融合语义信息的最优位置选择算法

李梦涵[1,2,3]，　闫彦彤[1,2,3]，　李丽红[1,2,3]

(1. 华北理工大学 理学院　河北 唐山 063210；2. 河北省数据科学与应用重点实验室　河北 唐山 063210；
3. 唐山市工程计算重点实验室　河北 唐山 063210)

摘要：目前,位置服务的广泛应用带来了个人信息安全的挑战。为应对这一挑战,研究人员致力于探究多种位置隐私保护策略。其中,融合语义信息的位置隐私保护算法成为研究的热点之一。利用语义信息提出了一种新的选择位置中心的思想,将该思想与语义距离融合,选择最佳匿名候选集合,从而保证位置集合的语义多样性和物理多样性。实验结果表明,相较于 DLS 算法、Enhanced-DLS 算法和 MMDS 算法,所提算法在语义和物理位置方面能够保证多样性,有效降低了位置数据的准确性,保护了用户的隐私。

关键词：位置服务；语义信息；位置中心；匿名候选集合

中图分类号：TO309　　**文献标志码**：A　　**文章编号**：1671-6841(2025)04-0088-07

DOI：10.13705/j.issn.1671-6841.2023263

Optimal Location Selection Algorithm for Fusing Semantic Information

LI Menghan[1,2,3], YAN Yantong[1,2,3], LI Lihong[1,2,3]

(1. *Department of Science, North China University of Science and Technology, Tangshan* 063210, *China*;
2. *Hebei Province Key Laboratory of Data Science and Application, Tangshan* 063210, *China*;
3. *Tangshan Key Laboratory of Engineering Calculation, Tangshan* 063210, *China*)

Abstract: Currently, the widespread application of location services poses challenges to personal information security. In response, researchers explored various strategies for location privacy protection, with algorithms incorporating semantic information emerging as a key focus. A new idea for selecting location centers was proposed using semantic information, integrating this concept with semantic distance to choose the optimal anonymous candidate set, thereby ensuring the semantic and physical diversity of the location set. Experimental results demonstrated that compared with DLS, Enhanced-DLS, and MMDS algorithms, the method maintained diversity in both semantic and physical aspects, effectively reducing the accuracy of location data and protecting user privacy.

Key words: location privacy; semantic information; location center; anonymous candidate set

0　引言

在当前数字化社会的背景下,基于位置的服务(location-based service,LBS)和定位技术得到了广泛应用,进而使用户位置隐私的问题受到了关注。在众多应用场景中,如社交网络、个性化广告推送、导航与路径规划等,常常涉及对用户位置信息的收集与应用。用户的位置数据含着极高的隐私性和敏感度,能透露个体的日常行为模式、偏好,甚至是精确的位置和行动轨迹等信息。不当的信息使用或泄露可能导致用户面临严重的安全威胁、经济损失,以及隐私权的侵犯。鉴于这些潜在的后果和风险,确保位置信息的严密保护与妥善管理显得至关重要。

收稿日期:2023-11-18
基金项目:河北省数据科学与应用重点实验室项目(10120201);唐山市数据科学重点实验室项目(10120301)
第一作者:李梦涵(1999—),女,硕士研究生,主要从事数据安全与隐私保护研究,E-mail:923175694@qq.com。
通信作者:李丽红(1979—),女,教授,主要从事数据挖掘、三支决策研究,E-mail:22687426@qq.com。

1　相关工作

为了保护用户位置隐私,国内外学者提出了如匿名集合[1-2]、差分隐私[3-4]、位置混淆[5-6]以及同态加密[7]等相关技术,目的是通过不同策略降低个人位置信息的可识别性和追踪风险。Gruteser 等[8]首次把 k-匿名概念引入位置隐私保护领域,通过构建一个含 $k-1$ 个邻近位置的集合隐藏真实位置。

在上述位置隐私保护方法的基础上,Niu 等[9]提出了基于熵度量的 DLS(dummy location selection, DLS)算法,实现 k-匿名的同时,通过 Enhanced-DLS 算法确保选择的位置点均匀分布于各区域。王洁等[10]提出了 MMDS(maximum and minimum dummy selection,MMDS)算法,保证了位置集合的语义,然后根据查询概率和地理位置的物理分散性得到最终假位置集合,解决了攻击者能够排除部分虚假位置的问题。杨洋等[11]提出一种矩形区域的 k-匿名位置隐私保护方法,用矩形区域范围代替用户位置进行匿名。文献[12-14]结合地理位置语义和其他背景信息降低用户位置泄露的概率。文献[15-17]结合概率分布、位置信息和 k-匿名,优化了哑元位置的生成和选取。文献[18]结合路网环境,提高算法对用户位置的保护能力。然而,k-匿名技术的局限在于它通常仅关注位置的地理属性,忽视了位置的语义信息,对抗背景知识攻击的效果有限,这可能使攻击者能够通过长期分析来揭露用户的具体位置。

上述提到的解决方案虽然能够有效应对真实用户匿名区域生成和哑元位置选择的问题,但它们在位置选择时缺乏对语义多样性的考虑,无法很好地平衡物理分散性和数据多样性,存在潜在的用户隐私泄露风险。因此,本文提出了一种融合语义距离的位置中心选择算法,以期更有效地保护位置隐私。本研究的主要贡献如下。

1) 选择物理位置候选集合,使集合中位置之间的相互距离尽可能远,提高位置集合的物理分散性。

2) 计算语义相似距离,提高最终位置候选集合的语义多样性。

3) 通过理论分析和实验结果的验证,所提出的方案能够较好地提高位置隐私的安全性、降低位置数据的准确度。

2　系统模型

2.1　系统架构

集中式架构的服务器模型由移动用户、第三方可信匿名(trusted third party,TTP)服务器和 LSP(location services platform,LSP)平台三部分组成,由于系统依赖第三方服务器的可靠性,很容易陷入瓶颈。TTP 本身存储着大量真实的用户位置信息,如果服务器受到攻击,会对用户造成严重的损失,甚至导致整个隐私保护方案的失效。因此,本文使用分布式架构(peer to peer,P2P),仅由移动用户和 LSP 组成,不需要可信的第三方匿名服务器,邻居位置的选择和请求查询服务都是在移动客户端完成的。

P2P 架构主要由 GPS 卫星定位系统、Wi-Fi 接入点(access point,AP)、移动用户和 LSP 组成,其主要功能如下。

1) GPS 卫星定位系统为移动终端提供当前位置的地理信息。

2) Wi-Fi 接入点为移动终端提供位置语义信息。

3) 移动用户是指有移动设备的人类实体。移动用户从 Wi-Fi 接入点获取区域内(包括真实位置在内)的位置信息,将真实位置藏匿在匿名候选集中发送给 LSP 服务平台。

4) LSP 服务平台接收到用户请求后,对匿名候选集中的位置全部进行查询,将结果返给移动终端。

2.2　相关定义

定义 1　用户的真实位置 l_{real}。包括用户位置的经度、纬度和位置名称。

定义 2　匿名度 k。表示每次向 LSP 服务器发送匿名集合的长度,并且攻击者能够识别出真实位置的概率为 $1/k$。

定义 3　物理距离候选集 $S_1 = \{l_1, l_2, \cdots, l_m\}$。表示满足物理距离的位置集合。

定义 4　语义距离候选集 $S_2 = \{l_1, l_2, \cdots, l_{k-1}\}$。表示满足语义多样性的位置集合。最终的位置候选集 RS 包括语义距离候选集 S_2 和真实位置 l_{real}。

2.3　语义距离计算方法

采用编辑距离(edit distance)来计算语义距离 dis_{sem},编辑距离是衡量两个字符串相似度的方法,较大的编辑距离意味着更低的相似度。当计算两个字符串间的编辑距离时,首先要建立一个动态规划矩阵。在这一矩阵 $\boldsymbol{D}$ 中,$\boldsymbol{D}[i,j]$ 是字符串之间的编辑距离,在本文中每个编辑操作(如插入、删除、替换)的成本设定在 0 和 1。

设有字符串 $A = a_1a_2\cdots a_n$ 和 $B = b_1b_2\cdots b_n$,若 $a_i = b_i$,则替换操作的成本为 0;若字符不同,则替换操作的成本为 1。因此,语义距离 dis_{sem} 表示将 A 转

化成 B 的最小变动次数。

2.4 物理距离

通常用位置之间的距离和来测量位置候选集所覆盖的范围,即

$$\sum_{i\neq j} d(c_i,c_j), \tag{1}$$

其中:$d(c_i,c_j)$ 表示位置 c_i 和 c_j 之间的距离。

然而,在选择邻居位置时,使用距离之和的方式可能不如距离乘积更好,距离乘积的方式能更好地扩展匿名区域。即

$$\prod_{i\neq j} d(c_i,c_j)。 \tag{2}$$

在图 1 中,A 是用户的真实位置,B 是距离 A 最远的邻居位置。假设有两个选择来分配第三个邻居位置(C 或 N)。如果根据距离之和来选择位置,则 C 和 N 被选中的概率相同。然而,从隐私的角度来看,选择 C 比选择 N 更有利,因为 C 将进一步扩大匿名区域。因此,本文选择使用位置间距离乘积的方式选择邻居位置。在这种情况下,$CA\cdot CB > NA\cdot NB$,选择 C 作为虚拟位置。

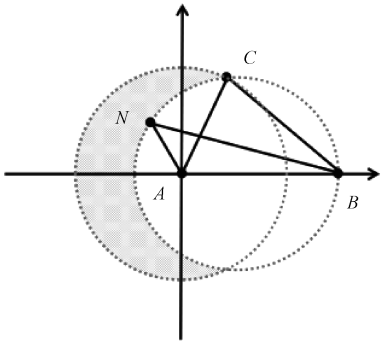

图 1 物理距离

Figure 1 Physical distance

2.5 匿名区域面积

匿名区域面积 D 是由假位置点 k 组成的凸包面积。凸包是给定点集内部的最小凸多边形。k 个位置点被用于隐私保护,而凸包的面积是衡量匿名程度的一个指标。随着凸包面积的增加,匿名程度也随之提高,从而能更好地保护用户的隐私。凸包面积的计算可以使用鞋带公式[19],即

$$D=\frac{1}{2}\left|\sum_{i=1}^{m}(x_iy_{i+1}-x_{i+1}y_i)\right|, \tag{3}$$

其中:m 表示位置候选集 RS 最外层位置点的个数。

2.6 用户隐私需求

每个用户有一个隐私需求 S,用二元组 (k,u) 表示,k 代表匿名度,在每次查询中,服务器能够获得真实位置,以及 $k-1$ 个邻居位置,并且攻击者识别真实位置的概率不超过 $1/k$。u 代表语义差异度,表示任意两个位置之间的语义距离 dis_{sem} 必须大于等于一个最小可接受值 u,即 $dis_{\text{sem}}(l_i,l_j)_{\min}\geqslant u$,以确保假位置集合中位置的语义多样性。

2.7 安全值-θ

安全值-θ 是用于衡量位置集 RS 与真实位置语义差异的度量标准,计算公式为

$$\theta=1-\frac{|SEM|}{C_k^2}, \tag{4}$$

其中:$SEM=\{l_{\text{sem}}\mid l_{\text{sem}}(l_i,l_j)\leqslant l\}$,$l_i$、$l_j$ 是位置候选集中的任意两个位置;l 是语义多样性的默认阈值。结果集 RS 称为安全值-θ 集合,安全值-θ 越大,表示生成的假位置集具有更大的语义差异度。

3 算法设计

本文提出的位置候选集生成算法 MM-DLS(maxmin-dummy location selection,MM-DLS)由以下两个算法实现:算法 1 采用最大最小距离生成物理距离候选集 S_1;在算法 2 中,通过计算候选集合 S_1 中位置间的编辑距离生成语义距离集合 S_2。最终将真实位置 l_{real} 与语义距离候选集合 S_2 合并成为位置候选集合 RS。

3.1 算法 1

使用算法 1 计算正方形区域中位置地理坐标的中心,得到 $2k$ 个位置中心,根据物理距离将尽可能远的对象作为位置中心。首先,将真实位置 l_{real} 作为第一位置中心,然后选择距离第一位置中心最远的样本作为第二位置中心。对于第二个位置中心之后的每一个位置中心,计算该点与所有位置中心的距离,选择乘积最大的点作为下一个位置中心。在确定所有位置中心之后,将包括 $2k$ 个位置中心的样本集合作为物理距离候选集 S_1。算法 1 伪代码描述如下。

算法 1 计算物理距离并获取虚拟位置集 S_1

输入:位置数据集 S_n,用户隐私需求 k。

输出:生成位置候选集合 S_1。

1) $k_1=2k$,$S_1=NULL$。

2) 将真实位置 l_{real} 作为第一位置中心 Z1。

3) $S_n=S_n-l_{\text{real}}$,$k_1=k_1-1$。

4) 找到距离 Z1 最远的位置 l_i,该位置被视为第二个位置中心 Z2。

5) $S_n\leftarrow S_n-l_2$,$S_1\leftarrow S_1\cup l_2$,$k_1=k_1-1$。

6) for i in *range* (k_1)

7) $\quad dis_{\max}=0$

8) $\quad$ for each l_i in S_n

9)　　if l_j not in S_1
10)　　$dis = haversine(l_i, l_j)$ for l_j in S_1
11)　　$dis_{all} = dis_{max} \cdot dis_{max}$
12)　　if $dis_{all} > dis_{max}$
13)　　$dis_{max} = dis_{all}$
14)　　$S_n \leftarrow S_n - l_i$
15)　　$S_1 = S_1 \cup l_i$
16)　　end if
17)　　end if
18)　end for
19) end for
20) return S_1

3.2　算法 2

在物理位置候选集 S_1 的基础上,通过计算编辑距离,从 S_1 中筛选出与真实位置语义距离相差最大的 $k-1$ 个位置,形成语义距离候选集 S_2。最终,将语义距离候选集 S_2 和真实距离 l_{real} 合并,形成最终候选集 RS。其中计算语义距离采用编辑距离的方法进行计算,计算编辑距离伪代码描述如下。

算法 2　计算语义编辑距离

输入:位置 l_i,位置 l_j。

输出:语义距离 dis_{sem}。

1) $S_i = l_i, S_j = l_j$。
2) $S_i = a_1 a_2 \cdots a_i, S_j = a_1 a_2 \cdots a_j$
3) $n_1 = length(S_i), n_2 = length(S_j)$。
4) if $n_1 = 0$ or $n_2 = 0$
5)　　return 0。
6) end if
7) 构造 $n_1 + 1$ 行,$n_2 + 1$ 列矩阵 $\boldsymbol{D}$。
8) for i from 0 to n_1
9)　　$D[i][0] = i$
10) end for
11) for j from 0 to n_2
12)　　$D[0][j] = j$
13) end for
14) for i from 1 to n_1
15)　　for j from 1 to n_2
16)　　if $S[i-1] = S[j-1]$
17)　　$cost = 0$
18)　　else
19)　　$cost = 1$
20)　　$D[i][j] = \min(D[i-1][j] + 1, D[i][j-1] + 1, D[i-1][j-1] + cost)$
21)　　end for
22) end for
23) $dis_{sem} = D[n_1][n_2]$。
24) return dis_{sem}。

3.3　安全性分析

在位置隐私保护中,如果 k 个位置处于聚集区域,则减少搜索范围可轻松地获取真实位置,这时 k-匿名只是满足数量上的要求,而未达到实际的匿名效果。在 MM-DLS 方法中,位置候选集是在算法 1 的基础上生成的,并均匀分布在匿名区域中。因此,真实位置与其他 $k-1$ 个位置区分的概率为 $1/k$,从而满足匿名效果。

在语义攻击中,攻击者可以根据邻居位置的语义关系来推断查询用户的隐私信息。地名的语义差异越大,位置的语义多样性就越好。在算法 2 中,通过选择距离真实位置语义距离最大的 k 个位置,形成语义距离位置候选集,从而满足地理语义多样性的要求。

综上所述,所提出的方法满足物理多样性和语义多样性的要求,能够有效保护位置隐私。

4　仿真结果与分析

4.1　实验设置

为了验证 MM-DLS 算法在选择最优位置时的有效性和性能,本研究在真实的位置数据集上进行了实验。实验数据集的选取范围包括纬度从 39.95°到 40.00°,经度从 116.30°到 116.35°的地理坐标范围,该数据集包含了 36 663 个位置信息点,覆盖了北京市海淀区的大部分区域。

为了更好地分析数据,将该地区划分成一个 10×10 的网格,并通过图 2 对数据分布情况进行可视化展示。

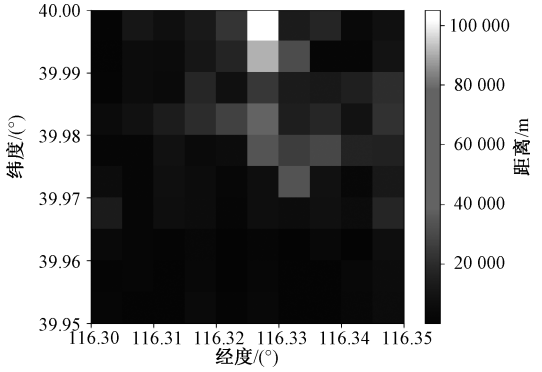

图 2　Geolife 数据热力图

Figure 2　Geolife data heatmap

此外,考虑到 Geolife 数据集[20]中的位置点未

提供相关的位置语义信息,采用高德地图来获取这些位置的相关语义信息以便进行实验研究。

实验使用 Python 语言编写,在 Intel Core i5 处理器和 8 GB 内存的计算机上运行。开发环境选用了 Pycharm,同时使用了 pandas、numpy 和 scikit-learn 等多个开源库。语义差异度为 8,语义距离阈值范围为[3,14]。

4.2 结果分析

本文采用物理分散性和语义分散性这两个度量标准来衡量匿名集 *RS* 的质量,将 MM-DLS 算法与同样使用位置技术的 DLS 算法[9]、Enhanced-DLS 算法[9]和 MMDS 算法[10]进行比较。

4.2.1 物理分散性 本文从三个方面对算法生成位置集的物理分散程度进行评估:最小距离、最大距离和匿名区域面积。当位置集合 *RS* 中位置间的最小距离、最大距离和匿名区域面积越大时,说明选取的位置在区域内分布得越均匀。

实验将 MM-DLS 算法、DLS 算法、Enhanced-DLS 算法和 MMDS 算法进行了比较,结果如图 3、图 4、图 5、图 6 所示。

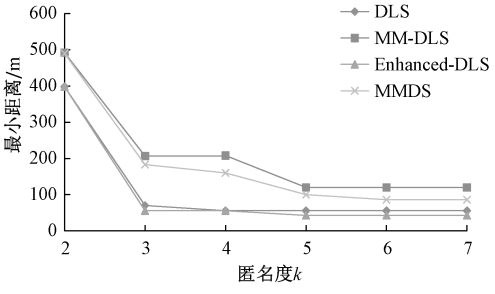

图 3 最小距离

Figure 3 Minimum distance

如图 3 所示,随着 k 的增加,四种算法生成的位置点间最小距离均呈现下降的趋势。MM-DLS 算法的最小距离显然比其他三种算法要大。因为 MM-DLS 算法优先选择与真实位置距离最远的点作为中心,重视位置间的物理分散性。相较而言,DLS 算法主要依据位置的查询概率熵形成候选集,而不考虑物理距离。而 Enhanced-DLS 和 MMDS 算法尽管考虑了物理距离,但在计算位置查询概率熵时可能排除了远距离位置,导致它们的最小距离随 k 的增大而趋近于 DLS 算法。实验结果表明,本文方法在保持物理位置分散性方面表现更佳。

如图 4 所示,当 $k \geqslant 3$ 时,MM-DLS 算法位置之间的最大距离最大。这是因为该算法初步以距离最远的点作为位置中心,进而以最终的位置中心形成物理距离候选集,确保位置间距离。图 5 和图 6 表明,当 k 较小时,MM-DLS 算法产生的匿名区域面积大于其他三种算法。当 k 较大时,MM-DLS 算法、Enhanced-DLS 算法和 MMDS 算法的匿名区域面积相似,且面积均大于 DLS 算法。这主要是由于本文提出的算法在保障位置分散性的同时,也确保了兴趣点类别的多样性。Enhanced-DLS 算法在考虑历史查询概率后,再考虑位置点间距离,而 DLS 算法则仅侧重于位置的历史查询概率。MMDS 算法在进行位置选择时,首先考虑了语义差异度大的位置,而在现实生活中,位置距离较远的地点,其语义差异度通常是较大的。

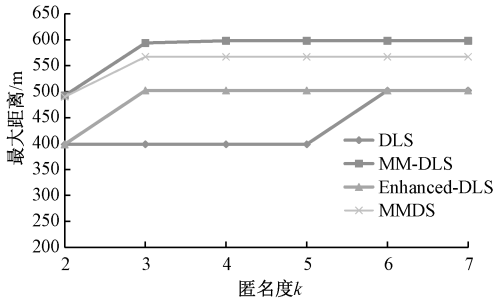

图 4 最大距离

Figure 4 Maximum distance

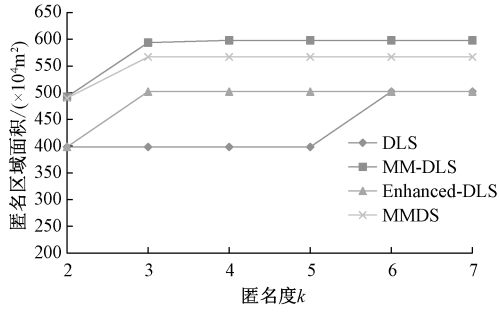

图 5 k 较小时匿名区域面积

Figure 5 Anonymity region area for small values of k

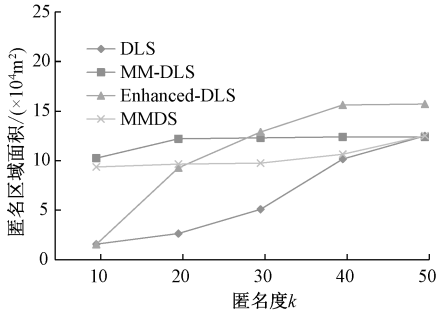

图 6 k 较大时匿名区域面积

Figure 6 Anonymity region area for big values of k

因此,本文提出的 MM-DLS 算法在与其他三种算法进行比较时,仍然具有较好的物理分散性。

4.2.2 语义多样性 本研究对比了 MM-DLS 算法、

DLS 算法和 Enhanced-DLS 算法的语义多样性。实验通过分析候选集中的语义多样性,计算了 θ 位置安全值,结果展示如图 7 所示。

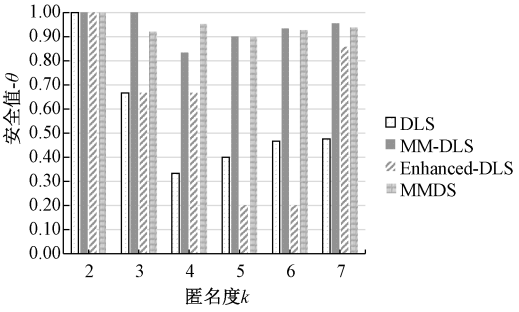

图 7　安全值-θ

Figure 7　safe value-θ

如图 7 所示,随着 k 值增加,MM-DLS 和 MMDS 算法的安全值-θ 接近于 1,符合语义多样性的要求,而 DLS 和 Enhanced-DLS 算法的安全值-θ 相对较低。这是因为 DLS 和 Enhanced-DLS 算法主要关注邻居位置间的查询概率,忽略了语义信息。高查询概率的位置多在热点区域,其语义相似性较高,导致这两种算法的语义多样性较差,安全值-θ 低。

本文通过实验对比表明,所提出的 MM-DLS 算法在选取邻居位置时展现出更佳的物理分散性和语义多样性,有效避免了攻击者利用地理语义信息特征对用户发起攻击。因此,该方法能有效保护用户的位置隐私。

5　结语

针对传统假位置隐私保护方案未充分考虑攻击者背景知识的问题,本文提出了一种融合语义的最优位置选择算法 MM-DLS。这一算法在保护用户隐私方面考虑了语义信息与物理分布等多重因素,从而有效降低攻击者推断出用户真实位置的可能性。首先利用距离乘积方法找到满足物理多样性要求的物理位置候选集合 S_1;随后,算法通过计算 S_1 中位置与真实位置之间的语义距离,筛选出语义距离较远的 $k-1$ 个位置,与真实位置一同构成最终的匿名集合。这样构成的匿名集合既符合物理多样性的要求,也满足语义多样性的标准。

实验从最小距离、最大距离、匿名区域面积及安全值-θ 四个维度对本文的 MM-DLS 算法与 DLS 算法、Enhanced-DLS 算法、MMDS 算法进行了比较。结果表明,MM-DLS 算法在邻居位置选择过程中有效保护了真实位置隐私,同时在物理分散性和语义多样性方面展现了优异性能,形成了高质量的位置集合,提高了算法效率和可扩展性。然而,该算法未考虑位置查询概率信息,可能不足以抵御拥有查询概率背景知识的攻击者,因此位置隐私保护的研究还要进一步深入。

参考文献:

[1] 冯亚平, 康海燕. 基于缓存的位置隐私保护方法研究[J]. 郑州大学学报(理学版), 2019, 51(4): 49-55.
FENG Y P, KANG H Y. A location privacy preserving method based on caching[J]. Journal of Zhengzhou university (natural science edition), 2019, 51(4): 49-55.

[2] PENG W P, MA D, SONG C, et al. A K-anonymous location privacy-preserving scheme for mobile terminals [EB/OL]. (2023-12-11)[2024-01-15]. https://publications.eai.eu/index.php/el/article/view/4468/2745.

[3] GAO H F, ZHANG Z Q, ZHAO H W. Personalized privacy protection based on space grid in mobile crowdsensing[J]. Applied sciences, 2023, 13(23): 126.

[4] ZHU L, LEI T T, MU J Q, et al. Differential privacy-based spatial-temporal trajectory clustering scheme for LBSNs[J]. Electronics, 2023, 12(18): 3767.

[5] KOU K Q, LIU Z B, YE H, et al. A location privacy protection algorithm based on differential privacy in sensor network[J]. International journal of embedded systems, 2021, 14(5): 432-442.

[6] KHODAEI M, PAPADIMITRATOS P. Cooperative location privacy in vehicular networks: why simple mix zones are not enough[J]. IEEE Internet of Things journal, 2021, 8(10): 7985-8004.

[7] ZHENG X D, YUAN Q, WANG B, et al. A homomorphic encryption based location privacy preservation scheme for crowdsensing tasks allocation[J]. Wireless personal communications, 2022, 126(1): 719-740.

[8] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[C]//Proceedings of the 1st international conference on Mobile systems, applications and services. New York: ACM Press, 2003: 163-168.

[9] NIU B, LI Q H, ZHU X Y, et al. Achieving k-anonymity in privacy-aware location-based services[C]//IEEE INFOCOM 2014-IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 754-762.

[10] 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.

[11] 杨洋, 王汝传. 增强现实中基于LBS的双重匿名位置隐私保护方法[J]. 南京师大学报(自然科学版), 2018, 41(3): 42-46.
YANG Y, WANG R C. Double anonymity location privacy protection based on LBS in augment reality[J]. Journal of Nanjing normal university (natural science edition), 2018, 41(3): 42-46.

[12] KUANG L, WANG Y, ZHENG X S, et al. Using location semantics to realize personalized road network location privacy protection[J]. EURASIP journal on wireless communications and networking, 2020, 2020(1): 435-465.

[13] ZHANG Y B,ZHANG Q Y,LI Z Y,et al. A k-Anonymous location privacy protection method of dummy based on geographical semantics[J]. International journal of network security,2019,21(6):937-946.

[14] 张学军, 杨昊英, 李桢, 等. 融合语义位置的差分私有位置隐私保护方法[J]. 计算机科学, 2021, 48(8): 300-308.
ZHANG X J, YANG H Y, LI Z, et al. Differentially private location privacy-preserving scheme with semantic location[J]. Computer science, 2021, 48(8): 300-308.

[15] 杨洋, 胡晓辉, 杜永文. 基于历史查询概率的k-匿名哑元位置选取算法[J]. 计算机工程, 2022, 48(2): 147-155.
YANG Y, HU X H, DU Y W. The k-anonymous dummy location selection algorithm based on historical query probability[J]. Computer engineering, 2022, 48(2): 147-155.

[16] 宋成, 金彤, 倪水平, 等. 一种面向移动终端的K匿名位置隐私保护方案[J]. 西安电子科技大学学报, 2021, 48(3): 138-145.
SONG C, JIN T, NI S P, et al. K-anonymous location privacy protection scheme for the mobile terminal[J]. Journal of xidian university, 2021, 48(3): 138-145.

[17] HUANG G L, DENG K, XIE Z J, et al. Intelligent pseudo-location recommendation for protecting personal location privacy[EB/OL]. (2019-07-05)[2023-10-15]. https://onlinelibrary.wiley.com/doi/10.1002/cpe.5435.

[18] 倪巍伟, 冯志刚, 闫冬. 基于路网环分布的隐私保护近邻查询方法[J]. 计算机学报, 2020, 43(8): 1385-1396.
NI W W, FENG Z G, YAN D. Location privacy preserving nearest neighbor query method based on circle distribution on road networks[J]. Chinese journal of computers, 2020, 43(8): 1385-1396.

[19] BRADEN B. The surveyor's area formula[J]. The college mathematics journal,1986,17(4):326-337.

[20] ZHENG Y,XIE X,Ma W Y. GeoLife: a collaborative social networking service among user, location and trajectory[J]. Bulletin of the IEEE computer society technical committee on data engineering,2010,33(2):32-39.