

基于差分隐私的社交网络位置近邻查询方法

金波^{1,2}, 张志勇^{1,2*}, 赵婷^{1,2}

(1. 河南科技大学 信息工程学院, 河南 洛阳 471023; 2. 河南省网络空间安全应用国际联合实验室(河南科技大学), 河南 洛阳 471023)
(* 通信作者电子邮箱 xidianzzy@126.com)

摘要:针对社交网络中近邻位置查询时个人位置隐私泄漏的问题,采用地理不可区分性机制对位置数据添加随机噪声,提出了一种隐私预算分配方法。首先,对空间区域进行网格化分割,根据用户在不同区域的位置访问量来个性化分配隐私预算;然后,为了解决在扰动位置数据集中近邻查询命中率偏低的问题,提出了一种组合增量近邻查询(CINQ)算法,以扩大需求空间的检索范围,并利用组合查询过滤冗余数据。在仿真实验中,与SpaceTwist算法相比,CINQ算法的查询命中率提高了13.7个百分点。实验结果表明,CINQ算法有效解决了因为查询目标的位置扰动所带来的查询命中率偏低问题,适用于社交网络应用中扰动位置的近邻查询。

关键词:差分隐私;隐私预算;近邻查询;位置隐私;地理不可区分性

中图分类号:TP393.08 **文献标志码:**A

Location nearest neighbor query method for social network based on differential privacy

JIN Bo^{1,2}, ZHANG Zhiyong^{1,2*}, ZHAO Ting^{1,2}

(1. School of Information Engineering, Henan University of Science and Technology, Luoyang Henan 471023, China;
2. Henan International Joint Laboratory of Cyberspace Security Applications (Henan University of Science and Technology),
Luoyang Henan 471023, China)

Abstract: Concerning the problem of privacy leak of personal location when querying the nearest neighbor location in social network, a geo-indistinguishability mechanism was used to add random noise to the location data, and a privacy budget allocation method was proposed. First, the spatial regions were divided into grids, and the personalized privacy budget allocation was performed according to the location hits of user in different regions. Then, in order to solve the problem of low hit rate of the neighbor query in the disturbance location dataset, a Combined Incremental Neighbor Query (CINQ) algorithm was proposed to expand the search range of the demand space, and the combination query was used to filter out the redundancy data. Simulation results show that compared with the SpaceTwist algorithm, the CINQ algorithm had the query hit rate increased by 13.7 percentage points. Experimental results verify that the CINQ algorithm effectively solves the problem of low query hit rate caused by the location disturbance of the query target, and it is suitable for neighbor queries for disturbed locations in social network applications.

Key words: differential privacy; privacy budget; nearest neighbor query; location privacy; geo-indistinguishability

0 引言

随着移动设备的广泛普及,基于位置的服务(Location-Based Services, LBS)得到了快速发展,为互联网用户带来了巨大的便利。在社交网络应用中,基于位置的近邻查询可以根据用户属性检索到具有共同兴趣点的附近用户,还可以根据空间距离发现潜在的邻近好友。同样,人们也日益关注可能带来的隐私泄漏风险,通过组合查询、交叉攻击等方式,攻击者可以推测出用户的空间位置、兴趣爱好、健康状况等隐私信息,这对用户的个人隐私安全构成了严重的威胁。因此,在保证位置服务效用性的同时,如何保护用户隐私安全成为了

研究焦点^[1]。

目前在位置近邻查询时,位置隐私保护主要的研究方法包括:匿名^[2-3]、混合区^[4-5]、假位置^[6-8]等。文献[2]中使用 k -匿名算法,通过第三方匿名服务器生成匿名区,保证查询用户在向LBS提供商发送请求时,有 $k-1$ 个位置数据与用户真实位置之间是无法区分的;然而匿名区的生成依赖于已知的背景知识,随着攻击者背景知识的增强,也可能造成隐私泄漏。文献[8]中提出了SpaceTwist增量近邻查询算法,使用客户机-服务器架构,摆脱了对第三方匿名服务器的依赖,在真实位置附近随机产生锚点,代替原有真实位置,进行增量近邻查询。文献[9]在文献[8]中算法的基础上,提出了一种双锚点

收稿日期:2020-01-03;修回日期:2020-03-05;录用日期:2020-03-11。

基金项目:国家自然科学基金资助项目(61972133);河南省中原千人计划中原科技创新领军人才项目(204200510021)。

作者简介:金波(1992—),男,河南信阳人,硕士研究生,CCF会员,主要研究方向:网络安全、位置隐私保护; 张志勇(1975—),男,河南新乡人,教授,博士生导师,博士,CCF高级会员,主要研究方向:网络空间安全、大数据、人工智能、可信计算、访问控制; 赵婷(1995—),女,山西长治人,硕士研究生,CCF会员,主要研究方向:应用密码学、云存储安全。

机制,利用第一个锚点的近邻查询供应空间与最小需求空间两个交点的中点作为第二个锚点,能有效提高查询命中率。文献[10]中提出了一种齐次增量近邻查询(Homogeneous Incremental Nearest Neighbor, HINN)算法,将需求空间扩大两倍,扩展检索区域,改善SpaceTwist算法中感兴趣区域围绕在锚点而不是真实位置的缺陷。但是,SpaceTwist及其改进算法中锚点的生成是随机的,位置隐私安全性难以度量和调节。文献[11]中提出了Geo-Indistinguishability位置保护机制,通过改进差分隐私模型,将Laplace机制应用到位置数据集中,是一种与背景知识无关且隐私强度可度量的位置隐私保护机制。文献[12]中提出了一种基于用户感兴趣区域的地理不可区分性位置扰动方法,根据给定的感兴趣区域对查询结果进行清洗,降低查询误差。虽然地理不可区分性机制能有效地保护位置隐私,但社交网络中使用差分隐私机制对位置数据添加噪声,用户上传到LBS服务器的是干扰位置,与传统的LBS近邻查询相比,查询的目标不再是具有真实位置的实体,例如:商场、餐厅,而是空间位置已经发生偏移的用户。现有的这些近邻查询方法考虑了查询位置因位置隐私保护导致位置偏移所带来的查询误差,但并没有考虑查询目标的位置偏移所带来的误差,存在严重的效用性问题。

针对以上问题,结合文献[8-9],本文首先根据地理位置的访问量,提出了一种用户位置隐私预算分配方法,该方法使用网格对用户的访问区域进行划分,以用户一定时间段内的访问量为依据,合理分配在对应区域的隐私预算,使用地理不可区分性机制对位置数据进行加噪,生成干扰位置;然后提出了一种组合增量近邻查询(Combined Incremental Neighbor Query, CINQ)算法,以保证供应空间包含查询目标的可能偏移区域,能有效降低因为查询目标位置发生偏移带来的误差。在真实数据集上进行实验验证了本文CINQ算法能够有效地提高近邻查询的命中率。

1 基于差分隐私的位置隐私保护

1.1 预备知识

定义1 差分隐私^[12-13]。差分隐私是Dwork在2006年提出的一种与背景知识无关的强隐私保护模型,适用于统计数据集,保证相邻数据集不会因为单个数据项的增加或者减少而导致隐私的泄漏,通过隐私预算 ϵ 的大小量化隐私保护程度,隐私预算越小,隐私保护程度越高,数据的可用性就越低;其实质就是对查询结果添加随机噪声,生成干扰数据。对于两个邻近数据集 D_1, D_2 ,则满足:

$$\Pr[M(D) \in S] \leq \exp(\epsilon) \cdot \Pr[M(D') \in S] \quad (1)$$

式中: M 表示随机函数, S 表示随机函数 M 的结果集。Laplace机制和指数机制是差分隐私中最常用的两种加噪机制,拉普拉斯机制适用于线性数据,指数机制适用于离散型数据。

定义2 地理不可区分性^[9]。它是标准差分隐私的变体,适用于单个位置数据,在以用户的真实位置为圆心、 r 为半径的圆形区域内,用户享有 ϵr 的隐私水平,隐私水平与隐私保护程度成反比, ϵr 越大,隐私水平越高,隐私保护强度则越小。在给定隐私半径 r 时,隐私保护强度要求越高,则 ϵ 越小。具

体定义如下:

$$M(x)(z) \leq e^{d(x,x')} M(x')(z) \quad (2)$$

式中: $x, x' \in X, z \in Z, X$ 为真实位置集合, Z 为可能出现的扰动位置集合; $d(x, x')$ 为两点之间的欧几里得距离。文献[9]

中在拉普拉斯机制的基础上进行改进,引入标准化因子 $\frac{\epsilon^2}{2\pi}$,将拉普拉斯机制延伸到二维空间,平面拉普拉斯机制的概率函数为:

$$D_\epsilon(x, z) = \frac{\epsilon^2}{2\pi} e^{-d(x, z)} \quad (3)$$

式中: $d(x, z)$ 表示 x, z 之间的欧几里得距离,然后将笛卡尔位置坐标转换为以真实位置 x 为原点的平面极坐标,使用干扰位置相对于真实位置的欧氏距离 r 和相对于极坐标的横轴夹角 θ 表示干扰位置。将式(3)转换为极坐标概率函数的形式为:

$$D_\epsilon(r, \theta) = \frac{\epsilon^2}{2\pi} e^{-\epsilon r} \quad (4)$$

推导出夹角 θ 和半径 r 的生成方法,其中 θ 可以表示成在 $[0, 2\pi)$ 区间;以 $\frac{1}{2\pi}$ 的均匀概率生成的随机数,半径 r 的计算公式为:

$$r = C_\epsilon^{-1}(\rho) = -\frac{1}{\epsilon} \left(W_{-1} \left(\frac{\rho - 1}{\epsilon} \right) + 1 \right) \quad (5)$$

式中: $W_{-1}(X)$ 函数表示朗伯 $W(X)$ 函数在区间 $(-\infty, -1)$ 的分支, ρ 是服从 $[0, 1]$ 均匀分布的随机数。

1.2 基于访问量的隐私预算分配

本文使用地理不可区分性机制生成干扰位置,在生成干扰位置之前,需要给用户的查询位置分配合理的隐私预算。由差分隐私的定义可知,位置隐私预算的大小代表着用户查询位置的敏感程度,位置敏感度越高,在生成干扰位置时则需要分配更小的隐私预算。用户在某区域的位置敏感度不仅与位置的自身特性相关,不同用户在相同区域的位置敏感度也存在差异,例如,相对于顾客而言,咖啡厅是休闲娱乐的场所,但对于咖啡厅工作人员,是他们工作的地方,两者在相同区域的位置敏感度存在较大差异。本文利用用户在一段时间内的位置访问量来计算位置的隐私预算,位置访问量能直接反映用户在该区域的敏感度,访问量越大,敏感度则越高,隐私预算则越小;但是,访问量也不能完全代表用户的位置敏感度,例如,正常情况下,人们去医院的次数比较少,但是医院区域的位置敏感度却很高,这和医院的自身特性相关,对于这些公有敏感区域,可以手动分配隐私预算(隐私预算的取值在0到1之间)。

通过网格化用户访问区域,统计在一定时间段内用户在不同区域的访问量,个性化计算用户访问位置的隐私预算。将用户访问区域以十字递进的方式划分为大小相等的网格,使用完全四叉树来存储每个单元格的信息。在完全四叉树中,叶子节点存储着单个用户在单元格区域的访问量,非叶子节点存储自身的空间范围以及子节点的索引信息。对用户区域进行网格化处理时,划分粒度可以动态调节,粒度越小,单元格的空间范围就越大,访问量可能就越大,位置敏感度就越

高,但位置敏感度的代表性会降低,反之亦然。用户区域网格化的模型如图 1 所示,每个单元格包含着用户在该区域的访问量数据和初始手动分配的隐私预算,其中使用 ∞ 表示未手动分配隐私预算。

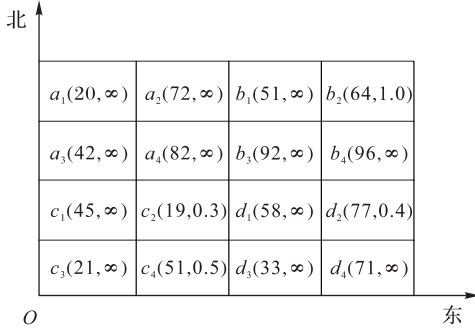


图 1 空间区域网格化

Fig. 1 Gridding of spatial regions

在对空间区域划分后,遍历四叉树中叶子节点,假设单个用户分配的总隐私预算为 E ,除手动划分隐私预算的单元格区域之外,每个单元格的区域隐私预算 ε_i 满足:

$$\varepsilon_i = \frac{1}{n_i} * \frac{E - \sum_j \varepsilon_j}{\sum_i \frac{1}{n_i}} \quad (6)$$

其中: n_i 为单元格区域的访问量; ε_j 为手动划分的隐私预算。 n_i 越大,分配的隐私预算 ε_i 则越少,隐私保护程度就越高。

已知位置区域的隐私预算,根据式(5)即可以计算真实位置 x 和扰动位置 z 之间的偏移量 r ,但 r 并不能取任意值,因为偏移量 r 越大,扰动位置的可用性就越低,为了保证数据的可用性,设置 r 的最大偏移量 $r_{\max}$,需保证 $r \leq r_{\max}$,伪代码如算法 1 所示。

算法 1 生成扰乱位置。

输入 真实位置节点 p ,最大偏移量 $r_{\max}$,隐私预算 ε ;

输出 加噪后的位置单元 p' 。

- 1) $r \leftarrow 0$;
- 2) Random ρ in $[0, 1]$, θ in $[0, 2\pi]$;
- 3) do
- 4) calculate $r \leftarrow C_{-1}(\rho)$;
- 5) until $r \leq r_{\max}$;
- 6) $p'.x = p.x + r * \cos(\theta)$;
- 7) $p'.y = p.y + r * \sin(\theta)$;
- 8) return p' ;

2 组合增量近邻查询

在第 1 章中,使用地理不可区分性机制对真实位置添加随机噪声,生成干扰位置,LBS 服务器记录的都是用户提交的扰乱位置,现有的近邻查询算法没有考虑到查询目标的位置扰动所带来的查询命中率降低的问题,如果直接在扰动位置数据集中进行近邻查询,命中率偏低。本文在 SpaceTwist 增量查询算法基础上,提出了一种组合增量近邻查询算法 CINQ,使用生成的干扰位置作为查询锚点。设用户的真实位置为 x ,需求空间半径为 R_{demand} ,供应空间的半径为 R_{supply} ,需

要保证: $R_{\text{supply}} \geq R_{\text{demand}} + \text{dis}(x, z)$,其中, $\text{dis}(x, z)$ 为真实位置和干扰位置之间的偏移量。然而,上面的条件只能在查询目标的位置未发生改变时才能保证较高的查询命中率,在社交网络中,查询目标的位置同样也发生干扰,在此基础上,需要扩大查询范围,满足 $R_{\text{supply}} \geq R_{\text{demand}} + \text{dis}(x, z) + r_{\max}$,其中 $r_{\max}$ 为最大偏移量,保证 R_{supply} 能够涵盖检索目标的可能偏移区域。由于查询范围扩大,也会产生大量的冗余位置数据,为了解决这个问题,首先对真实查询位置重复加噪,并根据生成的扰动位置进行增量近邻查询,由于每次查询都能涵盖大部分的需求空间以及可能的偏移区域,因此,通过组合查询的方式对多个近邻查询结果取交集,缩小查询结果的规模,能有效过滤冗余数据。

图 2(a)~(c)表示在真实位置数据集中 SpaceTwist 的查询过程,其中阴影区域代表供应空间。图(a)为查询的初始状态,需求半径 R_{demand} 为无穷大,需求空间为整个查询空间;图(b)为查询的中间状态,此时,供应空间在不断扩大,需求空间的范围在不断缩小;图(c)为查询结束的临界状态,此时,如果供应空间中包含的位置节点数大于或等于查询个数 k ,则查询结束;否则,进一步扩大需求空间。而在图(d)中,查询目标也添加了随机噪声,例如:真实位置 e 通过位置扰动后生成的干扰位置为 e' ,按照原来的 SpaceTwist 算法进行查询,图(d)的供应空间与图(c)相比,两者空间区域存在较大差异,导致查询命中率降低。图(e)中通过设置最大偏移量和扩大供应空间的查询范围,使供应空间能够包含查询目标的可能偏移区域,可提高查询命中率。在图(f)中,点 p, z 都是真实位置 x 生成的干扰位置,阴影区域为两点供应空间的交集,可以看出,相比图(e),图(f)中供应空间的区域范围在缩小,从而过滤掉部分的空间位置节点,但是包含在两个供应空间公共区域中的查询目标位置节点不会被过滤掉。组合增量近邻查询伪代码如算法 2 所示。

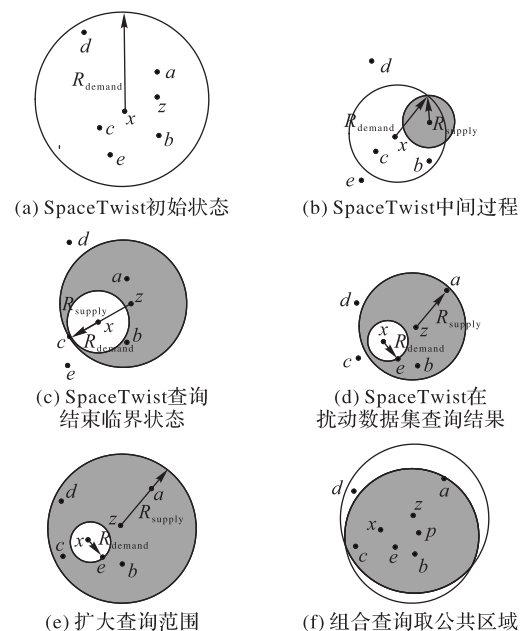


图 2 组合增量近邻查询

Fig. 2 Combined incremental neighbor query

算法2 组合增量近邻查询。

输入 真实位置 x , 干扰位置 z , 最大偏移量 $r_{\max}$, 查询目标数 K_{result} , 过滤次数 f_{num} ;

输出 过滤结果集 result 。

```

1)  $R_{\text{demand}} \leftarrow \infty$ ; //初始需求空间半径
2)  $R_{\text{supply}} \leftarrow 0$ ; //初始供应空间半径
3)  $\text{num} \leftarrow 0$ ; //初始检索结果个数
4) while ( $R_{\text{supply}} + \text{dis}(x, z) + r_{\max} > R_{\text{demand}}$ ) do
5)   Send an INN query to LBS server;
6)   for each  $q$  //遍历查询结果集
7)      $\text{num}++$ ;
8)     if ( $\text{dis}(z, q) < R_{\text{supply}}$ )
9)        $R_{\text{supply}} \leftarrow \text{dis}(z, q)$ ;
10)    end if
11)     $R_{\text{demand}} \leftarrow \text{dis}(x, q)$ ;
12)    insert  $q$  into  $\text{result}$ ;
13)  end for
14) end while
15) if  $\text{num} < K_{\text{result}}$  then
16)   expand the  $R_{\text{supply}}$ ;
17) end if;
18) for ( $i = 1; i < f_{\text{num}}; i++$ )
19)    $\text{result}' \leftarrow$  repeat generate perturbation location  $z$  and
      incremental query;
20)    $\text{result} \leftarrow \text{result} \cap \text{result}'$ ;
21) end for;
22) return  $\text{result}$ ;
```

3 实验与结果分析

实验在 MAC 系统上用 Matlab 实现, 运行环境为 Intel Core i5、CPU 2400MHz、8 GB 内存, 实验数据是 CyVOD^[14] 平台收集的 34 127 条位置数据。

3.1 性能分析

将本文 CINQ 算法与文献[3]中的 SpaceTwist 算法和文献[10]中的 HINN 算法进行比较, 采用以下两个指标来评价算法的有效性。

查询命中率 假设用户真实位置在真实位置集合近邻查询结果集为 p , 用户干扰位置在真实位置集合或干扰位置集合中近邻查询结果集为 p' , 则查询命中率表示为 $|p \cap p'|/|p|$ 。

响应时间 用户从发出近邻查询请求到获取查询结果之间的时间间隔。

在查询命中率的比较中, 由于用户在空间区域分布的不均匀性, 随机选择 6 个用户作为查询用户, 编号为 (1, 2, 3, 4, 5, 6), 通过 SpaceTwist 算法和本文 CINQ 算法, 在相同查询兴趣点数 $k = 8$ 的条件下, 比较命中率的变化情况。如图 3 所示, 在扰动位置数据集中, SpaceTwist 和 HINN 的命中率明显低于本文方案, 这是因为这二者都没有考虑到查询目标的位置偏移, 而本文 CINQ 算法则能有效地解决查询目标的位置偏移导致的查询命中率下降的问题, 扩大供应区域的查询范围, 包涵查询目标可能的偏移区域。

对于响应时间, 随机选择一个位置点作为用户查询位置, 在不同查询个数 k 条件下比较响应时间的变化情况, 如图 4 所示。在相同的查询位置条件下, 本文 CINQ 算法的响应时间比

SpaceTwist 算法长, 这是由于本文 CINQ 算法扩大了查询范围, 并增加了组合查询的过程; 但是结合命中率和响应时间两者而言, 在具有较高的命中率同时, 保证相对较短的响应时间, 是可以接受的。

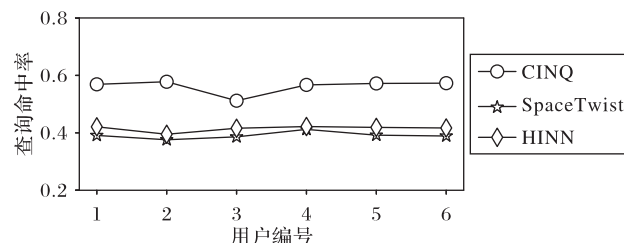


图3 查询命中率对比

Fig. 3 Comparison of query hit rate

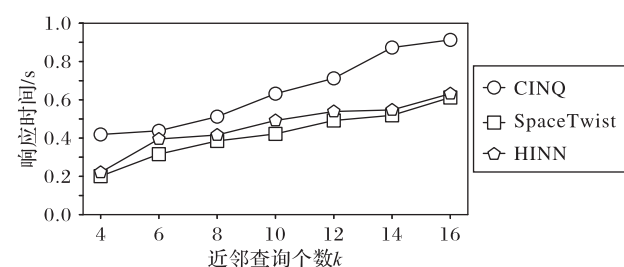


图4 响应时间对比

Fig. 4 Comparison of response time

3.2 组合查询次数对算法的影响

在通过组合查询过滤冗余数据时, 查询次数影响查询结果, 随机选择一个位置点作为用户查询位置, 近邻查询个数 $k = 8$, 在不同查询次数下, 比较对查询结果的影响, 如图 5 所示。在组合查询次数增多时, 冗余数据量会降低, 在多次查询取交集的过程中, 也会造成目标结果数据的丢失; 当组合查询次数等于 3 时, 查询结果具有较少的冗余数据量和较高的查询命中率。

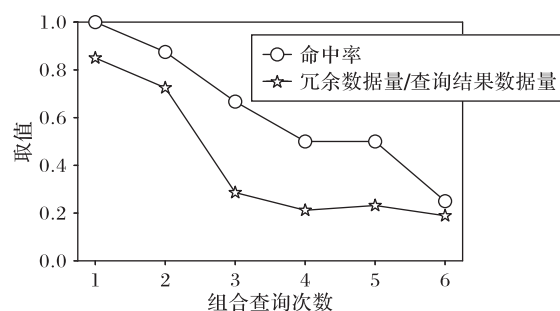


图5 组合查询次数对查询结果的影响

Fig. 5 Impact of combined query times on query results

4 结语

本文在基于地理不可区分性机制上, 提出了一种隐私预算分配方法, 能够根据用户的隐私需求, 个性化分配隐私预算; 并进一步提出了组合增量近邻查询算法 CINQ, 解决了传统近邻查询方法在扰动位置数据集中查询命中率偏低的问题, 显著提升了查询命中率。在下一步工作中, 如何在保证较高的命中率的同时, 保证较低的时间消耗和带宽消耗, 将是研究的重点所在。

参考文献 (References)

- [1] 万盛, 李凤华, 牛犇, 等. 位置隐私保护技术研究进展[J]. 通信学报, 2016, 37(12): 124-141. (WAN S, LI F H, NIU B, et al. Research progress on location privacy-preserving techniques [J]. Journal on Communications, 2016, 37(12): 124-141.)
- [2] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial a temporal cloaking[C]// Proceedings of the 2003 International Conference on Mobile Systems, Applications and Services. New York: ACM, 2003:31-42.
- [3] CHOW C Y, MOKBEL M, AREF W G. Casper*: query processing for location services without compromising privacy [J]. ACM Transactions on Database Systems, 2009, 34(4): No. 24.
- [4] BERESFORD A R, STAJANO F. Mix zones: user privacy in location-aware services [C]// Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops. Piscataway: IEEE, 2004:127-131.
- [5] HOH B, GRUTESER M. Protecting location privacy through path confusion [C]// Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks. Piscataway: IEEE, 2015:194-205.
- [6] HONG J I, LANDAY J A. An architecture for privacy-sensitive ubiquitous computing [C]// Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services. New York: ACM, 2004: 177-189.
- [7] JUNG K, JO S, PARK S. A game theoretic approach for collaborative caching techniques in privacy preserving location-based services [C]// Proceedings of the 2015 International Conference on Big Data and Smart Computing. Washington, DC: IEEE Computer Society, 2015, 1: 59-62.
- [8] YIU M L, JENSEN C S, HUANG X, et al. SpaceTwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services [C]// Proceedings of the 24th International Conference on Data Engineering. Piscataway: IEEE, 2008:366-375.
- [9] SUN R, XIANG G, GAO Q, et al. A study of location privacy protection about k interesting points query based on double anchors [C]// Proceedings of the 2018 Ubiquitous Positioning, Indoor Navigation and Location-Based Services. Piscataway: IEEE, 2018: 1-7.
- [10] ZHOU C, MA C, YANG S, et al. A location privacy preserving method based on sensitive diversity for LBS [C]// Proceedings of the 11th IFIP International Conference on Network and Parallel Computing, LNCS 8707. Berlin: Springer, 2014:409-422.
- [11] ANDRÉS M E, BORDENABE N E, CHATZIKOKOLAKIS K, et al. Geo-indistinguishability: differential privacy for location-based systems [C]// Proceedings of the 2013 ACM Conference on Computer and Communications Security. New York: ACM, 2013: 901-914.
- [12] 罗惠雯, 龙士工. 基于用户感兴趣区域的地理不可区分性的位置扰动算法[J]. 计算机应用, 2020, 40(3): 760-764. (LUO H W, LONG S G. Location perturbation algorithm based on geo-indistinguishability of user's region of interest [J]. Journal of Computer Applications, 2020, 40(3): 760-764.)
- [13] DWORK C, KENTHAPADI K, MCSHERRY F, et al. Our data, ourselves: privacy via distributed noise generation [C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 4004. Berlin: Springer, 2006:486-503.
- [14] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating noise to sensitivity in private data analysis [C]// Proceedings of the 3rd Theory of Cryptography Conference, LNCS 3876. Berlin: Springer, 2006:265-284.
- [15] ZHANG Z, SUN R, ZHAO C, et al. CyVOD: a novel trinity multimedia social network scheme [J]. Multimedia Tools and Applications, 2016, 76(18):18513-18529.

This work is partially supported by the National Natural Science Foundation of China (61972133), the Project of Leading Talents in Science and Technology Innovation for Central Plains of Thousands of People Plan in Henan Province (204200510021).

JIN Bo, born in 1992, M. S. candidate. His research interests include network security, location privacy protection.

ZHANG Zhiyong, born in 1975, Ph. D., professor. His research interests include cyberspace security, big data, artificial intelligence, trusted computing, access control.

ZHAO Ting, born in 1995, M. S. candidate. Her research interests include applied cryptography, cloud storage security.