基于不可信环境的移动位置隐私保护

刘学军 陈玉凤 李 斌
(南京工业大学电子与信息学院 南京 211800)

摘 要 近年来,随着移动计算和位置设备的发展,位置隐私保护受到学术界的广泛关注,人们提出很多匿名算法来保护用户的隐私信息。但是现有的方法要么不适用于移动环境,要么没有考虑现实不可信环境。针对这些问题提出了基于博弈论的动态规划匿名算法 Dynamic_p。此方法是在已有的可解决不可信环境下的位置隐私保护 Privacy_1[8]方法基础上提出的,通过将匿名组先组建成匿名树,然后从下到上,子节点与父节点博弈算出锚点。层层递归,最后算出整个匿名组的锚点。用户通过使用锚点代替实际位置来发起位置近邻查询,通过概率统计选出候选位置,最后通过位置计算算出最终的理想位置点。仿真实验表明,此方法在位置匿名方法上有更好的处理效率,并且能应用于移动的不可信环境中。

关键词 移动计算,位置服务,隐私保护,博弈,动态规划
中图法分类号 TP311 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.2.023

Mobile Location Privacy Protection Based on Untrusted Environment

LIU Xue-jun CHEN Yu-feng LI Bin
(College of Electrionc and Information, Nanjing Tech University, Nanjing 211800, China)

Abstract With the development of mobile computing and location equipment technologies, location privacy protection receives extensive attention from academia in recent years. A lot of anonymity algorithm has been put forward to protect users' privacy information. However, the existing methods is either not suitable for mobile environment, or do not consider the untrusted environment. In light of these problems, this paper put forward Dynamic_p which is dynamic planning anonymity algorithm based on game theory. This method is proposed on the basic of Privacy_1[8] solving the privacy protection in the suspect environment. First it turns anonymous group into anonymous tree, and then child node cooperates with the parent node to calculate the anchor through game from the tree's bottom to top, finally it calculates the entire anchors of anonymous group through layers of recursive. After that, users initiate location neighbor query through using anchor of anonymous group instead of actual location, then select candidate locations by probability statistics, finally calculate the final ideal location through computation. Simulation results show that this method has better performance, and can be applied to mobile untrusted environment.

Keywords Mobile computing, Location services, Privacy protection, Game, Dynamic planning

1 引言

近年来基于位置服务逐渐走入人们的生活,以智能化的互动方式给人们的生活带来了极大便利,使人们对其需求出现了大量增长。但是,人们在享受各种位置服务带来的便捷的同时,个人隐私信息泄露问题逐渐引起了广大学者的关注,成为近年来研究的重点之一。

一般而言,移动位置服务中的隐私保护可以分为两种:位置隐私[1]和查询隐私[2]。一般情况下用户不希望位置服务提供商知道自己当前的位置,同时也不希望自己提出请求的内容被获知。前者属于位置隐私,后者属于查询隐私。

为了解决移动位置服务中的隐私保护问题,文献[3]中提出了位置 k-匿名模型:当一个移动用户的位置无法与其他 $(k-1)$ 个用户的位置相区别时,称此位置满足位置 k-匿名。此模型既适用于位置隐私保护,也适用于查询隐私保护。为了解决位置隐私保护中的差异性问题,文献[4]提出了 p-敏感模型。此模型考虑了查询敏感度和语意差异性,要求在一个匿名集中敏感查询个数所占比例不超过 p。对于连续查询与发送模型,文献[5]提出了一种连续查询算法和基于熵理论的度量方式。而对于移动攻击模式下的位置隐私保护,文献[6]提出了移动环境下的 LBS 匿名算法 Mclique,以及其快速版本 Fclique。但是它基于可信的中心匿名服务器,容易使其成为性能瓶颈,并且每次有节点离开时都要更新多个匿名图,效率太低。

位置服务中现有的查询大多针对 snapshot 查询类型。然而,连续查询是移动位置服务中一种常见且重要的查询类

到稿日期:2014-02-04 返修日期:2014-06-07 本文受国家自然科学基金(61073197),江苏省科技支撑计划(SBE201077457)资助。
刘学军(1970-),男,博士,副教授,主要研究方向为数据库、数据挖掘、传感器网络、隐私保护等;陈玉凤(1988-),女,硕士生,主要研究方向为数据挖掘、隐私保护,E-mail:chen_yufeiye@163.com(通信作者);李 斌(1979-),男,讲师,主要研究方向为数据挖掘、传感器网络。

型，具有位置频繁更新和实效性的特点[7]。将现有的位置匿名算法直接应用于连续查询隐私保护将会导致：1）连续查询隐私泄露，攻击者通过多次取交集便可算出具体的移动用户的查询请求；2）加剧匿名服务器的负担，移动对象连续发生位置更新，并且每一次更新均需要重新生成匿名集，造成匿名服务器的负担，使匿名服务器成为系统结构的瓶颈；3）很多网络资源被用于传输频繁的位置更新和生成新的匿名集，造成网络拥堵。

文献[7]中提出了 δ_p-隐私模型和 δ_p-质量模型来均衡隐私保护与服务质量这一矛盾，即通过匿名框的周长形式化定义匿名位置的可用性，并将其定义为两个移动对象间的时序相似性，利用两个对象的相似性提出了一个贪心算法，从而保护用户的位置隐私和查询隐私。但是文献[7]采用的是中心服务器结构的方式，容易使中心服务器成为性能瓶颈，并且使用的贪心匿名算法并未考虑增量式的匿名匹配方式，浪费了大量资源并且效率偏低。

文献[8]提出了基于博弈论的用户相互协作的位置隐私保护方法，此方法通过用户之间的相互博弈协作，计算出其协作组的锚点，用锚点代替用户实际位置发起位置近邻查询，最终能够获得比较准确的位置服务。这种方法不需要 k-匿名也能达到 k-匿名的效果，避免了匿名服务器成为性能瓶颈，同时还能解决文献[9]中未解决的不可信环境下的用户合作问题。本文在文献[8]的基础上提出了基于博弈论的动态规划匿名方法 Dynamic_p。此方法主要通过用户相互合作的博弈运算，不需 k-匿名技术但能达到 k-匿名的效果，适用于不可信环境；同时通过动态规划方案可以将已有工作中用户相互合作的博弈位置隐私保护算法 Privacy_1[8] 加以延伸用到移动环境下，也就是将用户之前的计算锚点继续保存起来，而不需要每次都重新计算新的锚点，可达到增量式的锚点计算。

本文第 2 节主要介绍了相关研究工作；第 3 节介绍本文的系统结构；第 4 节介绍位置隐私保护方法；第 5 节介绍本文提出的方法的实验仿真；最后总结本文工作。

2 相关工作

基于位置隐私保护的研究已经引起了许多学者的关注并取得了一定的研究成果。在对移动对象的基于位置的服务请求进行响应时，必须首先确定所采用的系统结构。位置匿名系统结构有 3 种：独立结构、中心服务器结构和分布式的点对点结构。独立结构中用户仅利用自己的知识，由客户端自身完成位置匿名的工作，从而达到保护位置隐私的目的；中心服务器结构在独立结构的基础上，增加了一个可信第三方中间件，由可信的中间件负责收集位置信息，对位置更新做出响应并负责为每个用户提供位置匿名保护；分布式点对点系统结构是移动用户与位置服务器的两端结构，即无中心服务器结构，移动用户之间需要相互信任协作从而寻找合适的匿名空间。现在大部分的工作集中在中心服务器结构和分布式点对点结构上[10]。

在移动环境下，位置隐私保护中主要考虑两点：位置匿名与查询处理。最初人们并没有把位置匿名与查询处理分开，而是将其二者合二为一地看待，即保护了位置隐私等同于保护了查询隐私[5]。位置 k-匿名模型是学术界广泛接受的模型，由 Gruteser 等人提出，随后很多人对此模型进行了修正[4,11]。

位置匿名的基本思想主要分为 3 种：1）发布假位置，即不发布真实服务请求的位置，单个用户便可以完成假位置的匿名；2）空间匿名，即用一个空间区域来表示用户的真实的精确位置，这样攻击者仅能知道用户在这个空间区域，但是无法确定在这个区域的哪个具体位置；3）时空匿名，即在空间匿名的基础上增加一个时间轴，在扩大位置区域的同时，延迟响应时间。延迟响应时间可以在这段时间中出现更多的用户，提出更多的查询，隐私匿名度更高。

文献[2]首次提出了连续查询隐私保护问题，将用户在初始时刻形成的匿名集作为查询有效期内的最终结果，从而解决连续查询隐私泄露的问题。然而该算法仅考虑移动对象初始时刻位置邻近性，却忽略了对象的运动，并且该算法无法保证服务即时响应，同时容易造成同一匿名集中的查询有效期相差过大。文献[11]也解决了连续查询隐私保护问题，文中假设在匿名区域内，用户位置并非均匀分布，采用信息理论中的熵来定义用户的位置隐私保护度。由于熵并不考虑用户的位置是否不同，可能造成 k 个用户重叠于一点的情况，从而产生位置隐私泄露。文献[7]改进了文献[2,11]，考虑了查询生命周期内的每一个时刻位置的邻近性，以及被匿名在一起的查询具有时效性相似的特点，而且既适用于连续查询又适用于 snapshot 的查询。但是该文中使用的中心服务器结构容易使中心服务器成为性能瓶颈，同时并没有考虑不诚信环境下的位置隐私保护。

文献[9]提出了一种基于用户协作的隐私保护方法 Coprivacy，即用户之间通过相互协作，不需要中心服务器及不需生成匿名区域而能达到 k-匿名的效果。但是 Coprivacy 方法是基于所有协作用户都是可信的情况，无法解决协作用户不可信的情况。文献[8]改进了文献[9]，为在现实不可信环境下更好地保护用户位置隐私，提出了一种基于博弈分析思想的用户协作的位置隐私保护方法 Privacy_1，此方法通过用户协作形成匿名组，用安全求和来计算锚点，解决了在现实不可信环境下不诚信合作的问题；同时根据用户的不同位置隐私需求，通过设置不同的隐私保护参数水平，达到不同的匿名保护效果，并且采用改进的增量查询方法提高近邻查询效率。然而文中的方法是基于静态环境下用户相互合作的位置隐私保护的，如用于移动环境下，易造成匿名失败并且容易引起位置隐私与查询隐私的泄露。

本文在文献[8]的基础上采用用户相互合作的博弈方法与基于分布式点对点结构的时空匿名技术，主要工作概括如下：

（1）先将匿名组转变为匿名树。

（2）然后递归式从下到上，每个子节点与父节点博弈算出锚点，每一棵子树的父节点用本子树算出的锚点代替自己的实际位置和自己的上一层子树继续博弈算出上一层的锚点。匿名组中的用户用最后算出的锚点代替真实位置向位置服务器提出位置服务的请求。

（3）在查询处理上，首先检测当前匿名组提出请求的数量是否达到了每个节点自己设计的查询匿名参数 k 的需求，没有达到则当前节点发出假查询直到达到自己的查询隐私参数 k 的要求，如达到则取本次查询获得的结果与前次查询获得的结果的交集中出现频率最高的位置点作为自己需求位置的候选点，如有出现多个候选点则再次进行矢量距离计算算出

最近的位置。

文中的博弈方法可解决不可信环境下的隐私保护问题，并且通过将匿名组转化成匿名树解决移动环境下的位置隐私；同时通过分层博弈可以达到局部更新，不需要因为每次匿名组用户的更新而使整个匿名组重新计算锚点，而且可以避免查询隐私的泄露。

3 系统结构

随着移动设备发展，客户端的计算能力和存储能力大幅度提升，将匿名计算模块放入客户端成为可能。本文采用的是无中心服务器的结构，系统主要由移动用户和位置服务提供商组成。移动用户通常为含有定位功能的终端设备，它包括通信协议、位置匿名、查询处理、速度监测、缓冲存储器。位置服务提供商主要提供的是最近邻查询与连续查询等服务。如图 1 所示，在我们提出的系统架构中，假定移动用户的移动速度不是很快，并且移动用户能够容忍一定的时延误差。

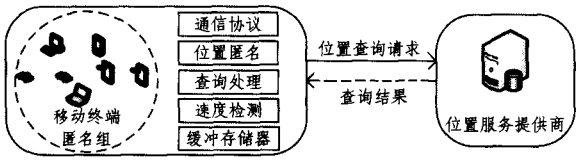


图 1 位置隐私保护系统结构

通信协议模块：移动用户支持 P2P 通信和移动无线互联网通信。其中 P2P 通信主要是用户在建立匿名组时用来自组织通信，移动无线互联网通信由移动用户用来向位置服务提供商发起位置服务的查询并且最终获得查询结果。P2P 通信主要通过无线局域网技术实现，而移动无线互联网主要通过 2G 和 3G 的移动网络实现。本模块是一种基于用户相互协作的协议。移动用户通过单跳与多跳方式组建匿名组进行通信[8]。

位置匿名模块：移动用户可以根据自己的隐私需求设置个性化参数 k，s 和 dt，其中 k 表示相对匿名度；s 表示用户的相对匿名区域；dt 表示最迟响应的时间间隔，即从用户发出查询到接收到最后的结果之间的最大时间间隔。通过匿名组建立匿名树，从下到上通过层层博弈算法算出锚点，用此时的锚点代替实际的位置，向位置服务发起位置服务的请求查询。

查询处理模块：移动用户在此模块中也可以设置个性化参数 k，表示在某个时刻提出查询请求的匿名数。匿名组中的用户使用该匿名组中的锚点代替实际位置向位置服务器发起范围近邻查询请求，并且检测当前时刻的查询请求是否大于等于用户的查询参数 k-匿名需求，如不满足则用户自己发出多个其他位置请求的服务，直到达到 k-匿名的需求。每个时间段位置服务返回给用户的都是离用户最近的 n 个位置，此模块只返回给用户输入的查询请求位置，并且自动选取多个时间段内出现频率最高的位置。如果有多个位置出现频率（称为候选位置）都一样，用户则采用最近邻查询方式，根据自己的实际位置与候选位置进行实际比较计算，算出哪个位置离自己最近。

速度检测模块：主要是移动用户自己检测自己当前的速度在下一时刻是否为即将离开的节点，如果是则发消息给自己的父节点，父节点则重新计算自己与孩子节点之间的锚点，并将计算出来的锚点代替自己位置发给父节点的父节点，直至根节点；当组内节点数小于匿名需求值 k 时，所有节点向外广播请求新的节点加入，哪个节点收到新节点的回应便将新节点作为自己的孩子节点，对有新节点加入的子树需重新博弈计算锚点并将计算出来的锚点发给自己的父节点。每个节点只需要维持两层关系，1）与自己孩子节点之间的关系，2）与父节点之间的关系，不需要知道整个匿名树。

缓冲存储器模块：用来存储本节点的父节点与孩子节点及每个时间段计算出来的锚点。在每一个时间段内，用户用前一个时间段计算出的锚点代替实际位置发起近邻查询；当匿名数小于 k 时广播匿名组成立请求；对于有离开或加入本匿名组的并且属于此子树的节点重新计算锚点，并将新计算出来的锚点传给自己的父节点。

4 移动位置隐私保护方法

本文研究的是在现实不可信及移动环境下用户的位置隐私保护方法，是在文献[8]的研究基础上增加的一个移动环境的条件。本文提出的方法步骤与文献[8]中的方法步骤类似，都是基于无中心服务器分布式的结构，通过用户相互协作计算出匿名组的锚点，不需要 k-匿名服务器的方法但能达到 k-匿名的效果，用锚点代替真实位置发出位置服务的查询，避免了使中心位置服务器成为性能瓶颈，同时又可以将方法更进一步地用于现实的不可信并且移动的环境中。本文中的博弈论定义请参考文献[8]。

4.1 预备知识

定义 1（通信协议） 在匿名集中节点与节点之间的通信协议是可靠的，即通信前先建立虚拟连接，通信结束后再释放虚拟连接。

定义 2（匿名树） 在一个匿名集中，

（1）每个节点用户都是某个节点的孩子节点及某些节点的父节点。

（2）对于一棵树的根，其父节点为空集；对于一棵树的叶子节点，其孩子节点为空集。

（3）每个节点只需要维持自己与父节点和子节点的关系，不需要知道整棵树的具体关系。

（4）每个节点在一跳广播范围内得到的回应节点便自动成为其孩子节点。

定义 3（匿名树的更新） 在一颗匿名树中，

（1）每个节点先检测自己是否为边界节点，如果是则把自己是边界节点的消息告诉自己的父节点及孩子节点，在匿名树中直接将其删除，然后父节点在匿名参数 k' 上减 1，同时将消息传给父节点的父节点直至根节点。

（2）若新的匿名个数 k' 值小于 k，再广播匿名组成立请求，当检测到有新节点回应时，将新的节点作为接受节点的孩子节点。

（3）在（1）、（2）的基础上对于变化的有新节点加入的子树则由父节点与自己的孩子节点成立博弈环重新计算锚点，并将计算出的锚点由父节点代替自己的实际位置传给父节点的父节点，上层父节点如没有子节点的加入则不需要重新博弈，只需更新锚点，否则需要重新博弈算出新的锚点，直至算出整个新树的锚点。对于没有节点变化的子树，只是简单地更新锚点，因为此时的子树相对而言应该是可信的。

定义 4（欧氏距离） $dist(p,q)$ 表示点 p 与点 q 在二维平面上的距离 $dist(p,q)=\sqrt{(p_x-q_x)^2+(p_y-q_y)^2}$，$d_i=R-dist(q_i,p)$，$i$ 代表节点 i，R 代表匿名区域的半径，$dist(q_i,p)$

代表节点 i 与中心节点 p 的欧氏距离。

定义 5(角度的计算) 如图 2 所示，γ 代表点 q_i 与中心节点 p 相对平面坐标的角度，∂ 代表节点 q_i 的速度 v 相对平面坐标的角度，θ 代表速度 v 相对点 q_i 与点 p 之间直线的角度，则 $\gamma=\arccos\frac{q_i.x-p.x}{q_i.y-p.y}$，$\partial=\arccos\frac{v_x}{v_y}$，$\theta=\partial-\lambda$。

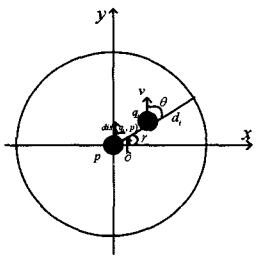


图 2 角度计算

4.2 算法评价标准

(1) 匿名成功率

匿名成功率是评价一个位置匿名算法有效性的重要指标之一。匿名成功率越高，匿名算法就越好。匿名成功率可以定义为：$SR=\frac{|S'|}{S}$，其中 S 是提出匿名请求的所有消息的集合，S' 是匿名成功的消息数，S' 是 S 的子集，是成功匿名的消息集合。

(2)消息处理时间

消息处理时间反映的是匿名算法的运行效率，它指的是一定规模移动用户的所有查询请求在多长时间内可以得到匿名处理。这是反映匿名算法好坏的重要指标之一。当然，处理时间越短越好，说明了匿名算法的高效性[10]。消息处理时间分为平均响应时间与查询处理时间。平均响应时间指用户发起从发现邻居形成匿名组开始到获得所需的查询结果所耗费的时间，查询处理时间指从提出位置查询到获得理想位置所耗费的时间。

(3)平均通信量

用户协作平均通信消息数量指移动用户通过发现邻居形成匿名组到获得锚点平均传输的消息数。平均通信量越大则算法复杂度越高，性能越低；平均通信量越低则算法复杂度越低，性能越高。

4.3 移动位置隐私保护算法实现

本文研究的是现实生活中的不可信环境中的移动位置隐私保护，是对文献[8]的延伸。本文讨论的方法假设发起匿名组成立请求的用户是可信的，用户的移动速度不是很快，并且能够容忍一定的时延误差。

4.3.1 匿名组的成立

如图 3 匿名组成立请求流程所示，对于匿名组成立请求，首先将匿名集转换成匿名树时，所有的节点只要维持两层关系，一是自己的父节点，二是自己的孩子节点，对于变化的子树重新博弈计算出锚点，父节点用计算出的锚点更新自己的实际位置，并转给父节点的父节点，然后上一层子树再次博弈算出新的锚点，这样递归，最终算出整个匿名集的锚点，便可实现 k-匿名的效果(具体的博弈算法请参照文献[8])。接着节点检测自己是否为边界节点，如是则将此节点删除并且整个匿名数减 1，否则保留并更新自己的位置。然后检测当前匿名数是否大于等于匿名参数 k，大于则因为有位置更新需要重新博弈算出锚点，否则广播匿名组成立请求，并更新匿名树。

具体的步骤如图 3 所示：匿名组成立请求，层层博弈算出锚点，位置查询，匿名树的更新，转为第二步。

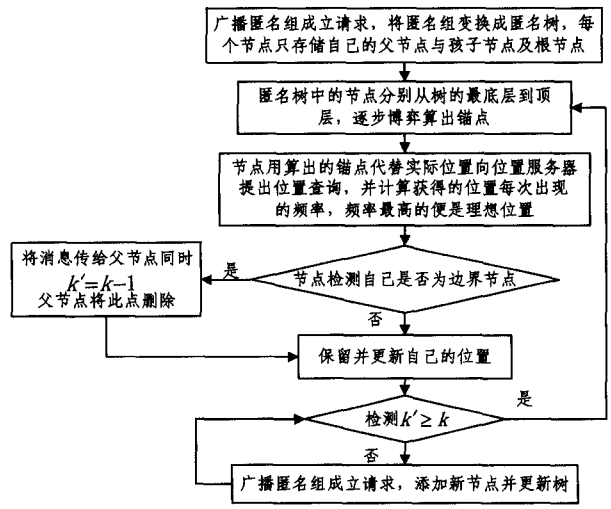


图 3 匿名组成立请求流程

算法 1 动态规划计算锚点

1. 对于新成立的匿名树
2. while(k≥n)//表示匿名数量达到要求
3. If(i 为叶子节点)
4. Then if(m=0)//m=0 表示树中有新节点
5. Then i 节点与父节点及兄弟节点博弈算出此子树的锚点//调用 Anchor_acquired (n,k)算法[3]
6. 算出的锚点代替父节点的实际位置，并且此父节点与自己的父节点及兄弟节点继续博弈算出锚点
7. Else m=1//m!=0 表示树中无新节点
8. i 节点将更新的位置信息给父节点，父节点重新计算锚点 $anchor=\frac{sum}{k}$，并将信息传给上一层父节点，直至根节点，并将新锚点广播给组内每一个成员
9. End then if
10. End if
11. Else then i 节点等待孩子节点来博弈计算锚点
12. 直到根节点计算出整个匿名组的锚点，并将锚点广播给组内的每一个节点
13. End else
14. //调用位置查询处理算法
15. 除根节点外，其他节点检测自己是否为边界节点//调用节点边界检测算法
16. If(i 节点为边界节点)
17. 则 i 节点的父节点将此节点信息删除，并且 k--//边界节点的删除
18. Else i 节点保留并更新自己的位置
19. End while
20. if(k<n)
21. 节点继续广播匿名组成立请求 //调用节点发现 Discover-Peers 算法[8]
22. 将新收到响应的节点自动变为发起节点的孩子节点 //新节点的添加
23. 转到第 3 步
24. End if

算法 2 边界节点检测算法

25. 对于中心节点 p，任一节点 i

26. If($d_i \leqslant v \cdot t \cdot \cos\theta$)

27. Then 节点 i 不为匿名组中的节点

28. Else 节点 i 为匿名组中的节点

29. End if

4.3.2 查询处理

图 4 示出查询请求流程。对于查询处理，用户每个时间段计算出来的锚点相对移动节点而言会有点误差，因为节点是在不停移动的，前一时刻是这个位置下一时刻就是另一个位置了，所以每次提出位置请求服务时必定是前一时刻计算出来的锚点，在两个时间段之间可以有更多的用户提出更多的位置服务查询，这样也实现了时间匿名，再加上空间匿名，整个便是时空匿名。用户每次查询前首先检测当前匿名组中发出查询请求数 n 是否大于等于查询匿名参数 k，如大于则用锚点代替实际位置发出范围近邻查询，否则发出多个假查询，直到达到 k-匿名的要求，然后用户将本次获得的查询结果与前一次结果的交集作为本次查询的候选位置集，最后从候选位置集中选出出现频率最高的位置作为最后的理想位置，如果多个候选位置概率一样，则用户自己再实际计算比较出最后的最近位置。

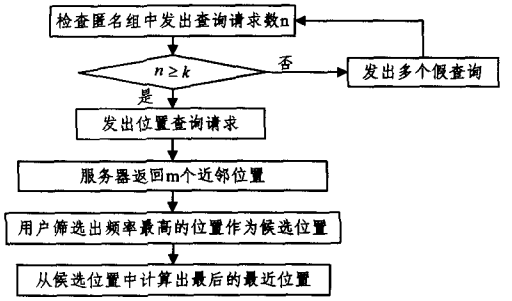


图 4 查询请求流程

算法 3 查询处理算法

1. 检测发出查询的数 n 是否大于等于查询匿名数 k

2. If(n≥k)

3. Then 节点在某一时间点利用计算出的锚点代替实际位置向位置服务提供商发起最近邻位置查询

4. Else then 节点 i 发起 k−n 次假查询

5. End if

6. w[n]←服务提供商返回最近的 n 个位置

7. a[i]←每个位置出现的次数 a[i]//a[i]存储每个位置的次数

8. $p[i] \leftarrow \frac{a[i]}{n \cdot m}$//m 代表第几次查询

9. 将 p[i]值按从大到小的顺序排序

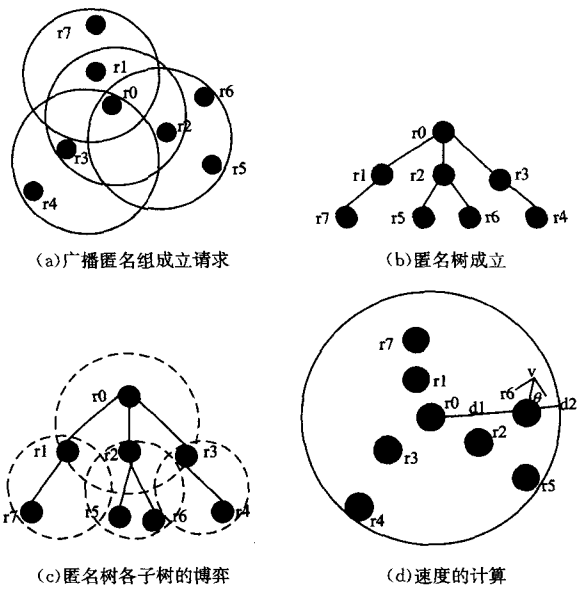
10. If(max(p[i]=1 and p[i]=p[++i])//表示多个候选值频率相同时

11. Then $\min(\sqrt{(x_i-u_{xj})^2+(y_i-u_{yj})^2})$//用户选出实际离自己位置最近的位置

12. End if

4.3.3 示例

例如图 5(a)，r_0 为发起组建匿名集点，r_0 广播匿名发起请求，在一跳范围内 r_1，r_2，r_3 收到了匿名请求，但不满足匿名集的数量，r_1，r_2，r_3 便再次广播匿名请求，则在二跳范围内 r_4，r_5，r_6，r_7 收到了匿名要求，创建了树，如图 5(b)与图 5(c)所示。首先 r_1 与 r_7，r_2 与 $r_5 r_6$，r_3 与 r_4 博弈算出各组的锚点，然后让将博弈后的锚点分别代替 r_1，r_2，r_3 的实际位置，最后再是 r_0 与 r_1，r_2，r_3 博弈算出整个匿名组的锚点。如图 5(d)所示，检测哪些节点最有可能移出匿名集(这里最有可能移出匿名集的节点为 r_7，r_5，r_6，r_4)。首先计算出 d_i，如图 5(d)速度的计算，如果 $d_i < v \cdot t \cdot \cos\theta$，则视节点为即将移出匿名集，否则视节点继续在匿名集中。在时间 t_i 如果节点离开匿名集则将节点从匿名树上删除，如果 $k<n$(k 为目前参加匿名的节点数目，n 为匿名需求参数)，则所有仍在匿名集的节点广播匿名请求，先接收到匿名组外节点的应答的节点便作为接收到应答的节点的孩子。如果有新的节点进入匿名集，则将节点添加到相应的分支树中去，同时对于刚刚添加或删除节点的分支树，重新计算当前的锚点，并将新的锚点传给父节点，父节点收到新的锚点后也重新进行锚点计算，直到传给了匿名组建立请求的节点 r_0，则此时也获得了新的锚点；否则只要分支树的节点仍然在匿名集中，即使相对整个树而言可能改变也无需重新博弈计算锚点。而此次获得的锚点存储在缓存存储器中留给下个时间点 t_{i+1} 使用，在 t_i 时刻向位置服务提供商提出请求的位置是 t_{i-1} 时刻计算得到的，也就是每次提出位置请求的锚点都是前一时间点计算出来的，同时在段时间内有更多的节点提出更多请求，以此便从之前的空间匿名变成了时空匿名。



(a)广播匿名组成立请求　(b)匿名树成立

(c)匿名树各子树的博弈　(d)速度的计算

图 5

5 实验

本文算法使用 C++编程语言实现。实验硬件环境是 2.9GHz处理器，4GB 的内存。操作系统平台是 Windows 7。

5.1 实验数据集和参数设置

实验数据采集用由移动数据管理研究界认可的 Thomas Brinkhoff 路网数据生成器[12]生成，它是基于城市 Oldenburg 的交通路网作为输入，生成模拟的移动用户数据。实验中使用数据的参数值如表 1 所列。

表 1 实验中使用到的数据

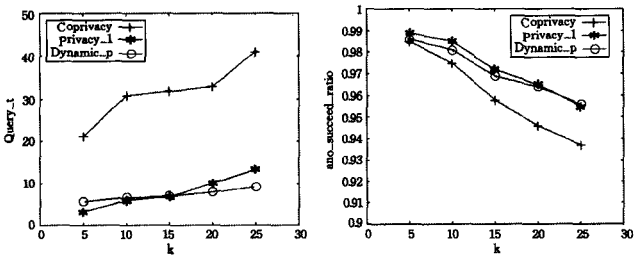
参数名称	平均值
移动用户数量	4000
匿名参数需求 k	10
隐私保护区域半径 s	500m
用户服务误差限制 δ	1
位置服务提供商对每次查询提供的对象个数 n	10

实验采用网络仿真器 NS2 来模拟一个简单的网络节点

环境以及验证本文算法的有效性。NS2 运行环境为 Cygwin +windows7，网络带宽为 1Mbps，移动用户使用该信道进行 P2P 通信。匿名处理算法与近邻查询算法采用 C++程序实现，并且还假设移动用户与位置服务提供商之间使用 3G 网络通信，带宽为 2Mbps。本文实验使用的数据与文献[8]的一样。

5.2 实验数据分析

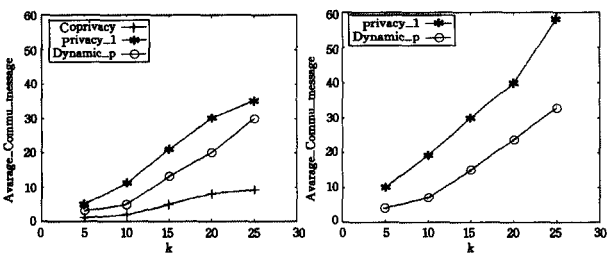
从图 6(a)可知，本文提出的方法的查询处理代价比 Coprivacy 稍低，在 k-匿名需求不高时查询处理代价比 Privacy_1 稍高，在 k-匿名需求高时，代价比 Privacy_1 稍低，因为本文的方法每次都是取前次结果的交集中概率高的。如果有多个候选位置一样才进行最近邻位置比较，而 Privacy_1 每次都需要最近邻的位置查询，容易导致重复工作，并且不适用于连续查询，所以在 k 需求低时表现不出优势，而在 k 需求高时，便表现出比 Privacy_1 的查询处理效率高的优势。从图 6(b)中可以看出，3 种方法的匿名成功率都很高并且都随匿名参数 k 的增加而下降，且本文方法的匿名成功率与 Privacy_1 接近。



(a) 查询处理代价　　(b) 匿名成功率

图 6

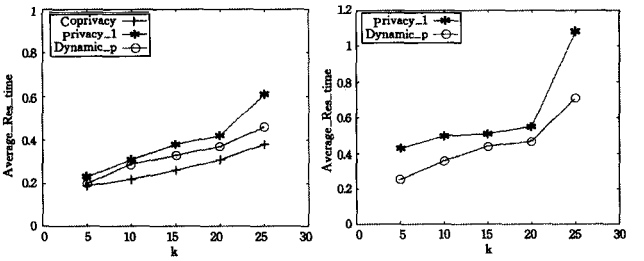
图 7(a)表示基于 0 个欺骗用户的平均通信量，也就是在可信环境下用户的平均通信量。从图中可以看出此平均通信量要比 Privacy_1 低比 Coprivacy 稍高，因为本文中的方法使用的是局部博弈的方法，这样可以将每次安全求和的博弈用户数减少到最低，通信量会比 Privacy_1 低，但是相对 Coprivacy 直接交际通信量会稍高点。图 7(b)表示基于 1 个欺骗用户的平均通信量，从图中可以看出 Dynamic_p 比 Privacy_1 的平均通信量低很多，尤其在 k-匿名需求变高时，通信量大大降低，因为文中的方式是局部博弈方法，这样每次估计欺骗用户的数量会大大减少，并且将数据分组博弈算锚点时的次数也会相应有所降低。所以本文中的 Dynamic_p 方法比 Privacy_1 在通信量方面要好很多。



(a)0 个欺骗用户的平均通信量　　(b)1 个欺骗用户的平均通信量

图 7

图 8(a)表示基于 0 个欺骗用户的平均响应时间，也就是在可信环境下得出的平均响应时间。图 8(b)表示基于 1 个欺骗用户的平均响应时间。从两幅图中可看出，Dynamic_p 的方法比 Privacy_1 的平均相应时间稍低，比 Coprivacy 方法的平均相应时间稍高。因为本文的方法是局部博弈的方法，而且在节点移动的情况下是局部更新锚点的方法，不需要每次都将整个匿名组进行博弈，这样大大减少了每次计算锚点的时间。



(a)0 个欺骗用户的平均响应时间　　(b)1 个欺骗用户的平均响应时间

图 8

结束语　传统的位置隐私保护方法大多采用可信第三方的结构，这往往需要大量的计算，且容易使第三方成为系统瓶颈和集中攻击的目标。Coprivacy[7] 方法使用用户相互协作的匿名隐私保护方法来保护组内用户的隐私，然而其只是基于所有用户可信的情况达到的位置隐私。文献[8]改进了文献[9]的方法，提出了 Privacy_1 方法，但是其不适用于移动环境下的位置隐私保护。本文基于前人的不足提出了 Dynamic_p 方法，主要的贡献就是提出了一种在不可信环境下用户移动位置的匿名保护，在文献[6]基础上提出了动态规划的匿名算法，将之前的整个匿名环变成一个个小环进行博弈算出小环的锚点，然后再一层层递归算出整个匿名组的锚点。本文的方法在锚点计算上，虽然算法效率稍有降低，但是可用于更接近现实移动环境的匿名情况。未来研究的工作可以考虑实际环境更为复杂的情况。

参 考 文 献

[1] Mokbel M F, Chow C Y, Aref W G. The new Casper: Query processing for location services without compromising privacy [C]// Proc of the 32nd Int Conf on Very Large Data Bases (VLDB). New York: ACM, 2006: 763-774

[2] Chow C, Mokbel M F. Enabling privacy continuous queries for revealed user locations[C]// LNCS 4605: Proc of the Int Symp on Advances in Spatial and Temporal Databases(SSTD). Berlin: Springer, 2007

[3] Gruteser M, Grunwal D. Anonymous usage of location-based services through spatial and temporal cloaking[C]// Proc of the Int Conf on Mobile Systems, Applications, and Services (MobiSys). New York: ACM, 2003: 163-168

[4] Xiao Zhen, Xu Jian-liang, Meng Xiao-feng. P-sensitivity: A semantic privacy-protection model for location-based services[C]// Proc of the 2nd Int Workshop on Privacy-Aware Location-Based Mobile Services(PALMS). Piscataway, NJ: IEEE, 2008: 47-54

[5] 林欣，李善平，杨朝晖. LBS 中连续查询攻击算法及匿名性度量[J]. 软件学报，2009(4)：1058-1068

[6] 彭志宇，李善平. 移动环境下 LBS 位置隐私保护[J]. 电子与信息学报，2011(5)：1211-1216

(下转第 141 页)

gers University Graduate School, 2010

[4] Jana S, Premnath S N, Clark M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments[C]// Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. ACM, 2009: 321-332

[5] Jakes W C, Cox D C. Microwave mobile communications[M]. Piscataway, NJ, USA: Wiley-IEEE Press, 1994: 11-50

[6] Aono T, Higuchi K, Ohira T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Transactions on Antennas and Propagation, 2005, 53(11): 3776-3784

[7] 王莅康, 吴越. 基于信道特征的协作密钥提取技术研究[J]. 信息安全与通信保密, 2011, 9(6): 98-101

[8] Wallace J W, Chen C, Jensen M A. Key generation exploiting MIMO channel evolution: algorithms and theoretical limits[C]// 3rd European Conference on Antennas and Propagation, 2009 (EuCAP 2009). IEEE, 2009: 1499-1503

[9] Mathur S, Trappe W, Mandayam N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel [C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. ACM, 2008: 128-139

[10] Patwari N, Croft J, Jana S, et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements[J]. IEEE Transactions on Mobile Computing, 2010, 9 (1): 17-30

[11] Hassan A A, Stark W E, Hershey J E, et al. Cryptographic key agreement for mobile radio[J]. Digital Signal Processing, 1996, 6 (4): 207-212

[12] Sayeed A, Perrig A. Secure wireless communications: Secret keys through multipath[C]// IEEE International Conference on Acoustics, Speech and Signal Processing, 2008 (ICASSP 2008). IEEE, 2008: 3013-3016

[13] Kitaura A, Sasaoka H. A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio[J]. Electronics and Communications in Japan (Part III: Fundamental Electronic Science), 2005, 88(9): 1-10

[14] Wang Q, Su H, Ren K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks [C]// 2011 Proceedings IEEE INFOCOM. IEEE, 2011: 1422-1430

[15] Wilson R, Tse D, Scholtz R A. Channel identification: Secret sharing using reciprocity in ultrawideband channels[J]. IEEE Transactions on Information Forensics and Security, 2007, 2 (3): 364-375

[16] Zhao J, Xi W, Han J, et al. Efficient and secure key extraction using CSI without chasing down errors[OL]. http://arxiv.org/abs/1208.0688

[17] Hsmida S T B, PierrotJ B, Castelluccia C. An adaptive quantization alg-orithm for secret key generation using radio channel measurements[C]// 2009 3rd International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2009: 1-5

[18] Rukhin A, Soto J, Nechvatal J, et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications[R]. Booz-Allen and Hamilton Inc Mclean Va, 2001

[19] Ye C, Reznik A, Shah Y. Extracting secrecy from jointly Gaussian random variables[C]// 2006 IEEE International Symposium on Information Theory. IEEE, 2006: 2593-2597

[20] Xiao L, Greenstein L J, MandaYam N B, et al. Using the physical layer for wireless authentication in time-variant channels[J]. IEEE Transactions on Wireless Communications, 2008, 7(7): 2571-2579

[21] Liu F J, Wang X, Tang H. Robust physical layer authentication using inherent properties of channel impulse response[C]// Military Communications Conference, 2011 (MILCOM 2011). IEEE, 2011: 538-542

[22] Mathur S, Reznik A, Ye C, et al. Exploiting the physical layer for enhanced security [J]. IEEE Transactions on Wireless Communications, 2010, 17(5): 63-70

[23] Zeng K, Govindan K, Mohapatra P. Non-cryptographic authentication and identification in wireless networks [J]. IEEE Transactions on Wireless Communications, 2010, 17(5): 56-62

[24] Shi L, Yuan J, Yu S, et al. ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks[C]// Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM, 2013: 155-166

[25] Jain S, Ta T, Baras J S. Wormhole detection using channel characteristics[C]// 2012 IEEE International Conference on Communications (ICC). IEEE, 2012: 6699-6704

[26] Zeng K, Govindan K, Wu D, et al. Identity-based attack detection in mobile wireless networks[C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2011: 1880-1888

[27] 张紫楠, 郭渊博, 杨奎武, 等. 通用可组合认证密钥交换协议[J]. 西安电子科技大学学报: 自然科学版, 2014, 41(5): 209-215

[28] Hammouri G, Ozturk E, Sunar B. A Tamper-Proof and lightweight aut-hentication scheme[J]. Pervasive and Mobile Computing, 2008, 4(6): 807-818

[29] Ozturk E, Hammouri G, Sunar B. Towards robust low cost authentication for pervasive devices[C]// Sixth Annual IEEE International Conference on Pervasive Computing and Communications, 2008 (PerCom 2008). IEEE, 2008: 170-178

[30] Schulz S, Sadeghi A R, Wachsmann C. Short paper: lightweight remote attestation using physical functions[C]// Proceedings of the Fourth ACM Conference on Wireless Network Security. ACM, 2011: 109-114

(上接第 113 页)

[7] 潘晓, 郝兴, 孟小峰. 基于位置服务中的连续查询隐私保护研究[J]. 计算机研究与发展, 2010, 47(1): 121-129

[8] 陈玉凤, 刘学军, 李斌. 基于博弈论的用户相互协作的位置隐私保护方法[J]. 计算机科学, 2013, 40(10): 92-97

[9] 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

[10] 潘晓, 肖珍, 孟小峰. 移动位置隐私保护[J]. 计算机科学与探索, 2007(10): 268-281

[11] Bamba B, Liu L. Supporting anonymous location queries in mobile environments with privacy grid[C]// Proc of Int Conf on World Wide Web (WWW). New York: ACM, 2008: 237-246

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