Computer Science and Application 计算机科学与应用, 2020, 10(4), 610-618
Published Online April 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.104063

Hans汉斯

Trajectory Anonymous Algorithm Based on *k*-Means++ against Similarity Attack

Xinglan Zhang, Wenjin Yang

Beijing University of Technology, Beijing
Email: 1183235940@qq.com

Received: Mar. 10th, 2020; accepted: Mar. 25th, 2020; published: Apr. 1st, 2020

Abstract

Aiming at the problems of how to choose the center of cluster and trajectory privacy leakage caused by the high similarity between the anonymous centralized trajectories, we propose a trajectory anonymous algorithm to resist trajectory similarity attacks. In the preprocessing process, the algorithm adopts trajectory synchronization to reduce information loss. In clustering process, we use *k*-means++ algorithm to construct the anonymous collection; to prevent the privacy leakage caused by the high slope similarity of trajectories in the set, at least *l* trajectories with different slopes are required to satisfy trajectory *k*-anonymity, and the difference value of trajectory slope in each class is required to be at least σ. Experimental results show that the proposal can effectively resist trajectory similarity attacks, reduce information loss comparing to other trajectory anonymous algorithms, enhance the data of availability, and achieve better trajectory privacy protection.

Keywords

Trajectory Privacy Preservation, l-Diversity, Trajectory (k,l,δ)-Anonymous Algorithm, *k*-Means++

基于*k*-means++的抗相似性攻击轨迹匿名算法

张兴兰，杨文金

北京工业大学，北京
Email: 1183235940@qq.com

收稿日期：2020年3月10日；录用日期：2020年3月25日；发布日期：2020年4月1日

文章引用：张兴兰，杨文金．基于 *k*-means++的抗相似性攻击轨迹匿名算法[J]. 计算机科学与应用，2020，10(4): 610-618. DOI: 10.12677/csa.2020.104063

摘　要

针对聚类中心的选择问题以及轨迹匿名集中轨迹间的相似性过高而泄露轨迹隐私的问题，提出基于*k*-means++的抗轨迹相似性攻击的轨迹(k,l,δ)-匿名算法。轨迹预处理的过程中，通过构造同步轨迹来减少信息损失；构建匿名集和时，本文采用*k*-means++算法来构建匿名集合，并且用(l,δ)-约束来限制轨迹匿名集合间的相似性构建包含k条轨迹的匿名集合。实验结果表明，该算法能够较好地构建匿名集合，能够有效抵制轨迹相似性攻击，相比其它算法减少了轨迹信息的损失，同时增强了轨迹数据可利用性，更好地实现了轨迹隐私保护。

关键词

轨迹隐私保护，*l*-多样性，轨迹(k,l,δ)-匿名算法，*k*-means++

1. 引言

随着全球定位系统的发展，基于位置服务[1] (LBS, location based services)的应用越来越广泛，人们通过这些应用可以发现最近的酒店、超市和医院等，它们正在改变着信息时代人们的生活[2] [3]。LBS 服务过程中会产生大量包含用户的会见、位置信息的数据。人们可以通过对这些数据进行分析、挖掘，得到大量可用信息以帮助决策者实施相关政策，例如通过分析某个区域内用户的轨迹信息，可以发现用户曾经或者未来感兴趣的位置，在这些位置建立相应的商场，广场等，帮助投资者实现盈利的最大化。然而，分析这些轨迹数据，也可以推断出用户的一些日常轨迹、身体情况等隐私信息，如果这些个人隐私信息被泄露，会对用户造成极大的威胁[4] [5] [6] [7] [8]。因此对用户轨迹隐私信息保护技术的研究，已经成为信息安全领域研究的重要内容之一。

在轨迹数据隐私保护过程中，轨迹的相似性是轨迹聚类和匿名化的重要因素。然而，如果匿名集合内的 k 条轨迹的太过相近，即它们在很长一段时间内经过同一个敏感区域，或者完全重合，那么也会泄露轨迹隐私信息的情况。文献[7]提出构建的轨迹 k-匿名集和要具有一定的差异性，以此来降低轨迹隐私信息泄露的风险，它通过采用最小边界矩形 MBR (Minimum Bounding Rectangle)大于一个给定阈值的方式来保证轨迹间的差异性。文献[8]首次用轨迹间夹角和距离构造轨迹图的边权的方法，文献[9]又在其基础之上设计了一种基于图划分的个性化隐私保护方法，利用轨迹距离和轨迹夹角度量来构造轨迹间边权，将构建轨迹 k-匿名集和转化为轨迹 k-子图的划分问题。Abul 等人[10]提出 NWA (never walk alone)方法，该方法提出了一个基于共定位的(k,δ)-匿名模型，首相将轨迹集合划分为互不相交的子集，其次利用聚类算法形成轨迹 k-匿名集合；Cai 等人[11]提出了一种以用户为中心的轨迹隐私保护方法以防止轨迹攻击。他们引入位置语义多样性以最大化轨迹隐私，攻击和防御问题被转化为贝叶斯 Stackelberg 方式以进行定量分析。对轨迹发布数据的隐私保护研究领域，已有大量学者进行了研究[12] [13] [14]。

这些隐私保护方法一定程度保护了轨迹隐私，但是均未考虑轨迹因相似而泄露轨迹信息的情况，另外，在轨迹聚类中心的选取上较为不合理，因此本文提出了基于 k-means++的轨迹(k,l,δ)-匿名算法。本

文有两个贡献，第一优化了轨迹聚类中心的选择，第二将轨迹斜率作为敏感属性，用(l,δ)约束轨迹相似度以解决轨迹相似性攻击问题。

2. 相关概念

定义 1 轨迹，移动对象 O 的轨迹 T 为三维时空坐标拟合的曲线，表示为 $T=\{Id,(x_1,y_1,t_1,v_1),(x_2,y_2,t_2,v_2),\cdots,(x_m,y_m,t_m,v_m)\}$，其中 Id 为移动对象的身份标识；(x_i,y_i) 为 O 在 i 时刻的位置坐标并且 $t_1<t_2<\cdots<t_m$；v_i 是在 t_i 时刻的速度。

定义 2 [14] 同步轨迹。两条不同的轨迹 T_p 和 T_q，如果轨迹 T_p 和 T_q 具有相同的时间序列，那么我们称 T_p 和 T_q 是同步轨迹；如果轨迹集合中的任意两条轨迹两两同步，则称轨迹集合是同步的。

然而，在我们实际环境中移动对象的轨迹往往不是同步的。主要有两个原因：一是由于移动终端或GPS对每个移动对象位置的采样时间不同；二是由于不同移动对象向位置服务器(LBS)发送请求服务的时间各不相同。另外，本文在做轨迹处理时，我们假设轨迹在2个样本时间点内匀速直线运动，对于轨迹 T_p 和 T_q 间不同时间坐标，通过在轨迹中插入相应时刻的位置坐标来实现轨迹 T_p 和 T_q 的同步。

定义 3 轨迹等价类。若轨迹 $T_1,T_2\cdots,T_{n-1},T_n,(n>0)$ 满足 1) $\forall T_i\in\{T_1,T_2,\cdots,T_n\}$ 的起始时间 $t_s^i\in[t_s-\Delta t,t_s+\Delta t]$，并且终止时间 $t_e^i\in[t_e-\Delta t,t_e+\Delta t]$；2) 任意轨迹 T_i,T_j 是同步的，那么轨迹 $T_1,T_2\cdots,T_{n-1},T_n,(n>0)$ 是一个轨迹等价类。

定义 4 Fréchet 距离[15]。设二元组 (S,d) 是一个度量空间，其中 d 是 S 上的度量函数。在单位区间[0,1]上的映射 $\gamma:[0,1]\to S$ 是连续映射，则称 γ 为 S 上的连续曲线。从单位区间到其自身的映射 $\zeta:[0,1]\to[0,1]$，满足如下三个条件：1) ζ 是连续的；2) ζ 是非降的，即对于任意 $x,y\in[0,1]$，且 $x\le y$，都有 $\zeta(x)\le\zeta(y)$ 成立；3) ζ 是满射，则称函数 ζ 为单位区间[0,1]的重参数化函数，且此时有 $\zeta(0)=0,\zeta(1)=1$。特别地，当 ζ 为恒等函数 $\zeta(x)=x$ 时，称 ζ 为平凡重参数化函数，否则，称 ζ 为非平凡重参数化函数。显然单位区间的重参数化函数有无穷多个。

设 A 和 B 是 S 上的两条连续曲线，即 $A:[0,1]\to S,B:[0,1]\to S$。又设 α 和 β 是单位区间的两个重参数化函数，即 $\alpha:[0,1]\to S,\beta:[0,1]\to S$。则曲线 A 和 B 的 Fréchet 距离 $F(A,B)$ 定义为

$$F(A,B)=\inf_{\alpha,\beta}\max_{t\in[0,1]}\left\{d\left(A(\alpha(t)),B(\beta(t))\right)\right\} \tag{1}$$

其中 d 是 S 上的度量函数。

定义 5 离散 Fréchet 距离[15]。设 $P:[0,n]\to V$ 是一个折线段曲线，我们用 $\sigma(P)$ 表示每个折线段的终点，即 $\sigma(P)=\{u_1,u_2,\cdots,u_p\}$，那么曲线 P 和 Q 的一个组合序列 $L=\left\{\left(u_{a_1},v_{b_1}\right),\left(u_{a_1},v_{b_1}\right),\cdots,\left(u_{a_m},v_{b_m}\right)\right\}$，且每个序列对都不相同，并且 $a_1=1,b_1=1,a_m=b_m$，对任意 i，有 $a_{i+1}=a_i+1$ 和 $b_{i+1}=b_i$ 或 $b_{i+1}=b_i$，因此组合序列对必须遵循曲线 P 和 Q 所有点的顺序，定义 L 的长度为所有序列对的最大距离，即 $\|L\|=\max_{i=1,2,\cdots,m}d\left(u_{a_i},v_{b_i}\right)$。那么折线段 P 和 Q 的离散 Fréchet 距离为：

$$\delta_{dF}(P,Q)=\min\{\|L\|\} \tag{2}$$

定义 6 轨迹之间的曼哈顿距离。任意两条轨迹 tr_a 和 tr_b 之间的曼哈顿为轨迹上所有位置点曼哈顿距离之和的平均值，定义为：

$$d(tr_a,tr_b)=\frac{1}{n}\left(\sum_{i=1}^{n}|x_{ai}-x_{bi}|+|y_{ai}-y_{bi}|\right) \tag{3}$$

定义 7 (l,δ)-约束。轨迹匿名集合 $Tr=\{tr_1,tr_2,\cdots,tr_k\}$ 满足 (l,δ)-约束，当且仅当轨迹匿名集合 Tr 中至少有 l 个不同斜率的轨迹，并且轨迹间斜率差异值至少为 δ。

定义 8 (k,l,δ)-匿名模型。匿名集合 Tr 中至少有 k 个轨迹，并且这些轨迹满足 (l,δ)-约束。

定义 9 轨迹相似性攻击。一个匿名集合中如果存在多条高度相似的轨迹，尤其是运行轨迹相近或者平行亦或者重复，那么攻击者可以对这些发布的轨迹数据进行推理就能获得这些轨迹的大致运动轨迹及其敏感信息，若发布的轨迹均经过同一敏感区域，攻击者可以推断出该集合内的所有轨迹均有很大概率经过该敏感区域，用户隐私也随之暴露，这种攻击模式我们称之为轨迹相似性攻击。

定义 10 轨迹斜率。轨迹数据的起始点、中间点和终止点所在线段的平均斜率。若采样轨迹片段 Tr 在起始时刻时位置为 (x_b,y_b)，中间时刻位置为 (x_t,y_t)，结束时刻位置为 (x_e,y_e)，则该轨迹斜率 K_n 为：

$$K_n=\begin{cases}\dfrac{1}{2}\left(\dfrac{y_t-y_b}{x_t-x_b}+\dfrac{y_e-y_t}{x_e-x_t}\right) & x_t\neq x_b, x_e\neq x_t\\ \dfrac{y_e-y_b}{x_e-x_b} & x_e\neq x_b, y_e=y_t\\ 0 & x_t=x_b\text{或}x_t=x_e\text{或}x_e=x_b\end{cases} \tag{4}$$

3. 基于 *k*-means++抗相似性攻击的轨迹匿名算法

3.1. 轨迹预处理

轨迹预处理过程有以下两个步骤，首先，我们选取具有相同开始时间和结束时间的轨迹构造轨迹等价类；针对实际环境中的移动对象同时开始并且同时结束的数量非常少，文献[9]采用轨迹集合中的最大开始时间和最小结束时间作为构造轨迹等价类的约束条件。这种方式存在的问题是如果轨迹的开始时间或者结束时间相差很大，构建轨迹集合时就会损失很多轨迹信息，同时在形成匿名集合时也会造成很大的信息损失。鉴于此，本文选取一个给定时间间隔内的轨迹以保证轨迹间的高相似性；其次，将第一步已经选取的轨迹通过轨迹同步化形成轨迹等价类。

例如，设轨迹的起始时间为 7:00，终止时间为 8:00，时间间隔为 5 分钟，那么选取轨迹开始时间在[6:55, 7:05]，结束时间在[7:55, 8:05]的所有轨迹，并将这些轨迹进行同步化，最终形成一个轨迹等价类。对于间隔时间 Δt 的选择，主要依据轨迹采样时间的稀疏程度，如果采样时间稀疏，那么间隔时间 Δt 可以相对大一点；如果采样时间点密集，则间隔时间 Δt 相应选取小一点。

算法 1 预处理算法 (Pre-process)

输入：原始轨迹集合 Tr

输出：轨迹等价类 Tr'

(1) for tr in Tr:

(2) If 轨迹的开始、结束时间在给定范围内那么

(3) 将 tr 添加到 Tr' 中

(4) for each $T_i,T_j\in Tr'$

(5) for $t_m\in ot(T_i,T_j)$

(6) If $t_m\in t_i$ and $t_m\notin t_j$

(7) 将 t_m 时间点插入 T_j 中

(8) else 将 t_m 时间点插入 T_i 中

(9) 返回 Tr'

3.2. 构建轨迹匿名集合

目前大部分轨迹隐私保护算法构建匿名集合时在选择聚类中心主要通过随机选取 k 个匿名中心，随

后构建匿名集合，这样的作法会导致轨迹匿名中心的选取不合理以至构建的匿名集合信息损失大，轨迹可用性降低，本文采用 *k*-means++算法构建匿名集合，解决了上诉问题。

算法 2 基于 *k*-means++的轨迹匿名算法

输入：预处理之后的轨迹等价类 Tr

输出：轨迹匿名集合 Tr'

(1) 随机选取一个轨迹作为第一个聚类中心 Tr_1

(2) 计算每个样本与当前已有类聚中心最短距离(即与最近一个聚类中心的距离)，用 $D(x)$表示；这个值越大，越可能成为轨迹的聚类中心

(3) 重复步骤二，直到选出 k 个聚类中心；

(4) 针对轨迹等价类中每个轨迹 Tr_i，计算它到 k 个聚类中心的距离并计算距离最小的聚类中心所对应的类中斜率差值是否满足 (l,δ) 约束，如果满足加入所在类，否则计算次近的类，以此类推；

(5) 针对每个匿名集合 C_i，重新计算聚类中心 $c_i=\frac{1}{|C_i|}\sum_{Tr_i\in C_i}Tr_i$ (即该匿名集合的质心)；

(6) 重复(4)，(5)直到聚类中心不在变化。

4. 轨迹隐私水平和数据可用性

本文主要从两个方面分析算法的可行性，一是 *k*-匿名的隐私保护程度即泄密风险，第二，分析轨迹数据的信息损失率即数据的可用性。

4.1. 隐私保护水平

隐私保护水平的评估主要评估匿名集合中轨迹被重新识别的概率，即由构建的匿名集合推断出原使集合记录的可能性，一般采用用匿名集合与原轨迹集合同一记录的相关程度来衡量。

定义 11 链接成功。匿名集合内任一轨迹记录 t，计算 t 到原始集合中所有轨迹记录的距离，得到距离 t 最近的记录集 t'，次近记录集 t''，如果 t' 或 t'' 是由 t 匿名化得到的，则称 t 链接成功。

基于距离的评估思想为：用匿名集合链接成功的记录所占比例大小作为泄密风险的测量，设 link_records 为匿名集合链接成功的记录数，total_records 为总记录数，则泄密风险值 LR 为：

$$\mathrm{LR}=\frac{\text{link\_records}}{\text{total\_records}} \tag{5}$$

4.2. 信息损失率

我们在计算信息损失率时，仅仅考虑构建轨迹匿名集合时造成的信息损失，不考虑轨迹预处理的信息损失。本文通过轨迹的匿名区域与整个轨迹空间区域的面积的比值来衡量信息损失，轨迹匿名区域与数据可用性成反比，匿名区域面积越大数据可用性越小，反之数据可用性越大，表示为：

$$IL=\frac{\sum_{i=1}^{p}\dfrac{\sum_{j=1}^{t}Area\left(x_{ji},y_{ji},t_j\right)}{MaxArea_i}}{p} \tag{6}$$

其中 $Area\left(x_{ji},y_{ji},t_j\right)$ 表示 t_j 时刻的匿名区域面积，$MaxArea_i$ 表示第 i 个匿名集合的最大面积，p 表示匿名集合的个数。

5. 实验结果与分析

5.1. 实验环境和数据

我们的实验环境为 Inte(R) Core(TM) i5-4590 CPU @3.30 GHz；8 G 内存；Microsoft Windows 7.sp。64 位操作系统；本算法在 pycharm 中实现。实验中使用的实验数据集是由 Brinkhoff 生成器基于德国奥尔登堡市交通地图生成的[16]，初始数据集如表 1 所示。第一列表示移动对象的编号，第二列是移动对象位置编号即表示该点是轨迹的第几个位置，第三列表示数据返回的概率，0 表示以百分百的概率生成数据点，第四列表示轨迹所处的时间；第五、六列表示轨迹所处的位置信息，第七列表示轨迹的当前速度；最后两列表示轨迹下一时刻将要到达的位置。

Table 1. Part of the data
表 1. 部分数据

对象编号	位置编号	数据返回概率	X 轴	Y 轴	速度	X 轴	Y 轴
41	62	0	15071.05005	24095.37797	59	15057	23925
40	62	0	5446.962785	13539.45939	134	5756	14288
39	63	0	5092.652393	24035.09312	26	5058	22845
38	63	0	12279.01879	15301.07878	134	12350	15144
37	63	0	6085.989021	24575.8497	59	6051	24596
36	63	0	13369.37702	14968.13312	50.25	13320	14972

5.2. 隐私保护水平

通过图 1 可以看出基于 k-means++的轨迹(k,l,δ)-匿名算法相比 CMPT，NWL 两种匿名算法泄密风险小很多。基于 k-means++算法构建的轨迹匿名集合更为合理，轨迹间的距离相比其它算法会小一点；另外，由于(l,δ)的约束，每个等价类在聚类时要求类内至少有 l 个轨迹斜率差异值至少为δ，避免了匿名集合间轨迹的过度相似，能够有效抵制轨迹相似性攻击，防止隐私泄露。

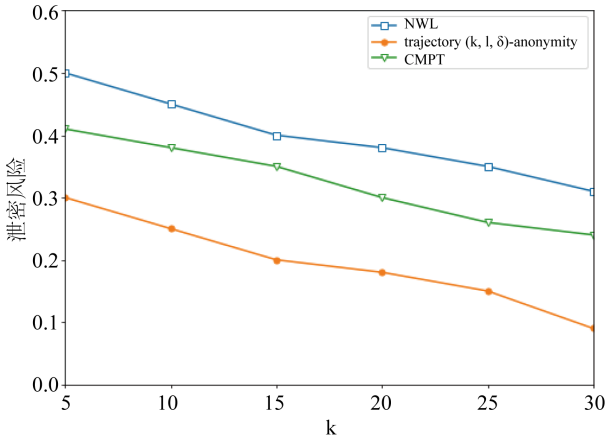

Figure 1. Different methods of disclosure risk
图 1. 不同方法的泄密风险

由图 2 可知，基于 k-means++的轨迹(k,l,δ)-匿名算法在取不同 k 值时，随着 δ 值的增加可以获得更

安全的匿名数据，大大减少了信息泄露的可能性。以上实验结果表明，本文算法具有一定的可用性。

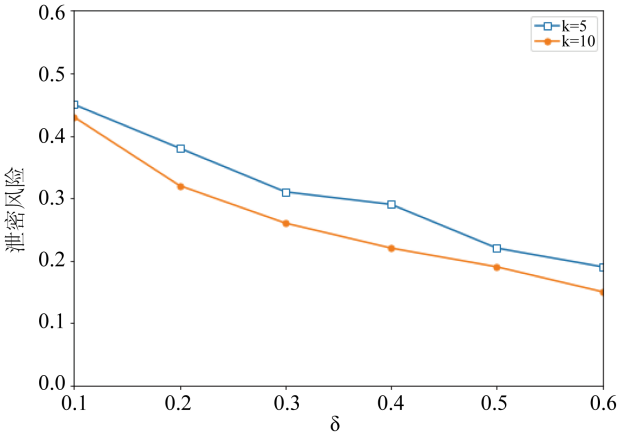

Figure 2. Different delta value changes correspond to the leak risk
图 2. 不同 δ 值变化对应的泄密风险

5.3. 轨迹信息损失

图 3 是 CMPT，NWL 匿名算法与基于 k-means++的 (k,l,δ)-匿名算法信息损失随着 k 值的变化的情况。基于 k-means++的 (k,l,δ)-匿名算法略微比其它两种算法的信息损失度低，这是由于尽管聚类时要保证轨迹间至少有 l 个斜率差异值至少为 δ，但是，本文采用 k-means++算法构建轨迹匿名集合相比于传统的聚类算法构建的匿名集合更为合理，轨迹间的距离更小，因此本文算法信息损失略低。

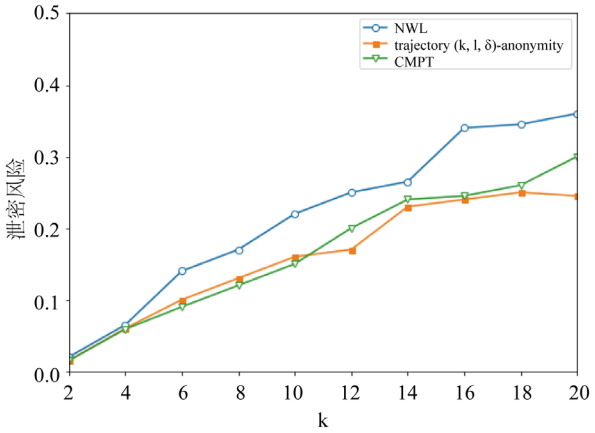

Figure 3. Information loss of different methods
图 3. 不同方法的信息损失

由图 4 可见，基于 k-means++的 (k,l,δ)-匿名算法随斜率差异值 δ 的增大，取不同 k 值时信息损失度均增大。随着 δ 增大，类内轨迹斜率取值差异增大，导致类内轨迹距离增大，从而增加了信息损失量。

5.4. 算法运行时间分析

图 5 是本文算法与其它两种匿名算法的运行时间比较。由于本文匿名算法要求在构建轨迹等价类时，满足 k-匿名的条件下同时满足至少有 l 个轨迹斜率差异值至少为 e 的轨迹，所以本文算法在 k 取值增加的情况下，运行时间会略微增加，但可忽略不计。

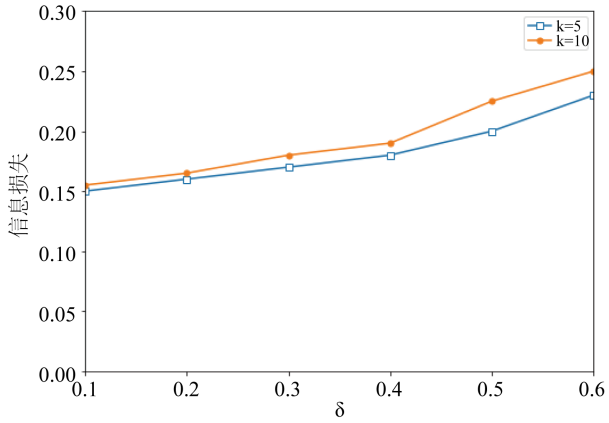

Figure 4. Information loss of different k values with delta change
图 4. 不同 k 值随 δ 变化的信息损失

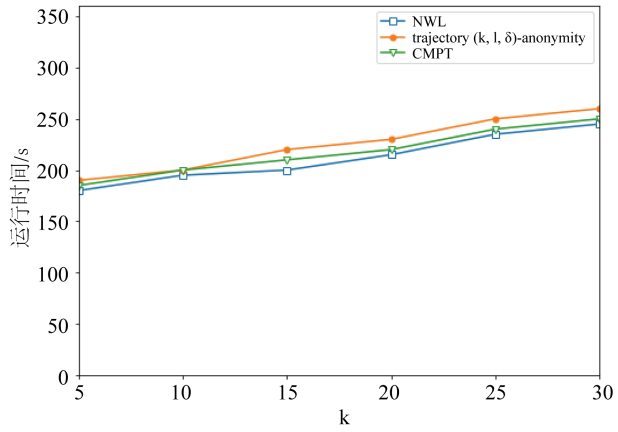

Figure 5. Running time of different methods
图 5. 不同方法的运行时间

6. 总结

本文提出的基于 k-means++的轨迹(k,l,δ)-匿名算法解决了聚类中心的选取问题以及因轨迹间的相似性过高导致泄露轨迹隐私泄的问题。相比其它轨迹 k-匿名算法，本文将轨迹斜率作为轨迹的敏感属性，优化了聚类中心的选择，以及增加了等价类内轨迹(l,δ)-约束，即要求匿名集在满足轨迹 k-匿名的同时还需满足至少有 l 个斜率差异值至少为δ，避免了因出现大量相似甚至于平行的轨迹而导致隐私的直接泄露的问题。实验结果表明本文算法得到的匿名算法在抵抗轨迹相似性攻击的能力方面更强，并且也保证了轨迹数据的可用性。

参考文献

[1] 哈吉德玛. 基于位置服务(LBS)的应用研究[J]. 现代信息科技, 2019, 3(4): 61-62.

[2] Xiao, Z., Yang, J.J., Huang, M., *et al*. (2017) QLDS: A Novel Design Scheme for Trajectory Privacy Protection with Utility Guarantee in Participatory Sensing. *IEEE Transactions on Mobile Computing*, **17**, 1397-1410. https://doi.org/10.1109/TMC.2017.2768360

[3] He, X., Jin, R. and Dai, H. (2018) Leveraging Spatial Diversity for Privacy-Aware Location Based Services in Mobile Networks. *IEEE Transactions on Information Forensics & Security*, **13**, 1524-1534. https://doi.org/10.1109/TIFS.2018.2797023

[4] Xiao, P., Chen, W., Sun, Y., *et al*. (2017) Continuous Queries Privacy Protection Algorithm Based on Spatial-Temporal Similarity Over Road Networks. *Journal of Computer Research & Development*, **54**, 2092-2101.

[5] 张学军，桂小林，伍忠东．位置服务隐私保护研究综述[J]．软件学报, 2015, 26(9): 2373-2395.

[6] 魏兴民，杜鹏懿．基于位置服务的隐私保护综述[J]．现代信息科技, 2019(8): 154-157.

[7] Machanavajjhala, A., Kifer, D., Gehrke, J., *et al*. (2006) L-Diversity: Privacy beyond Kanonymity. *ACM Transactions on Knowledge Discovery from Data*, **1**, 3. https://doi.org/10.1145/1217299.1217302

[8] Gao, S., Ma, J.F., Sun, C., *et al*. (2014) Balancing Trajectory Privacy and Data Utility Using a Personalized Anonymization Model. *Journal of Network and Computer Applications*, **38**, 125-134. https://doi.org/10.1016/j.jnca.2013.03.010

[9] 杨静，张冰，张健沛，等．基于图划分的个性化轨迹隐私保护方法[J]．通信学报, 2015(3): 1-11.

[10] Abul, O., Bonchi, F. and Nanni, M. (2008) Never Walk alone: Uncertainty for Anonymity in Moving Objects Databases. In: *Proceedings of the International Conference on Data Engineering*, 376-385. https://doi.org/10.1109/ICDE.2008.4497446

[11] Cai, H.-F., Yang, H.-X. and Wang, S. (2014) A Clustering-Based Privacy-Pre-Serving Method for Uncertain Trajectory Data. 2014 *IEEE* 13*th International Conference on Trust, Security and Privacy in Computing and Communications* (*TrustCom*), Beijing, China, 49-62. https://doi.org/10.1109/TrustCom.2014.5

[12] Dai, J. and Liang, H. (2015) A Method for the Trajectory Privacy Protection Based on the Segmented Fake Trajectory under Road Networks.

[13] 吴英杰，唐庆明，倪巍伟．基于聚类杂交的隐私保护轨迹数据发布算法[J]．计算机研究与发展，2013，50(3): 578-593.

[14] Huo, Z., Huang, Y. and Meng, X.F. (2011) History Trajectory Privacy-Preserving through Graph Partition. In: *Proceedings of the* 1*st International Workshop on Mobile Location-Based Service*, ACM Press, New York, 71-78. https://doi.org/10.1145/2025876.2025891

[15] Agarwal, P.K., Avraham, R.B., Kaplan, H., *et al*. (2014) Computing the Discrete Fréchet Distance in Subquadratic Time. *SIAM Journal on Computing*, **43**, 429-449. https://doi.org/10.1137/130920526

[16] Brinkhoff, T. (2003) Generating Traffic Data. *IEEE Data Engineering Bulletin*, **26**, 19-25.