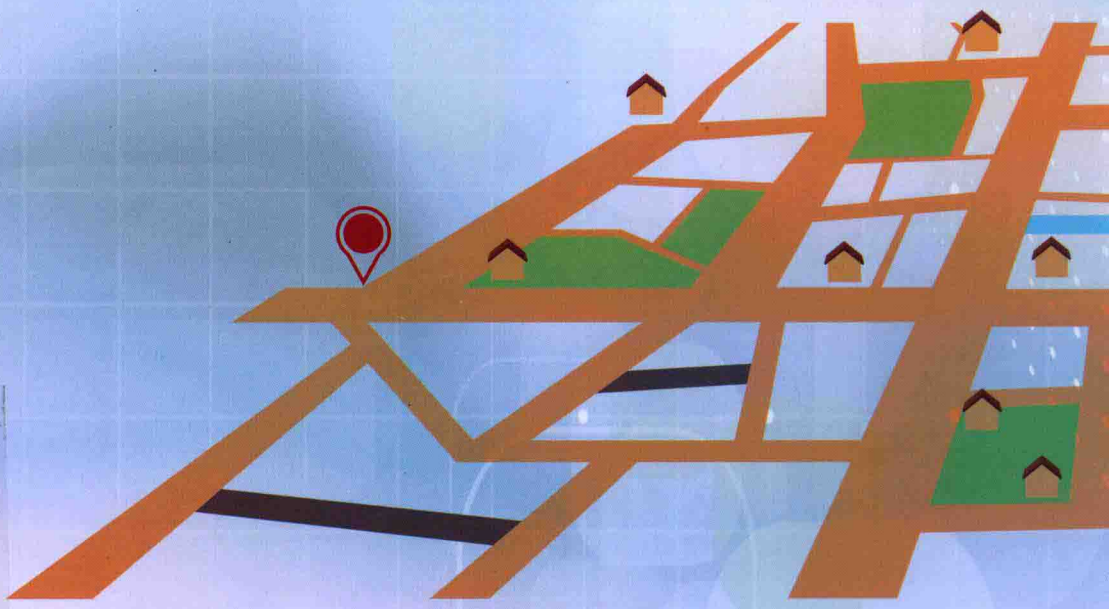
协作保护位置隐私

张　磊◎著



東北大學出版社
Northeastern University Press

协作保护位置隐私

张 磊 著

东北大学出版社

·沈 阳·

图书在版编目（CIP）数据

协作保护位置隐私 / 张磊著. — 沈阳：东北大学出版社，2018.8

ISBN 978-7-5517-1979-7

Ⅰ. ①协… Ⅱ. ①张… Ⅲ. ①最佳位置确定－隐私权－信息安全－安全技术－研究 Ⅳ. ①P204

中国版本图书馆 CIP 数据核字(2018)第 184572 号

本书简介

本书针对基于位置服务中的隐私保护问题，在用户协作的基础上提出了相应的解决方法，分别针对快照查询、连续查询、路网环境查询、半可信协作用户制定了相应的解决方法和度量标准，并且，在考虑攻击者可利用差分攻击的情况下，基于关联概率不可区分的广义差分隐私提出了相应的隐私保护方法。该书既可作为基于位置服务隐私保护相关研究者的参考，也可作为信息安全相关专业学生对隐私保护问题探讨的普及性读物。

出 版 者：东北大学出版社
地址：沈阳市和平区文化路三号巷 11 号
邮编：110819
电话：024－83683655(总编室) 83687331(营销部)
传真：024－83687332(总编室) 83680180(营销部)
网址：http://www.neupress.com
E-mail: neuph@neupress.com
印 刷 者：沈阳市第二市政建设工程公司印刷厂
发 行 者：东北大学出版社
幅面尺寸：170mm×240mm
印 张：8.25
字 数：162 千字
出版时间：2018 年 8 月第 1 版
印刷时间：2018 年 8 月第 1 次印刷
责任编辑：李 佳
责任校对：周晓天
封面设计：潘正一

ISBN 978-7-5517-1979-7 定 价：32.00 元

前　言

作为定位技术的一种重要服务类型，随着智能手机的普及，基于位置服务成为当前移动应用中的重要组成部分。这种通过用户提供自身位置获得所需查询结果的服务，一方面为用户带来日常生活中的各种便利；另一方面不可避免地带来潜在的隐私泄露威胁。针对隐私泄露问题，当前，大量的隐私保护方法均基于可信的中心服务器提出，但是由于中心服务器可成为攻击焦点或服务瓶颈，使得人们对这种类型的隐私保护方法一直存在质疑。因此，基于用户协作的隐私保护方法被大量地提出并逐渐被人们所接受。然而，由于基于位置服务的使用方式与使用环境差异，简单地通过用户协作来完成隐私保护显然是不恰当的，而且，这种方式更面临着一些挑战性的问题未能被解决。例如，快照查询下，协作用户需共享该匿名组中的最大匿名值，无法通过降低匿名要求来获得个性化的匿名服务；连续查询下攻击者可利用协作用户差异识别某一特殊用户，且已有方法一般假设协作用户具有相同的移动方向和移动速度，这在实际部署中是不现实的；路网环境下的环境限制，使得部分欧氏空间下的协作用户方法无法提供隐私保护，且很难在路网移动环境中找到足够的协作用户完成匿名值建立；存在半可信协作用户在构建匿名组的过程中窃取用户隐私的情况；基于 k-匿名模型的隐私保护方法很难应对统计攻击，尤其是差分攻击。

针对上述问题，本书展开了以下几个方面的研究工作。

① 基于用户协作的快照查询隐私保护。针对快照查询中已有的隐私保护方法只能共享匿名组中最大匿名值这一问题，基于用户设备的短距离通信能力，提出了查询分块随机交换的隐私保护方法。该方法通过将用户自身的查询信息按照设定的匿名值进行分块，并通过与协作用户或协作用户之间的随机数量查询分块交换，实现多跳通信范围内的匿名组建立。最后，利用同一查询可建立对应匿名组这一特性，实现了隐私保护过程中每一用户的个性化隐私保护。

② 基于用户协作的连续查询隐私保护。针对攻击者可通过协作用户差异识别某一特殊用户的问题，以及现有方法对协作用户的强假设性，基于协作用户 cache 和短距离通信能力，提出了一种通过查询分块建立匿名组，并通过协

作用户 cache 提供连续查询结果的隐私保护方法。该方法利用快照查询中的随机交换查询分块的思想，通过协作用户保存该查询分块反馈的查询结果，在申请用户移动到邻近协作用户且进行连续查询时，可通过协作用户 cache 的查询结果提供服务，进而减少申请用户与 LBS 服务器之间的信息交互，降低申请用户隐私信息泄露的可能性。

③ 基于用户协作的路网环境隐私保护。针对路网环境下已有的针对欧氏空间的隐私保护方法无法有效提供隐私保护，且很难在路网移动环境中寻找到足够的协作用户建立匿名组的问题。基于 mix-zone 技术提出利用协作用户实现攻击者无法关联进出 mix-zone 用户的隐私保护方法。在该方法中，可在 mix-zone 中通过协作用户集合建立匿名组，同时，经过协作，用户之间的查询信息和查询时间间隔交换，在完成信息共享之后，形成信息集合，通过离开 mix-zone 之后利用信息集合进行连续查询，以此实现对路网环境下连续查询的位置不可关联，进而保护用户的个人隐私。

④ 基于半可信协作用户的位置隐私保护。针对基于协作用户的隐私保护方法需要面对半可信协作用户的问题，基于属性基加密思想，提出了一种协作用户部分解密的隐私保护方法。在该方法中，申请用户将自身的查询进行两轮加密之后，发送给中心服务器，由中心服务器在较广的通信范围内寻找协作用户，并将查询发送给协作用户。协作用户在具有相同属性的情况下，可部分解密申请用户信息。在整个过程中，无论是中心服务器，还是协作用户，均无法获得申请用户不愿公开的任何信息，且以半可信 LBS 服务器为首，攻击者也无法通过属性关联获得用户隐私信息，进而达到了可针对不同攻击者攻击行为的隐私保护目的。

⑤ 关联概率不可区分的位置隐私保护方法。针对基于 k-匿名模型的隐私保护方法很难应对统计攻击，尤其是差分攻击的问题，基于广义差分隐私，提出了 ε-位置-查询关联隐私保护模型。同时，根据这一模型的特点，依靠用户位置偏移这一思想，提出了关联概率不可区分的隐私保护方法，并基于这种方法定义了三种随机算法，以这三种算法来实现用户的位置隐私保护。通过用户的位置中偏移，用户与协作用户之间可实现多种关联概率的不可区分性，有效地抵抗了攻击者通过背景知识推测出的关联概率获取用户位置隐私的关联攻击行为和差分攻击行为。

著　者

2018 年 6 月

目　录

第1章 绪 论

移动通信技术的飞速发展带来了高性能智能终端的普及和人们生活习惯的改变。作为一种典型的智能终端应用，基于位置服务(location-based service，LBS)为人们提供了交通导航、近邻兴趣点查询、商业广告推送和网络交友等诸多便捷服务。然而，这种服务的获取需要用户提供所需的服务信息与自身的真实位置，并基于自身位置获得由 LBS 服务器提供的相关服务。但是，位置本身是一种具有时空关联特性的信息，这些特性可用来关联用户的敏感信息，进而导致用户隐私的泄露。随着用户隐私被泄露，将会带来一系列的严重问题：一方面用户隐私的泄露可能会造成用户生活习惯、宗教信仰及健康情况等不愿公开信息的扩散，带来日常生活中的不便；另一方面，用户隐私信息又可能为别有用心的攻击者提供潜在的背景信息，为诸如盗窃、抢劫等人身伤害事件的发生提供了便利条件。因此，隐私泄露成为基于位置服务所需要解决的重要问题[1,2]。

1.1 研究背景及意义

据维基百科统计结果显示，至 2017 年，全球智能手机数量达到 23.89 亿，中国的智能手机量达到 7.17 亿[3]。而据美国的商业统计数据网站 statista 对 2015 年 7 月美国本土智能手机使用基于位置服务的统计结果表明，90.33%的智能手机用户使用基于位置服务，在这些使用基于位置服务的用户中，年龄在 18—29 岁的用户达 95%，30—49 岁的用户达 94%，50 岁以上的用户仍可达 82%[4]。显然，LBS 已成为与用户年龄无关的智能手机中使用程度最高、发展最快的移动应用。尽管 LBS 已取得了显著的应用效果，并被各个不同年龄段的用户所使用，但该项服务仍处于发展阶段。同样，基于 statista 网站 2015 年 8 月的统计结果显示，智能手机用户每天使用 LBS 寻找日常生活信息的比例仍然较低，其中，使用率最高的墨西哥仅占 27%，而智能手机使用更广的美国用户反而更少，其日常 LBS 的使用率仅占 16%[5]。这充分说明，当前 LBS 仍处

在一个高速发展阶段，仍存在巨大的商业市场空间等待开发，其全球收益仍将不断攀升。

作为智能手机普及较为广泛的中国，以高德地图、微信位置共享和去哪儿旅行等为代表的一大批 LBS 的应用正逐渐兴起，并为广大用户提供导航、最近邻兴趣点查询及商业广告推荐等日常生活中的便捷服务。并且，随着我国自主研发的北斗卫星导航系统(beidou navigation satellite system)的逐步发展成熟，我国卫星定位技术将摆脱大量依赖 GPS 的现状，对于国内 LBS 的发展也将起到促进作用，相关的产业和技术在不断完善和发展的同时势必会产生该服务的一段真空地带等待人们开发。在 LBS 技术带动产业发展的同时，将会有更多智能手机用户选择使用 LBS，为技术发展带来持续动力，使得我国 LBS 能够呈现一种良性的循环发展态势。

伴随着 LBS 的广泛应用及高速发展，人们逐渐发现，在享受这种服务所带来的便利的同时，用户不得不面对服务与个人隐私保护不可兼得的尴尬局面。在该服务中，用户若想获得所提供的服务项目，首先需要将自身的查询与真实位置发送给 LBS 服务器，这使得用户的位置信息可以很轻易地被 LBS 服务器或其他服务实体所获得，进而这些实体在历史信息发布、被黑客攻击或者商业利益的诱惑下，很容易将用户的个人信息泄露出去，造成用户的个人隐私泄露。同样，据 statista 网站公布的 2015 年统计数据显示，有 34%的用户因为个人隐私安全问题而关闭 LBS 应用，有 18%的用户甚至尝试避免使用 LBS 的应用，以防止个人隐私的泄露[6]。隐私泄露问题已成为继精确定位之后严重影响和制约 LBS 发展的首要问题。对于 LBS 所带来的对个人隐私泄露问题的担忧，甚至有网友绘制了如图 1.1 所示的 LBS 时时刻刻监控用户的尴尬画面。可以说，若不能有效地解决 LBS 中的隐私泄露问题，LBS 将无法取得繁荣发展的局面，无法成为人们日常生活中不可替代的智能手机应用。

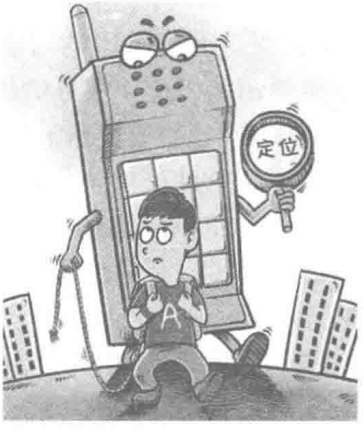


图 1.1　LBS 带来的威胁

通常，LBS是一种由服务提供商根据用户提供的位置反馈或推送所需信息的一种服务方式。在这种服务下，用户的一些信息如身份标识、位置和查询信息等共同组成了基于位置的服务请求。在LBS提供商获得由用户发送的服务申请后，根据服务提供商保存或者云端保存的数据信息提供查询结果，并将结果反馈给服务申请用户，从而完成提交、处理、反馈的服务过程。这种服务随着技术水平的提高可分为主动式和被动式两种不同的服务方式。所谓主动式服务是指用户每次提供自身包含用户位置信息在内的查询信息给LBS服务器，在LBS服务器反馈查询结果之后完成整个服务过程。而被动式服务是指由用户提供当前的查询信息，在用户的移动过程中仅进行位置更新，而LBS服务器需要不断地根据用户位置更新反馈给用户相应的查询结果。根据这两种不同的服务方式，可以将LBS划分为快照查询服务和连续查询服务。

在快照查询服务中，用户的查询信息是按照身份标识、真实位置和查询信息这样的组成结构发送给LBS服务器的。因此，在这种服务下，保护用户的个人隐私仅需要切断每次位置和查询信息与用户身份标识之间的关联关系即可实现。而在连续查询服务中，用户向位置服务提供商发送形如“$Q=(ID, L_i, I, P)$”的查询给LBS服务器。其中：ID表示用户的身份标识；$L_i=(x_i, y_i)$表示请求所处位置；I表示时间间隔；P表示查询兴趣点，如餐厅、加油站等。此时，用户的查询信息不仅包含身份标识、真实位置和查询信息，还包括查询时间间隔这样的提交信息，以及移动速度、移动方向等更多的潜在属性轮廓信息，因而，其隐私保护还需切断用户身份标识与用户所能表现一切潜在的属性轮廓信息之间的关联关系，其隐私保护的难度更大。另外，以数据挖掘和数据分析为首的数据处理技术在另一侧面又对用户隐私造成一定的威胁。例如，Su等人[7]通过连续位置校正，可以轻易地分析获得用户的位置轨迹，进而找到用户在连续移动过程中所经过的任何兴趣点，泄露用户的个人隐私。Chen等人[8]可通过构造和比较用户移动轮廓的方法，在众多移动用户中准确地识别某一用户。李雯等人[9]甚至能够基于用户的运动趋势预测用户潜在的移动位置。Tang等人[10]更是基于马尔科夫模型准确地预测连续查询过程中用户所处的每一个查询地点。以上种种表明，LBS的隐私保护研究已迫在眉睫，LBS的用户急需获得有效的方法或应用以提供完善的隐私保护服务。

1.2 国内外研究现状

当前，LBS存在泄露用户个人隐私的问题已随着这种服务的大范围推广和应用引起了广泛的关注。以美国计算机协会(ACM)和美国电气电子工程师协

会(IEEE)为首的著名科技组织先后组织多次重要国际会议和重要的期刊专刊，对 LBS 的隐私保护研究进行了持续关注。同时，以施普林格(Springer)和爱思唯尔(Elsevier)为代表的国际出版集团也加强了对相关技术的报道。以 S&P、CCS、ICDE、INFOCOM、SIGMOD、VLDB 等为代表的国际著名会议则积极为 LBS 隐私保护的技术提供了高水平交流平台，而以 TDSC、TMC、TIFC、TVT、Information Sciences 为首的重要国际期刊则进一步将研究细节、研究成果和评价指标公布给广大研究者和相关企业，为 LBS 隐私保护产品的开发提供了有益辅助。

在国内，以中国计算机学会(CCF)及中国网络空间安全协会(CSAC)为主的科研机构也提高了对 LBS 隐私保护的重视程度，增加了对相关研究方法、研究成果的支持力度，并通过旗下会刊(如：计算机学报、计算机研究与发展、通信学报等)增加了对相关研究的报道篇幅。同时，由于我国自主研制的北斗卫星导航系统的逐步发展完善，国内对于 LBS 的应用市场逐步从 GPS 等国外定位技术转到北斗定位技术，使得国内对于阻碍 LBS 发展的隐私问题更加关注，并在近年的国家自然科学基金项目的资助政策上有所倾斜，其资助数量逐年提升。但是，我国对于 LBS 隐私保护的研究水平相对较低，这是由于东西方文化背景之间的差异及我国在定位系统方面的发展情况所造成的。相信随着我国社会发展的不断进步，人们对个人隐私安全问题认识程度的逐步增强，更重要的是核心定位技术和定位系统的逐步国产化，我国 LBS 用户数量将会持续增加，并且对于 LBS 隐私问题也将会持续进行关注。这些发展变化又将反过来促进我国对位置隐私保护技术发展的研究。

当前，已存在的 LBS 的隐私保护方法根据采用的系统架构，可简单分为集中式系统架构和分布式系统架构两种不同类型。另外，有些方法将两种架构方式混合使用，这些方法被称为混合架构。集中式系统架构又可称为中心服务器架构，这种类型的隐私保护方法提出较早，并涌现了较多相应方法的变种，这些方法一般基于一个可信的中心服务器，由中心服务器将用户提出的位置服务请求信息加以调整或处理，在满足 k -匿名或其他隐私模型的情况下发送给位置服务提供商，以此保护用户的隐私信息。而分布式系统架构又被称为无中心服务器的系统架构，此类方法则存在两种不同的隐私保护思想，一种是通过用户自身携带的设备对用户信息进行加密处理，利用隐私信息检索、不经意传输或同态加密等密码学相关技术，在整个查询过程中保障用户的查询信息不会公开给任意一方，实现用户信息零泄露的信息查询；另一种是利用用户携带设备的短距离通信能力，在用户单跳或多跳通信范围内，通过寻找到满足用户隐私要求的协作用户，利用协作用户实现将申请用户隐藏的目的。

针对这两种不同的隐私保护类型，本章首先从集中式系统架构的隐私保护

技术的研究进展展开描述，同时，对分布式系统架构的隐私保护技术的产生原因和发展过程加以阐述。对基于这两种架构的隐私保护方法进行阐述的同时，本章又在系统架构的前提下，根据服务类型的差异，分别从快照查询和连续查询两个方面加以说明。

1.2.1 集中式系统架构的隐私保护技术

集中式系统架构的隐私保护技术是指通过一个可信的第三方中心服务器(trusted third party，TTP)完成对用户提交位置的泛化、模糊或者隐藏。这种技术最早来源于 Marco Gruteser 等人[11]在2003年借鉴数据库中常用的 k-匿名(k-anonymity)机制提出了位置 k-匿名模型。在该模型中，申请者提交包含自身位置在内的至少 k 个位置给服务器，使得从攻击者角度来看，申请者在某一时间周期内的位置无法与其他 $k-1$ 个用户的位置相区别，则称该位置满足位置 k-匿名。2005年，Gedik 等人[12]认为提交的自身位置尽管能够被其他 $k-1$ 个位置所泛化，但是攻击者可能会通过用户差异分析这些位置中潜在的真实位置，因此，提出将申请者提交的位置更换成为一个位置区域，通过一个较大的位置区域集合进一步将真实位置所模糊。其后，基于 k-匿名机制，语义多样性[13]和查询多样性[14]被相继提出，极大地丰富了隐私保护的约束机制。2009年，Poolsappasit 等人[15]发现不同用户对隐私的定义有所差别，认为中心服务器应该能够根据用户个人之间的隐私界定差异提供个性化的隐私保护服务。同年，Xu 等人[16]针对个性化隐私保护问题，提出中心服务器应根据用户自身对隐私情况的感受提供隐私保护和位置服务，以此获得较好的隐私保护和服务质量之间的平衡。针对相同区域内多次对同一目标进行查询可能会缩减匿名区域，进而令攻击者能够识别申请用户的情况。2010年，Talukder 等人[17]通过按照隐匿区域中的时间顺序动态地生成解体集的方式，利用中心服务器将申请用户隐匿于动态变化的匿名用户当中，有效地抵抗了多查询攻击。2012年，Shokri 等人[18]注意到隐私保护程度和服务程度之间的矛盾关系，提出一种基于贝叶斯博弈的优化方案，使得中心服务器能够在线性程序计算时间内提供最优的隐私保护策略和服务策略之间的转换。2013年，Andrés 等人[19]针对潜在的基于概率推测的攻击行为，提出了地理位置的不可区分性，通过中心服务器利用差分隐私保护模型解决位置隐私保护中的问题。同年，Assam 等人[20]则根据查询内容的识别保护问题，基于差分隐私保护模型提出了查询内容不可知的隐私保护方法，并借助卡尔曼过滤和指数机制实现时空数据的差分隐私保护。与 Andrés 等人通过添加大量的满足某种分布的虚假位置实现差分隐私保护的方法不同，Dewri[21]认为攻击者可能掌握这种分布情况，进而识别出添加的虚假位

置，提出应添加满足拉普拉斯变换的虚假位置，以降低每个添加位置之间的关联约束。2014 年，Nicolás 等人[22]进一步优化了 Andrés 等提出的地理位置不可区分的方法，通过降低线性约束规划的方式降低隐私保护技术对位置服务质量的影响。同年，Vincent 等人[23]测试了这种隐私保护技术，并公布了这种隐私保护方法在实际环境中的测试结果。2015 年，Chatzikokolakis 等人[24]公布了基于以上方法的工程实施结果。同年，Lin 等人[25]通过使用聚类的方法，实现了基于中心服务器的查询和位置同时匿名用户的快速寻找。2016 年，Tang 等人[26]考虑到存储在移动云环境下的用户位置可能会泄露用户隐私情况，通过对地理信息和长期一致性方面的考虑，实现了一种可长期保护用户位置隐私的保护方法。2017 年，Shokri 等人[27]从博弈论的角度对位置隐私保护的理论框架和优化策略进行了理论阐述，并利用线性机制来实现对隐私保护策略的制定和优化。

随着 LBS 的发展，人们更多地选择采用主动式的连续服务，通过连续的位置更新，不断地获得由服务器反馈回来的服务结果，使得申请者能够在不断的移动过程中持续地获得这种服务。这使得对申请者当前位置简单泛化、模糊或者隐藏不能够行之有效地保护其个人隐私，因此，基于中心服务器的帮助，Bhuvan 等人[28]在 2008 年基于位置网格提出了移动环境下的连续查询隐私保护。2009 年，Ghinita 等人[29]则根据用户移动的方向和速度夹角，提出了一种临时匿名方案，以此实现对基于速度链接攻击的隐私保护。同年，Wang 等人[30]便尝试在路网环境下使用连续匿名框实现隐私保护。2010 年，潘晓等人[31]提出 δp-隐私模型和 δq-质量模型，通过扩张变化的匿名区域实现对连续查询服务下的申请者连续位置隐私保护。2012 年，Pan 等人[32]提出一种可扩展匿名区域的隐私保护方法，在一定程度上实现了短距离移动范围内的用户位置匿名。2012 年，Ryo 等人[33]利用可表现等待状态的虚假位置，进一步刻画了虚假轨迹与真实轨迹之间的相似关系，使用相似轨迹来保护用户的连续位置。2013 年，Hashem 等人[34]考虑到攻击者可利用连续匿名区域之间相互重叠情况识别潜在的匿名用户，提出了一种对用户离开匿名区域之前的查询进行预计算的隐私保护方法，在为用户提供连续查询结果的同时有效地防止了攻击者通过匿名区域重叠识别匿名用户的攻击行为。2014 年，Niu 等人[35]利用假位置泛化了用户位置与用户查询之间的关联关系。同年，Hwang 等人[36]通过对连续位置服务中产生的位置、路段、时间及轨迹等多种状态产生的匿名标准，实现了对连续位置中申请者查询属性的属性泛化，进一步通过轨迹泛化保护申请者的位置隐私。2015 年，Schlegel 等人[37]将申请者所在区域划分为等量的单元格，通过 LBS 服务器获取指定单元格内兴趣点的方式将申请者的查询目标加以模糊，并利用获取随机单元格内兴趣点的方式将申请者的真实位置隐藏。

同年，Lin 等人[25]利用中心服务器计算连续位置集合中位置与查询聚类的方法，实现了位置和查询的共同匿名。2016 年，Hara 等人[38]通过考虑真实环境下的位置约束，提出了一种可以更有效地防止攻击者识别的假位置生成方法，以此降低攻击者对虚假位置的识别概率。同年，Zhang 等人[39]进一步考虑到攻击者通过背景知识识别潜在假位置的情况，提出了一种虚假位置与虚假位置环境共存的隐私保护方法，进一步完善基于假位置的隐私保护技术。2017 年，Zeberga 等人[40]通过建立安全区域的方法，实现了对路网环境下直线移动的 k - 近邻查询隐私保护。

在众多的连续隐私保护方法中，锚点和 mix-zone 方法由于使用较多又可认为中心服务器隐私保护方法中的特例。2008 年，Yiu 等人[41]首先通过一个被称作锚点的假位置来代替申请者的真实位置，使所有该锚点附近的申请者在进行位置服务时，使用锚点位置代替真实位置，利用偏移后的位置完成真实位置隐藏。2011 年，Yiu 等人[42]进一步完善了这种方法。在 2015 年马春光和周长利[43-46]针对 SpaceTwist 无法有效地计算用户与锚点相反方向 kNN 的问题，提出了一种逐步缩小供应空间的改进方法，同时，针对锚点部署情况，分别提出了基于 voronoi 预划分和注入假查询的隐私保护方法，扩展了锚点方法的应用环境。2016 年，倪巍伟等人[47]使用路网环境中制定的安全区域，将连续位置模糊的方法应用在路网环境。

在利用中心服务器实现 mix-zone 方面，2003 年，Beresford 等人[48]提出了 mix-zone 技术。mix-zone 可以看作一个黑盒区域，用户驶入该区域时可以与该区域中其他用户进行身份交换，由于在该区域中攻击者无法获知用户身份标识的更改过程，因而，无从获知更改后的身份标识与用户之间的关联情况。Freudiger 等人[49]在 2007 年首先优化了这种方法使得在实际部署中降低了对 mix-zone 的部署个数要求。2009 年，Julien 等人[50]从博弈论中纳什均衡的角度，分析了在 mix-zone 中用户潜在的合作意向，并给出了在不完全信息的情况下，使用中心服务器提供的简单入门策略即可实现 mix-zone 中对称的贝叶斯纳什均衡，证明了 mix-zone 可实现区域内用户遵循规则的隐私保护。2009 年，Freudiger 等人[51]又将 mix-zone 方法引入到路网环境中。针对矩形 mix-zone 区域易通过速度等属性估算出用户离开的时间和方向问题，2011 年，Palanisamy 等人[52]提出了非矩形 mix-zone 区域的概念。2013 年，Ying 等人[53]提出了一种车辆网络环境下的动态部署 mix-zone 的方法，便于灵活地满足用户提出的隐私要求。同年，Gao 等人[54]将 mix-zone 应用到对于用户参与性感知的位置轨迹隐私保护中。2014 年，Palanisamy 等人又根据非矩形 mix-zone 提出了基于该非标准形状的时空耽搁 mix-zone[55-56]，以此降低通过时空关联特性推测出驶入与驶出用户之间的关联概率。Sun 等人[57]在 2015 年针对动态部署 mix-zone 的问

题，提出了一种优化，使得部署的 mix-zone 能够满足更多用户的隐私保护需求。同年，Ying 等人[58]考虑到 mix-zone 建立环境的缺陷，提出一种通过对协作用户进行激励，并自主建立 mix-zone 进行车辆网络下用户隐私保护的方法。

近年来，应用中心服务器来实现隐私保护的方法层出不穷，因为中心服务器具有强大的计算、处理和存储功能，使得在 LBS 隐私保护中不同的方法能够有效地处理诸如用户属性泛化、模糊、隐藏等相关操作。但是随着研究的深入，这种中心服务器结构所带来的问题也逐渐体现出来。首先，作为整个隐私保护的处理中心，中心服务器保存着所有申请者的相关信息，这使得中心服务器成为了攻击者的攻击焦点，大量的攻击方法和攻击行为将会集中在中心服务器上，一旦中心服务器被攻破，将会造成巨大的隐私泄露事故；其次，作为所有隐私服务的处理中心，中心服务器面临着巨大的处理压力，当某一时间段大量申请者集中申请隐私保护服务时，极有可能会造成中心服务器处理速度和处理能力的降低，进而影响到 LBS 的服务质量；最后，由于一些广泛存在的对能够提供中心服务的大型机构的不断质疑，使得当前很难找到能够被广大用户共同接受的中心服务器提供部门，同时，由于该类方法需要部署大量的中心服务器，其基础设施投入与经营问题也阻碍着该类技术的实际部署。

1.2.2 分布式系统架构的隐私保护技术

针对集中式系统架构隐私保护技术存在的问题，研究者一直在考虑通过用户自身设备实现中心服务器功能的隐私保护方法。与集中式系统架构不同，分布式系统架构采用如图 1.2 所示的系统架构，整个隐私保护的处理过程均通过用户自身的移动设备来完成，由于隐私保护思想的差异，这种技术又可以分为基于加密的隐私保护技术和基于用户协作的隐私保护技术。

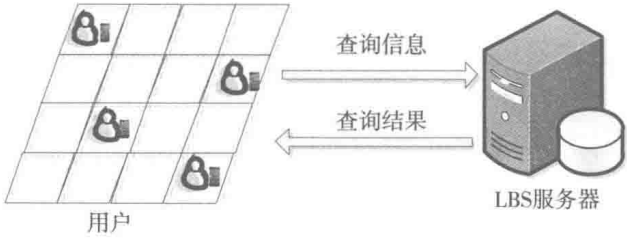


图 1.2 分布式系统架构的隐私保护框架

（1）基于加密的隐私保护技术

在基于加密的位置隐私保护技术中，PIR(privacy information retrieval)隐私信息检索备受关注。2008 年，Ghinita 等人[59]将可计算 PIR 引入到位置隐私保

护研究中，通过使用计算 PIR 的方法来解决位置隐私保护中的秘密计算最近邻查询问题。同年，Khoshgozaran 等人[60]提出了硬件 PIR 的方法，通过协处理器提高检索数据的模糊性和处理速度。2009 年，Khoshgozaran 等人[61]通过螺旋扩张和希尔伯特扩张，来加速服务器端进行 PIR 检索时的检索速度。2011 年，Khoshgozaran 等人[62]进一步优化了之前所提出的 PIR 方法，使得该方法能够对 k-最近邻进行检索。同年，Ghinita 等人[63]考虑到 LBS 中的数据同样需要加以保护，在 PIR 方法的基础上增加了对 LBS 中数据的保护协议，并根据动态调整数据建立分层索引，以支持 PIR 方法进行高效的检索。2013 年，Wightman 等人[64]根据地理经纬度中小数点后面位数较多的特点，针对用户选择的不同小数点位数，其对应的地理网格区域的差异较大，提出了一个根据地理范围差异进行查询的通信量较少的一个 PIR 方法。2014 年，Xi 等人[65]一改 PIR 方法应用于 NN 或 kNN 查询的情况，将 PIR 方法应用于多跳最短路径导航中，尽管计算开销较大，但是扩展了 PIR 的应用范围。2014 年，杨松涛等[66]基于 PIR 提出了一种中心服务器结构的隐私保护模型，实现了完美匿名和盲查询。同年，杨松涛等[67]借鉴安全多方计算理论，提出了一种无协作分布式结构下的位置隐私保护方法。2015 年，杨松涛等[68]基于 k-匿名的思想，利用 PIR 方法保证了查询结果在检索过程中的隐私性，实现了服务提供者在无法知道用户精确查询结果的前提下为用户提供基于位置的服务。在非 PIR 的方法中，2013 年，Buchanan 等人[69]基于加密技术实现了一种能够同时提供快照查询和连续查询两种不同服务情况下的隐私保护方法。2014 年，Russell 等人[70]利用同态加密和不经意传输进一步增强了加密技术对于用户隐私的保护，使得在整个 LBS 的过程中包括该区域内所有用户及半可信的 LBS 服务器均无法获知申请者的隐私信息。同样，基于 paillier 的公钥加密系统，2016 年，Yi 等人[71]利用同态加密技术实现了同时保护移动申请者位置和查询隐私最近邻相似 kNN 查询，并且该方法可应用于多维离散属性的查询隐私保护。同样，基于加密的隐私保护算法可用来分享共同的隐私集会地点，2012 年，Ashouri 等人[72]就基于匿名否决网络和同态加密实现了对最近邻集会地点的秘密计算和秘密发送。2014 年，Bilogrevic 等人[73]提出了一种对秘密集会地点的优化方法，降低了用户之间进行距离秘密计算的处理轮次。2015 年，Ashouri 等人[74]对其提出的秘密计算集会地点的方法进行了改进，并通过两个不同阶段对隐私轮廓隐匿和多方安全计算，进一步提高用户的隐私保护级别。2016 年，Aivodji 等人[75]将这种秘密计算集会地点的方法应用在用户拼车的真实场景下，实现对拼车用户起始和目标位置的隐私保护。同年，Wang 等人[76-77]进一步优化这种秘密计算集会地点的方法，提出了一种基于同态加密仅需一轮计算即可获得公平集会地点的隐私保护方法。