普拉斯噪声，若其随机化后的计数大于阈值θ，则保留该节点继续扩展子节点，否则剪枝。此外，为了提高算法效率，可以将所有零计数节点依次添加Lap$(1/\bar{\varepsilon})$拉普拉斯噪声的过程，改进为采用离散化拉普拉斯机制，依据二项分布$B(m,p_\theta)$抽样生成参数k。其中m为所有零计数节点个数，$p_\theta=(1/2)\exp(-\bar{\varepsilon}\theta)$表示每个零计数节点随机化后取值大于阈值$\theta$的概率。然后随机选择$k$个零计数子节点，令其计数大于阈值$\theta$，且取值满足式(9)分布

$$P(x)=\begin{cases}0, & \forall x<\theta\\ 1-\exp(\bar{\varepsilon}\theta-\bar{\varepsilon}x), & \forall x\geq\theta\end{cases} \tag{9}$$

经过上述步骤处理，少数零计数节点加噪后大于阈值被保留，也有少部分真实节点加噪后被剪枝，导致树结构发生变化。基于该树生成的轨迹集合满足差分隐私保护。

在遍历前缀树生成输出轨迹序列集之前，还需要对节点计数进行一致性处理，消除由于随机噪声导致的父节点计数及其子节点计数和之间的差异。一致性约束定义规定父节点的计数大于等于其所有子节点的计数之和。对修正后的前缀树进行深度优先遍历，即生成可供发布的序列集合。

前缀树的高度由数据集中最长的轨迹长度所决定，而树的高度影响了每个步骤被分配的隐私预算。因此为了限定输出数据误差，应限定轨迹集的最大长度，对过长轨迹截断处理，但这很可能导致某些频繁子序列丢失。针对此问题，文献[31]提出一种变长N-gram模型(又称搜索树模型，参见图4)，可提取任意长度轨迹中的n-元子轨迹片段，并发现最大长度为n的频繁子轨迹。为了减少噪声注入，该方案采用适应性隐私预算分配方案取代了均一化分配方案。其背景在于剪枝操作使得树中部分路径长度不足h。对于这些较短路径中的节点，可以为其分配较均一化方案中更多隐私预算配额($\bar{\varepsilon}>\varepsilon/h$)，避免隐私预算浪费。由于搜索树是由“加噪-扩展”迭代生成，因此某节点加噪处理时其路径长度仍未知，需要某种方法对其近似估计。令$P_{\max}$表示从当前节点v向其所有子节点转移概率的最大值，

其值可以根据马尔科夫假设，由数据集中位置转移概率的统计近似求得。依据公式$c(v)\cdot(P_{\max})^{h_v}=\theta$对剩余路径长度做最大估计，可得

$$h_v=\min\left(\lg_{P_{\max}}\frac{\theta}{c(v)},n_{\max}-i\right) \tag{10}$$

相应地，对该节点的隐私因子的估计值为：$\varepsilon_v=\bar{\varepsilon}/h_v$。其中$\bar{\varepsilon}$为当前剩余隐私因子。由于降低了注入噪声规模，N-gram方案消除了对轨迹长度的限制，可以支持长达14,795个状态的轨迹[31]，top-K频繁子轨迹发现召回率(TPR)提升效果也非常显著。但其所能支持的数据状态空间仍然十分有限。

为了解决实际应用中位置网格粒度选择的困境，以及轨迹分布不均衡问题，文献[32,33]提出了一种折中性的多层次前缀树的方法(Differentially Private Trajectory, DPT)，采用不同层次代表不同粒度的地理网格结构。通过层次参考系统映射(hierarchical reference systems mapping)，将轨迹按照速度特性分解表示为多个轨迹片段，分别被映射到不同层次的参考系统中，从而兼顾了不同类型轨迹的粒度需求。例如，当运动轨迹呈现出运动速度快，轨迹较为平缓特点时，采用高层的参考系统，节点精度较低；反之则映射于底层参考系统中，节点精度高。通过在不同层次上的分解与映射，极大地降低了描述一条轨迹所需的坐标点数目。相应地，DPT方法为轨迹数据集构造了一个前缀树集合，HRS→$\{T_1,T_2,\cdots,T_M\}$。其中的每个前缀树只负责记录某一个层次下的子轨迹序列集。树中每个节点都有两种类型子节点；一类是在同一层次系统下的9个子节点，分别代表下一步可能的9个移动方位；另一类是M个子节点，代表下一步可能移动到的其他参考系统。假定某条轨迹被分为如下3个片段，分别记录于RS2, RS3和RS2参考系统对应的前缀树中。图5表示了该轨迹片段在RS2前缀树中的存储方式。

(1) $(4,1)_2$, $(5,1)_2$, $(2,0)_3$;

(2) $(2,0)_3$, $(3,0)_3$, $(4,0)_3$, $(5,0)_3$, $(6,1)_3$, $(6,1)_3$, $(6,1)_3$, $(13,3)_2$;

(3) $(13,3)_2$, $(13,4)_2$, $(13,5)_2$, $(14,6)_2$。

在图5中root被视为第0层。坐标点$(4,1)_2$令位于第1层的节点“(4, 1)”计数加1操作；类似地，二元序列“$(4,1)_2(5,1)_2$”令第2层的节点“(4, 1)(5, 1)”的计数加1；三元序列“$(4,1)_2(5,1)_2(2,0)_3$”比较特殊：因为坐标$(2,0)_3$属于RS3，

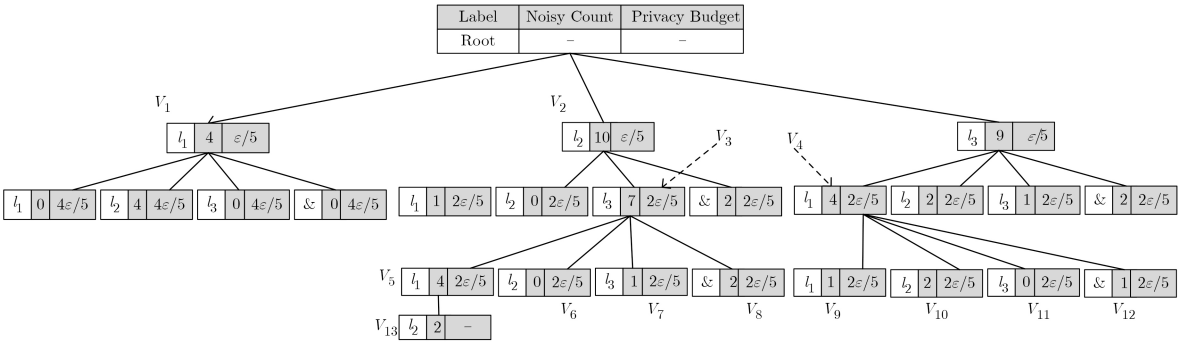


图 4 基于N-gram的搜索树方法

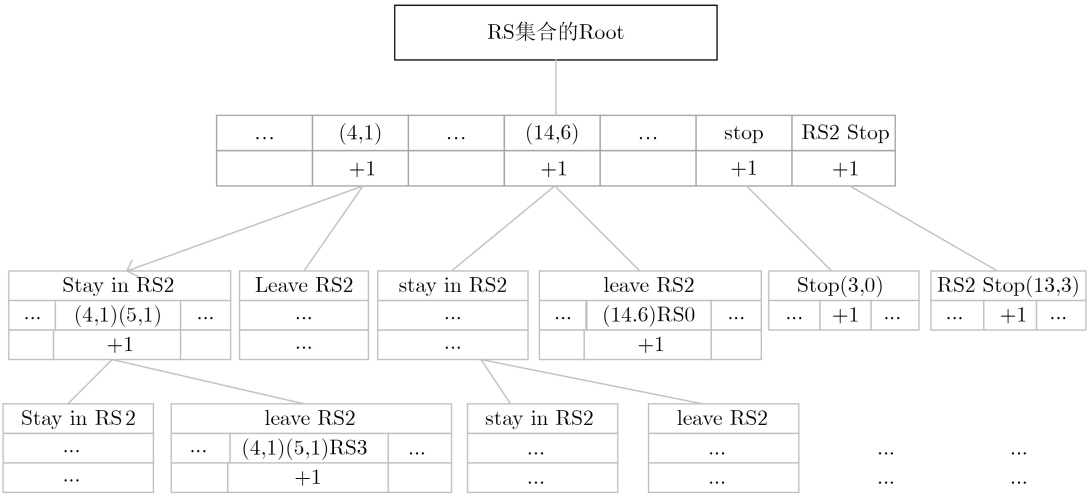


图 5 轨迹片段在RS2前缀树中的表达示例

所以该序列最终令第3层节点“(4, 1)(5, 1)RS3”的计数加1。按照上述规则可以将整条轨迹中相应部分添加到RS2前缀树中。

前缀树节点添加噪音以及剪枝等步骤与前面类似，不再赘述。值得一提的是，为了降低总体误差，DPT方案不仅为节点添加随机噪声，还选择随机丢弃部分前缀树，因此方案误差由两部分构成：$\mathrm{Error}\left(F^{+},\varepsilon_{\mathrm{r}},k,D\right)=\sum_{T_m\in F^{+}}N_m\left(\varepsilon_{\mathrm{r}},k\right)+\sum_{T_m\in\left(F^{\mathrm{full}}-F^{+}\right)}k.c_m(D)^2$。前者为每个前缀树节点添加拉普拉斯噪声引入的误差，后者是随机丢弃一部分前缀树造成的误差。相应地，整体隐私预算分配为两部分，ε=ε_{s}+ε_{r}，其中ε_{s}是用于为选择树添加随机噪声，ε_{r}用于对前缀树节点计数添加Laplace噪声。为了实现误差Error最小化，即通过搜索算法对参数F^{+}(前缀树集合)与k(前缀树高度)的选择优化，得到参数F^{+}和k的最优解或近似最优解。DPT方案较早期方法[30,31]显著提升了轨迹直径分布的准确度、起终点匹配度以及F1-score等指标，在相同的隐私预算下提高了轨迹数据的可用性。

3.2.2 基于聚类的差分隐私轨迹发布

差分轨迹隐私发布中另一类重要方法基于位置聚类的思想。在位置精度高、候选位置集合规模巨大，且每个位置数据相对稀疏的场景下，该类方法较树重构方法更为通用。考虑的问题为：若每条轨迹可被抽象表示为一个由位置与时间构成的二元组序列，$T_i=(l_1,t_1)\to(l_2,t_2)\to\cdots\to(l_n,t_n)$，如何对轨迹集合$T$进行净化处理，使其成为满足差分隐私要求的可发布的数据集T'？

基于聚类的轨迹发布仍然采用了分阶段处理的思想[34]，按照时间将长度为$|T|$的轨迹集处理分为$|T|$个阶段，在每个阶段对所有位置进行聚类分组，用每个聚类中心点替代该聚类中所有真实位置点，产生扰动后的轨迹数据集。正由于采用计算生成的聚类中心点取代了前缀树方法中的真实位置，降低了候选位置数目，所以基于聚类的轨迹发布可以在支持更高精度的位置表示的同时，避免状态爆炸问题。

可以看出，有两项处理需要引入随机化噪声，分别是：(1)聚类中心点的随机化；(2)对轨迹计数的随机化。相应的隐私预算包括两部分$\varepsilon=\varepsilon_1+\varepsilon_2$。后者噪声注入方法是拉普拉斯机制并进行一致性修订，不再赘述。下面介绍聚类分组随机化处理方法。

采用经典聚类算法如k-means算法可以实现位置点聚类。若给定了分组数量参数g，根据其聚类分配策略p，可不断迭代计算每个位置点与各聚类分组的距离，修订其所属分组，最终得到稳定的g个聚类分组。在聚类中心点的随机化时，不再采用上述经典聚类分配策略，可以随机分组，采用指数机制在所有可能分配策略中选择分配策略$\tilde{p}$。

若定义在某个随机分配策略$\tilde{p}$下，每个位置点到其所属聚类分组的距离均值为$\mathrm{MeanDist}\left(\tilde{p}\right)$，则根据k-means原理显然有$\mathrm{MeanDist}\left(\tilde{p}\right)\geq\mathrm{MeanDist}\left(p\right)$。可以将打分函数定义为式(11)的形式，采用指数机制选择聚类分组策略。与经典分配策略接近的策略$\tilde{p}$更大概率会被选中，也可以理解为距离接近的点更高概率会被聚类在一组

$$u\left(D,p\right)=\frac{\mathrm{MeanDist}\left(\tilde{p}\right)}{\mathrm{MeanDist}\left(p\right)}\tag{11}$$

在上述步骤中参数g(聚类分组数目)的选择是一个关键因素。一般来说，g取值增大，则分组中的位置更趋紧密，聚类中心与位置的距离更小，因而数据可用性更好。但同时应该注意，随着g取值增大，不同轨迹合并的几率下降，每条轨迹的计数相应减少了。因而，g取值过大时反而会在添加Laplace噪音后降低数据可用性。因而g的取值应在一定合理区间，并与轨迹长度$|T|$及轨迹集大小n相关。

由于采用高斯机制对所有的分配策略打分的过程时间复杂度是$O(|T|mgn^g)$，其中n为所有用户轨迹总数，m为维度，分配策略数量为n^g种，在实现中耗时过高。可以通过选择指数机制中权值较高者作为候选项，减少分配策略的候选空间来降低复杂度，提高算法效率[35]。

图6描述了该方案1次执行过程。首先将集合D根据时间点分为$|T|$个子集$L_i,(1\leq i\leq|T|)$；然后设置聚类的分组数目参数g，并基于k-means算法依次对每个子集L_i采用聚类分配策略$\tilde{p}$，将其分为g个分组。最后，用聚类后的中心点代替原始轨迹数据集D的轨迹点，从而得到扰动后的轨迹集S。在图6中，g=2, $|T|$=4。

轨迹聚类方法满足ε-差分隐私。即使攻击者掌握了D的相邻数据集D'(D'包含除轨迹T以外的其他所有轨迹),也无法通过发布的数据集D得知轨迹T的信息。

3.3 连续轨迹发布隐私保护模型

3.2节所述各类轨迹隐私保护方法在ε-DP模型框架下，将轨迹发布视为一系列连续位置的发布，在每个步骤添加适当的噪声(相当于每个轨迹点注入Lap($|L|/\varepsilon$)的噪声，$|L|$为轨迹长度)，利用的组合特性确保总体满足隐私预算为ε的差分隐私要求。为了保持发布数据的可用性，要求轨迹集中任何轨迹满足最大长度约束，这极大地限定了发布数

原始轨迹集合D

NO	t_1	t_2	t_3	t_4	轨迹
T_1	1	1	1	1	$(l_1,t_1)\rightarrow(l_2,t_2)\rightarrow(l_3,t_3)\rightarrow(l_4,t_4)$
T_2	1	1	1	1	$(l_5,t_1)\rightarrow(l_6,t_2)\rightarrow(l_7,t_3)\rightarrow(l_8,t_4)$
T_3	1	1	1	0	$(l_9,t_1)\rightarrow(l_{10},t_2)\rightarrow(l_{11},t_3)$
T_4	0	1	1	1	$(l_{12},t_2)\rightarrow(l_{13},t_3)\rightarrow(l_{14},t_4)$
T_5	1	1	1	1	$(l_{15},t_1)\rightarrow(l_{16},t_2)\rightarrow(l_{17},t_3)\rightarrow(l_{18},t_4)$
T_6	0	0	1	1	$(l_{19},t_3)\rightarrow(l_{20},t_4))$
T_7	1	1	1	0	$(l_{21},t^1)\rightarrow(l_{22},t^2)\rightarrow(l_{23},t_3)$

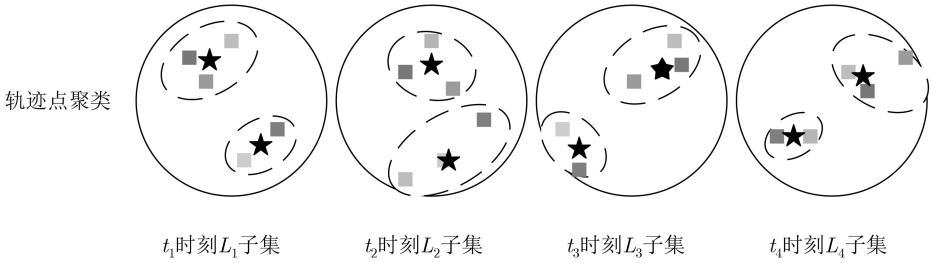


图 6 轨迹聚类方法过程示意图

据的使用范围。而连续发布的轨迹数据之间存在的高度关联性使得该问题变得更加困难。本小节介绍适用于理论上无限长用户连续轨迹数据发布方法，旨在解决如下连续数据动态发布问题：如果从t_1，t_2，至t_{i-1}时刻的所有已发布位置数据(已注入噪音)均满足隐私保护模型要求，那么如何对t_i时刻的位置信息添加随机化噪声，使得该时刻发布的数据也同时满足隐私保护模型要求？

3.3.1 本地化差分隐私模型下的轨迹隐私保护

本地化差分隐私(LDP)的目标在于解决服务器不可信场景下数据安全采集与分析问题。与经典集中式差分隐私模式不同，在LDP模式下，用户提交数据之前先于本地进行随机化加噪处理，然后于服务器端进行统计与分析。目前LDP被广泛应用于热门网址发现[36]、常用表情图标筛选、热点频率统计[37]等场景，以实现用户隐私保护的数据采集与分析。

同理，若用户在位置轨迹信息采集时将地理位置交与不可信服务器，则等同于已经失去位置隐私，后续保护机制也失去了意义。但是技术实现上并不能直接应用已有的Rappor[36], SH[37]等经典LDP算法，原因在于，连续提交的多个数据之间显然存在某种程度的关联，用户不可能产生随机移动。例如，受到移动速度与路网结构等因素影响，在已知用户在t_{i-1}时刻位置的前提下，用户在t_i时刻可能出现的位置范围就十分有限。一方面，如果添加噪声时未考虑这些因素，则攻击者可以利用掌握的用户历史位置信息及位置转移概率来推测当前准确位置，使得原有ε-DP机制失效。另一方面，若考虑所有位置之间的迁移可能性，容易导致噪音添加过度，降低数据可用性。

针对上述问题，文献[38]在对攻击者能力进行合理假设基础上提出了一种LDP轨迹隐私保护方法，对攻击者能力予以最大假定。假设攻击者有能力掌握(1)用户轨迹的1阶马尔科夫模型矩阵M; (2)用户在t_{i-1}时刻以及之前的所有真实地理位置。

当攻击者看到用户t_i时刻发布的加噪位置y_i时，存在$\Pr[x_i|M,y_i,x_{i-1}]$的概率可以推测出用户的真实地理位置x_i。在此假定下用户的隐私保护需求为：在t_i时刻发布的用户地理位置y_i对于任意一组可能的候选地理位置x_i与$x_i^{'}$，都满足式(12)约束

$$\mathrm{e}^{-\varepsilon}\leq\frac{\Pr\left[\mathrm{Noise}\left(x_i\right)\right]=y_i|x_{i-1})}{\Pr\left[\mathrm{Noise}\left(x_i^{'}\right)\right]=y_i|x_{i-1})}\leq\mathrm{e}^{\varepsilon}\tag{12}$$

若无特殊限定，要求在所有用户可能位置集合上，且对于任意一组位置x_i与$x_i^{'}$都严格满足上述差分隐私约束，那么为了满足ε-DP所添加的噪声，将导致地理位置坐标随机偏移过大而不可用。因为一旦t_i时刻发布的加噪地理位置y_i ($y_i=\mathrm{Noise}\left(x_i,x_{i-1},x_{i-2},\cdots\right)$)与$t_{i-1}$时刻的真实位置$x_{i-1}$在语义和位置连续性等方面存在巨大偏差，位置$y_i$就失去了价值，与之相关的LBS服务也将失效。

为了解决上述问题，文献[38,39]从以下几方面着手改进，提高了发布数据可用性。

(1) 提出了δ-位置集合(δ-Location Set)概念限定了x_i与$x_i^{'}$的取值范围。具体来说，根据用户在任意时刻t_i的真实地理位置，为其产生相对应的δ-位置集合，它既是用户在该时刻最可能处于的位置集合，也是攻击者可用于推测地理位置的选择范围。在该集合中随机选择某位置替换真实的地理位置进行发布。定义如下。

定义8(δ-位置集合 δ-location set) 令$\Pr[x_i|M,x_{i-1}]$表示t时刻用户处于位置x_i的先验概率，若该值不小于1–δ，则将其添加到t时刻的δ-位置集合ΔX_t中。用公式表示为

$$\Delta X_t = \min\left\{x_i | \sum_{x_i} \Pr[x_i|M, x_{i-1}] \geq 1-\delta\right\} \quad (13)$$

相应地，隐私保护需求被限定为在任何时刻，δ-位置集合中的位置都满足差分隐私保护。即：对于任意时刻t下的δ-位置集合ΔX_t中的任意两个位置x_i与$x_i^{'}$，以及任意输出y_i，满足

$$\mathrm{e}^{-\varepsilon} \leq \frac{\Pr\left[\mathrm{Noise}\left(x_i\right)=y_i\right]}{\Pr\left[\mathrm{Noise}\left(x_i^{'}\right)=y_i\right]} \leq \mathrm{e}^{\varepsilon} \quad (14)$$

(2) 进一步优化噪声添加方式。通过对全局敏感度的深入分析，发现采用经典的L1范式距离计算多维空间中的数据敏感度，会造成不必要的浪费。通过定义敏感度壳(sensitivity hull)，即由δ-位置集合中任何两点之间的距离向量所构成集合的凸集，更为逼近真实的敏感度，从而减少注入的噪声规模。

定义9 敏感度壳(sensitivity hull) 对于一个查询f以及一个δ-位置集合ΔX_t, Δf为由该集合中任意一对位置点(x_1, x_2)之间的差值构成的集合，则敏感度壳是集合Δf的凸壳，表示为

$$\begin{aligned} &\Delta f = \bigcup\nolimits_{x_1,x_2\in\Delta X_t} f\left(x_1\right) - f\left(x_2\right) \\ &K = \mathrm{Conv}\left(\Delta f\right) \end{aligned} \quad (15)$$

基于定义9可以将敏感度壳视为查询核，应用K-norm机制[40]所产生的2维噪声分布添加噪声。K-norm机制基于凸多面体均匀采样思想，将t时刻的地理位置x_i随机化为y_i (y_i=Noise(x_i))发布，并通过平面的各向同性确保δ-location set中的任何一点对位置y_i输出概率没有实质差异。

(3) 为了摆脱对先验概率的依赖，解决在先验概率为零的特殊情形下(例如用户首次出现在某个位置，对所有位置的先验转移概率均为0), ΔX_t可能为空集，从而导致方法失效的问题，可将候选位置集合的定义由δ-location set扩展为(δ, r)-dataset[39]。其中新参数r代表坐标半径。该dataset中包含t_i时刻以真实位置x_i为圆心、r为半径的范围内候选地理位置集合。相应地，添加噪音的敏感度与r的大小相关，表示为

$$\Delta f = \max_{p_i,p_j\in(\delta,r)-\mathrm{dataset}} \mathrm{dist}\left(p_i, p_j\right) \quad (16)$$

3.3.2 基于PufferFish-Privacy的轨迹隐私保护

由于轨迹内部相邻时刻位置点存在高度关联性，采用经典ε-DP容易导致噪声添加不足或过度。PufferFish隐私框架[17]作为经典差分隐私的扩展，其表达能力更为宽泛，是一种非常实用的模型。

定义6给出了ε-Pufferfish隐私框架描述。在轨迹数据发布场景中，集合S作为需要保护的秘密数据，通常用于描述每个时刻用户的真实地理位置。Θ作为信念分布(belief distribution)集合，表示数据之间客观存在的关联，以及攻击者所能提前掌握的先验知识。其形式与应用密切相关。假如考虑单个用户相邻时刻位置之间的关联性，将轨迹理解为1阶马尔科夫链，那么θ分布表示位置转移概率；假如多个用户位置之间存在关联，那么分布θ表示位置与社交关系的联合分布概率。

应用中面临的实际问题是采用何种机制对数据添加噪声，能满足ε-PufferFish隐私要求。文献[41]中给出了一种基于wasserstein距离的通用噪声添加机制，称为Wasserstein机制。

令$u_{i,\theta}$与$u_{j,\theta}$分别表示当变量真实值为s_i或s_j、且关系分布为θ时，输出变量x的概率分布函数，$W_\infty(u_{i,\theta}, u_{j,\theta})$表示两者的wasserstein距离。若$W$为所有wasserstein距离的上确界，则在输出值上添加Lap(W/ε)噪音。则

$$\begin{aligned} u_{i,\theta} &= P\left(F\left(X\right)=\cdot|s_i,\theta\right) \\ u_{j,\theta} &= P\left(F\left(X\right)=\cdot|s_j,\theta\right) \end{aligned} \quad (17)$$

$$W = \sup\nolimits_{(s_i,s_j)\in Q,\theta\in\Theta}\left(W_\infty\left(u_{i,\theta}, u_{j,\theta}\right)\right) \quad (18)$$

Wasserstein机制是一种通用机制，但实现效率较低，在某些具体问题上可以采用更高效的噪声添加方法。例如，当分布可表示为贝叶斯网络时，采用基于MQM (Markov Quilt Mechanism) 机制可以更高效地添加噪声满足ε-Pufferfish隐私。而当轨迹数据具有较强的时序特征，且时序数据之间的关联可以表示为联合拉普拉斯分布时，可以采用FGS-PufferFish机制[42]向频域中的傅里叶系数添加噪声，确保发布的用户移动轨迹序列满足ε-PufferFish隐私。

3.4 对比分析

基于差分隐私模型的轨迹数据发布是近年来受到广泛关注的研究内容，其研究进展受到差分隐私、轨迹隐私保护等相关领域进展的影响。表2对基于差分隐私保护的轨迹数据发布方法进行了对比与总结[1)]。

从安全性角度出发，前述各方案采用Laplace机制、EM机制或两者兼而有之进行噪声注入，分别满足ε-DP模型、(ε, δ)-DP模型与ε-PufferFish模型等不同程度隐私要求。其中，ε-DP模型的隐私保护要求最为严格，而后两类模型要求较为松弛。需要指出的是，即使是隐私保护程度相同的方案，其注入噪声规模也不尽相同，导致方案可用性存在较大差异。前述方案实验中对特定数据进行了测试

1) 在表2中的时间复杂度分析中，n表示轨迹或位置数据集合的样本数目，m表示轨迹平均长度。

表 2　基于差分隐私保护的轨迹信息发布方法比较

类型	数据发布方法	隐私保护模型	隐私保护机制	发布数据类型	时间复杂度分析
空间直方图	四叉索引树，KD-索引树，K叉平均树，PrivTree	$(\varepsilon,\delta)-$DP	Laplace机制	位置直方图	噪音的全局敏感度和树高相关，构建四叉树结构的复杂度为$O(n\cdot\lg n)$
	EH-DP, privSH	ε-DP ε-DP	Laplace机制和指数机制	轨迹直方图	构建EH数据结构的复杂度为$O\ (mn)$
	位置熵(LE)	$(\varepsilon,\delta)-$DP	Laplace机制	位置熵直方图	用到了平滑敏感度替代全局敏感度，添加噪音较少，计算所有地理位置的熵需要遍历用户的地理位置，复杂度为$O(mn)$
轨迹集合发布	前缀树，n-gram, DPT, PST	ε-DP	Laplace机制	移动轨迹数据集	构建前缀树的复杂度为$O(mn\cdot\lg m)$
	K-means聚类，OPT K-means聚类	ε-DP	Laplace机制和指数机制	移动轨迹数据集	若聚类为k，迭代次数平均为t，由于采用差分隐私指数机制，复杂度为$O\ (mktn^k)$
连续轨迹发布	δ-位置集合，(δ,r)-位置集合	ε-DP	Laplace机制	单个轨迹点	假设攻击者知道用户的移动模式，使噪音添加的更合理。时间复杂为$O(m\lvert\Delta X\rvert)$ (其中$\lvert\Delta X\rvert$为构建位置集合大小)
	Wasserstein机制，MQM机制，FGS-PufferFish机制	ε-PufferFish隐私	Laplace机制	单条轨迹	时间复杂度为$O\ (nkm^2\cdot\lg m)$ (其中k为PufferFish定义的空间关联的最大区域)

与验证，分别采用了KL散度(KL-divergence)[29]、平均相对误差(average relative error)[22,23,25,31,41,42]、豪斯多夫距离(Hausdorff distance)[34,35]、准确率(accuracy)和F1-score[26,27,32,38,39]等指标评估隐私保护结果的可用性，读者仍可以根据添加噪声规模大致判定其通用误差范围。以满足ε-DP的Laplace方案为例，当其由隐私因子分别为ε_1与ε_2的两个算法组合而成时，每个方案的准确度上界为$O((\Delta f/\varepsilon_1)\ln\ (1/\beta))$与$O((\Delta f/\varepsilon_2)\ln\ (1/\beta))$[43]；即以$1-\beta$的概率可以确信结果的误差范围。对于表2中的相同类型发布方法，读者也可以自行使用类似方法大致估计方案结果的可用程度。总体来说，由于直方图查询的全局敏感度较低，净化处理后的统计数据误差相对较小，因而实用性更容易满足应用需求。但是只能支持计数等受限查询。此外，与经典的支持差分隐私的直方图发布方法相比，高维空间数据发布必须有效解决大范围查询所面临的噪声累积难题。与之相比，直接发布净化后的位置轨迹数据集可满足用户的任意查询，但也面临更大的技术挑战。一般将轨迹抽象为一个序列，通过一系列顺序处理步骤来实现整条轨迹的隐私保护。由于顺序处理步骤意味着隐私预算的拆分，所以可以处理的轨迹长度受到一定限制。若在实际应用中需要处理无限长连续轨迹发布，需要采用更为宽松的隐私保护模型，如(ε,δ)–DP, ε-PufferFish隐私等，将任意两个相邻数据集的要求放松为仅限定在用户可达位置的部分数据集上满足要求，以大幅降低所添加的噪声，提高数据在实际应用的可用性。

4　未来研究挑战

虽然目前差分隐私在地理位置、轨迹等空间数据发布上已获取了很大进展，但随着应用场景的不断变化，以及AI领域新技术的不断涌现，未来仍然有许多关键性研究问题有待进一步解决。下面列举几个可深入研究的方向供研究人员参考：

(1) 连续发布轨迹数据差分隐私保护

在差分隐私框架下实现轨迹连续发布往往导致隐私预算快速耗尽。随着发布次数的增长，累积噪声迅速增大，发布结果的可用性急剧下降。现有的替代性的方法包括采用动态的局部敏感度、平滑敏感度取代全局敏感度[29]，采用流数据滑动窗口进行截断分析处理[44]等。此外，连续轨迹数据之间的关联性也往往需要添加额外噪声，进一步降低数据可用性。近年来在差分隐私领域，以PufferFish隐私为代表的通用模型受到越来越多的关注，取代经典差分隐私模型用于关联数据、局部敏感数据的差分隐私保护。但是满足PufferFish隐私的轨迹数据发布方法，以及高效的噪声生成机制仍十分有限，有待深入研究。

(2) 深度学习与轨迹差分隐私保护框架

基于神经网络的机器学习技术在图像、自然语言处理等领域的成功极大地推动了该学科技术的发展，对隐私保护技术领域也产生了重要影响。Abadi等人[45]在Tenserflow框架下实现了支持差分隐私的随机梯度下降(SGD)算法，显示个体数据差分隐私保护并不会过多影响学习效率与效果。此外，研究者提出了一系列基于循环神经网络(Recurrent

Neural Network, RNN)的轨迹重识别方法，基于轨迹-用户交叉熵损失函数[46]、双目标神经网络[47]、注意力机制[48]、seq2seq模型[49]等训练RNN编码器，得到了具有良好抗噪能力的轨迹表示。记录层级差分隐私保护并不足以实现轨迹身份匿名。深入理解深度学习与差分隐私技术的相互作用，构建新型差分隐私保护框架，是未来值得探究的重要方向之一。

(3) 支持自主定义隐私预算的轨迹数据发布

在差分隐私轨迹数据发布中，隐私预算ε的设置与选取既与数据质量密切相关，也与用户对个人隐私信息的重视程度息息相关。如何平衡服务质量与公开隐私数据之间的博弈关系，属于用户个性化选择范畴。目前已有若干个性化差分隐私保护方法，实现了中心模型下的交互式均值等统计信息发布[50,51]，以及本地模型下的离散分布估计[52]与热门地理位置挖掘[53]等。但是如何在个人轨迹采集与发布中实现对多隐私因子支持，在允许用户自主控制其位置数据采样频率与质量的同时保证服务质量，则有待未来结合应用进一步分析与研究。

5 结束语

差分隐私保护技术采用了攻击者能力最大化假定、安全性强，不受新型攻击出现的影响，近年来被越来越多地应用于位置、轨迹数据安全发布，取得了丰富的成果。从实际应用角度看，差分隐私轨迹发布算法的设计重点在于，如何在保护隐私的同时兼顾可用性，合理设计隐私预算因子，降低实现机制算法复杂度，生成高质量的净化数据集。本文对基于差分隐私理论的轨迹隐私保护技术进行了总结，讨论了轨迹数据持续发布、本地化隐私保护、深度学习等因素带来的问题与挑战，希望能对本领域的研究者有所帮助。

参 考 文 献

[1] BAO Jie, HE Tianfu, RUAN Sijie, *et al*. Planning bike lanes based on sharing-bikes' trajectories[C]. The 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, Canada, 2017: 1377–1386.

[2] YUAN Jing, ZHENG Yu, ZHANG Chengyang, *et al*. T-drive: Driving directions based on taxi trajectories[C]. The 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, San Jose, USA, 2010: 99–108.

[3] TOCKAR A. Riding with the stars: Passenger privacy in the NYC Taxicab dataset[EB/OL]. https://research.neustar.biz/author/atockar/, 2018.

[4] W-Pwn. 健身APP泄露军事机密, 包括中国南海[EB/OL]. https://zhuanlan.zhihu.com/p/33405626, 2018.

[5] CHEN Zhenyu, FU Yanyan, ZHANG Min, *et al*. The de-anonymization method based on user spatio-temporal mobility trace[C]. The 19th International Conference on Information and Communications Security, Beijing, China, 2017: 459–471.

[6] ABUL O, BONCHI F, and NANNI M. Never walk alone: Uncertainty for anonymity in moving objects databases[C]. The 24th IEEE International Conference on Data Engineering, Cancun, Mexico, 2008: 376–385.

[7] TERROVITIS M, POULIS G, MAMOULIS N, *et al*. Local suppression and splitting techniques for privacy preserving publication of trajectories[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2017, 29(7): 1466–1479. doi: 10.1109/TKDE.2017.2675420.

[8] YAO Lin, WANG Xinyu, WANG Xin, *et al*. Publishing sensitive trajectory data under enhanced l-diversity model[C]. The 20th IEEE International Conference on Mobile Data Management, Hong Kong, China, 2019: 160–169.

[9] 冯登国. 大数据安全与隐私保护[M]. 北京: 清华大学出版社, 2018: 194–219.

[10] DWORK C. Differential privacy[C]. The 33rd International Colloquium on Automata, Languages and Programming, Venice, Italy, 2006: 1–12. doi: 10.1007/11787006_1.

[11] ZHU Tianqing, LI Gang, ZHOU Wanlei, *et al*. Differentially private data publishing and analysis: A survey[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2017, 29(8): 1619–1638. doi: 10.1109/TKDE.2017.2697856.

[12] MCSHERRY F and TALWAR K. Mechanism design via differential privacy[C]. The 48th Annual IEEE Symposium on Foundations of Computer Science, Providence, USA, 2007: 94–103.

[13] MCSHERRY F D. Privacy integrated queries: An extensible platform for privacy-preserving data analysis[C]. The 2009 ACM SIGMOD International Conference on Management of Data, Rhode Island, USA, 2009: 19–30.

[14] DWORK C, KENTHAPADI K, MCSHERRY F, *et al*. Our data, ourselves: Privacy via distributed noise generation[C]. The 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Peterbury, Russia, 2006: 486–503.

[15] KIFER D and MACHANAVAJJHALA A. No free lunch in data privacy[C]. The 2011 ACM SIGMOD International Conference on Management of Data, Athens, Greece, 2011: 193–204.

[16] GEHRKE J, LUI E, and PASS R. Towards privacy for social networks: A zero-knowledge based definition of privacy[C]. The 8th Conference on Theory of Cryptography, Providence, USA, 2011: 432–449.

[17] KIFER D and MACHANAVAJJHALA A. Pufferfish: A

framework for mathematical privacy definitions[J]. *ACM Transactions on Database Systems*, 2014, 39(1): Article No.3. doi: 10.1145/2514689.

[18] DWORK C. A firm foundation for private data analysis[J]. *Communications of the ACM*, 2011, 54(1): 86–95. doi: 10.1145/1866739.1866758.

[19] DWORK C, MCSHERRY F, NISSIM K, *et al*. Calibrating noise to sensitivity in private data analysis[C]. The 3rd Theory of Cryptography Conference, New York, USA, 2006: 265–284.

[20] QARDAJI W, YANG Weining, and LI Ninghui. Differentially private grids for geospatial data[C]. The 29th IEEE International Conference on Data Engineering, Brisbane, Australia, 2013: 757–768.

[21] CORMODE G, PROCOPIUC C, SRIVASTAVA D, *et al*. Differentially private spatial decompositions[C]. The 28th IEEE International Conference on Data Engineering, Washington, USA, 2012: 20–31.

[22] ZHANG Jun, XIAO Xiaokui, and XIE Xing. PrivTree: A differentially private algorithm for hierarchical decompositions[C]. The 2016 International Conference on Management of Data, San Francisco, USA, 2016: 155–170.

[23] HAY M, RASTOGI V, MIKLAU G, *et al*. Boosting the accuracy of differentially private histograms through consistency[J]. *Proceedings of the VLDB Endowment*, 2010, 3(1/2): 1021–1032.

[24] XIAO Yonghui, XIONG Li, and YUAN Chun. Differentially private data release through multidimensional partitioning[C]. The 7th Workshop on Secure Data Management, Singapore, 2010: 150–168.

[25] XIE Hairuo, TANIN E, and KULIK L. Distributed histograms for processing aggregate data from moving objects[C]. 2007 International Conference on Mobile Data Management, Mannheim, Germany, 2007: 152–157.

[26] XIE Hairuo, TANIN E, KULIK L, *et al*. Euler histogram tree: A spatial data structure for aggregate range queries on vehicle trajectories[C]. The 7th ACM SIGSPATIAL International Workshop on Computational Transportation Science, Dallas/Fort Worth, USA, 2014: 18–24.

[27] GHANE S, KULIK L, and RAMAMOHANARAO K. Publishing spatial histograms under differential privacy[C]. The 30th International Conference on Scientific and Statistical Database Management, Bozen-Bolzano, Italy, 2018: Article No.14.

[28] HARDT M, LIGETT K, and MCSHERRY F. A simple and practical algorithm for differentially private data release[C]. Advances in Neural Information Processing Systems, Lake Tahoe, USA, 2012: 2339–2347.

[29] TO H, NGUYEN K, and SHAHABI C. Differentially private publication of location entropy[C]. The 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, Burlingame, USA, 2016: Article No. 35.

[30] CHEN Rui, FUNG B C M, DESAI B C, *et al*. Differentially private transit data publication: A case study on the montreal transportation system[C]. The 18th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Beijing, China, 2012: 213–221.

[31] CHEN Rui, ACS G, and CASTELLUCCIA C. Differentially private sequential data publication via variable-length n-grams[C]. The 2012 ACM Conference on Computer and Communications Security, Raleigh, USA, 2012: 638–649.

[32] HE Xi, CORMODE G, MACHANAVAJJHALA A, *et al*. DPT: Differentially private trajectory synthesis using hierarchical reference systems[J]. *The VLDB Endowment*, 2015, 8(11): 1154–1165. doi: 10.14778/2809974.2809978.

[33] HE Xi, RAVAL N, and MACHANAVAJJHALA A. A demonstration of VisDPT: Visual exploration of differentially private trajectories[J]. *The VLDB Endowment*, 2016, 9(13): 1489–1492. doi: 10.14778/3007263.3007291.

[34] HUA Jingyu, GAO Yue, and ZHONG Sheng. Differentially private publication of general time-serial trajectory data[C]. 2015 IEEE Conference on Computer Communications, Hong Kong, China, 2015: 549–557. doi: 10.1109/INFOCOM.2015.7218422.

[35] LI Meng, ZHU Liehuang, ZHANG ZIjian, *et al*. Achieving differential privacy of trajectory data publishing in participatory sensing[J]. *Information Sciences*, 2017, 400/401: 1–13. doi: 10.1016/j.ins.2017.03.015.

[36] ERLINGSSON Ú, PIHUR V, and KOROLOVA A. Rappor: Randomized aggregatable privacy-preserving ordinal response[C]. The 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, USA, 2014: 1054–1067.

[37] BASSILY R and SMITH A. Local, private, efficient protocols for succinct histograms[C]. The 47th Annual ACM Symposium on Theory of Computing, Portland, USA, 2015: 127–135.

[38] XIAO Yonghui and XIONG Li. Protecting locations with differential privacy under temporal correlations[C]. The 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, USA, 2015: 1298–1309.

[39] WANG Shuo, SINNOTT R, and NEPAL S. Protecting the location privacy of mobile social media users[C]. IEEE International Conference on Big Data, Washington, USA, 2016: 1143–1150.

[40] HARDT M and TALWAR K. On the geometry of differential privacy[C]. The 42nd ACM Symposium on

Theory of Computing, Cambridge, UK, 2010: 705–714.

[41] SONG Shuang, WANG Yizhen, and CHAUDHURI K. Pufferfish privacy mechanisms for correlated data[C]. The 2017 ACM International Conference on Management of Data, Chicago, USA, 2017: 1291–1306.

[42] OU Lu, QIN Zheng, LIAO Shaolin, *et al*. An optimal pufferfish privacy mechanism for temporally correlated trajectories[J]. *IEEE Access*, 2018, 6: 37150–37165. doi: 10.1109/ACCESS.2018.2847720.

[43] DWORK C and ROTH A. The algorithmic foundations of differential privacy[J]. *Foundations and Trends® in Theoretical Computer Science*, 2014, 9(3/4): 211–407. doi: 10.1561/0400000042.

[44] KELLARIS G, PAPADOPOULOS S, XIAO Xiaokui, *et al*. Differentially private event sequences over infinite streams[J]. *Proceedings of the VLDB Endowment*, 2014, 7(12): 1155–1166. doi: 10.14778/2732977.2732989.

[45] ABADI M, CHU A, GOODFELLOW I, *et al*. Deep learning with differential privacy[C]. The 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016: 308–318.

[46] GAO Qiang, ZHOU Fan, ZHANG Kunpeng, *et al*. Identifying human mobility via trajectory embeddings[C]. The 26th International Joint Conference on Artificial Intelligence, Macao, China, 2017: 1689–1695.

[47] WANG Guowei, LIAO Dongliang, and LI Jing. Complete user mobility via user and trajectory embeddings[J]. *IEEE Access*, 2018, 6: 72125–72136. doi: 10.1109/ACCESS.2018.2881457.

[48] ZHOU Fan, GAO Qiang, TRAJCEVSKI G, *et al*. Trajectory-user linking via variational autoencoder[C]. The 27th International Joint Conference on Artificial Intelligence, Stockholm, Sweden, 2018: 3212–3218.

[49] LI Xiucheng, ZHAO Kaiqi, CONG Gao, *et al*. Deep representation learning for trajectory similarity computation[C]. The 34th IEEE International Conference on Data Engineering, Paris, France, 2018: 617–628.

[50] JORGENSEN Z, YU Ting, and CORMODE G. Conservative or liberal? Personalized differential privacy[C]. The 31st IEEE International Conference on Data Engineering, Seoul, South Korea, 2015: 1023–1034.

[51] LI Haoran, XIONG Li, JI Zhanglong, *et al*. Partitioning-based mechanisms under personalized differential privacy[C]. The 21st Pacific-Asia Conference on Knowledge Discovery and Data Mining, Jeju, South Korea, 2017: 615–627.

[52] YE Yutong, ZHANG Min, FENG Dengguo, *et al*. Multiple privacy regimes mechanism for local differential privacy[C]. The 24th International Conference on Database Systems for Advanced Applications, Chiang Mai, Thailand, 2019: 247–263.

[53] CHEN Rui, LI Haoran, QIN A K, *et al*. Private spatial data aggregation in the local setting[C]. The 32nd IEEE International Conference on Data Engineering, Helsinki, Finland, 2016: 289–300.

冯登国：男，1965年生，中国科学院院士，研究员，研究方向为网络与信息安全.

张 敏：女，1975年生，研究员，研究方向为数据安全与隐私保护.

叶宇桐：男，1993年生，博士生，研究方向为差分隐私保护技术.