计算机工程与应用
Computer Engineering and Applications
ISSN 1002-8331,CN 11-2127/TP

《计算机工程与应用》网络首发论文

题目： Voronoi 图划分实现位置数据发布隐私保护
作者： 薛佳楣，张磊，玄子玉
网络首发日期： 2018-09-03
引用格式： 薛佳楣，张磊，玄子玉．Voronoi 图划分实现位置数据发布隐私保护．计算机工程与应用. http://kns.cnki.net/kcms/detail/11.2127.TP.20180831.1116.008.html

Voronoi 图划分实现位置数据发布隐私保护

薛佳楣，张　磊，玄子玉

XUE Jiamei, ZHANG Lei, XUAN Ziyu

佳木斯大学 信息电子技术学院，黑龙江 佳木斯 154007
College of Information Science and Electronic Technology, Jiamusi University, Jiamusi, Heilongjiang 154007, China

XUE Jiamei, ZHANG Lei, XUAN Ziyu. The Voronoi diagram division for location data privacy protection publishing. Computer Engineering and Applications

Abstract：As the location data are important to the user, it makes the publishing of location data is easier to reveal the privacy of the user. Thus, in order to cope with this problem, we proposed a Voronoi based scheme. In this scheme, entropy is used to measure the probability between the published location and sensitive location. Then with the result of entropy, the centre of each cell about the Voronoi diagram is chosen, and each centroid has the same probability to be correlated to any sensitive position, so the adversary cannot obtain the privacy of the user through correlation probability guess. Based on the above strategy, a ε-sensitive correlation privacy metric is provided to measure the private level of prepared data, this metric scheme is based on the theory of ε-differential privacy, and is rigorous in mathematical justification. So the privacy level of our proposed scheme is verified with the principle of ε-sensitive correlation privacy and the process is proposed in security analysis. At last, the comparative experiment is proposed with several targets setting, and the results with some detailed analysis are provided to further verify the advantage of our scheme in both of privacy protection level as well as the usability of the published data.

Key words：Information technology; ε-sensitive correlation; Voronoi diagram; Location data publishing; Entropy; differential privacy

摘　要：针对位置这一特殊数据发布的隐私问题，提出了基于 Voronoi 图预划分的隐私保护策略。该策略通过信息熵计算处理待发布位置与敏感位置关联关系，并利用关联最低位置作为图心建立 Voronoi 图。进而利用 Voronoi 单元格特性将待发布的位置信息替换为图心位置，以此实现敏感信息隐藏的目的。在信息隐藏的基础上，利用广义差分隐私原理，提出了基于位置发布数据的 ε--敏感位置关联隐私模型，并证明本文所提出的方法能够满足该模型。最后，通过比较实验进一步证明了所提出的算法在隐私保护能力和发布数据可用性方面的优势，并对实验结果进行了详细的成因分析。

关键词：信息技术；ε-敏感位置关联；Voronoi 图；位置数据发布；信息熵；差分隐私
文献标志码：A　**中图分类号**：TP311　doi：10.3778/j.issn.1002-8331.1803-0265

基金项目：黑龙江省自然科学基金项目(No.F2015022)；黑龙江省普通本科高等学校青年创新人才培养计划（No.UNPYSCT-2017149, No.UNPYSCT-2017175）；佳木斯大学基础研究类项目（No.JMSUJCM2016-009）；国家级大学生创新创业训练项目（No.201810222033）。

作者简介：薛佳楣(1974－), 女, 硕士, 副教授,研究领域为：数据库、软件工程、数据隐私, E-mail: xuejiameixzy@163.com; 通讯作者：张磊(1982－), 男, 博士, 讲师, 研究领域为信息安全, 隐私保护, E-mail: 8213662@163.com; 玄子玉 (1975－), 男, 硕士, 副教授，研究领域为电工理论与新技术、信息安全硬件。

1 引言

作为一种特殊的数据形式，位置数据是一种既存在自身敏感特性，又可被用作于其它敏感信息相关联的特殊数据。一方面位置数据本身能够泄露用户的行为隐私；另一方面，由位置数据衍生出的各种数据又可用来分析用户的家庭住址、工作场所、生活习惯等用户固有的生活信息。因此，对这种数据的发布与一般的数据信息发布的隐私处理又存在着差异。对于位置数据的隐私保护，当前存在两方面的研究：一种是对实时位置数据的保护，另一种是对发布位置数据的保护。实时位置数据的保护方面主要使用 k-匿名[1]，通过可信的第三方服务器，将用户自身位置与至少 k-1 个其它位置共同提交给服务提供者，令攻击者无法在 k 个位置中准确识别真实位置。在此基础上发展出语义多样性[2]与查询多样性[3]。近年来对于这一类方法的研究主要集中在连续查询的轨迹泛化[4-6]、无中心服务器的隐私保护[7-9]以及连续位置的可关联性[10-12]等方面问题的解决上。

Fung 等人[13]对位置数据发布的隐私泄露问题展开综述，并对主要隐私保护方法进行了整理分类。在之后的研究中，将位置数据发布的隐私保护归结为抑制和泛化两方面。在抑制方法中，Chen 等人[14]在 k-匿名基础上通过对连续位置数据的抑制建立 $(K,C)_L$-隐私保护模型。Terrovitis 等人[15]基于局部抑制的特性和数据分离，进一步提高发布的位置轨迹隐私保护能力。赵婧等人[16]通过抑制对位置轨迹数据处理，降低攻击者分析用户隐私的可能。

泛化的方法与抑制有所不同，该方法基于 k-匿名，通过在待发布数据中添加噪声数据，在不影响统计分析结果的前提下提供隐私保护服务。早期，这类方法主要通过寻找相似数据实现。Bonchi 等人[17]提出利用聚类将同类位置轨迹数据聚集，完成对同类位置轨迹数据的泛化。Chow 等人[18]利用层次扩展隐匿区间，通过最大范围数据发布实现位置泛化。随着数据分析及数据挖掘新方法的提出与应用，位置数据发布的隐私研究过渡到针对用户个性化、属性以及统计分析攻击方面上。其中主要有 Lu 等人[19]针对用户的隐私需求问题提出的个性化轨迹匿名标准；Zheng 等人[20]针对属性信息识别位置问题提出的属性轮廓泛化方法；以及 Li 等人[21]考虑到攻击者可采用差分攻击获取用户隐私，而提出的位置轨迹数据差分隐私保护方法；Xu 等人[22]从敏感位置转换方面入手，将待发布数据中的敏感信息剔除或转换；Bonchi 等人[17]则通过连续位置的中间节点进行模糊化处理，利用起始位置代替整个移动过程；Sui 等人[23]更是对用户连续移动可能产生的停留位置加以关注，并通过建立时空隧道交换子轨迹以达到轨迹隐私保护的目的；Wang 等人[24]则在道路监控的情况下，利用马尔科夫预测提供了实时数据发布的隐私保护。

毫无疑问，以上隐私保护方法在很大程度上保障了发布数据中的用户隐私，但是未能有效的处理敏感位置与待发布位置之间的关联关系，攻

击者仍可通过该关系猜测位置隐私。同时，以上方法存在较为严重的数据损耗，使用者很难获得有价值的数据分析或数据挖掘结果。针对以上不足，基于 Voronoi 图的预划分，提出了一种将位置数据替换为 Voronoi 图心的隐私保护方法，利用图心代替真实位置实现发布数据的隐私保护。该方法利用信息熵计算图心与敏感位置之间的关联关系，通过选择概率彼此相等的位置实现发布位置脱敏。同时，利用单元格中位置与中心点的距离远低于其它位置这一特性，最大程度的保障了发布数据的可用性。最后，通过实验对比可以发现，本文所提出的算法具有较好的隐私保护能力和极好的数据可用性。

2 基于 Voronoi 图的位置数据替换

2.1 Voronoi 图心选择

在 Voronoi 图中，随机选择图心并利用图心代替敏感位置是不行的。因为存在以下攻击漏洞。假设随机选择图心位置，并以其为非敏感位置替代该单元格中的所有位置，那么一旦图心位置是敏感位置或邻近敏感位置，则发布的数据可能构成安全威胁。文献[25，26]分别对此问题提出了相应的图心选择方法。因此，在图心选择上提出了基于信息熵的脱敏位置选择方法。该方法首先检测图心位置是否为敏感位置，然后计算图心位置与其周围敏感位置之间的关联信息熵，仅当信息熵最大时，将其作为图心。

设存在图心 l_v，敏感位置 $L_s=(l_{s1},l_{s2},\ldots,l_{sn})$，其中 n 表示该敏感位置数量，则图心位置与敏感位置之间的关联情况可用表示为：

$$p_i=\frac{l_v\to l_i}{l_v\to L_s},0\le i\le n \tag{1}$$

将 p_i 带入公式(2)之后，可得到该位置的信息熵取值，当该值最大时，表示该位置与敏感位置之间不存在关联，攻击者无法从发布的位置推断出敏感位置。

$$H=-\sum_{i=1}^{n}p_i\log_2 p_i \tag{2}$$

根据 Jaynes 最大熵原理，当 $p_1=p_2=\ldots=p_n$ 时，可取得最大熵，即

$$H_{\max}=-\frac{1}{n}\log_2\frac{1}{n} \tag{3}$$

对于任意位置 $l_i\in L_s$，有 l_i 与图心位置 l_v 之间的关联概率彼此相等，即通过 l_v 可推测出该位置与敏感位置中任意位置的关联性相等，攻击者无法在发布的位置集合中，推测出用户敏感位置，进而保护位置隐私。在对多候选图心选择时，设存在集合 $L_v=(l_{v1},l_{v2},\ldots,l_{vm})$，其中 m 表示当前所需的图心数量，此时需要对候选图心进行信息熵计算。算法 1 给出了信息熵的计算过程。

算法 1 Voronoi 图心选择

输入：候选图心位置集合 L_v，敏感位置集合 L_s

输出：可用图心位置集合 L_{vu}

1) for(i=1; i<=m; ++i)
2) for(j=1; j<=n; ++j)
3) $p_j=\frac{l_i\to l_j}{l_i\to L_s}$;//计算图心位置与敏感位置之间的关联概率
4) $H_i=-\sum_{j=1}^{n}p_j\log_2 p_j$;//计算图心位置信息熵
5) if(H_i==max)
6) $L_{vu}=l_i$;//将位置加入到图心集合
7) else
8) break;
9) end if
10) end

11) end

通过两轮循环运算，可选定图心位置。在该算法的 3-4 行，通过建立图心与敏感位置之间的关联概率计算得到该图心的信息熵取值。在算法的 5-9 行，对该取值进行判断，从而确定当前位置是否可作为图心进行数据替换。

2.2 基于 Voronoi 图心的位置数据替换

在获得图心坐标之后，需要按照选定图心建立 Voronoi 单元格。假设存在如图 1 所示的北京某地区待发布位置数据，且在该区域中存在△所标注的敏感位置，按照设定 8 个单元格划分，将敏感位置带入算法 1 可得到如*型所示图心坐标集合，然后以图心坐标集合建立 Voronoi 图，可获得图 1 中按照实线划分后的单元格。

图 1　待发布位置信息区域图

在获得 Voronoi 图之后，可将待发布数据中的位置数据替换为该单元格的图心坐标，将可能造泄露的位置信息替换为非敏感且不可关联的坐标。本文使用文献[9]中所提出的关联概率不可区分思想，即对于指定图心位置 l_v 以及敏感位置坐标集合 $L_s=(l_{s1},l_{s2},\ldots,l_{sn})$，其关联概率满足 $K(L_s,l_v)\to P(Z)$，其中，Z 是记录值集合，概率分布的相似性用算法 M 定义。

$$M_P(\mu_1,\mu_2)=Sup_{z\in Z}\,|\,\mu_1(z)\text{-}\mu_2(z)\,| \tag{4}$$

当 $\mu_1(z)$，$\mu_2(z)$ 同时为 0 或者 ∞ 时，$|\,\mu_1(z)\text{-}\mu_2(z)\,|=0$，即 $M_P(\mu_1,\mu_2)$ 在 μ_1,μ_2 对每个值 z 有相似概率。M_P 表示 p 和 p' 之间的不可区分级别，该值越小，表示敏感位置与图心位置之间相关的可能性越低，即将图心位置与某一敏感位置相关联的可区分性越低，其不可区分性越强。当该值超过设定时，可认为攻击者能够将泛化位置与某一敏感位置相关联，猜测用户到达或经过这一敏感位置，进而分析获得其隐私。因此，经过脱敏后可得到在 $M(p,p')$ 度量下的广义差分隐私——ε-敏感位置关联隐私。

ε-敏感位置关联隐私可定义为：若机制 $P(K(L_s),l_v)\to P(Z)$ 满足 ε-敏感位置关联隐私，当且仅当对于敏感位置集合 $L_s=(l_{s1},l_{s2},\ldots,l_{sn})$ 中的任意敏感位置 l_s 和 l'_s，存在：

$$M_P(p(K(l_s),l_v),p(K(l'_s),l_v))\le\varepsilon M_P(p(l_s,l_v),p(l'_s,l_v)) \tag{5}$$

可等价为 $K(l_s,l_v)(z)\le e^{\varepsilon M_P(p(l_s,l_v),p(l'_s,l_v))}K(l'_s,l_v)(z)$，对于所有 $z\in Z$。参数 ε 可看做是对 M_P 的缩放。所有位于当前单元格中的位置数据，在位置替换后将满足 ε-敏感位置关联隐私。即所有位置与当前单元格内的敏感位置之间的关联关系不可区分。此时，对待发布数据的处理如算法 2 所示。

算法 2 待发布数据处理

输入：待发布位置集合 L，Voronoi 图心位置集合 L_{vu}

输出：泛化后位置集合 L'

1)　将待发布数据集合 L 按照图心集合 L_{vu} 划分为指定数量的 Voronoi 多边形区域；

2)　for(j=1; j<=L.num; ++j)//待发布数据集中的位置

3)　　for(i=1; i<=L_{vu}.num; ++i)

4)　　R(i)为当前 Voronoi 图所划定区域;

5)　　if($l_j\in R(i)$)

6) $l_j.co = l_i.co$; //将位置坐标转换为图心坐标

7) else

8) continue;

9) end if

10) end

11) end

该算法通过划定的 Voronoi 多边形将待发布位置转换为图心，并通过图心替代实现位置集合的 ε-敏感位置关联隐私。算法 3-10 行将每个待发布位置转换为图心位置，5-9 行是对待发布位置是否属于当前多边形单元格的判断。

2.3 安全性分析

通过将待发布位置转换为 Voronoi 单元格中心，可实现隐私保护操作。该操作取决于图心位置与单元格中的敏感位置之间的不可区分程度。根据 ε-敏感位置关联隐私的定义，ε 取值越小发布数据的隐私保护程度越高。设用户位于待发布数据中的任一敏感位置 l_s，该位置位于可建立单元格的待发布位置数据集合。由于该区域可按照信息熵建立 Voronoi 图，且每个图心位置与当前单元格中的敏感位置满足最大熵，可认为敏感位置 l_s 与图心位置之间的关联值等于图心与另一随机敏感位置 l'_s 之间的关联值，即 $p(l_s,l_v)=p(l'_s,l_v)$，此时攻击者无法关联敏感位置。将 l_s 和 l'_s 带入到公式(4)，可得

$$\begin{aligned} K(l_s,l_v)(z) &\le e^{\varepsilon M_P(p(l_s,l_v),p(l'_s,l_v))}K(l'_s,l_v)(z) \\ &= e^{\varepsilon M_P(p(l_s,l_v),p(l_s,l_v))}K(l'_s,l_v)(z) \end{aligned} \tag{6}$$

由于 $M_P(p(l_s,l_v),p(l_s,l_v))\neq 0$，若满足 $K(l_s,l_v)(z)=K(l'_s,l_v)(z)$ 则 ε=0。本文算法将 l_s 和 l'_s 分别替换为 l_v，此时，$K(l_s,l_v)(z)=K(l'_s,l_v)(z)$ 可转换为 $K(l_v,l_v)(z)=K(l_v,l_v)(z)$，因此在算法处理完成之后，可得到 ε=0，即经过本文算法处理过的用户位置信息满足 ε-敏感位置关联隐私且 ε 可取到最小值。

3 实验验证

3.1 实验设定及测试标准

为了验证算法的隐私保护能力和数据可用性，将通过模拟实验与同类算法相比较。实验使用百度地图收集的位置集合，运行环境为 1.70 GHz Intel Core i5，内存为 4 GB 的笔记本电脑，使用 matlab R2017a 模拟。隐私保护能力使用信息熵和隐私数据处理比例加以度量。数据可用性将从发布数据的关联规则数量，位置偏移距离以及数据保持率等三个方面加以比较。

在隐私保护能力比较方面，敏感位置关联的成功概率为 $p(i)$，则信息熵表示为：

$$H(i)=-\sum_{i=1}^{n}p(i)\log_2 p(i) \tag{7}$$

隐私数据处理比例表示为隐私信息的处理比例，设未处理的数据量为 I_f^p，处理后的数据量为 I_a^p，则该比例可表示为：

$$P(I)=(I_f^p-I_a^p)/I_f^p \tag{8}$$

在可用性方面，关联规则数量使用 apriori 算法加以挖掘。位置偏移距离则根据发布数据与待发布数据的距离差计算。设发布后集合为 L_a，待发布集合为 L_f，则偏移量表示为：

$$D_m=|L_a-L_f|=\sum_{i=1}^{n}|l_{ai}-l_{fi}| \tag{9}$$

数据保持率表示发布数据量与待发布数据量的比值。设位置发布后的数据量为 D_a，待发布数量为 D_f，则数据保持率可表示为：

$$D_l=(D_f-D_a)/D_f \tag{10}$$

参与对比的算法有 KCL-Local 算法[1]，p-confidentiality 算法[7]以及 ECC 算法[4]。实验结果和结果分析进一步验证了本文算法的优越性。

3.2 实验结果及结果分析

从图 2 给出的攻击者猜测用户位置的信息熵可以看出，信息熵取值随着敏感位置数量的增加而增大。这是由于敏感位置的增加令攻击者更难将该范围内的位置与不确定敏感位置相关联，增加了攻击难度。在对比算法中，本文算法能够获得最大熵，这是由于该算法满足 ε-敏感位置关联隐私，令发布的位置与敏感位置之间的关联关系彼此相等，攻击者很难在相等的关联概率中将用户位置与敏感位置相关联。p-confidentiality 算法的表现好于另两种算法，这是由于该算法将敏感位置模糊为设定区域，在这个区域中用户位置与敏感位置之间关联关系模糊，其效果与本文所提出的方法相似。KCL-Local 算法采用抑制来实现隐私保护，该方法未能有效的将关联关系模糊或者泛化，攻击者仍然能够有效的猜测出某一指定位置。最后，ECC 算法在信息熵取值方面表现最差，该方法通过聚类实现对待发布数据隐私保护，其处理过程就是对同一类位置信息的泛化，并未对关联关系加以处理，攻击者很容易通过位置关联的方式猜测到用户的敏感位置。

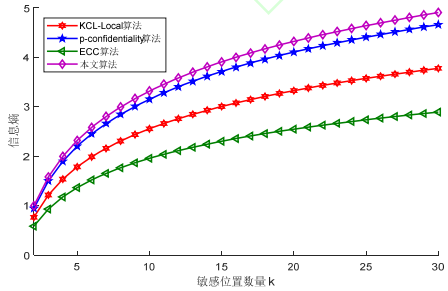

图 2 信息熵取值

图 3 给出了不同算法的隐私数据处理比例。在这几种算法中，本文算法对每一待发布位置加以处理，仅未处理图心位置重合数据，因此其隐私数据处理比例最高，且不受数据量增加影响。p-confidentiality 算法与本文算法类似，也是通过限定区域对待发布的位置加以模糊，但是该方法并未针对所有数据，因此在数据处理比例要低于本文算法。在另两种算法中，KCL-Local 算法对敏感信息进行抑制发布，该处理过程并不能保障所有的数据均被抑制，因此其隐私数据处理比例稍低。同时，该算法由于数据量的增加，其抑制的数据反而减少，这导致隐私数据处理比例在数据量增加的情况下逐渐减少。最后，ECC 算法使用聚类对隐私数据加以处理，整个过程并未对数据进行特殊处理，并且随着数据量的增加聚类数量未处理的位置数量相对增加，导致该算法随数据量增加其隐私数据处理比例反而降低。

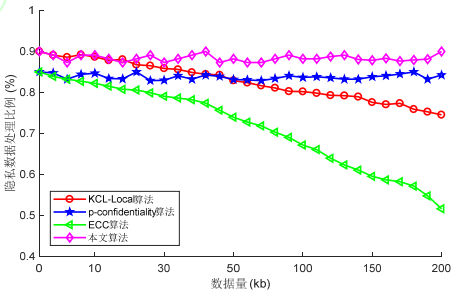

图 3 隐私数据处理比例

通常，发布位置数据是用来挖掘潜在的可用性及规则。图 4 给出了不同算法进行挖掘所获得的关联规则数量。从该图中可以看出，参与比较的几种算法均随着数据量的增加而挖掘出更多的关联规则。其中，ECC 算法取得的关联规则数量最多，这是因为该算法利用聚类进行泛化处理，并未破坏数据中的关联特性，能够最大限度的保留数据可用性。本文算法和 p-confidentiality 算法

处理过的数据其关联规则数量相差不大，这是由于这两种算法均基于指定区域进行模糊或位置转换，其数据信息被转换为图心位置或模糊区域，在一定程度上破坏了关联特性，其挖掘出的关联规则数量要少于 ECC 算法。最后，KCL-Local 算法由于抑制了部分数据，使得原始数据中很多基本的关联关系受到抑制，因此较难将发布数据相关联，其关联规则数量最少。

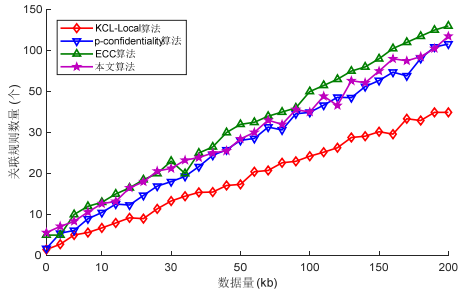

图 4　关联规则数量

图 5 给出了位置数据偏移距离的差异。从该图中可以看出，所有算法均随着数据量增加而增大偏移量。这是由于所有算法处理后的位置数据与未处理的位置数据之间存在差异，导致了位置数据偏移量的增加。在这些算法中，KCL-Local 算法的偏移距离总量最大，该算法使用抑制，删除掉的数据与原数据之间存在较大差异，导致了随着数据量的增加其偏移距离增加较快。ECC 算法存在聚类算法共同的弱点，在聚类过程中将边缘离散数据剔除，导致了 ECC 算法与 KCL-Local 相似。本文算法的表现稍差于 p-confidentiality 算法，这是由于本文算法将敏感位置替换为图心，使得发布位置产生偏移，但是由于 Voronoi 图的基本特性，其处理过的位置数据的偏移量有限。最后，p-confidentiality 算法的位置数据偏移距离最小，这是由于该算法仅利用模糊区域泛化真实位置，其位置并未偏移或偏移较小。

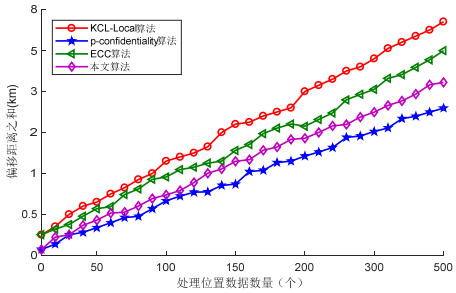

图 5　位置偏移距离

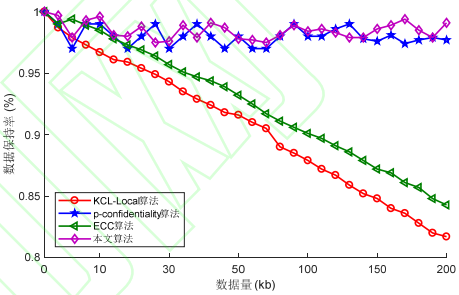

图 6　数据保持率

图 6 给出了不同算法数据保持率的差异。从该图中可以看出，本文算法和 p-confidentiality 算法的数据保持率最高，且不随着数据量的增加而改变。这是由于这两种算法均未对待发布数据进行删除等破坏操作，最大程度的保障了数据的完整性。在另两种算法中，ECC 算法正如在上一段所述的那样，聚类对数据的删除处理导致边缘数据的大量删除。最后，KCL-Local 算法利用抑制实现隐私处理，在整个数据的发布过程中，较多的数据因为敏感问题而受到了不同程度的抑制，且随着数据量的增加待发布数据中的敏感数据同样增多，其抑制的数据量也随之增加，因而该算法的数据保持率最小。

综上，通过隐私保护能力和发布数据可用性两个方面的比较，可以看出本文算法相比于参与

比较的几种同类算法具有更好的隐私保护能力，且具有更高的发布数据可用性。

4 结论

本文针对位置数据，通过使用 Voronoi 图对待发布数据的位置空间进行划分，并使用图心位置代替敏感位置，以此实现对发布位置的隐私保护。算法在执行过程中使用了信息熵，以此计算关联关系实现位置脱敏，且使用基于广义差分隐私的 ε-敏感位置关联隐私进行隐私度量。对比实验进一步验证了所提出的算法的隐私保护性和数据的可用性。随着研究的继续，今后的工作将在如何处理图形数据发布的隐私保护和实时位置数据的隐私保护方面展开。

参考文献：

[1] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking [C]. Proceedings of the Proceedings of the 1st International Conference on Mobile Systems, Applications and Services, 2003: 31-42.

[2] Xiao Z, Xu J, Meng X. p-Sensitivity: A semantic privacy-protection model for location-based services [C]. Proceedings of the International Conference on Mobile Data Management Workshops, 2008: 47-54.

[3] Fuyu L, Hua K A, Ying C. Query l-diversity in location-based services [C]. Proceedings of the Mobile Data Management: Systems, Services and Middleware, 2009 MDM '09 Tenth International Conference, 2009: 436-442.

[4] 张磊, 马春光, 杨松涛, 等. 抗轨迹差异识别攻击的相似轨迹实时生成方法[J]. 哈尔滨工程大学学报, 2017, 2017(7): 1173-1178.

[5] Wang Y, Xia Y, Hou J, et al. A fast privacy-preserving framework for continuous location-based queries in road networks[J]. Journal of Network and Computer Applications, 2015, 53(2015): 57-73.

[6] 马春光, 张磊, 杨松涛. 位置轨迹隐私保护综述[J]. 信息网络安全, 2015, 2015(10): 24-31.

[7] MA Chunguang, ZHANG Lei, YANG Songtao, et al. Achieve personalized anonymity through query blocks exchanging[J]. China Communications, 2016, 13(11): 106-118.

[8] MA Chunguang, ZHANG Lei, YANG Songtao, et al. Hiding Yourself Behind Collaborative Users When Using Continuous Location-Based Services[J]. Journal of Circuits, Systems and Computers, 2017, 26(7): 1750119: 1750111-1750119:1750125.

[9] Niu B, Zhu X Y, Li Q H, et al. A novel attack to spatial cloaking schemes in location-based services[J]. Future Generation Computer Systems, 2015, 2015 (49): 125-132.

[10] 张磊, 马春光, 杨松涛, 等. 关联概率不可区分的位置隐私保护方法 [J]. 通信学报, 2017, 38(8): 37-49.

[11] 张磊, 马春光, 杨松涛, 等. 基于属性基加密的用户协作连续查询隐私保护策略[J]. 通信学报, 2017, 38(9): 76-85.

[12] Dargahi T, Ambrosin M, Conti M, et al. ABAKA: A novel attribute-based k-anonymous collaborative solution for LBSs [J]. Computer Communications, 2016, 85(2016): 1-13.

[13] Fung B C M, Wang K, Chen R, et al. Privacy-preserving data publishing: A survey of recent developments [J]. ACM Computing Surveys, 2010, 42(4): 14.

[14] Chen R, Fung B C M, Mohammed N, et al. Privacy-preserving trajectory data publishing by local suppression[J]. Information Sciences, 2013, 231(2013): 83-97.

[15] Terrovitis M, Poulis G, Mamoulis N, et al. Local Suppression and Splitting Techniques for Privacy Preserving Publication of Trajectories[J]. IEEE Transactions on Knowledge & Data Engineering, 2017, 29(7): 1466-1479.

[16] 赵婧, 张渊, 李兴华, et al. 基于轨迹频率抑制的轨迹隐私保护方法[J]. 计算机学报, 2014, 37(10): 2096-2106.

[17] Bonchi F, Lakshmanan L V S, Wang H. Trajectory anonymity in publishing personal mobility data[J]. SIGKDD Explor Newsl, 2011, 13(1): 30-42.

[18] Chow C-Y, Mokbel M F. Trajectory privacy in location-based services and data publication[J]. SIGKDD Explor Newsl, 2011, 13(1): 19-29.

[19] Lu Q, Wang C, Xiong Y, et al. Personalized Privacy-Preserving Trajectory Data Publishing[J]. Chinese Journal of Electronics, 2017, 26(2): 285-291.

[20] Zheng X, Cai Z, Yu J, et al. Follow But No Track: Privacy Preserved Profile Publishing in Cyber-Physical Social Systems[J]. IEEE Internet of Things Journal, 2017, PP(99): 1-1.

[21] Li M, Zhu L, Zhang Z, et al. Achieving Differential Privacy of Trajectory Data Publishing in Participatory Sensing[J]. Information Sciences, 2017.

[22] Yabo X, Fung B C M, Ke W, et al. Publishing sensitive transactions for itemset utility[C]. Proceedings of the Data Mining, 2008 ICDM '08 Eighth IEEE International Conference, 2008: 1109-1114.

[23] Sui P, Wo T, Wen Z, et al. Privacy-Preserving trajectory publication against parking point attacks[C]. 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (Uic/Atc) Ubiquitous Intelligence and Computing, 2013, 569-574.

[24] Wang C, Liu H, Wright K-L, et al. A privacy mechanism for mobile-based urban traffic monitoring[J]. Pervasive and Mobile Computing, 2015, 20(2015): 1-12.

[25] Ma Chunguang, Zhou Changli, Yang Songtao. A voronoi-based Location privacy-preserving method for continuous query in LBS[J]. International Journal of Distributed Sensor Networks, 2015, 11(3): 1-17.

[26]肖剑川, 许力, 叶阿勇, 等. 基于 Voronoi 图的路网轨迹隐私保护研究[J]. 信息网络安全, 2016, 2016(6): 15-21.