基于增量近邻查询的位置隐私保护方法

王鹏飞 李千目 朱保平
(南京理工大学计算机科学与工程学院 南京 210094)

摘 要 随着基于位置的服务在人们日常生活中日益普及,个人的位置隐私正面临着严重的威胁。基于增量近邻查询思想,结合反映人口分布的路网环境,提出了一种新的位置隐私保护方法。该方法通过P2P系统结构摆脱了传统中心服务器结构的局限,解决了单点脆弱性问题,同时可以保证在P2P系统结构中代理用户非可信情况下用户的隐私安全。最后,在路网密度不同的模拟数据集上对提出的方法进行了实验,结果验证了该方法的有效性。

关键词 基于位置的服务,位置隐私,路网环境,P2P网络,增量近邻查询
中图法分类号 TP309.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.3.033

Location Privacy Protection Method Based on Incremental Nearest Neighbor Query

WANG Peng-fei LI Qian-mu ZHU Bao-ping
(School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract With the growing popularity of location-based services in people's daily life, personal location privacy is facing a serious threat. This paper proposed a new location privacy protection method based on incremental nearest neighbor query, which considers network environment reflecting the population distribution. Using the P2P system structure, the method gets rid of the limitations of traditional central server architecture and solves the vulnerability of single point. Meanwhile, this method can guarantee the user's privacy in the case that proxy user in P2P system architecture is non-credible. Finally, the proposed method was evaluated in simulated data sets of different road density and the result verifies the validity of the method.

Keywords Location-based services, Location privacy, Road network environment, P2P networks, Incremental nearest neighbor queries

1 引言

近年来,随着智能移动终端的高速普及以及无线通信技术的不断发展,基于位置的服务(Location Based Service, LBS)[1]渗透到了人们生活的方方面面。基于位置的服务是指移动终端利用各种定位技术获得自己当前的位置,并提出与用户位置有关的服务。这种服务给人们的生活带来了极大的方便,潜移默化地改变了人们的生活方式。随着LBS的快速发展,位置隐私问题日益受到人们的关注。例如在用户享受最近邻查询"离我最近的医院在哪里"、最短路径查询"XX餐厅的最近路径"等服务的过程中,攻击者通过截获用户的查询信息,能够推测出用户的个人信息、位置信息等。这对用户个人的隐私造成了巨大威胁,因而位置隐私保护问题亟待解决。

用于位置隐私保护的系统结构包括客户端服务器结构、中心服务器结构、移动P2P结构等。基于客户端服务器结构,用户可以向位置服务器发送k个位置信息,其中包括用户的真实位置和$k-1$个假位置,使得位置服务器无法分辨出用户的真实位置[2];用户还可以构造出包括用户位置的匿名区[3],位置服务器根据用户提交的匿名区无法定位用户的准确位置。客户端服务器结构易于实现,但是移动终端必须具备强大的计算能力和存储能力,而且只利用自身的知识进行匿名,无法利用周边环境中其他用户的位置信息,所以不仅容易受到攻击者的攻击,而且会造成可共享资源的浪费。文献[4,5]基于中心服务器结构提出了位置k匿名技术,即用户提出位置服务的需求时,不是直接发送包括自身确切位置的单个LBS请求到位置服务器,而是采用了匿名服务器,该匿名服务器收集k个相邻用户的请求并构造匿名区发送给位置服务器。由于匿名服务器需不断进行匿名处理以及查询结果的求精,其负担过大,而且当匿名服务器被攻击者控制或者攻击的时候,会给整个系统带来严重的隐私泄露问题。移动P2P结构不需要固定基础设施,用户提出服务请求时,通过多跳路由随机选定一个对等点作为代理,然后该对等点把用户的服务请求发送给服务器,服务器将查询结果集返回给该对等点,

到稿日期:2014-04-08 返修日期:2014-07-16 本文受国家自然科学基金:融合泛在网的协同防护与安全风险预测(61272419),江苏省自然科学基金项目:无线传感网的全域安全检测技术(BK2011370),中国博士后基金项目:泛在网络环境下的智能安全防护(2012M521089),江苏省博士后资助计划:无线感知网络系统的可信控制与防危分析(1201044C),江苏省产学研联合创新基金-前瞻性联合研究项目(BY2012022)资助。
王鹏飞(1989—),男,硕士生,主要研究方向为信息安全,E-mail:763395288@qq.com;李千目(1979—),男,博士,教授,主要研究方向为网络与信息安全;朱保平(1964—),男,博士,副教授,主要研究方向为信息安全与理论。

该对等点对查询结果过滤后返回给查询用户[6]。该体系结构适用于无固定基础设施的移动网络，如 Ad hoc，但其假定了每个对等点都是可信任的，当对等点中存在攻击者时，用户的位置隐私保护就难以保证。因此现有的技术和方案已经难以满足用户的要求，研究在合适的系统结构下的有效位置隐私保护方法成为一个日益迫切的问题。

本文在 P2P 系统结构下结合路网环境，改进了增量近邻查询算法来保护位置隐私，其优势在于：1)用户在寻求代理用户时首先参考路网密度构造匿名区，以匿名区代替真实位置来保证 P2P 系统结构下对等点非可信时的位置隐私需求；2)查询用户根据兴趣点的分布情况估算出查询点的位置，使得通讯开销可控的同时保证返回的结果集满足查询用户的要求；3)对增量近邻查询过程进行了改进，使查询可以覆盖查询用户期望的 k 近邻结果范围。

2 基于增量近邻查询的位置隐私保护方法

本文提出的位置隐私保护方法的系统结构由移动终端和位置服务器组成，如图 1 所示。移动终端具备基本的定位功能，其不仅能够通过移动基站与位置服务器通信，还能与其他用户进行 P2P 通信，其中发起查询请求的是查询用户（记为 U_c），接收查询用户请求并向位置服务器提出增量近邻查询的是代理用户（记为 U_a）。位置服务器提供基于位置的近邻查询、范围查询等服务。

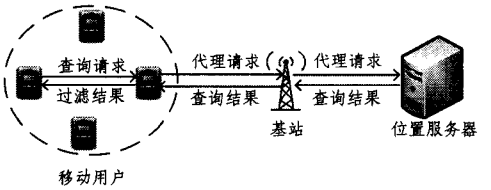


图 1 位置隐私保护方法系统结构

定义 1（查询请求 Q_c） 查询用户 U_c 以 $Q_c=\{u_{id}, o, r, s, con\}$ 的形式向代理用户 U_a 发起查询请求，其中 u_{id} 表示用户标识符，$o=(x,y)$ 表示 U_c 的匿名区圆心点经纬度坐标，r 表示匿名区半径，s 表示 U_c 估算出的增量近邻查询的查询点，con 表示 U_c 的查询请求内容。

定义 2（代理请求 Q_a） 代理用户 U_a 以 $Q_a=\{u_{id}, s, con\}$ 的形式向位置服务器发出代理查询请求，其中 u_{id} 表示代理用户的标识符，s 表示从查询请求 Q_c 中获得的增量近邻查询的查询点，con 表示从查询请求 Q_c 中获得的查询用户 U_c 的查询内容。

基本思想：每个用户基于无线通讯协议自组织成一个 P2P 网络，查询用户 U_c 进行 LBS 查询时，首先通过移动终端获取自己的真实位置 q；然后 U_c 与位置服务器通信，获取匿名区和查询点并形成查询请求 Q_c；U_c 在 P2P 近邻列表中随机选择一个代理用户 U_a，U_a 与位置服务器通信建立连接，发起增量近邻查询，得到查询结果集；最后 U_a 将过滤后的查询结果返回给 U_c。

2.1 匿名区的设计

P2P 网络不能保证代理用户 U_a 的可信度，所以查询用户 U_c 发出 LBS 查询时，向 U_a 提出的查询请求不能包含用户的准确位置。U_c 需要形成大小适中的匿名区，随机选取容易导致 U_c 与 U_a、U_a 与位置服务器的通讯开销不可控。本文提出的匿名区构造方法参考了路网密度，因为路网密度和人口密度有正相关关系，路网密集的地方人口密度也相应较大。而且在实验中，路网信息相对稳定且是现成的，而人口流动频繁，信息较难获取。

定义 3（路网粒度 λ） 设 G_i 为平面空间区域中的任意一个子空间区域，s 为 G_i 的周长，l 为 G_i 内道路总长度，则定义 $\lambda=l/s$ 为 G_i 的路网粒度。

为了算法容易实施且不失一般性，我们把位置服务器负责的二维空间视为一个正方形 G，然后十字递归分割 G，直到分割成的每个正方形空间的 λ 不大于一个给定值。U_c 向位置服务器发出 LBS 请求前先从位置服务器获得对 G 的分割结果。为了减小 U_c 与位置服务器的通信开销，我们使用四叉树结构来存储这些基本单元空间，四叉树中每个节点对应一块分割区域，且每个节点的数据域中存储区域中心点坐标、区域边长、区域内道路长度等信息，区域中心点坐标、区域边长用于确定对应的分割区域，区域内道路长度用于估算查询点。四叉树结构中叶节点对应基本单元空间，非叶节点对应需要继续分割的区域。U_c 得到分割结果后递归搜索该四叉树，找到自己所在的单元空间，并将该单元空间的外接圆区域作为 U_c 的匿名区。

2.2 查询点估算方法

代理用户 U_a 需要合适的查询点来向位置服务器发起增量近邻查询请求，随机选择查询点可能会带来两种情况：1)查询点距离匿名区距离过小，增量近邻查询结束时返回的结果集数量过少，不能满足查询用户 U_c 的 k 近邻需求；2)查询点与匿名区距离过大，增量近邻查询结束时返回的结果集过大，消耗大量通讯开销，影响服务响应时间。

本文提出的增量近邻查询要求查询结果集维持在一个相对稳定的规模，使得通讯开销可控的同时保证返回的结果集满足 U_c 的要求。查询点估算方法为：U_c 向位置服务器请求区域分割结果时发送查询主题（如餐馆、医院等）至位置服务器，位置服务器返回区域分割四叉树的同时附带了数据集上该主题的密度因子 α（单位长度的道路上分布的兴趣点数）；根据 α 和单元空间的道路长度计算出每个单元空间中分布的兴趣点数；以匿名区所在的单元空间为中心向四周扩大搜索范围，直到搜索范围内估算的兴趣点数满足查询用户的需求；构造此搜索范围的最小外接圆，把该外接圆上的任意一点作为查询点。这样可以解决查询点与匿名区距离过大或过小的问题，具体分析如 2.3 节所述。

2.3 增量近邻查询

文献[8]提出的 SpaceTwist 方法使用了增量近邻查询的思想。如图 2 所示，o 为查询用户 U_c 的真实位置，s 为 U_c 随机选取的查询点，位置服务器以 s 为中心进行近邻查询，并不断扩大查询范围，返回的查询结果与 s 的距离不断增加。SpaceTwist 方法提出了需求空间（Demand Space）和供应空间（Supply Space）的概念。需求空间是以 o 为圆心，当前返回的查询结果中离 o 最近的查询结果与 o 的距离为半径的圆形区域。供应空间是以 s 为圆心，最近返回的查询结果（即当前距离 s 最远）与 s 的距离为半径的圆形区域。SpaceTwist 增量近邻查询的基本思路为：U_c 初始化需求空间半径 R 为∞、初

始化供应空间半径 γ 为 0，计算 s 到 o 的距离 L；位置服务器依次将近邻查询结果 $\{p_1, p_2, \cdots, p_n\}$ 返回给 U_c；U_c 分别计算返回的查询结果与 s 和 o 的距离，更新 R、γ，直到满足 $\gamma \geqslant R+L$，则供应空间完全包含需求空间，查询结束。

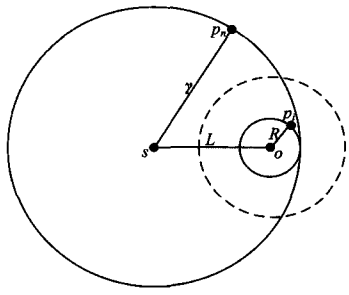


图 2　增量近邻查询的临界情况图

根据对该算法的描述，可以得到如图 2 所示的临界情况，此时 p_n、p_i 满足 $dis(p_n,s)=dis(p_i,o)+L$，在返回的结果序列中 p_i 距离 o 点最近，而 p_n 距离 s 点最远（即最后返回的结果点），此时圆 s 正好完全包含实线圆 o。实线圆 o 范围内只包含了最近邻结果 p_i，所以 o 点的期望 k（k>1）近邻查询结果范围必然大于实线圆 o 的范围，2.2 节中我们可以估算出期望的查询范围，在图 2 中用虚线圆表示，显然该增量近邻查询（圆 s）无法完全覆盖期望的查询范围。

现在问题的关键是如何使增量近邻查询完全覆盖期望的查询范围，根据 2.2 节中查询点估计的算法，U_c 期望的 k 近邻结果在以匿名区中心 o 为圆心、查询点与 o 的距离为半径的圆形区域内。因此本文对上述增量近邻查询方法进行改进，使需求空间始终不小于该圆形区域，这样保证增量近邻查询结束时的范围包含 U_c 期望的 k 近邻结果范围（即图 2 中的虚线圆区域）。

定义 4（供应空间）　以查询点 s 为圆心的圆形空间，其半径 γ 为最近返回的查询结果与 s 的距离。

定义 5（需求空间）　与查询用户 U_c 的匿名区具有相同圆心 o 的圆形空间，其半径 R 为位置服务器返回查询结果 p_i 到匿名区圆心 o 的距离，其中 p_i 为已返回的查询结果中最接近 o 同时与 o 的距离又不小于 $dis(s,o)$ 的查询结果点，即 R 满足：

$$R=\min(dis(p_i,o)\,|\,dis(p_i,o)\geqslant dis(s,o), i\in[1,m]) \quad (1)$$

这样能保证需求空间始终不小于 U_c 期望的 k 近邻结果范围。其中 m 表示位置服务器当前已返回的结果数，p_i 表示其中的任一查询结果，min() 表示取最小值，$dis(x,y)$ 表示两点之间的距离。

改进的增量近邻查询算法：U_a 收到 U_c 的查询请求后形成代理请求 Q_a，并将 Q_a 发送给位置服务器；U_a 初始化供应空间半径 γ 为 0，初始化需求空间半径 R 为∞，计算查询点到需求空间圆心的距离 $dis(s,o)$；位置服务器以查询点为中心进行近邻查询并不断将结果返回给 U_a；U_a 计算返回的查询结果与查询点的距离，更新 γ；U_a 计算返回的查询结果与匿名区中心的距离 $dis(p_i,o)$，若 $dis(p_i,o)$ 不小于 $dis(s,o)$ 且小于当前的 R，则更新 R 使其等于 $dis(p_i,o)$；每次更新 γ 和 R 后检查是否满足 $\gamma \geqslant R+dis(s,o)$，若满足则供应空间完全包含需求空间，查询结束，算法描述如表 1 所列。

表 1　增量近邻算法设计

```
输入：匿名区中心坐标 o，查询点坐标 s，查询内容 con
输出：查询结果集 result
result←new max-heap{p,dis(o,p)};
R←∞;
γ←0;
send an INN query with Qa={uid,s,con};
while (R+dis(o,s) >γ) do
    p←the new point from the server;
    γ←dis(s,p);
    if(dis(p,o)>=dis(s,o) and dis(p,o)<R)
        R←dis(p,o);
    Insert into result with {p,dis(o,p)};
Terminate the INN query at the server
Return result
```

根据对改进的增量近邻查询算法的描述，可以得到如图 3 所示的临界情况。此时的 p 和 p_n 满足 $dis(p_n,s)=dis(p,o)+dis(s,o)$，以 o 为圆心、R 为半径的圆为查询结束时的需求空间的范围，根据需求空间的定义，p 是虚线圆外最接近虚线圆的一个查询结果，这样可以在保证查询范围覆盖 U_c 期望的 k 近邻结果范围的同时尽量缩小查询范围，减小通信开销。我们将查询结束时的 p 称为查询临界点。

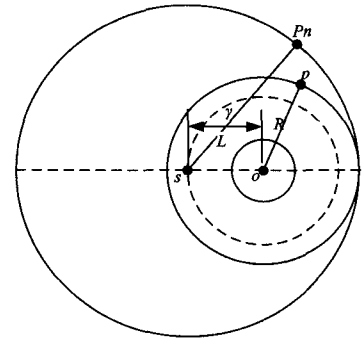


图 3　改进的增量近邻查询临界图

3　性能分析

3.1　隐私保护度分析

在本文提出的位置隐私保护方法的系统结构中，代理用户 U_a 和位置服务器都是非可信的，所以从这两个方面分析提出的方案的隐私保护度。

U_a 是非可信的意味着攻击者可以从 U_a 处截获查询请求 $Q_c=\{u_{id}, o, r, s, con\}$、位置服务器返回的查询结果集 $\{p_1, p_2, \cdots, p_n\}$ 等信息。攻击者可以从 Q_c 中解析出 U_c 的身份标识信息 u_{id}，在没有背景知识进行关联攻击时攻击者无法推断出用户的身份信息。此外攻击者可以获取以 o 为圆心、r 为半径的匿名区，接着攻击者可以根据结果集 $\{p_1, p_2, \cdots, p_n\}$ 构造 Voronoi 图，根据 Voronoi 图的性质，U_c 肯定位于其中的一个生成元 $V(p_i)$ 中。假设与匿名区有重合的 Voronoi 图生成元个数为 $m(m<n)$，则推断出 U_c 在某个生成元 $V(p_i)$ 中的概率为 $1/m$，且无法推断出准确的位置。所以本文提出的方法可以保证在 P2P 系统结构下对等点非可信时的位置隐私。

再从位置服务器上的信息被攻击者截获的角度分析本方案的隐私保护度。位置服务器主要进行的是相对查询点的增量近邻查询，所以我们主要分析增量近邻查询的隐私保护度。对攻击者有用的信息包括查询点 s 和有序查询结果集 $\{p_1, p_2, \cdots, p_n\}$，攻击者假设 $p_i(1\leqslant i\leqslant n)$ 为查询临界点，根据增量

近邻查询的查询结束条件，查询用户 q 的位置范围满足下面的条件：

$$dis(s,p_{n-1})<dis(q,p_i)+dis(q,s)\leqslant dis(s,p_n) \quad (2)$$

其中，p_i 和 s 是定值，q 到 p_i 和 s 的距离之和大于定值 $dis(o,p_{n-1})$ 且小于等于定值 $dis(o,p_n)$。根据椭圆的定义，q 位于两椭圆 $f(p_i,s,p_{n-1})$ 和 $f(p_i,s,p_n)$ 范围之间，则攻击者推测出查询用户位置的概率 $P(p_i)$ 为：

$$P(p_i)=\frac{1}{n}\times\frac{f(p_i,s,p_n)-f(p_i,s,p_{n-1})}{\pi\times dis(s,p_n)^2} \quad (3)$$

3.2 服务质量分析

本文提出的位置隐私保护方法的服务质量主要从查询效率和服务精度两方面考虑。在查询效率方面，本方案采用了自组织的 P2P 网络，相对于中心服务器结构来说，非中心化的 P2P 网络对并发性的查询请求提供了负载均衡的保障，不会成为系统性能提升的瓶颈。此外，代理用户请求增量近邻查询前，通过估算 k 近邻结果范围来选择查询点，有效控制了供应空间过大时的通信开销。在服务精度方面，代理用户与位置服务器的增量近邻查询属于精确位置查询方法，可以准确得到基于用户位置的近邻结果。

4 实验

实验使用 Thomas Brinkhoff 路网数据生成器[11]对路网进行模拟。为了对比不同路网密度对提出方案的影响，实验采用了两个不同的实验数据集：德国奥登堡(Oldenburg)公路网络数据(记为 S_{OB})和美国圣华金(San Joaquin)公路网络数据(记为 S_{SJ})，两个数据集的基本参数如表 2 所列。由路网粒度 λ 的计算公式 $\lambda=l/s$ 得到 S_{OB} 的路网粒度为 139.343，S_{SJ} 的路网粒度为 17.563。路网粒度主要是反映移动对象和兴趣点的密集程度，为了实验容易实施，我们设定移动对象、兴趣点与道路长度成正比，设定两个数据集上的兴趣点密度因子 α 都为 50，则 Thomas Brinkhoff 路网数据生成器为 S_{OB} 生成 14070 个移动对象和 703500 个兴趣点(POIs)，为 S_{SJ} 生成 48246 个移动对象和 2412300 个兴趣点，并且这些移动对象和兴趣点都沿着道路随机分布。实验设定查询用户期望返回的查询结果数 k 为 20。

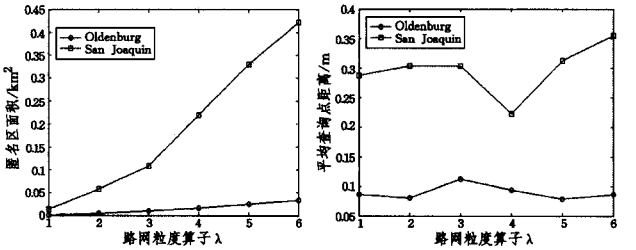
表 2 两个实验数据集参数对比

参数	SOB	SSJ
顶点数	6105	18496
边数	7035	24123
区域长/m	26915	716904
区域宽/m	23572	656570
路网粒度	139.343	17.563

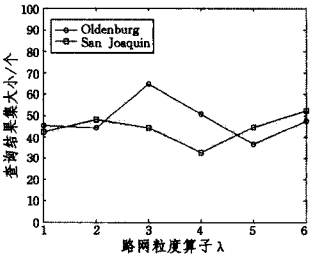
4.1 路网密度对算法的影响

实验分别在路网密度不同的两块数据集上进行，随机选取 100 个点作为查询用户的位置，这 100 个用户分别计算不同 λ 下的匿名区面积、匿名区中心到查询点的距离以及增量近邻查询结果集大小(即增量近邻查询满足结束条件时位置服务器返回的结果数而非查询用户得到的结果数)。

如图 4(a)所示，路网粒度 λ 与匿名区大小呈正相关，所以路网粒度越大，为得到匿名区需要分割的次数越小，且在相同路网粒度 λ 下，路网密度越大的数据集分割成的平均匿名区面积越小。如图 4(b)所示，同一数据集中不同路网粒度 λ 下估算的查询点与匿名区中心的距离在一个定值处上下波动，且在相同路网粒度 λ 下，路网密度越大的数据集估算出的查询点距离匿名区越近。如图 4(c)所示，在不同数据集上不同的路网粒度 λ 下，返回的查询结果集都大概维持在一个定值。这是因为在确定查询点时，我们估算出了查询用户期望 k 近邻结果范围，查询结束时供应空间能覆盖该范围，这样可以使得通信开销可控的同时保证返回的结果集满足查询用户的要求。



(a)不同 λ 时的匿名区面积　(b)不同 λ 时的查询点距离

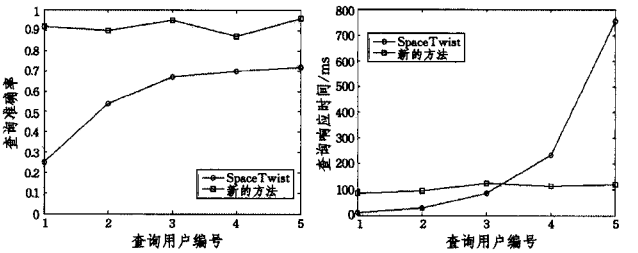


(c)不同 λ 时的结果集大小

图 4

4.2 与 SpaceTwist 算法的性能对比

我们从查询准确率和查询响应时间两方面对比分析 SpaceTwist 算法与本文提出的方法的性能。其中查询准确率是用户实际的 k 近邻结果在返回的结果中占的比例；查询响应时间是从查询用户发出查询请求到收到查询结果的时间。实验随机选取 Oldenburg 路网数据集中的 5 个用户为查询用户(依次编号为 1,2,3,4,5)，重复执行 SpaceTwist 算法和本文提出的算法 100 次。SpaceTwist 算法的查询点是随机选取的，为了便于实验观察，我们设定 SpaceTwist 算法的查询点与查询用户的距离(单位 m)分别为 10、50、100、200、400，统计每次实验的查询准确率和查询响应时间，并计算每个用户的平均值，如图 5 所示。



(a)与 SpaceTwist 的查询准确率对比　(b)与 SpaceTwist 的响应时间对比

图 5

图 5(a)反映了两种方法在查询准确率上的差异，用户通过新的方法得到的查询结果和实际的 k 近邻结果基本相符，准确率达到了 90%左右；而 SpaceTwist 的查询准确率随着查询点距离的增加将逐渐上升并趋于一个稳定值，但始终达不到新的方法的准确率。根据 2.3 节的分析，SpaceTwist 的查

(下转第 184 页)

[C]// 2013 IEEE 29th International Conference on Data Engineering Workshops (ICDEW). IEEE, 2013: 318-321

[15] Alamri S, Taniar D, Safar M, et al. Spatiotemporal indexing for moving objects in an indoor cellular space[J]. Neurocomputing, 2013, 122: 70-78

[16] Alamri S, Taniar D, Safar M, et al. A connectivity index for moving objects in an indoor cellular space [J]. Personal and Ubiquitous Computing, 2014, 18(2): 287-301

[17] Yang B, Lu H, Jensen C S. Probabilistic threshold k nearest neighbor queries over moving objects in symbolic indoor space [C]// Proceedings of the 13th International Conference on Extending Database Technology. ACM, 2010: 335-346

[18] Xu J, Guting R H. MWGen: a mini world generator[C]// 2012 IEEE 13th International Conference on Mobile Data Management (MDM). IEEE, 2012: 258-267

[19] http://www.modulargenius.com/default.aspx

(上接第 161 页)

询范围无法覆盖用户期望的 k 近邻结果的范围，而新的方法首先估算出 k 近邻结果范围，并将需求空间定义为不小于该范围，所以查询结束时得到的查询结果能基本满足实际情况。

算法复杂度和结果集的通信开销都会影响到如图 5(b)所示的查询响应时间。新的方法由于返回的结果数稳定，其响应时间也相对稳定；而 SpaceTwist 在查询点距离增加时，返回结果数迅速增加，查询响应会变得很慢。但在算法复杂度方面，新的方法需要构造匿名区、估算查询点，所以在返回相同结果数时的响应时间比 SpaceTwist 的更多，但这些时间消耗完全在可以承受的范围内。

结束语 本文提出了一种新的基于增量近邻查询思想的位置隐私保护方法，该方法使用 P2P 系统结构，查询用户委托代理用户完成查询请求，并且考虑了路网环境对查询结果的影响。本文提出的方法与现有的 SpaceTwist 方法相比具有以下优点：

1)查询用户以匿名区代替真实位置向代理用户发起查询请求。移动 P2P 结构不能保证每个对等点是可信的，用户发起查询请求时要将请求发送给代理用户，为了防止不可信的代理用户带来的隐私威胁，用户在寻求代理用户前首先要构造匿名区，以匿名区代替真实位置来保证位置隐私需求，而且查询用户在构造匿名区时考虑了路网密度因素。

2)通过估算用户期望的 k 近邻查询范围来确定增量近邻查询的查询点。代理用户向位置服务器发起以查询点为中心的增量近邻查询，在 SpaceTwist 方案中，查询点是随机选择的，这样会带来查询通讯开销和查询结果集不可控制的问题。本文考虑了路网密度对查询结果的影响，通过估算用户期望的 k 近邻查询范围来确定增量近邻查询的查询点。

3)增量近邻查询可以覆盖查询用户期望的 k 近邻结果范围。确定了查询点之后，代理用户向位置服务器提出增量近邻查询，本文对 SpaceTwist 方案中的增量近邻查询进行了改进，改变了需求空间的定义和查询结束的条件，使查询范围可以覆盖查询用户期望的 k 近邻结果范围。

参 考 文 献

[1] 周傲英，杨彬，金澈清，等. 基于位置的服务：架构与进展[J]. 计算机学报，2011，34(7)：1155-1171

[2] Kido H, Yanagisawa Y, Satoh T. An anonymous communication technique using dummies for location-based services[C]// International Conference on Pervasive Services, 2005 (ICPS'05). IEEE, 2005: 88-97

[3] 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. ACM, 2003: 31-42

[4] Gedik B, Liu L. Protecting location privacy with personalized k-anonymity: Architecture and algorithms[J]. IEEE Transactions on Mobile Computing, 2008, 7(1): 1-18

[5] Mokbel M F, Chow C Y, Aref W G. The new Casper: query processing for location services without compromising privacy[C]// Proceedings of the 32nd International Conference on Very Large Data Bases. VLDB Endowment, 2006: 763-774

[6] 黄毅，霍峥，孟小峰. CoPrivacy：一种用户协作无匿名区域的位置隐私保护方法[J]. 计算机学报，2011，34(10)：1976-1985

[7] Li Qian-mu, Li Jia. Rough Outlier Detection Based Security Risk Analysis Methodology[J]. China Communications, 2012, 5(7): 14-21

[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]// IEEE 24th International Conference on Data Engineering, 2008 (ICDE 2008). IEEE, 2008: 366-375

[9] Pan X, Xu J, Meng X. Protecting location privacy against location-dependent attacks in mobile services[J]. IEEE Transactions on Knowledge and Data Engineering, 2012, 24(8): 1506-1519

[10] Li Qian-mu, Zhang Hong. Information Security Risk Assessment Technology of Cyberspace: a Review[J]. Information- an International Interdisciplinary Journal, 2012, 15(11): 4677-4684

[11] Brinkhoff T. A framework for generating network-based moving objects[J]. GeoInformatica, 2002, 6(2): 153-180

[12] Li Qian-mu, Hou Jun, Qi Yong, et al. The Rule Engineer Model on the high-speed processing of Disaster Warning Information [J]. Disaster Advances, 2012, 5(4): 432-437

[13] Shin K G, Ju X, Chen Z, et al. Privacy protection for users of location-based services [J]. Wireless Communications, IEEE, 2012, 19(1): 30-39

[14] Li Qianmu. Mulitiple QoS Constraints Finding Paths Algorithm in TMN[J]. Information-an International Interdisciplinary Journal, 2011, 14(3): 731-738

[15] Li Qian-mu, Hou Jun, Qi Yong. A classification matching and conflict resolution method on meteorological disaster monitoring information[J]. Disaster Advances, 2013, 6(1): 415-421

[16] 蔡朝晖，张健沛，杨静. 一种基于多态关联挖掘的位置服务优化查询方法[J]. 计算机科学，2014，41(1)：286-289