软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(9):2373−2395 [doi: 10.13328/j.cnki.jos.004857]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

位置服务隐私保护研究综述*

张学军[1,2,3], 桂小林[1,3], 伍忠东[2]

[1](西安交通大学 电子与信息工程学院,陕西 西安 710049)

[2](兰州交通大学 电子与信息工程学院,甘肃 兰州 730070)

[3](陕西省计算机网络重点实验室(西安交通大学),陕西 西安 710049)

通讯作者: 桂小林, E-mail: xlgui@mail.xjtu.edu.cn

摘 要: 由于位置感知移动电子设备的繁荣,位置服务(LBS)几乎在所有的社会和商业领域广泛流行.虽然 LBS 给个人和社会带来了巨大利益,但也给用户的隐私造成了严重威胁.因为用户享受 LBS 的同时需要向不可信的 LBS 提供商泄露其位置和查询属性,而附加在这些信息上的上下文揭露了用户的兴趣爱好、生活习惯、健康状况等.如何保护用户的隐私免受恶意提供商的侵犯,对 LBS 生态系统的健康发展至关重要,因而引起了研究者的广泛关注.对 LBS 隐私保护的研究现状与进展进行综述.首先介绍 LBS 隐私的概念和威胁模型;然后,从系统结构、度量指标、保护技术等方面对现有的研究工作进行细致的分类归纳和阐述,重点阐述当前 LBS 隐私保护研究的主流技术:基于扭曲法的隐私保护技术;通过对各类技术性能和优缺点的分析比较,指出了 LBS 隐私保护研究存在的问题及可能的解决方法;最后,对未来研究方向进行了展望.

关键词: 基于位置的服务/位置服务;位置隐私;查询隐私;隐私度量

中图法分类号: TP309

中文引用格式: 张学军,桂小林,伍忠东.位置服务隐私保护研究综述.软件学报,2015,26(9):2373−2395. http://www.jos.org.cn/1000-9825/4857.htm

英文引用格式: Zhang XJ, Gui XL, Wu ZD. Privacy preservation for location-based services: A survey. Ruan Jian Xue Bao/Journal of Software, 2015,26(9):2373−2395 (in Chinese). http://www.jos.org.cn/1000-9825/4857.htm

Privacy Preservation for Location-Based Services: A Survey

ZHANG Xue-Jun[1,2,3], GUI Xiao-Lin[1,3], WU Zhong-Dong[2]

[1](School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

[2](School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China)

[3](Shaanxi Province Key Laboratory of Computer Network (Xi'an Jiaotong University), Xi'an 710049, China)

Abstract: Location-based service (LBS) has recently become popular in almost all social and business fields due to the boom of location-aware mobile electronic devices. LBS, albeit providing enormous benefits to individuals and society, poses a serious threat to users' privacy as they are enticed to disclose their locations and query attributes to untrusted LBS providers via their LBS queries. Moreover, the contextual information attached to these locations and service attributes can reveal users' personal interests, life styles, health conditions, etc. How to preserve users' privacy against potentially malicious LBS providers is of vital importance to the well-being of LBS ecosystem, and as such, it attracts great attentions from many researchers. This paper provides a review of the state-of-the-art of privacy preserving for LBS. First, the concept and threat model of LBS privacy are presented. Then, the existing schemes for preserving users' LBS privacy are described in detail from the aspects of architecture, metric and technology. Next, a pointed discussion is placed on

* 基金项目: 国家科技重大专项 (2012ZX03002001); 国家自然科学基金(61472316, 61172090, 61163009, 61163010); 高等学校博士学科点专项科研基金(20120201110013); 陕西省科技攻关项目(2012K06-30, 2014JQ8322); 中央高校基础科学研究基金(XJJ2014049, XKJC2014008); 陕西科技创新项目(2013SZS16-Z01/P01/K01); 兰州交通大学青年科学基金研究项目(2014026)

收稿时间: 2014-05-22; 修改时间: 2014-06-20, 2015-03-30; 定稿时间: 2015-05-14

the latest mainstream technology, with emphasis on the distortion-based technology. Further, following a comprehensive comparison and analysis of the performance and defects of various technologies, the problems and possible solutions for LBS privacy preserving are pointed out. Finally, some future research directions are provided.

Key words: location-based service; location privacy; query privacy; privacy quantification

随着无线通信技术和移动定位技术的发展,越来越多的移动设备具备 GPS 精确定位功能,使得位置服务(LBS)日益风行,是为移动用户提供的最有前途的服务之一.LBS 是指基于移动设备的地理位置和其他信息,为移动用户提供的信息和娱乐服务[1],其典型应用包括地图类应用(如 Google Maps)、兴趣点检索(如 AroundMe)、优惠券或折扣提供(如 GroupOn)、GPS 导航(如 TomTom)和位置感知社会网络(如 Foursquare)等.早期的 LBS 系统主要用于军事和涉及国家重要利益的民用领域.目前,LBS 已被广泛应用在军事、政府产业、商业、医疗、紧急救援、民生等领域[2].美国著名的市场研究公司 ABI Research 发布预测,LBS 全球总收入将由 2009 年的 26 亿美元上升到 2014 年的 140 多亿美元.然而,LBS 在给个人和社会带来巨大好处的同时,也引发了严重的隐私关注.因为用户获取 LBS 时需要报告他们的位置信息,而位置数据既直接包含了用户的隐私信息,又隐含了用户通常想保护的其他个人敏感信息,如家庭住址、生活习惯、健康状况和社会关系等.因此,把这些私人信息泄露给不可信的第三方(如 LBS 提供商),会打开滥用个人数据的大门,对用户各方面的隐私带来严重威胁.例如,从匿名 GPS 数据中能推断出个人的家庭地址、工作单位和社会关系[3,4],预测出用户过去、现在和将来的位置[5],推断出个人的行踪[6];甚至可以利用室内位置信息推断出个人的工作角色、年龄、爱好(如是否抽烟)等[7].因此,对用户的 LBS 隐私进行保护是一个至关重要的问题.

移动互联网、社会网络、大数据等新兴技术的发展和广泛使用,使得 LBS 隐私保护问题越来越严重,成为工业界和学术界广泛关注的热点问题.2003 年,Beresford 提出位置隐私的概念[8],开启了对 LBS 隐私保护研究的先河.此后,LBS 隐私保护日渐成为信息技术领域的研究热点,许多著名的国际会议及期刊陆续发表了大量 LBS 隐私保护的相关研究成果.本文综述 LBS 隐私保护研究的最新进展.发表的文献中,已有一些关于 LBS 隐私保护的综述文献:Ghinita[9]从私有查询和轨迹匿名两个方面对位置隐私进行了综述,但没有涉及隐私度量和查询隐私;Krumm[10]着重评述了匿名、模糊化隐私保护技术和一些利用位置数据几何性质的隐私侵犯算法,但没有涉及系统结构和查询隐私;霍峥等人[11]从传统关系数据隐私保护向时空方向拓展的角度对数据发布中的轨迹隐私保护和 LBS 中的轨迹隐私保护关键技术进行了分析和比较,但没有涉及查询隐私;Shin 等人[12]总结了 LBS 通用隐私威胁模型,分析比较了各种 LBS 隐私保护技术及度量指标,但对系统结构和保护技术的综述不够全面.而且,这几篇论文发表较早,无法收录之后的 LBS 隐私保护研究新进展.本文从 LBS 隐私的概念入手,分析 LBS 的隐私威胁模型,总结 LBS 隐私保护的体系结构和度量指标.依据不同 LBS 隐私保护技术在隐私保护度和服务质量之间的权衡,分类阐述基于政策法、扭曲法和加密法的 LBS 隐私保护技术研究进展,特别是新近的研究进展,全面比较和分析不同技术的优缺点及适用场景,并探讨未来的研究方向.

本文第 1 节介绍 LBS 隐私保护关键问题.第 2 节介绍 LBS 隐私保护系统结构.第 3 节阐述 LBS 隐私保护度量指标.第 4 节详细阐述和分析各种 LBS 隐私保护技术.第 5 节是各种主要 LBS 隐私保护技术的性能评估和比较.第 6 节总结全文并探讨未来的研究方向.

1 LBS 隐私保护关键问题

1.1 理解LBS隐私

LBS 应用的一个典型例子是关于最近兴趣点(POIs)的搜索引擎,如 Google Maps.用户使用具有 GPS 定位功能的移动设备向 LBS 服务器(也称 LBS 提供商)发送包含他当前位置和感兴趣服务属性(如医院等)的 LBS 请求,服务器会返回少量和用户指定服务属性相匹配的兴趣点,而且这些兴趣点在地理上接近于用户的当前位置.一般而言,一个 LBS 请求可看成是 LBS 服务器空间数据库上的一个查询,如:

SELECT TOP(k) FROM *POI* WHERE type=U_{poi} ORDER BY DISTANCE (*POI.location*,*userLoc*) ASC,

其中,*POI* 是兴趣点空间数据库;U_{poi} 是服务属性值,即查询内容;*userLoc* 是用户的当前位置;*k* 是预定义参数.通常,*userLoc* 在排序函数中被指定为常量,且要与 U_{poi} 一起发送给 LBS 服务器.为了叙述方便,将 LBS 查询定义为一个 4 元组$\langle u,t,loc,U_{poi}\rangle$,*u* 是用户标识,*loc* 是用户在 *t* 时刻提交查询的位置,U_{poi} 是服务属性.

用户在方便地访问各种 LBS 时,会不可避免地在网络中遗留下大量的数字踪迹和服务属性,附加在这些数字踪迹或服务属性上的上下文能揭露用户的个人习惯、兴趣爱好、人际关系、身体状况等私人信息.因此,将这些个人信息暴露给不可信的第三方势必会造成严重的隐私关注.LBS 隐私关注存在两个方面:查询隐私和位置隐私.查询隐私和 LBS 查询中 U_{poi} 的泄露相关,位置隐私与 LBS 查询中 *loc* 的泄露和滥用有关.

下面综合各种文献,给出与 LBS 隐私相关的一些描述性定义.

定义 1(隐私). 隐私是指个人、组织或机构等实体不愿意被外部知晓的信息,如个人兴趣爱好、政治信仰、公司的财务状况等等.

定义 2(个人隐私). 个人隐私一般是指数据拥有者不愿意披露的私人敏感信息,如兴趣爱好、健康状况、收入水平、宗教信仰和政治倾向等.由于人们对隐私的限定标准不同,所以对隐私的定义也就有所差异.一般来说,任何可以确定是个人的,但个人不愿意披露的信息都可以认为是个人隐私.

定义 3(位置隐私). 位置隐私是一种特殊的个人隐私,是指直接与 LBS 查询中的 *loc* 相关的个人敏感信息(如访问的位置是敏感的)以及由 *loc* 推理出的其他个人敏感信息(如兴趣爱好、健康状况、宗教信仰等).

个人的位置包括其现在或过去访问的位置[8,13]:实时位置可使攻击者(本文定义 LBS 服务器为攻击者)找到用户在哪,过去的位置则可帮助攻击者发现用户是谁、住哪、想做什么等.所以,位置隐私涉及:① 用户是否被精确定位;② 用户的个人敏感信息是否被从他访问的位置中推断出来.因此,位置隐私保护既要保护用户过去和现在位置本身的敏感信息不被泄露,又要防止攻击者通过用户位置推理出其他个人敏感信息.

定义 4(查询隐私). 查询隐私是一种特殊的个人隐私,是指与 LBS 查询中的 U_{poi} 相关的个人敏感信息(如查询内容是敏感的)或者从 U_{poi} 中推理出的其他个人敏感信息(如兴趣爱好,健康状况等).

服务属性及其与用户之间的关联往往被认为是敏感的,因为服务属性本身说明了用户的兴趣类别,会直接泄露用户的个人偏好或需求[14].所以,查询隐私涉及:① 用户是否被攻击者识别或去匿名;② 用户的私人敏感信息是否被从他请求的服务属性中推断出来.因此,查询隐私保护既要保证服务属性本身的敏感信息不被泄露,又要防止攻击者通过服务属性和用户的关联推断出其他个人敏感信息.

虽然位置隐私和查询隐私有区别,但它们也密切相关:一方面,如果用户被定位或跟踪(位置隐私泄露),那么他也相对容易被去匿名(查询隐私泄露),如,采用空间受限识别攻击[15]可以很容易俘获用户的查询隐私;另一方面,如果用户被识别,那么他的位置隐私也相对容易被泄露,因为在这种情况下,攻击者有更多可用的信息(如对用户的历史跟踪记录)来成功获得与位置相关的推理性攻击(如移动追踪攻击).

定义 5(LBS 隐私). LBS 隐私是一种特殊的个人隐私,是指由请求 LBS 所产生的查询隐私和位置隐私.

1.2 LBS隐私威胁

LBS 系统通常由移动终端、定位系统、通信网络和 LBS 服务器 4 部分组成,如图 1 所示:移动终端(如智能手机)向 LBS 服务器发送包含用户位置的 LBS 查询;定位系统(如 GPS)实时获取移动终端发送 LBS 查询时的位置;通信网络(如 3G 网络)传输 LBS 查询和从服务器返回的查询结果;LBS 服务器响应用户的查询,并返回定制结果.用户的隐私可能会在 3 个地方泄露:首先是移动终端,如果用户的移动设备被捕获或劫持,那么就会变成恶意的,可能会主动泄露用户的私有信息(包括但不限于位置信息),如何保护用户移动终端的安全本身也是一个非常活跃的研究话题,这里不做深入探讨,有兴趣的读者可参阅文献[16];其次是用户的 LBS 查询和返回结果在通过无线网络传输时,有可能被窃听或遭受中间人攻击,这可以通过传统的加密和散列机制解决;最后是 LBS 服务器,因为一个恶意的攻击者可能就是 LBS 服务器的拥有者或维护者,也可能是俘获并掌控 LBS 服务器的恶意攻击者.这两种情况下,恶意攻击者都能够访问存储在 LBS 服务器上的所有信息,如 IP 地址、用户每次提交的位置和服务属性等.虽然在说明通用 LBS 隐私威胁模型时没有对 LBS 的使用设定额外的要求(如假设用户必须登录后才能使用 LBS),但是攻击者仍能够利用一些侧通道(如每个查询的 IP 地址)和复杂的目标追踪算法把连续

的匿名LBS查询和用户关联起来.为了简化隐私保护问题,通用LBS隐私威胁模型都假定LBS服务器是恶意或不可信的,其他部分则是安全可信的.本文讨论的所有隐私保护技术都基于该通用隐私威胁模型.

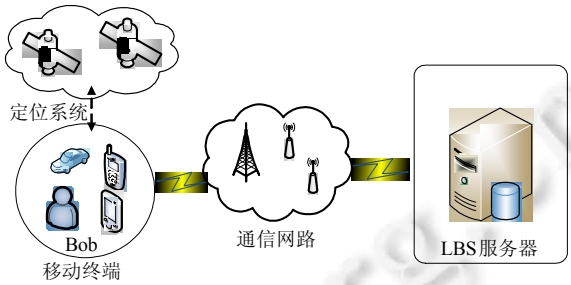


Fig.1 A common LBS architecture

图 1 LBS 通用系统架构

用户使用各种LBS应用时,LBS服务器会收集包含在查询中的用户位置或服务属性.受利益或好奇心驱使,攻击者会结合相关的背景知识,并利用各种攻击方法(如空间受限攻击和基于观察的识别攻击[15]、关联推理攻击[17]、位置相依性攻击[18−20]等),直接或间接的重构出用户希望保护的LBS隐私.经典的LBS隐私保护技术针对这种隐私威胁,确保用户在访问各种LBS应用时不会泄露个人隐私且能获得有用的服务,如使用隐私政策的访问控制策略[21,22]、针对快照查询的位置匿名化方法[15,23]、针对连续查询的轨迹匿名化方法[24−26]等.但是这些经典的隐私保护技术在面对大数据、社会网络等新兴技术时会遇到许多新的隐私威胁,例如:考虑攻击者从社会网络中获取的用户资料等背景知识,基于位置 k 匿名的隐私保护机制就会泄露用户的查询隐私[27];利用获取的位置大数据之间的关联等背景知识,可对精心匿名的位置数据进行成功的反匿名[28].这是因为攻击者可以利用这些新兴技术持续地收集用户的历史信息,并能从更多渠道获取用户的位置或与位置相关的非位置等各种类型的数据,从而使其具备掌握更多背景知识的能力.这样,攻击者将获取的各方面数据、位置和非位置数据之间的关系以及可用的背景知识等相结合,就能以很高的确定性推测出用户的个人敏感信息,从而使得经典LBS隐私保护技术不能提供充分的隐私安全保障.因此,如何防止攻击者利用获取到的各方面的数据并结合可用的背景知识来全面推测用户的LBS隐私,是应对新形势下LBS隐私威胁亟待解决的关键问题.

1.3 LBS隐私保护技术分类及性能评估

1.3.1 LBS隐私保护场景

下面来看一个例子,Alice使用智能手机请求“查询离我最近的肿瘤医院”.该查询由LBS服务器做出响应,并返回结果.由于LBS服务器不可信,Alice的敏感信息有可能被泄露或滥用.为了保护隐私,Alice通常不会与LBS服务器直接交互,而事先通过隐私保护技术对查询进行模糊化处理后再提交.该场景实际包含了LBS隐私保护的两个方面:位置隐私保护和查询隐私保护.例如,Alice不希望任何人知道她目前所在的位置(医院),也不希望任何人知道自己提出了哪方面的查询(与肿瘤相关的医院查询).前者是位置隐私保护的范畴,后者是查询隐私保护的范畴.这种场景下的LBS隐私保护技术是根据用户的个性化隐私需求进行信息论意义上的全面保护.因此,隐私保护技术需要解决以下几个关键问题:

(1) 如何准确地度量用户隐私的披露风险;

(2) 如何选择有效的隐私保护机制全面保护用户的隐私;

(3) 如何权衡用户的隐私水平、服务质量和资源开销.

当前,该场景下的LBS隐私保护技术主要针对用户不同程度的隐私需求,权衡隐私保护效果和服务可用性.

1.3.2 LBS隐私保护技术分类

保护用户的隐私是成功部署LBS应用的基本要求[9].目前,已提出了许多隐私保护策略来增强用户的隐私,但没有任何一种单一策略能够提供完全的解决方案.本文将LBS隐私保护技术分为3类.

(1) 基于政策法的LBS隐私保护技术.

这一技术是指通过制定一些常用的隐私管理规则和可信任的隐私协定来约束服务提供商能公平、安全的使用用户 LBS 查询中的位置信息或服务属性,如 IETF 的 GeoPriv[21]和 W3C 的 P3P[22].由于隐私政策系统本身并不能够执行隐私保护,往往依赖经济、社会和监管压力等,因而不能实现对用户隐私的有效保护,也不会在隐私和服务质量损失之间进行一定的权衡.

(2) 基于扭曲法的 LBS 隐私保护技术.

这一技术是指在 LBS 查询暴露给 LBS 服务器之前,事先对查询中的时空信息或服务属性进行适当地修改或扭曲,使LBS服务器无法获得精确的位置信息或服务属性.由于发送给LBS服务器的是经过扭曲的信息,会导致服务质量的损失,所以必须在用户希望保护的隐私水平和他们必须接受的服务质量损失之间进行必要的权衡.但是这类技术的实现往往依赖于攻击者的先验知识,易于遭受具有数据分布特征等背景知识的攻击.差分隐私[29]对背景知识不够敏感,可应用在 LBS 隐私保护中以抵御具有任意背景知识的攻击者[30,31].基于扭曲法技术的关键是:如何在考虑攻击者背景知识和推理能力的情况下设计出最佳的隐私保护方法,从而在满足用户最大容忍服务质量的前提下,尽可能降低用户隐私的披露风险[32].

(3) 基于加密法的 LBS 隐私保护技术.

这一技术指的是通过使用加密技术使用户的 LBS 查询对 LBS 服务器完全不可见,从而达到隐私保护的目的.这类技术在确保服务质量的情况下,不会泄露任何用户的位置信息,实现了更严格的隐私保护,如基于隐私信息检索的 LBS 保护技术[33].但是,基于加密法的技术没有考虑隐私度量问题,不能实现对位置隐私的全面保护,因此也无法在隐私和服务质量损失之间做出权衡.虽然最近提出的全同态加密技术[34]可以在不解密用户查询的情况下返回正确的查询结果,但效率仍是很大的问题.最新的研究说明:由于高效的数据访问方式会暴露数据之间的顺序,所以能提供完全隐私的高效加密方法是不存在的[35].

3 类技术各有优缺点:基于政策法的技术实现简单,服务质量高,但隐私保护效果差;基于扭曲法的技术效率较高,在服务质量和隐私保护上取得了较好的平衡,但位置信息或服务属性存在一定的不准确性,易遭受具有完全背景知识的攻击;基于加密法的技术能够完全保证数据的准确性和安全性,可以提供更严格的隐私保护,但需要额外的硬件和复杂的算法支持,计算和通信开销很大.

1.3.3 LBS 隐私保护技术性能评估

LBS 隐私保护技术需要在保护用户隐私的同时兼顾服务质量与开销.本文从以下 3 个方面度量 LBS 隐私保护技术的性能:

(1) 隐私保护度:反映 LBS 隐私保护技术披露隐私多寡的程度,一般用披露风险来描述,即:攻击者根据观察到的LBS查询以及其他可用背景知识可能披露LBS隐私的概率.披露风险依赖于攻击者掌握的背景知识,攻击者掌握的背景知识越多,隐私披露风险越大.本文使用位置隐私度量指标和查询隐私度量指标来量化披露风险;

(2) 服务质量:反映用户的 LBS 查询经隐私保护技术处理后获得服务结果的好坏,一般由查询响应时间和查询准确性来度量.在相同的隐私保护强度下,用户获得的服务质量越高,说明隐私保护技术越好;

(3) 开销:反映使用LBS隐私保护技术所带来的代价,包括预处理和运行时发生的存储、计算和传输代价.存储代价主要发生在预处理时;现有技术下,预处理代价通常较小,在选择隐私保护技术时被忽略;运行时的计算和传输代价一般使用隐私保护技术实现算法的时间复杂度和通信协议的通信复杂度来度量.LBS 隐私保护技术要在满足隐私保护度和服务质量的前提下尽量减少开销.

2 LBS 隐私保护系统结构

LBS 隐私保护技术以在线或离线的方式和不同的体系结构来实现:离线方式中,所有 LBS 查询中的时空信息对 LBS 隐私保护技术都是可用的;在线方式中,对 LBS 查询信息的修改是在用户不同时间访问新位置时实时执行的[23].LBS 隐私保护技术一般通过 3 种系统结构实现:集中式、分布式和混合式.

- 集中式结构由移动终端、可信匿名服务器、LBS 服务器组成,如图 2 所示.

用户使用移动终端向 LBS 服务器发送 LBS 查询,并获得最终的查询结果.可信匿名服务器包含匿名处理模块和查询结果精炼模块:匿名处理模块把移动终端发送过来的精确位置模糊化,并转发给 LBS 服务器;查询结果精炼模块接收 LBS 服务器返回的结果集对其进行精炼,并将精炼后的最终结果返回给移动终端.集中式结构具有用户的全局信息,隐私保护效果好,移动终端和匿名服务器之间的通信开销较小.但缺点是:① 匿名服务器可能成为系统的性能瓶颈和唯一攻击点;② 匿名服务器拥有所有用户的位置信息或服务属性等完全知识,一旦匿名服务器被攻破,可能会带来严重的隐私威胁;③ 现实中,部署具有大量用户的可信匿名服务器非常困难.

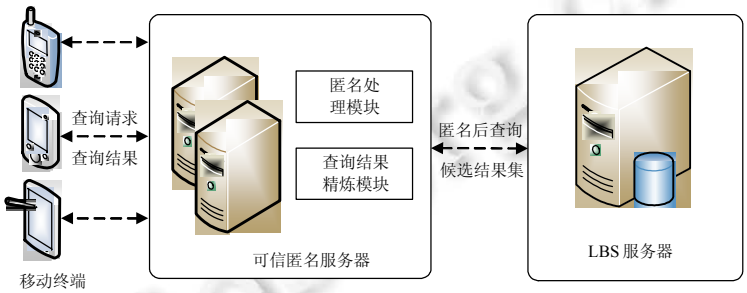


Fig.2 Centralized anonymization server-based architecture

图 2 集中式结构

- 分布式结构由移动终端和 LBS 服务器组成,如图 3 所示.

移动终端之间通过 P2P 协议,利用单跳和多跳通信形成一个匿名组,查询用户模糊化其位置为包含组内所有用户的空间区域,并将其转发给服务器,LBS 服务器返回包含正确结果的候选集,用户之间通过彼此协作完成隐私保护.分布式结构的优点:① 消除了系统的性能瓶颈;② 具有用户的全局信息,隐私保护效果好.缺点:① 增加了移动终端的通信和计算开销,在实际应用中无法有效保证参与隐私保护的其他用户是可信的;② 当服务请求用户附近没有足够的对等用户时,匿名过程很难完成.

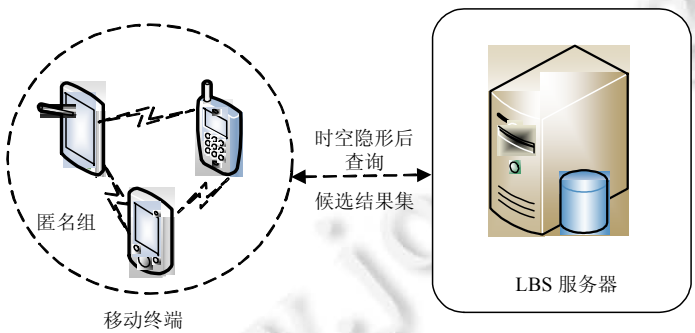


Fig.3 Distributed mobile device-based architecture

图 3 分布式结构

- 混合式结构由移动终端、可信匿名服务器、LBS 服务器组成,如图 4 所示.

移动终端通过可信匿名服务器请求服务,也可基于个性化的隐私、响应时间以及服务质量需求使用 P2P 协议完成隐私保护.匿名服务器拥有用户的身份、服务请求、位置等完全知识.混合式结构集成了集中式和分布式结构的优点,能够很好地平衡客户端和匿名服务器之间的负载[36]减少了匿名服务器由大量移动终端位置更新导致的负荷;在用户分布稀疏的情况下,仍能保证服务的可用性;但缺点是系统参数众多,设置和调整非常复杂,严重影响了它的实用性.

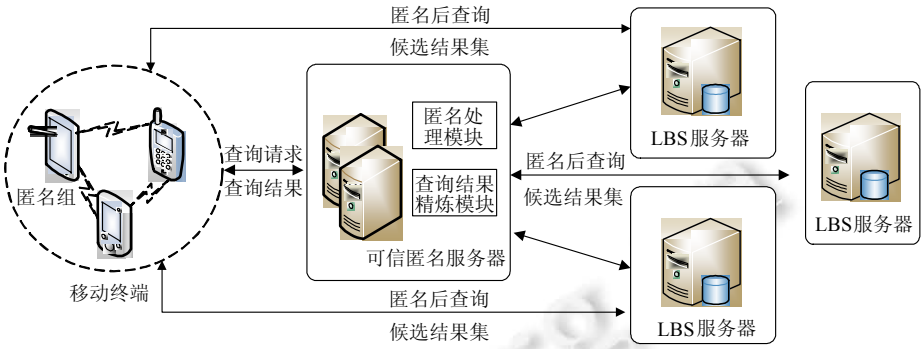


Fig.4 A hybrid architecture

图 4 混合式结构

3 LBS 隐私保护度量指标

为了评估和比较各种 LBS 隐私保护技术在实际中的隐私保护效果,一个系统的隐私度量方法是必不可少的.通过对隐私保护技术的度量,可以分析和确定影响用户隐私保护度的各种关键因素与需求,帮助设计者在隐私保护技术设计过程中平衡和优化各种需求,以便找到最好的隐私保护方法和度量指标[37].在 LBS 隐私保护领域,已有许多隐私度量指标,如 *k*-匿名、位置熵等.但这些指标大都针对特定的应用、攻击模型和隐私威胁,很难被泛化[38].即使是某一特定应用,也会发现各种可用的指标.例如,度量匿名通信网络的匿名水平有 Shannon 熵、最小熵、hartley 熵等.因此,目前仍不清楚它们中哪一个最适合给定的隐私保护场景[12].对已有隐私量化方法的全面比较,有利于学术界和工业界更好地理解其研究现状.目前,这方面的开创性研究[23,39]考虑了攻击模型、隐私威胁、用户数据模型、隐私保护技术、度量指标等多种影响用户隐私的因素,构建了一种统一的隐私量化模型,它能全面比较各种隐私保护机制和度量指标在不同攻击模型下的有效性.本文将 LBS 隐私度量指标分为查询隐私度量指标和位置隐私度量指标进行阐述.

3.1 查询隐私度量指标

k 匿名[40]最早使用在关系数据库的数据发布隐私保护中,核心思想是将准标识符 *QI* 进行泛化,使得单条记录无法和至少其他 *k*–1 条记录区分.Gruteser 等人[15]最先把关系数据库的 *k* 匿名概念引入 LBS 隐私保护领域,提出了位置 *k* 匿名.它是指 LBS 查询中的位置对应的是一个包含至少 *k* 个不同用户的区域,攻击者无法从这 *k* 个用户中分辨出真正的查询者.由这 *k* 个用户组成的集合称为匿名集,包含这 *k* 个用户的位置区域称为隐形区域.虽然该指标既能度量位置隐私又能度量查询隐私,但最近的研究证明,它对位置隐私无效[41].由于简单,位置 *k* 匿名已被多种方法采用(如时空隐形[15]、空间隐形[42]等)且在许多方面得到了精炼,如:通过定义信息泄露,量化隐形算法中位置信息的披露风险[43];利用位置多样性,确保隐形区域内包含至少 *l* 个不同的语义位置[44].由于位置 *k* 匿名定义没有考虑攻击者的背景知识,所以它在很多场合下不能正确反映用户的隐私保护度[27],除非攻击者的背景知识被合理地假设了.如:由扰动产生的哑元位置只有在攻击者看来同样可能是真实位置时才有用,任何可以排除这些哑元位置的背景知识(哑元位置是真实位置的概率较低)会立刻违反位置 *k* 匿名定义.为了避免这个问题,已有一些相应的对策,如:文献[26]考虑了普适、拥挤、均匀等概念来生成哑元位置,尽力使它们看起来更真实;文献[44]考虑了用户位置分布来生成隐形区域;文献[45]考虑了用户查询上下文和移动模型,使用服务属性的多样性来度量用户的查询隐私.从攻击者的角度看,服务属性越多样化,用户隐私的披露风险就越小.

位置熵是另一个被广泛使用的 LBS 隐私度量指标,它度量攻击者从一个或一系列位置更新中获得的信息量.熵[46]最早用于度量匿名通信中的隐私,攻击者的目标是识别系统中某个传输消息的发送者或接收者.每个用户都被分配了一个可能是消息真正发送者或接收者的概率,并用与这个概率相关随机变量的熵值作为系统的匿名度.随后,位置熵被广泛应用在 LBS 隐私度量中,用于度量查询隐私或位置隐私,这取决于熵如何定义.虽然

位置熵有广泛应用,但就如何选择合适的概率密度计算熵还没达成共识,目前仅有查询隐私度量中的混合区[8]、地理图网格[47]、某车辆轨迹的位置采样点[48]、某区域内用户的历史轨迹[49]等概率密度函数被深入研究了.位置熵虽能度量攻击者关于用户或位置的不确定性,但不能反映攻击者是否成功地获知了不同的用户位置,而且很少考虑攻击者的背景知识[39].为此,一些方法扩展了位置熵的概念,提出了一些新的指标来更好地量化查询隐私.例如:P-熟知度轨迹[49]利用某公共区域内所有用户历史轨迹的位置熵来度量该区域被用户熟悉的程度;互信息匿名[50]考虑了攻击者具有用户位置和相关的非位置数据,并利用查询被扰动前后用户的先验和后验知识来计算位置熵.平均时间混淆[48,51]和平均距离混淆[51,52]也建立在位置熵的概念之上:平均时间混淆度量隐私为攻击者成功追踪用户运动轨迹的时间,即,攻击者能正确跟随用户车辆轨迹直到不能再以充分的肯定性确定车辆踪迹时的时间;平均距离混淆以同样的方式定义,度量用户的隐私为攻击者正确跟踪用户运动轨迹的距离,即,攻击者能正确跟随车辆轨迹直到不能再以充分的肯定性来确定车辆踪迹时的距离.

3.2 位置隐私度量

位置熵也可用于度量位置隐私,关键在于熵的定义.例如,文献[53]应用不可观察性的概念,允许用户通过指定泄露给 LBS 服务器的位置及可能被用户访问的兴趣点数量来直观地定义位置熵;文献[54]考虑了隐形区域内用户的数量及分布来定义位置熵;文献[55]考虑隐形区域 c 内每个用户所有可能足迹的概率分布来定义位置熵 $E(c)$,并用 $2^{E(c)}$度量隐形区域的位置隐私.

期望距离误差[6,23]是量化位置隐私的一种自然方法,它直观地反映了攻击者利用观察到的模糊位置和掌握的背景知识猜测用户真实位置的准确程度.许多工作依赖于这一概念,如:文献[6]通过交叉用户的路径来迷惑攻击者,使追踪用户的路径成为一个挑战;文献[23]形式化了与攻击者推理攻击相关的精确性、确定性和正确性概念,提出了一个类似但更为普遍使用的期望距离误差指标,该指标能适用于正确定义攻击者的估计值和真实值之间距离的任何攻击模型,已被应用于以服务质量和用户属性为约束的最优位置模糊化机制[32]、以带宽和服务质量为约束的最优位置隐私保护机制[56]和基于用户合作的位置隐蔽化机制[57].期望距离误差以及基于这一概念的模糊化机制显式地定义在攻击者的先验知识之上,一旦现实中的攻击者具有一些在先验知识中没有假设的背景知识,则模糊化机制就不能有效地保护位置隐私[31].差分隐私[29]无需考虑攻击者所拥有的任何可能的背景知识,是目前能够针对攻击者先验知识进行普遍保护的最有效技术.相对于 k 匿名,不依赖攻击者先验知识的差分隐私指标开始在 LBS 隐私保护中引起重视[30,31],将成为 LBS 隐私保护的一个有潜力的研究方向.

基于 PIR 的 LBS 隐私保护技术通过把位置隐私保护问题转化为邻近查询问题,提出了一个理论意义上的解决方案.基于 PIR 的方法不需要隐私度量指标,因为隐私保护是通过加密技术获得的,位置信息不会泄露给攻击者.对攻击者而言,通过用户和服务器之间的通信来发现用户的位置信息在计算上不可解.

4 LBS 隐私保护技术

4.1 基于政策法的LBS隐私保护技术

隐私政策依赖 LBS 提供商实现和执行,主要采用分布式体系结构.它既能保护位置隐私又能保护查询隐私,这取决于政策的具体设计.隐私政策用于禁止 LBS 查询$\langle u,t,loc,U_{poi}\rangle$中 loc 的某些用途被不正当使用的一种基于信任的机制,其目标是能够提供足够灵活的适应个体用户、个别情况和交易需求的隐私保护.基于政策法的技术主要依赖经济、社会和监管压力等促使 LBS 提供商能按照隐私管理规则和可信任的隐私协定,公平、安全地使用 LBS 查询中的位置信息.GeoPriv 和 P3P 是两个比较有名的基于政策法的技术:

- GeoPriv 工作组[21]采用存在信息数据格式作为位置隐私的隐私政策系统,关注如何在 Internet 协议中合理地表示位置信息并研究位置信息被创建、存储或使用时的相关隐私问题,工作组的目标是提供能广泛适用于位置感知应用的详细规范.为了保护位置隐私,GeoPriv 规范定义了一个位置对象,封装了单个用户的位置和隐私政策.隐私政策的核心是描述信息可被接受使用的规则;
- P3P[22]用于保护用户的数据隐私,它可以帮助 Web 用户向提供商表达他们的数据使用和管理规则、理

解提供商提供的政策,这极大地促进了与隐私相关的一些决策.对于普通 Web 用户,P3P 在 LBS 中的应用被认为是加强对隐私政策的理解和对提供商的信任.虽有很多优点,但 P3P 缺乏提供商对隐私政策执行的详细说明.为了依赖 P3P,用户必须信任提供商能完全忠诚地遵守 P3P 政策.

基于政策法的技术会继续发展和完善,但它仅是对 LBS 隐私保护问题的部分回答:首先,隐私政策往往非常复杂且在频繁更新、高度动态的位置感知环境中的实用性至今仍未得到检验;其次,隐私政策系统本身并不能执行隐私保护,需要依赖经济、社会和监管压力等.因此,隐私政策最终易于导致个人信息的无意或恶意披露.

4.2 基于扭曲法的LBS隐私保护技术

基于政策法的技术易于导致隐私的泄露,需要更强执行力的技术来保护用户隐私,因为用户掌控他的 LBS 查询信息越多,就越会感到安全,也越有利于全球 LBS 生态系统的繁荣.过去几年里,基于扭曲法的 LBS 隐私保护技术已成为 LBS 隐私保护社区最活跃的研究方向[58].它是指对 LBS 查询中$\langle u,t,loc,U_{poi}\rangle$的原始数据进行必要的扰动,以避免攻击者获得用户的真实数据,同时要能保证用户不受妨碍地获得服务.采用的技术主要包括假名(删除或用一个临时的标识代替用户身份)、随机化(添加哑元)、模糊化(泛化或扰动查询中的时空信息)和隐蔽化(对攻击者隐蔽整个查询).对每种技术按照采用的体系结构和度量指标进行分类阐述.

4.2.1 假 名

假名技术采用了集中式结构,因为假名的发布、使用、撤销等需要在可信服务器上完成.假名技术是将 LBS 查询$\langle u,t,loc,U_{poi}\rangle$中的 u 用一个临时的假名代替或者直接删除 u,以达到打破用户身份和查询之间的联系.假名是一个对象的标识而非真实的名字[59],不包含用户能被识别的信息.因此,LBS 查询不会被连接到用户标识上,从而保护了用户的查询隐私.通常,为了增强假名的有效性,往往需要结合一些复杂的加密方法[60].仅仅采用假名并不能充分地保护查询隐私,因为攻击者可以通过多种方式(如监测手机的信号等)获得用户的位置,并借助一些公开的信息确定用户的身份[15].例如,用户 U 发送了一个 LBS 查询 q,其中包含用户的 loc.攻击者 A 得到了 q,且知道 loc 是专属于用户 U 的,则攻击者基本可以肯定 q 是由 U 发出的.通过查询地址黄页,攻击者 A 就可以确定用户 U 的身份.用户的身份一旦被确定,所有其他敏感信息都将泄露.通过频繁改变假名,可以减少攻击者利用积累的历史信息推断用户身份或行为的机会[8],但是如果用户的偏好数据被存储在服务器上,攻击者仍可能会把连接到单个用户数据上的所有假名关联起来.另外,用户运动的时空信息存在关联,即使频繁更换假名,用户仍会被跟踪识别.利用混合区能增强假名更换的有效性[8,61],混合区内用户不会提出任何请求也不接收任何信息.离开混合区时,每个用户都被分配一个新的假名,这使得攻击者追踪用户很困难.虽然混合区削弱了攻击者关联用户新旧假名的能力,但如果攻击者考虑用户的移动模型,则混合区的有效性显著下降.引入假名更换发生时刻或地点测定的模糊性,可以增强混合区的有效性[62,63],但在混合区内不进行任何通信,导致服务质量下降.为了减轻这个问题,混合区要保持较小的规模,这反过来又限制了假名的不可连接.即使混合区被优化配置,攻击者的成功仍相对很高[64].单混合区易遭受具有先验知识[65]的推理攻击,会导致用户身份和运行轨迹的泄露.为了获得期望的隐私保护水平,多混合区部署[17]可以增强查询隐私的保护度.混合区旨在保护查询隐私,因为它使混合区外不同假名连接到查询用户上变得困难,从而很难识别出真正查询用户.

位置 k 匿名和位置熵指标可用来评估混合区的有效性.位置熵指标会产生关于不确定性的更准确估计,有效减少了用户移动轨迹的泄露风险,被认为是设计隐私保护系统的一个有用指标.但假名技术易于遭受数据挖掘技术的威胁,因为用户的身份能从用户的位置信息中推断出.另外,由于身份信息被隐藏,这类技术对需要身份认证和个性化需求的应用是一个阻碍.

4.2.2 随机化

随机化是指在 LBS 查询$\langle u,t,loc,U_{poi}\rangle$中加入随机哑元(哑元可以是 loc 或 U_{poi}),并将哑元查询和真实查询一起发送给 LBS 提供商.但是随意地对查询进行随机化并不能保护隐私,哑元查询只有在攻击者看来同样可能是真实查询时才有用.随机化采用分布式结构,用户在移动终端上产生哑元查询,并将其和真实查询一起提交,LBS 提供商响应所有查询并向用户返回所有结果.图 5 是随机化的一个例子,其中,A 是用户所在的位置.为了保护位置隐私,用户查询离其最近的饭店时,先用设备随机产生两个哑元位置 B,C,然后将其和 A 一起发送,LBS 提供商

响应查询并返回距每个查询位置(*A*,*B*,*C*)最近的饭店列表.用户根据其位置过滤列表,得到离自己真实位置最近的饭店列表.如果产生的哑元位置和真实位置的差别很大,那么很容易被攻击者区分.因此,随机化技术的关键是如何以智能的方式产生有效的哑元,从而使攻击者很难识别真实的查询且不会耗费太大的开销.

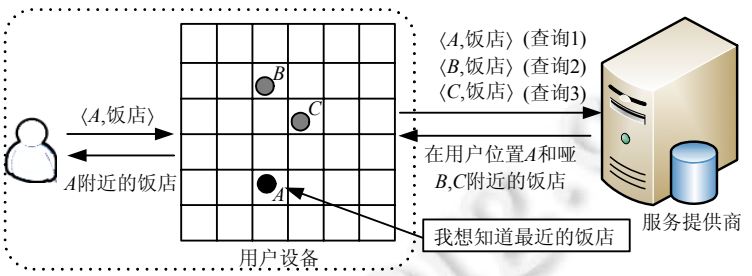


Fig.5 Example of randomization

图 5 随机化示例

文献[26]最先使用了随机化技术,它考虑了诸如普适、拥挤、均匀等指标来产生和那些真实用户移动模式相近的哑元位置,试图使它们看起来更真实.但由这些哑元位置组成的历史数据中的移动特征与真实对象的移动特征具有很大的差别,甚至产生的一些位置可能是实际中不可用的位置(如在海洋里),很容易被攻击者识别.因此,哑元位置的产生需要考虑真实环境的一些约束,如运动的一致性、路网、移动速度等[66],以及用户运动模式的真实特点,如用户移动一段距离或时间后可能会有停留等[67],以防止攻击者区分出这些哑元位置.随机化技术也被用来保护查询隐私,如 DUMMY-Q 方法[45]产生的哑元是 U_{poi},哑元的产生考虑了查询上下文和用户的运动模型.通过将真实查询隐藏在多个位置相同但 U_{poi} 不同的哑元查询中来迷惑攻击者,增加了攻击者观察服务属性的不确定性.产生的 U_{poi} 越多样化,用户的查询隐私就越高.

虽然随机化技术通过添加哑元获得了一定的隐私保护,但产生能迷惑攻击者的有效哑元是一项艰巨的任务[68],因为哑元查询要在空间和时间上看起来像真实查询,最近的研究[69]在这方面取得了一些进展.另外,产生哑元的最优算法仍然是一个开放性的问题.

4.2.3 模糊化

模糊化是指泛化或扰动 LBS 查询$\langle u,t,loc,U_{poi}\rangle$中的$\langle t,loc\rangle$,使攻击者无法识别查询用户及精确位置.泛化是指以可控的方式降低查询中$\langle t,loc\rangle$的精度,通常用一个区域或时段来代替,以便一定数量的用户和查询用户共享相同的$\langle t,loc\rangle$.区域和时段的计算称为隐形.泛化包括空间泛化和时间泛化:空间泛化在一定程度上降低查询中 *loc* 的精度,以满足用户的隐私需求,并确保用户不受妨碍地获得 LBS 服务;时间泛化通过增加位置数据时间域 *t* 的不确定性来减少 *loc* 的精度.扰动是指在 *loc* 中以可控的方式有意地引入部分错误,如用锚点代替真实位置[70],但数据仍要满足给定的服务质量要求.

4.2.3.1 基于集中式结构的隐私保护技术

匿名服务器负责泛化和扰动 LBS 查询的$\langle t,loc\rangle$,并将由模糊数据得到的查询结果转换为用户需要的结果.空间泛化技术通常采用位置 *k*-匿名将用户提交的精确位置点模糊为一个包含至少 *k* 个不同用户的隐形区域,使得攻击者无法获得查询用户的精确位置或身份.图 6(a)给出了某一时刻用户 u_1~u_6 的空间位置划分,表示成四分树结构.为了保护隐私,用户希望每次提交给 LBS 服务器的是一个包含 $k(k=3)$个用户的隐形区域,而不是只包含自己的位置.于是,u_1将包含自己和u_2,u_3的左下角阴影区域,u_4将包含自己和u_5,u_6的右上角阴影区域作为自己的位置提交给 LBS 服务器.LBS 服务器根据隐形区域计算其中所有位置点的查询结果,并返回给匿名服务器.

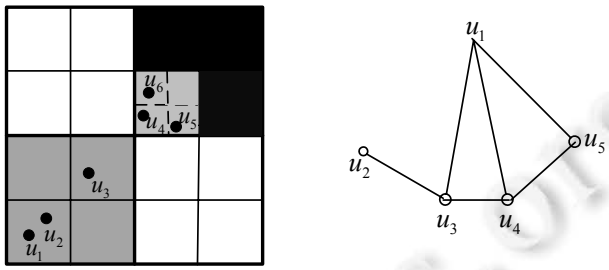
一方面,空间泛化技术如时空隐形(IC)[15],CliqueCloak[71,72],Casper[42],hilbASR[73]等旨在保护查询隐私,要求攻击者在 *k* 个不同用户组中不能推断出哪个用户执行了查询;查询 l-diversity[74],m-invariance[14],p-sensitivity[75]等模糊了查询中的敏感 U_{poi},增加了攻击者关联用户和敏感 U_{poi} 的不确定性,保护了查询隐私;

另一方面,这类技术如位置多样性[44]、PrivacyGrid[76]、位置协商 GLON[77]也保护了位置隐私,要求攻击者

在一组共享一些语义性质的 k 个兴趣点中不能区分出用户的真实位置.

基于 k 匿名的空间泛化技术提交给 LBS 服务器的是一个包含 k 个点的隐形区域而非精确的位置点,服务器需要在该区域内选择若干参考位置进行查询,选择的参考位置越多越能得到准确的结果,但这增加了服务器的负载、响应时间和系统通信量,降低了服务质量.因此,需要在隐私和服务质量之间进行必要的权衡[32].在满足用户隐私需求的条件下,尽可能减小隐形区域以提高服务质量.如图 6 所示,实际上,u_4 不需要提交整个右上角的 4 个区域,而只需将右上角浅色区域提交即可,这样可以减少传输结果.利用三角形两边之和大于第 3 边的性质,可求得更小传输的隐形区域[42].除了当前位置,用户的历史位置数据也被用来增强用户的位置隐私,隐形中产生的 k 匿名轨迹(KAT)[24]极大地减小了隐形区域,显著降低了计算和通信开销.

为了增强空间泛化技术在连续查询隐私保护[78]以及基于攻击者先验知识的隐私保护[73,79]中的有效性,隐形区域的产生需要考虑用户移动位置之间的相关性(如 KAA[54])以及抵御知道隐形区域生成策略和用户空间分布的恶意攻击者(如政策感知 k 匿名算法 PAKA[79]、hilbASR 算法[73]),从而在满足用户隐私需求的情况下,尽可能减小隐形区域.另外,隐形区域的产生也要考虑用户个性化隐私需求的影响.因为用户的隐私需求是动态的、多样性的,会随空间和时间的不同有所不同[55].文献[80]考虑到隐私需求需要保证两个连续提交的隐性区域间在速度上是可达的,并根据用户的实际速度修正了提交的隐形区域,这种隐私需求在文献[18,19,72]中得到扩展,允许每个用户具有不同的隐私要求.比如在图 6(a)中,用户 u_1 要求提交的隐形区域至少包含 2 个用户,而用户 u_4 要求提交的隐形区域至少包含 3 个用户,为了满足每个用户的不同隐私需求,每一时刻各个用户之间的关系可用图 6(b)表示,其中,考虑速度因素后依然可以保护隐私的用户之间用边相连.为了应对个性化的隐私需求,每个用户都要维护图 6(b)中包含自己的最大点团.在图中寻找最大点团是一个 NP-hard 问题,ICliqueCloak 算法[18]增量的维护每个用户的最大点团,减少了用户请求的响应时间.由于路网、用户密度、移动速度等因素影响,空间泛化技术有时容易失效,需要考虑使用时间泛化技术来实现用户的隐私需求[18,19,25,72,81].



(a) 四分树 (b) 点团

Fig.6 Example of spatial generalization

图 6 空间泛化示意图

许多基于 k-匿名的泛化技术已被证明不能充分地保护 LBS 隐私[41],但是具有差分隐私保证的扰动技术已被证明可以有效地抵御具有任意背景知识的攻击者[30,31].文献[30]提出了一个组合差分隐私和 k 匿名的位置隐私保护机制,要求从这 k 个固定位置(定义为匿名集)中的任意一个产生同一扰动位置的概率应该是相似的.文献[31]基于泛化的差分隐私提出了形式化的位置隐私定义和随机化的噪声添加技术,允许用户泄露足够的位置信息来获得期望的服务,同时能满足提出的隐私概念.

Path Confusion[6]运用期望距离误差量化攻击者估计用户精确位置的准确性,通过路径扰动获得隐私保护.Path Confusion 首先定义应用程序对一组用户路径容忍的平均位置错误,然后,当每两个用户路径接近时,就扰动用户路径使其交叉以迷惑攻击者跟踪错误的用户,增加了攻击者关联用户和路径的难度.但是,算法的有效性依赖于用户路径的特征.当攻击者具有位置的先验知识和用户的公共移动模型时,扰动算法是否能够保护隐私仍是一个开放性的问题.这个方法可以保护位置隐私和查询隐私,因为它降低了攻击者追踪用户的能力,增加了攻击者估计位置和用户精确位置之间的距离误差.CacheCloak[47]也采用扰动技术,它缓存整个预测路径的 LBS

响应,并用这些响应回复用户查询.从提供商的角度看,CacheCloak 在不损失位置精度的情况下实现了实时位置隐私保护.但提供商仅能观察到CacheCloak预测的交叉路径,很难推断出查询用户的真实位置.CacheCloak解决了隐私保护和服务可用性之间不平衡的问题,但它运用 Cache 信息响应用户查询,系统的扩展性是一个很重要的问题.这种方法旨在保护位置隐私和查询隐私,因为它增加了位置匿名和用户移动的不可追踪性.

基于P-熟知度的位置模糊模型FBP[49]允许用户通过指定一个用户所在的公共区域而非 k 值来表示隐私需求,并把该公共区域作为用户的位置发送给服务器.FBP 采用四分树结构防止攻击者把 LBS 查询和用户关联起来.FBP 是一个查询隐私保护技术,因为它能防止攻击者识别出所选匿名集中缺少其他用户时的查询发送者.

4.3.2.2 基于分布式结构的隐私保护技术

由于集中式结构的缺点,隐私保护技术发展的趋势越来越倾向于基于分布式结构的隐私保护技术.在这类技术中,扰动或泛化 LBS 查询的时空信息由移动终端来完成.基于 k 匿名的模糊化技术虽然更适合集中式结构,但也有研究者提出了一些方法在分布式结构中实现它,其思想为:查询用户首先模糊自己的位置,并向邻近的用户广播;收到广播的邻近用户将自己模糊化后的位置发送给查询用户,直到查询用户收到至少 k–1 个用户的位置.查询用户随机选择 k–1 个用户与自身构成一个 k 匿名集,并将包含该匿名集的隐形区域或任意一个非查询用户的位置发送给 LBS 提供商.显然,这种方法需要查询用户和邻近的至少 k–1 个用户相互协作才能实现隐形,这增加了整个方法的通信复杂度,例如,CloakP2P[82]形成的隐形区远远大于实际需要,且在许多情况下攻击者能以远大于 1/k 的概率识别出查询请求者.MobiHide[83]使用 Hilbert 曲线将二维空间用户坐标映射到一维空间,通过在转换空间内生成包含 k 个用户的隐形区域,提供了接近理论边界 1/k 的隐私保证.基于 Proximity 的方法[84]使用查询用户的代理信息而非当前位置进行隐形,代理信息通过用户移动设备接收到的信号强度或信号到达的时间差来构建.然而,如果查询用户无法探测到附近足够多的用户,则这种方法可能会变得无效.CAP[85,86]利用位置数据和网络通信来保护用户的查询隐私,它通过构造 VHC-mapping 获得 k 匿名效果.因为在移动设备上执行 k 匿名需要地图知识,下载整个地图到移动设备上会带来了严重的计算和存储开销.VHC-mapping 把二维的地理位置投影到一维空间,并使用四分树保持道路密度信息,减少了计算和存储开销.为了不泄露与查询用户形成 k 匿名的其他相遇参与者,SMILE[87]通过选择位置哈希值的前缀长度来保护查询隐私,但是该方法很难应用在广范围的 LBS 服务中,因为相遇参与者的概念可能在某种服务中不存在.

基于非 k-匿名的分布式技术也被研究了,如利用假位置或地标代替用户的真实位置来获得相应的 LBS 服务.因为攻击者并不知道用户的真实位置,保护了用户的位置隐私.SpaceTwist[70]随机选择锚点代替用户的真实位置向服务器发起多轮增量近邻查询,每个用户根据自己的真实位置和增量近邻查询结果计算得到精确的查询结果.位置隐私保护度由锚点和真实位置的距离确定.SpaceTwist 虽避免了由区域查询造成的高计算和通信开销,但隐私保护度不高.CoPrivacy[88]扩展了 SpaceTwist,增强了用户的位置隐私,它通过用户间的协作形成 k 匿名组,并用该匿名组的区域密度中心作为锚点,增量的从 LBS 服务器中获得近邻查询结果.

4.2.4 隐蔽化

隐蔽化是指通过从 LBS 服务器上完全删除和隐藏 LBS 查询$\langle u,t,loc,U_{poi}\rangle$来达到保护用户隐私的目的,主要思想是:用户请求 LBS 时不是向 LBS 服务器发送查询,而是向自己附近的同伴(如附近其他可访问的用户设备)请求查询信息,从而对 LBS 服务器隐蔽查询,最大化了用户的位置隐私.文献[89]首先提出了隐蔽化方法,已经拥有一些具体位置信息(最初来于提供商,存储在用户设备的缓存中)的用户可以将它传递给正在搜索这样信息的其他附近用户.在信息过期之前,可以转手多次,用户之间可以通过无线 P2P 的方式进行交互.但由于没有考虑用户的移动模型,其实用性大打折扣.最近,他们使用位置区域集合上的离散隐马尔可夫链形式化了用户的移动模型,极大地提高了方法的实用性[57].隐蔽化技术采用分布式结构,使用攻击者的期望估计误差量化位置隐私.

4.3 基于加密法的LBS隐私保护技术

基于扭曲法的技术通过向 LBS 服务器提供模糊的位置或服务属性实现了隐私保护,但当用户需要更高的隐私时,这类方法要么提交非常不精确的查询数据,要么无法提交查询信息,从而无法获得服务.基于加密法的隐私保护技术通过加密 LBS 查询$\langle u,t,loc,U_{poi}\rangle$,使其对服务器完全不可见以达到保护隐私的目的.基于加密法的

隐私保护技术采用分布式体系结构,在确保服务可用性的情况下不会泄露任何用户的位置信息,实现了更严格的隐私保护.本文将其分为基于隐私信息检索的技术和基于空间转换的技术.

4.3.1 基于隐私信息检索的隐私保护技术

隐私信息检索(PIR)协议[90,91]最早用于访问网络中的外包数据,允许用户在服务器不知道其任何查询请求的情况下,从数据库中秘密地检索所需信息.它的实现方法按照隐私保护度的强弱分为基于计算能力的 PIR 协议和基于信息论的 PIR 协议[28]:基于计算能力的 PIR 协议通过降低理论上不可解或计算上不可行难题的复杂度,来保证攻击者无法区分用户对不同数据项的访问;基于信息论的 PIR 协议保证攻击者不管拥有多么强的计算能力,都无法区分用户对不同数据项的访问.由于基于信息论的 PIR 协议返回查询结果的传输代价太大,所以目前常采用基于计算能力的 PIR 协议.基于 PIR 的隐私保护技术[33,92−94]建立在 PIR 协议之上:数据库被设定为一个 n 位的二进制字符串 X(如图 7 所示),用户想要查找字符串 X 中第 i 位的值(如 X_i).为了保护隐私,用户向服务器提交一个加密 LBS 查询 $q(i)$,服务器做出响应并返回查询结果 $r(X,q(i))$,用户对查询结果 $r(X,q(i))$解密得到 X_i.虽然不同的 PIR 协议会有不同的通信代价和计算开销,但对基于 PIR 的 LBS 隐私保护技术来说,使用 PIR 协议访问 LBS 服务器的方法都是通过提供一个数据的编号(如 X_i)向服务器安全地获取这个数据的内容.需要说明的是:仅仅保护用户每一次检索数据块的隐私并不能保证用户整个查询请求的隐私,因为用户的一个 LBS 查询往往需要多次访问数据块才能获得结果,如汽车行驶中的路线导航查询,需要多次提交不同的起点和目的地.由于不同的位置会在一个查询中导致不同的 PIR 访问次数,所以攻击者可能会利用这些信息推测用户的当前位置[92−94].因此,为了避免攻击者的推测,就需要通过访问一些无用的数据块使用户在不同位置提交的查询都具有相同的 PIR 访问次数.但是,保证每次 PIR 访问不泄露用户信息会带来性能上的极大开销.为了消除这些性能上的开销,有研究者提出通过对原始数据进行预处理来加速服务的访问.当前,基于 PIR 的 LBS 隐私保护技术主要针对最近邻(NN)查询[33,92,93]和最短路径计算[94]中隐私泄露问题.

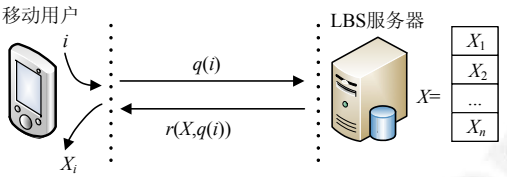
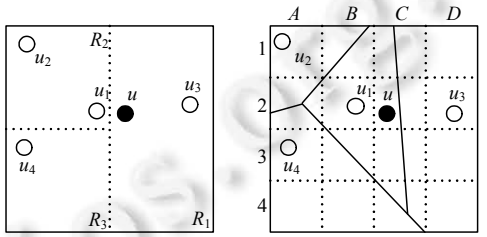


Fig.7 Framework for private information retrieval

图 7 隐私信息检索理论框架

NN 查询及其变体(如 k-NN)是 LBS 中常用的一类重要空间查询技术,用于搜索距离用户最近的一个或多个查询对象(如 POIs).当 LBS 服务器不可信时,NN 查询面临严峻的位置隐私泄露风险.已有一些工作逐步解决了保证严格隐私的 NN 查询[33]和 k-NN 查询问题[92,93].文献[27]为二进制数据(如 X)构建了基于计算的 PIR 协议 cPIR,cPIR 采用加密技术且依赖于事实:在给定 $q(i)$的情况下,攻击者几乎不可能通过计算找出 i 的值;但是用户能够很容易根据 LBS 服务器的响应值 $r(X,q(i))$计算出 X_i 的值.作者将 NN 查询分为近似 NN 查询和精确 NN 查询,并说明了如何应用 cPIR 以可接受的代价秘密地计算离用户位置最近的 POIs.图 8 给出了应用 PIR 寻找用户位置最近邻位置点的示意图.图 8(a)描述了近似 NN 查询:u 是查询用户,LBS 包含 4 个兴趣点 u_1,u_2,u_3,u_4.离线阶段,LBS 产生所有 POIs 的 kd-树索引,并把空间划分为 3 个区域 R_1,R_2,R_3.为了响应查询,服务器首先发送区域 R_1, R_2,R_3 给用户 u,用户查找包含自己的区域(如 R_1);然后,利用 PIR 来请求区域 R_1 中的所有 POIs.因此,服务器并不知道哪个区域被查询了.用户接受 R_1 中的 POIs(加密形式),并计算它的 NN 是 u_3.但结果是近似的,因为它的真实 NN 是 u_1.由于采用了 kd-索引,查询与任何点接近的索引就可以通过相同次数的 PIR 访问来完成,因此,攻击者不能区分用户的不同查询,无法推测用户的位置隐私.图 8(b)描述了精确 NN 查询:在预处理阶段,服务器为兴趣点集合计算维诺图(Voroni),每个兴趣点 u_i 被分配到它的维诺单元.按照维诺图定义,u_i 是其所在维诺单元内任意兴趣点的 NN.服务器在维诺图上叠加任意粒度的规则网络,每个网络单元存储关于它和维诺单元相交的信息,如

D_1存储$\{u_3\}$,C_3存储$\{u_1,u_3\}$.根据请求的查询,用户 u 首先检索网络粒度,计算包含 u(如 C_2)的网格单元,然后 u 利用 PIR 请求 C_2 的内容,接收加密形式的$\{u_1,u_3\}$并计算 u_1 为它的精确 NN.cPIR 协议不会泄露任何空间信息且能防止任何类型的基于位置的攻击(如关联攻击),但是它仅能应用在支持基于 PIR 协议的 LBS 服务器中,而且导致了服务器和移动设备都难以承受的计算和通信开销.文献[92]通过模糊 LBS 查询并基于 PIR 来处理范围和 k-NN 查询,获得了比 cPIR 更小的通信和计算复杂度.文献[93]采用安全硬件辅助的 PIR 协议,通过 k-NN 查询成功取得了很强的位置隐私.它将一个 k-NN 分解为一系列的数据库块检索,每个块检索都由安全硬件 PIR 执行,从而防止服务器识别出数据库块,而且所有查询都遵循混淆"块访问"模式的通用查询规则.因此,攻击者不能区分查询位置和数据空间中的其他任何位置,无法推测用户的位置隐私.



(a) 近似近邻 (b) 精确近邻

Fig.8 Finding the nearest neighbor of u with PIR

图 8 利用 PIR 查找用户 u 的最近邻示意图

最短路径计算是 LBS 中另一类最常见的查询.虽然很有用,但也引发了严重的隐私关注,因为暴露用户的位置和其目的地可能会泄露用户的个人隐私信息.应用基于 PIR 的隐私保护技术既可以保护用户的位置隐私,又可以得到正确的查询结果.文献[94]最先应用 PIR 协议研究了交通路网的最短路径查询隐私问题,通过提出简明索引策略获得了合理的检索时间,实现了最短路径计算的强隐私保护.但是,由 PIR 引发的时空开销仍远高于未受保护的查询处理,通过考虑数据特征和结构对网络数据进行压缩是一个可能的解决方案.

4.3.2 基于空间转换的 LBS 隐私保护技术

基于空间转换的隐私保护技术通过使用加密技术(空间填充曲线和单项哈希函数)把 LBS 查询$\langle u,t,loc,U_{poi}\rangle$中的 loc 和所有 U_{poi} 转换到一个不同的空间中,并在该加密空间中评估查询,以便只有用户自己能把转换数据映射为原来的空间信息[95−97].存储在 LBS 服务器上的数据以及用户提交的位置数据都被加密了,服务器在不泄露加密位置对应真实位置的情况下返回正确的查询结果.例如,基于 Hilbert 曲线的位置匿名方法 HilCloak[95]首先将整个空间旋转一个角度,在旋转后的空间中用密钥 H 建立 Hilbert 曲线,密钥只有用户和可信实体知道.在查询准备阶段,可信实体把每个兴趣点 p_i 转换为 Hilbert 值 $H(p_i)$,并上传到服务器上.查询时,用户 q 提交 $H(q)$给服务器,服务器返回离 $H(q)$最近的 Hilbert 值.HilCloak 可以保证用户任何位置分布的隐私,但仅能保证一次查询的隐私.文献[96]组合双曲线查询解析技术和加密哈希函数增强了 HilCloak 抵御具有强大先验知识攻击者的位置隐私,并降低了查询复杂度.文献[97]针对标准 Hilbert 曲线在转换兴趣点时没有考虑兴趣点分布特征,且划分粒度相同无法实现分级访问控制的问题,提出了一种新的空间转化方法.位置数据的转化采用随兴趣点分布特征变化的自适应 Hilbert 曲线,实现了多粒度的隐私保护.

5 LBS 隐私保护技术分析比较

本节对 3 类隐私保护技术进行对比分析,列举他们的优缺点和代表技术,见表 1.从计算开销、通信开销、隐私保护度、服务质量等方面对 3 类隐私保护技术的性能进行比较分析,见表 2.

从表 1、表 2 可以看出:每类技术都针对不同的应用需求,有各自的优缺点和性能表现,没有一种方法能够解决隐私保护的所有问题,具体方法的选择取决于应用场景和用户的实际隐私需求.当对隐私要求不高且需要获得很高服务质量时,采用基于政策法的隐私保护技术比较合适.当更加关注用户的隐私保护甚至要求完美的

隐私保护而不太注重计算和通信开销时,基于加密法的隐私保护技术是不错的选择.如何降低开销、提高实用性,是这类技术研究的关键.基于扭曲法的隐私保护技术能以较低的计算开销取得较好的隐私保护度,在满足用户个性化隐私需求的同时能提供较好的服务质量,但数据失真严重.如何根据用户隐私需求和给定的攻击模型设计满足服务质量和资源开销的优化隐私保护算法,是这类技术研究的一个重要方向.

Table 1 Comparison of the policy, distortion, and encryption based schemes

表 1 基于政策、扭曲和加密法的隐私保护方法比较

方法分类	主要优点	主要缺点	代表技术
基于政策法的LBS隐私保护技术	简单,容易实现,服务质量高	隐私度不高,假定LBS可信,自身不能解决隐私	IETF GEOPRIV[21], W3C P3P[22]
基于扭曲法的LBS隐私保护技术	简单,容易实现,在服务质量和隐私水平之间有较好的平衡	会受到基于数据特征推测的攻击,有隐私泄露风险,位置数据有失真	Path confusion[6], MixZone[8,61], IC[15], CliqueCloak[71], Casper[42], KAA[54], FBP[49], Dummy[26], DUMMY-Q[45], L2P2[55], KAT[24], PAKA[79], CloakP2P[82], Proximity[84], SpaceTwist[70], l-diversity[74], CacheCloak[47], GLON[77], ICliqueCloak[18], hilbASR[73], CAP[85], SMILE[87]
基于加密法的LBS隐私保护技术	隐私度、服务质量高	计算和通信开销大,部署复杂,需设计优化算法	基于空间转换的技术[95−97], PIR-based[33,92−94]

Table 2 Comparison of performance of the policy, distortion, and encryption based schemes

表 2 基于政策、扭曲和加密法隐私保护方法性能比较

方法分类	隐私保护度	计算开销	通信开销	服务质量
基于政策法的隐私保护技术	低	低	低	高
基于扭曲法的隐私保护技术	较高	低	中	较高
基于加密法的隐私保护技术	高	高	高	较高

表 3 分析对比了主要 LBS 隐私保护技术的分类、体系结构、隐私方法分类、隐私指标、隐私保护度和服务质量/开销等.隐私保护度用“高”、“中”、“低”,服务质量用“好”、“一般”、“差”来分别描述.

Table 3 Comparison of all LBS privacy protection techniques

表 3 各种 LBS 隐私保护技术比较

方法名称	方法分类	体系结构	隐私分类	隐私指标	隐私保护度	服务质量/开销
GeoPriv[21]	政策法	分布式	查询/位置隐私		低;取决于服务、社会、经济、监管压力等	好;精确查询
P3P[22]						
Mix zones[61]	扭曲法	集中式	查询隐私	位置k匿名和熵	中;取决于混合区中用户的假名个数	好;由混合区大小衡量,时间复杂度为$\Theta(\|V\|^2\|E\|)$,$\|V\|$是位置点数,$\|E\|$是位置点连接边数
Dummy[26]		分布式	位置隐私	普适、拥挤和均匀	低;取决于噪声位置的数量	差;由添加噪声后的位置数据的分辨率衡量,时间复杂度为$\Theta(k)$,k哑元数目,通信开销大
DUMMY-Q[45]			查询隐私	查询多样性	中;取决产生噪声服务属性的数量	好;由产生多样性服务属性的概率衡量,时间复杂度$\Theta(4^h d/h)$,h是四分树高度
IC[15]		集中式	查询隐私	位置k匿名	高;取决于匿名集中用户的个数	差;由隐形区域的面积衡量,时间复杂度$\Theta(k^2)$,k是用户指定的隐私参数
KAT[24]				位置k匿名	高;取决于同一匿名集中轨迹的数目	一般;由每时刻产生隐形区的面积衡量,时间复杂度为$\Theta(km)$,m轨迹数目,k隐私参数
hilbASR[73]					中;取决于匿名集中的用户数目	好;由产生隐形区域的面积衡量,时间复杂度为$\Theta(\log N+k)$,N是hilbert索引的数目,k是隐私参数

Table 3 Comparison of all LBS privacy protection techniques (continued)

表 3 各种隐私保护技术比较(续)

方法名称	方法分类	体系结构	隐私分类	隐私指标	隐私保护度	服务质量/开销
L2P2[55]	扭曲法	集中式	位置隐私	位置 k 匿名和熵	高;取决于每时刻匿名集中的用户数目	一般;由每时刻隐形区的面积衡量,时间复杂度 $\Theta(mL)$,m 是连续查询数,L 是四分树的高度
ICliqueCloak[18]			查询隐私	位置 k 匿名和熵	高;取决于匿名集中用户数目	一般;由隐形区域的面积衡量,时间复杂度为 $\Theta(\|V\|.\|M\|^2+\|V\|.\log\|V\|)$,$\|V\|$图的顶点数,$\|M\|$最大点团的个数
GLON[77]			位置隐私	位置 k 匿名	中;取决于位置混淆集的位置点的数目	好;由每时刻位置分辨率衡量,时间复杂度 $\Theta(n^2)$,n 是位置混淆集的大小
Geo-indis[31]				差分隐私	高;取决于参数ε和 r	一般;由添加的 Laplace 噪声的数量衡量
Pathconfusion[6]			查询/位置隐私	期望距离误差	低;主要取决于产生的假出发点、目的地的个数	差;由假出发点、目的地的数量衡量,时间复杂度 $\Theta(kN^3)$,k 是轨迹的数量,N 是轨迹片段的数量
FBP[49]				PPT	高;取决于匿名集内轨迹的数量	好;由每时刻产生的隐形框的面积衡量,时间复杂度为 $\Theta(km)$,通信开销小
CloakP2P[82]		分布式	查询隐私	位置 k 匿名	中;取决于匿名组中的用户数目	一般;由隐形框的面积衡量时间复杂度为 $\Theta(k)$,通信开销大
Proximity[84]			位置隐私		高;取决于同一聚类中的邻近用户的数量	一般;由最小 k 聚类的直径衡量,时间复杂度为 $\Theta(\log n)$,n 为用户数目
CAP[85]			查询隐私		中;取决于隐形区域内的用户数目	好;由查询返回结果的排序和真实排序之间的差别衡量,时间复杂度为 $\Theta(n)$,n 兴趣点数
SpaceTwist[70]			位置隐私	欧式距离	低;取决于真实位置和锚点的距离	好;精确查询,通信开销 $\Theta(\sqrt{n})$,时间复杂度 $\Theta(k)$,k 为用户指定的匿名参数,n 为兴趣点数目
MobiCrowd[57]				估计误差	高;取决于用户合作水平	一般;由用户的查询产生概率衡量.
PIR[33,92–94]	加密法	分布式	位置隐私		高;取决于 PIR 协议的安全性	好;计算复杂度 $\Theta(n)$,通信复杂度 $\Theta(\sqrt{n})$,n 是数据集的大小
HilCloak[95,96]					高;取决于转换函数的安全性	好;KNN 计算复杂度 $\Theta(k^{2^{2N}}/n)$,通信复杂度 $\Theta(K)$,N 曲线的度

可以看出:隐私保护度主要取决于匿名集中用户或轨迹的数目、添加噪声的数量、真假位置间的距离、模糊后的位置和原始位置的相似度、用户的合作水平和加密协议的性能等;服务质量由隐形区域的大小、真假位置的欧式距离、用户的查询产生率等来衡量.综合比较,基于扭曲法的隐私保护技术在隐私保护度和服务质量之间获得了较好的平衡,是目前 LBS 隐私保护的主流技术.基于加密法的隐私保护方法需要降低计算和通信开销,进一步提高其实用性.

6 总结展望

随着智能终端的普及和无线网络的快速发展,LBS 已成为用户最受欢迎的服务之一.但 LBS 也带来严重的隐私威胁,引起了用户、服务商和政府主管部门的重视以及学术界和工业界的重大兴趣.目前,已提出了大量的隐私保护技术来保证用户在享受 LBS 的同时不会侵害他们的隐私.本文对近几年该领域的研究成果进行了回顾:首先,分析了 LBS 隐私保护的关键问题和体系结构;然后,对隐私度量指标进行了总结;接着,对已有的隐私保护技术进行了分类;在此基础上,介绍了基于政策法、扭曲法和加密法的隐私保护技术,特别对当前的主流技术基于扭曲法的隐私保护技术进行了详细的分析;最后,对各类隐私保护技术进行了比较分析,指出了存在的问题

和可能的解决方法.总的来说,LBS 隐私保护研究仍处在起始阶段,有很多挑战性问题需要进一步研究:

(1) 系统的 LBS 隐私量化机制研究

位置隐私保护技术的发展依赖于量化位置隐私的能力[10],因此,位置隐私的量化对开发 LBS 隐私保护系统至关重要.然而,目前 LBS 隐私保护的研究主要集中在隐私保护技术的研发上,而对隐私保护系统可信性的评估和给定隐私保护技术有效性的度量还不够完善和成熟,明显缺乏系统化的度量方法来说明和量化各种隐私保护技术.而且已有的一些隐私量化机制对攻击者的背景知识和推理能力的假设不够完整,使得对已有隐私保护机制的评价和比较仍然存在着问题,可能会导致错误评估给定隐私保护系统提供的隐私保护度.文献[23]首先在这方面做了成功的努力,但文中的度量框架仅针对基于匿名和模糊的隐私保护方法,缺乏足够的泛化能力把所有的隐私保护技术纳入其中.另外,框架也没有考虑服务质量、各种 LBS 和不是以固定时间间隔提交查询对隐私度量的影响.因此,如何继续完善隐私度量框架,考虑影响 LBS 隐私保护的角色、数据、网络和查询提交时间等,提出能正确度量所有 LBS 隐私保护技术的指标和系统的量化机制,仍然是一个非常具有挑战性的问题.

(2) 混合加密技术的 LBS 隐私保护新方法研究

基于扭曲法的 LBS 隐私保护技术并不能完全保证用户的隐私不泄露,如时空隐形,当隐形框内的用户比较集中时,极端情况下集中在一点,用户的位置信息就有可能泄露.近年来,有学者提议在这类方法中加入适当的加密理论(如 PIR)以增强 LBS 隐私保护的强度.随着移动终端计算能力的提升,静态位置数据的加解密性能已经获得了很好的解决,但动态位置数据更新时的加解密性能仍是一个很大的挑战问题.由于 LBS 应用面对的设备(汽车、智能手机等)种类和数量庞大,还会频繁地移动,因此会产生海量、频繁更新的位置数据,而且这些数据有可能有缺失和非连续.在考虑动态数据加解密性能时,如何设计融合加密技术的优化 LBS 隐私保护新方法以保护动态位置数据获取有效服务过程中的 LBS 隐私泄露问题,也是一个非常重要的研究方向.

(3) 新兴技术应用中的 LBS 隐私保护技术研究

社交网络、移动互联网、大数据等新兴技术的出现提高了人们的生活质量,但也给 LBS 隐私保护带来新的挑战.因为移动定位手机已很普及,这些新兴技术一旦被采用,就会在短时间内变得非常流行且会拥有大量的活跃用户,典型的例子是移动社交网.如果这些新兴技术被误用或滥用,将会造成非常严重的危害.已有的 LBS 隐私保护技术直接应用在这些新兴技术中,不能有效保护用户的隐私.目前,这方面的研究已受关注,如移动社交网络位置推理性攻击[98]、近邻服务位置隐私保护[99]、移动社交网络位置与缺席隐私保护[100],但还处在初始阶段,需要继续发展和完善.特别是由这些新兴技术应用产的大数据,使攻击者能够从多种渠道和途径获得关于用户的更多背景知识来重构用户的隐私.因此,如何针对攻击者的背景知识考虑用户多种数据之间的关系,为新兴技术应用定制合适的 LBS 隐私保护模型,是一个很有前途的研究方向.我们认为,引入差分隐私是一个可行的解决方法.因为差分隐保护无需考虑攻击者所拥有的任何可能的背景知识,而且它建立在坚实的数学基础之上,对隐私保护进行了严格的定义并提供了量化评估方法,可以大大增强隐私保护处理结果的可靠性.另外,隐私保护问题一般都在新技术应用部署之后才考虑,如何在开发新技术应用工程的过程中把隐私保护作为一个主要的需求考虑,是一个重要的问题,包括形式化说明隐私需求和研究形式化的工具来证明隐私保护系统的有效性.

(4) 支持密文检索的空间外包数据隐私保护技术研究

随着各种感知设备的快速发展,LBS 提供商或其他机构已经收集了大量与位置相关的数据,使其维护和管理数据的成本持续上升.云计算为 LBS 提供了一种运营模式,即:LBS 提供商并不一定拥有自己的云平台,而是将自己的位置数据和服务外包给云服务商.查询用户直接向云服务商提出查询,云服务商将满足条件的查询结果返回给用户.但由于数据与服务的外包,导致非可信的云服务商有可能对外包数据进行窃取或篡改,造成用户隐私泄露及查询质量下降.在空间数据隐私保护方面,密文计算技术[101]在处理基于距离的查询方面(范围查询、KNN 查询)存在限制,无法在服务端完成密文数据大小的比较.另外,云服务商可能会提供不诚实的服务,对用户的检索结果进行篡改或删除[102,103].因此,研究适用于空间数据外包特征、支持空间数据密文检索和对检索结果进行完整性验证能力的隐私保护技术,是一个很有挑战性的问题.

(5) 个性化的 LBS 隐私保护工具

智能终端的普及和免费地图/导航软件的广泛使用,使面向公众的服务成为 LBS 的主体,如“基于位置的电子商务应用”、“基于位置的用户上下文感知及信息服务”等.用户在使用这些服务时,应当有权利和责任来保护他们的私有信息不被泄露.因此,急切需要开发能集成已有 LBS 系统的个性化隐私保护工具,如开发最小化的基于位置电子商务活动的信息泄露协议以及具有 LBS 隐私保护的浏览器等,这方面的研究工作比较少见.

隐私保护是一个复杂的社会问题,包括政策、技术、心理学和政治学等多个方面.隐私保护技术仅仅解决了问题的一个方面,识别和克服决策者在部署隐私保护技术时面临的非技术问题也同样重要,如服务质量的下降、有价值信息的丢失、开销代价和复杂度的增加等.因此,跨学科研究是解决这一问题的关键,迫切需要隐私保护领域的计算机科学家与心理学、社会学、公共政策研究等方面的社会科学家一起进行跨学科研究.来自不同学科的对隐私问题的深入理解,可以更好地帮助 LBS 隐私保护技术的发展与成功应用.

致谢 在此,我们向对本文的工作给予支持和建议的同行表示衷心的感谢.

References:

[1] Lee B, Oh J, Yu H, Kim J. Protecting location privacy using location semantics. In: Proc. of the 17th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining (KDD 2011). New York: ACM Press, 2011. 1289−1297. [doi: 10.1145/2020408.2020602]

[2] Zhou AY, Yang B, Jin CQ, Ma Q. Location-Based service: Architecture and progress. Chinese Journal of Computers, 2011,34(7): 1155−1171 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01155]

[3] Gambs S, Killiijian MO, Cortez MNdP. Show me how you move and I will tell you who you are. Trans. on Data Privacy, 2011, 2(4):103−126. [doi: 10.1145/1868470.1868479]

[4] Krumm J. Inference attacks on location tracks. In: Proc. of the 5th Int'l Conf. on Pervasive Computing. Toronto: Springer-Verlag, 2007. 127−143. [doi: 10.1007/978-3-540-72037-9_8]

[5] Song CM, Qu ZH, Blumm N, Barabási AL. Limits of predictability in human mobility. Science, 2010,327(5968):1018−1021.

[6] Hoh B, Gruteser M. Protecting location privacy through path confusion. In: Proc. of the 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks. Piscataway: IEEE, 2005. 194−205. [doi: 10.1109/SECURECOMM.2005.33]

[7] Matsuo Y, Okazaki N, Izumi K, Nakamura Y, Nishimura T, Hasida K, Nakashima H. Inferring long-term user properties based on users location history. In: Proc. of the 20th Int'l Joint Conf. on Artificial Intelligence. Hyderabad: Morgan Kaufmann Publishers, 2007. 2159−2165.

[8] Beresford AR, Stajano F. Location privacy in pervasive computing. IEEE Pervasive Computing, 2003,2(1):46−55.

[9] Ghinita G. Private queries and trajectory anonymization: A dual perspective on location privacy. Trans. on Data Privacy, 2009,2(1): 3−19.

[10] Krumm J. A survey of computational location privacy. Personal and Ubiquitous Computing, 2009,13(6):391−399.

[11] Huo Z, Meng XF. A survey of trajectory privacy preserving techniques. Chinese Journal of Computers, 2011,34(10):1820−1830 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01820]

[12] Shin KG, Ju XE, Chen ZG, Hu X. Privacy protection for users of location-based services. IEEE Wireless Communications, 2012, 19(1):30−39. [doi: 10.1109/MWC.2012.6155874]

[13] Liu L. From data privacy to location privacy: Models and algorithms. In: Proc. of the 33th Int'l Conf. on Very Large Data Bases. Vienna: VLDB Endowment, 2007. 1429−1430.

[14] Dewri R, Ray I, Ray I, Whitley D. Query m-Invariance: Preventing query disclosures in continuous location-based services. In: Proc. of the 11th Int'l Conf. on Mobile Data Management. Piscataway: IEEE, 2009. 95−104. [doi: 10.1109/mdm.2010.52]

[15] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. In: Proc. of the 1st Int'l Conf. on Mobile Systems, Applications, and Services. San Francisco: ACM Press, 2003.31−42.

[16] Bose A, Hu X, Shin KG, Park T. Behavioral detection of malware on mobile handsets. In: Proc. of the 6th Int'l Conf. on Mobile Systems, Applications, and Services. Breckenridge: ACM Press, 2008. 225−238. [doi: 10.1145/1378600.1378626]

[17] Liu XX, Zhao H, Pan M, Yue H, Li XL, Fang YG. Traffic-Aware multiple mix zone placement for protecting location privacy. In: Proc. of the 31th Annual IEEE Int'l Conf. on Computer Communications. Piscataway: IEEE, 2012. 972−980.

[18] Pan X, Xu JL, Meng XF. Protecting location privacy against location-dependent attacks in mobile services. IEEE Trans. on Knowledge and Data Engineering, 2012,24(8):1506−1519. [doi: 10.1109/tkde.2011.105]

[19] Xu JL, Tang XY, Hu HB, Du J. Privacy-Conscious location-based queries in mobile environments. IEEE Trans. on Parallel and Distributed Systems, 2010,21(3):313−326. [doi: 10.1109/tpds.2009.65]

[20] Ghinita G, Damiani ML, Silvestri C. Preventing velocity-based linkage attacks in location-aware applications. In: Proc. of the 17th ACM SIGSPATIAL Int'l Conf. on Advances in Geographic Information Systems. New York: ACM Press, 2009. 246−255.

[21] IETF, geographic location/privacy working group. 2012. http://datatracker.ietf.org/wg/geopriv/charter/

[22] W3C, platform for privacy preferences (P3P) project. 2012. http://www.w3.org/P3P

[23] Shokri R, Theodorakopoulos G, Le Boudec JY, Hubaux JP. Quantifying location privacy. In: Proc. of the 32nd IEEE Symp. on Security and Privacy. Oakland: IEEE, 2011. 247−262. [doi: 10.1109/Sp.2011.18]

[24] Xu T, Cai Y. Exploring historical location data for anonymity preservation in location-based services. In: Proc. of the 27th IEEE Int'l Conf. on Computer Communications. Phoenix: IEEE, 2008. 1220−1228. [doi: 10.1109/infocom.2007.103]

[25] Hwang RH, Hsueh YL, Chung HW. A novel time-obfuscated algorithm for trajectory privacy protection. IEEE Trans. on Service Computer, 2014,7(2):126−139. [doi: 10.1109/TSC.2013.55]

[26] Kido H, Yanagisawa Y, Satoh T. An anonymous communication technique using dummies for location-based services. In: Proc. of the 2nd Int'l Conf. on Pervasive Services. Santorini: IEEE Computer Society, 2005. 88−97. [doi: 10.1109/perser.2005.1506394]

[27] Chen XH, Pang J. Measuring query privacy in location-based services. In: Proc. of the 2nd ACM Conf. on Data and Application Security and Privacy. New York: ACM Press, 2012. 49−60. [doi: 10.1145/2133601.2133608]

[28] Wang L, Meng XF. Location privacy in big data era: A survey. Ruan Jian Xue Bao/Journal of Software, 2014,25(4):693−712 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4551.html [doi: 10.13328/J.cnki.jos.004551]

[29] Dwork C. Differential privacy. In: Proc. of the 33rd Int'l Colloquium on Automata, Languages and Programming. Venice: Springer-Verlag, 2006. 1−12. [doi: 10.1007/11787006_1]

[30] Dewri R. Local differential perturbations: Location privacy under approximate knowledge attackers. IEEE Trans. on Mobile Computing, 2013,12(12):2360−2372. [doi: 10.1109/tmc.2012.208]

[31] Andrés ME, Bordenabe NE. Geo-Indistinguishability: Differential privacy for location-based system. In: Proc. of the 20th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2013. 901−914. [doi: 10.1145/2508859.2516735]

[32] Shokri RS, Thedorakopoulos G, Troncoso C, Hubaux JP, Le Boudec JY. Protecting location privacy: Optimal strategy against localization attacks. In: Proc. of the 19th ACM Conf. on Computing and Communications Security. Raleigh: ACM Press, 2012. 617−627.

[33] Ghinita G, Kalnis P, Khoshgozaran A, Shahabi C, Tan KL. Private queries in location based services: Anonymizers are not necessary. In: Proc. of the 2008 ACM SIGMOD. New York: ACM Press, 2008. 121−132. [doi: 10.1145/1376616.1376631]

[34] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proc. of the 41st ACM Sympo. on Theory of Computing. New York: ACM Press, 2009. 169−178. [doi: 10.1145/1536414.1536440]

[35] Yao B, Li FF, Xiao XK. Secure nearest neighbor revisited. In: Proc. of the 29th IEEE Int'l Conf. on Data Engineering. Piscataway: IEEE, 2013. 733−744. [doi: 10.1109/icde.2013.6544870]

[36] Zhang CY, Huang Y. Cloaking locations for anonymous location based services: A hybrid approach. Geoinformatica, 2009,13(2): 159−182. [doi: 10.1007/s10707-008-0047-2]

[37] Ma ZD, Kargl F, Weber M. A location privacy metric for V2X communication systems. In: Proc. of the 2009 IEEE Sarnoff Symp. Piscataway: IEEE, 2009. 1−6. [doi: 10.1109/SARNOF.2009.4850318]

[38] Rebollo-Monedero D, Parra-Arnau J, Diza C, Forné J. On the measurement of privacy as an attacker's estimation error. Int'l Journal of Information Security, 2013,12(2):129−149. [doi: 10.1007/s10207-012-0182-5]

[39] Shokri R. Quantifying and protection location privacy [Ph.D. Thesis]. Ecole Polytechnique Federale de Lausanne, 2013.

[40] Sweeney L. *K*-Anonymity: A model for protecting privacy. Int'l Journal of Uncertainty, Fuzziness and Knowledge-Based System, 2002,10(5):557−570. [doi: 10.1142/S0218488502001648]

[41] Shokri R, Troncoso C, Díaz C, Freudiger J, Hubaux JP. Unraveling an old cloak: *k*-Anonymity for location privacy. In: Proc. of the 2010 ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2010. 115−118.

[42] Mokbel MF, Chow CY, Aref WG. The new Casper: Query processing for location services without compromising privacy. In: Proc. of the 32nd Int'l Conf. on Very Large Data Bases. Seoul: VLDB Endowment, 2006. 763−774.

[43] Tan KW, Lin YM, Mouratidis K. Spatial cloaking revisited: Distinguishing information leakage from anonymity. In: Proc. of the 11th Symp. on Spatial and Temporal Database (SSTD). LNCS 5644, Springer-Verlag, 2009. 117−134.

[44] Xue MQ, Kalnis P, Pung HK. Location diversity: Enhanced privacy protection in location based services. In: Proc. of the 4th Symp. on Location and Context Awareness. LNCS 5561, Springer-Verlag, 2009. 70−87. [doi: 10.1007/978-3-642-01721-6_5]

[45] Pingley A, Zhang N, Fu XW, Choi HA, Subramaniam S, Zhao W. Protection of query privacy for continuous location based services. In: Proc. of the 30th IEEE Conf. on Computer Communications. Piscataway: IEEE, 2011. 1710−1718.

[46] Serjantov A, Danezis G. Towards an information theoretic metric for anonymity. In: Proc. of the Workshop on Privacy Enhancing Technologies. LNCS 2482, Springer-Verlag, 2003. 41−53. [doi: 10.1007/3-540-36467-6_4]

[47] Meyerowitz J, Choudhury RR. Hiding stars with fireworks: Location privacy through camouflage. In: Proc. of the 15th Annual Int'l Conf. on Mobile Computing and Networking. New York: ACM Press, 2009. 345−356. [doi: 10.1145/1614320.1614358]

[48] Hoh B, Gruteser M, Xiong H, Alrabady A. Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking. IEEE Trans. on Mobile Computing, 2010,9(8):1089−1107. [doi: 10.1109/tmc.2010.62]

[49] Xu T, Cai Y. Feeling-Based location privacy protection for location-based services. In: Proc. of the 16th ACM Conf. on Computer and Communications Security (CCS 2009). New York: ACM Press, 2009. 348−357.

[50] Zhang XJ, Gui XL, Feng ZC, Tian F, Yu S, Zhao JQ. A quantifying framework of query privacy in location-based service. Journal of Xi'an Jiaotong University, 2014,48(2):8−13 (in Chinese with English abstract). [doi: 10.7652/xjtuxb201402002]

[51] Shokri R, Freudiger J, Jadliwala M, Hubaux JP. A distortion-based metric for location privacy. In: proc. of 8th ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2009. 21−30. [doi: 10.1145/1655188.1655192]

[52] Hoh B, Gruteser M, Herring R, Ban J, Work D, Herrera JC, Bayen AM, Annavaram M, Jacobson Q. Virtual trip lines for distributed privacy-preserving traffic monitoring. In: Proc. of the 6th Int'l Conf. on Mobile Sytems, Applications and Services. New York: ACM Press, 2008. 15−28. [doi: 10.1145/1378600.1378604]

[53] Chen Z. Energy-Efficient information collection and dissemination in wireless sensor networks [Ph.D. Thesis]. University of Michigan, 2009.

[54] Xu T, Cai Y. Location anonymity in continuous location-based services. In: Proc. of the 15th Annual ACM Int'l Symp. on Advances in Geographic Information Systems. New York: ACM Press, 2007. 1−8. [doi: 10.1145/1341012.1341062]

[55] Wang Y, Xu DB, He X, Zhang C, Li F, Xu B. L2P2: Location-Aware location privacy protection for location-based services. In: Proc. of the 31th IEEE Conf. on Computer Communications. Orlando: IEEE, 2012. 1996−2004.

[56] Herrmann M, Troncoso C, Diaz C, Preneel B. Optimal sporadic location privacy preserving systems in presence of bandwidth constraints. In: Proc. of the 12th ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2013. 167−178.

[57] Shokri R, Theodorakopoulos G, Papadimitratos P, Kazemi E, Hubaux JP. Hiding in the mobile crowd: Location privacy through collaboration. IEEE Trans. on Dependable and Secure Computing, 2014,11(3):266−279. [doi: 10.1109/TDSC.2013.57]

[58] Shokri R, Theodorakopoulos G, Danezis G, Hubaux JP, Le Boudec JY. Quantifying location privacy: The case of sporadic location exposure. In: Proc. of 11th Int'l Symp. on Privacy Enhancing Technologies. Waterloo: Springer-Verlag, 2011. 57−76.

[59] Pfitzmann A, Hansen M. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, unobservability, pseudonymity, and identity management (v0.34). 2010. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

[60] Schaub F, Ma ZD, Kargl F. Privacy requirements in vehicular communication systems. In: Proc. of the IEEE Int'l Conf. on Computational Science and Engineering. Piscataway: IEEE, 2009. 139−145. [doi: 10.1109/cse.2009.135]

[61] Beresford AR, Stajano F. Mix zones: User privacy in location-aware services. In: Proc. of the 2nd IEEE Annual Conf. on Pervasive Computing and Communication Workshops. Piscataway: IEEE, 2004. 127−131. [doi: 10.1109/PERCOMW.2004.1276918]

[62] Huang LP, Yamane H, Matsuura K, Sezaki K. Towards modeling wireless location privacy. In: Proc. of the 5th Int'l Workshop on Privacy Enhancing Technology. Cavtat: Springer-Verlag, 2005. 59−77. [doi: 10.1007/11767831_5]

[63] Huang LP, Yamane H, Matsuura K, Sezaki K. Silent cascade: Enhancing location privacy without communication qos degradation. In: Proc. of the 3rd Int'l Conf. on SPC 2006. Springer-Verlag, 2006. 165−180. [doi: 10.1007/11734666_13]

[64] Freudiger J, Shokri R, Hubaux JP. On the optimal placement of mix zones. In: Proc. of the 9th Int'l Symp. on Privacy Enhancing Technologies. Seattle: Springer-Verlag, 2009. 216−234. [doi: 10.1007/978-3-642-03168-7_13]

[65] Ma CYT, Yau DKY, Yip NK, Rao NSV. Privacy vulnerability of published anonymous mobility traces. In: Proc. of the 16th Annual Int'l Conf. on Mobile Computing and Networking. New York: ACM Press, 2010. 185−196.

[66] Suzuki A, Iwata M, Arase Y, Hara T, Xie X, Nishio S. A user location anonymization method for location based services in a real environment. In: Proc. of the 18th ACM SIGSPATIAL Int'l Conf. on Advances in Geographic Information System. New York: ACM Press, 2010. 398−401. [doi: 10.1145/1869790.1869846]

[67] Kato R, Iwata M, Hara T, Suzuki A, Xie X, Arase Y, Nishio S. A dummy-based anonymization method based on user trajectory with pauses. In: Proc. of the 20th ACM SIGSPATIAL Int'l Conf. on Advances in Geographic Information System. New York: ACM Press, 2012. 289−300. [doi: 10.1145/2424321.2424354]

[68] Chow R, Golle P. Faking contextual data for fun, profit, and privacy. In: Proc. of the 8th ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2009. 105−108. [doi: 10.1145/1655188.1655204]

[69] Niu B, Li QH, Zhu XY, Cao GH, Li H. Achieving *k*-Anonymity in privacy-aware location-based services. In: Proc. of the 33th IEEE Conf. on Computer Communications. Piscataway: IEEE, 2014. 754−762. [doi: 10.1109/infocom.2014.6848002]

[70] Yiu ML, Jensen S, Huang XG, Lu H. SpaceTwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In: Proc. of the IEEE 24th Int'l Conf. on Data Engineering. Piscataway: IEEE, 2008. 366−375.

[71] Gedik B, Ling L. Location privacy in mobile systems: A personalized anonymization model. In: Proc. of the 25th IEEE Int'l Conf. on Distributed Computing Systems. Piscataway: IEEE, 2005. 620−629. [doi: 10.1109/ICDCS.2005.48]

[72] Gedik B, Ling L. Protecting location privacy with personalized *k*-anonymity: Architecture and algorithms. IEEE Trans. on Mobile Computing, 2008,7(1):1−18. [doi: 10.1109/TMC.2007.1062]

[73] Kalnis P, Ghinita G, Mouratidis K, Mouratidis K, Papadias D. Preventing location-based identity inference in anonymous spatial queries. IEEE Trans. on Knowledge and Data Engineering, 2007,19(12):1719−1733. [doi: 10.1109/TMC.2007.1062]

[74] Liu FY, Hua KA, Cai Y. Query l-diversity in location-based services. In: Proc. of the 10th Int'l Conf. on Mobile Data Management. Piscataway: IEEE, 2009. 436−442. [doi: 10.1109/mdm.2009.72]

[75] Xiao Z, Xu JL, Meng XF. P-Sensitivity: A semantic privacy-protection model for location-based services. In: Proc. of the 2nd Int'l Workshop on Privacy-Aware Location-based Mobile Services. Piscataway: IEEE, 2008. 47−54. [doi: 10.1109/MDMW.2008.20]

[76] Bamba B, Liu L, Pesti P, Wang T. Supporting anonymous location queries in mobile environments with privacygrid. In: Proc. of the 17th Int'l World Wide Web Conf. New York: ACM Press, 2008. 237−246. [doi: 10.1145/1367497.1367531]

[77] Duckhan M, Kulik L. A formal model of obfuscation and negotiation for location privacy. In: Proc. of the 3rd Int'l Conf. on Pervasive Computing. Munich: Springer-Verlag, 2005. 152−170. [doi: 10.1007/11428572_10]

[78] Lin X, Li SP, Yang ZH. Attacking algorithms against continuous queries in LBS and anonymity measurement. Ruan Jian Xue Bao/ Journal of Software, 2009,20(4):1058−1068 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3428.html

[79] Deutsch A, Hull R, Vyas A, Zhao KK. Policy-Aware sender anonymity in location based services. In: Proc. of the IEEE 26th Int'l Conf. on Data Engineering (ICDE 2010). Piscataway: IEEE, 2010. 133−144. [doi: 10.1109/icde.2010.5447823]

[80] Yigitog E, Damiani ML, Abul O, Silvestri C. Privacy-Preserving sharing of sensitive semantic locations under road-network constraints. In: Proc. of the 13th IEEE Int'l Conf. on Mobile Data Management. Piscataway: IEEE, 2012. 186−195.

[81] Palanisamy B, Lin L. Mobimix: Protecting location privacy with mix-zones over road networks. In: Proc. of the IEEE 27th Int'l Conf. on Data Engineering. Piscataway: IEEE, 2011. 494−505. [doi: 10.1109/ICDE.2011.5767898]

[82] Chow CY, Mokbel MF, Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proc. of the 14th ACM Int'l Symp. on Advances in Geographic Information Systems. New York: ACM Press, 2006. 171−178.

[83] Ghinita G, Kalnis P, Skiadopoulos S. MOBIHIDE: A mobilea peer-to-peer system for anonymous location-based queries. In: Proc. of the 10th Int'l Symp. on Advances in Spatial and Temporal Databases, Vol.4605. Boston: Springer-Verlag, 2007. 221−238.

[84] Hu HB, Xu JL. Non-Exposure location anonymity. In: Proc. of the 25th IEEE Int'l Conf. on Data Engineering. Piscataway: IEEE, 2009. 1120−1131. [doi: 10.1109/icde.2009.106]

[85] Pingley A,Yu W, Zhang N, Fu XW, Zhao W. CAP: A context-aware privacy protection system for location-based services. In: Proc. of the 29th IEEE Int'l Conf. on Distributed Computing Systems Workshops (ICDCS 2009). Piscataway: IEEE, 2009. 49−57.

[86] Pingley A, Yu W, Zhang N, Fu XW, Zhao W. A context-aware scheme for privacy-preserving location-based services. Computer Networks, 2012,56:2551−2568. [doi: 10.1016/j.comnet.2012.03.022]

[87] Manweiler J, Scudellari R, Cox LP. Smile: Encounter-Based trust for mobile social services. In: Proc. of the 16th ACM conf. on Computer and Communications Security (CCS 2009). New York: ACM Press, 2009. 246−255. [doi: 10.1145/1653662.1653692]

[88] Huang Y, Huo Z, Meng XF. CoPrivacy: A collaborative location privacy-preserving method without cloaking region. Chinese Journal of Computers, 2011,34(10):1976−1985 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01976]

[89] Shokri R, Papadimitratos P, Theodorakopoulos G, Hubaux JP. Collaborative location privacy. In: Proc. of the 8th IEEE Int'l Conf. on Mobile Adhoc and Sensor Systems. Piscataway: IEEE, 2011. 500−509. [doi: 10.1109/mass.2011.55]

[90] Kushilevitz E, Ostrovsky R. Replication is not needed: Single database, computationally-private information information retrieval. In: Proc. of the 38th IEEE Symp. on Foundations of Computer Science. Piscataway: IEEE, 1997. 364−373.

[91] Chor B, Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. Journal of ACM, 1998,45(6):965−981.

[92] Khoshgozaran A, Shahabi C, Shirani-Mehr H. Location privacy: Going beyond *k*-anonymity, cloaking and anonymizers. Knowledge and Information Systems, 2011,26(3):435−465. [doi: 10.1007/s10115-010-0286-z]

[93] Papadopoulos S, Bakiras S, Papadias D. Nearest neighbor search with strong location privacy. Proc. of the VLDB Endowment, 2010,3(1):619−629. [doi: 10.1145/2020408.2020602]

[94] Mouratidis K, Yiu ML. Shortest path computation with no information leakage. Proc. of the VLDB Endowment, 2012,5(8): 692−703. [doi: 10.14778/2212351.2212352]

[95] Khoshgozaran A, Shahabi C. Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy. In: Proc. of the 10th Int'l Conf. on Advances in Spatial and Temporal Databases. Boston: Springer-Verlag, 2007. 239−257.

[96] Khoshgozaran A, Shirani-Mehr H, Shahabi C. Blind evaluation of location based queries using space transformation to preserve location privacy. Geoinformatica, 2013,17(4):599−634. [doi: 10.1007/s10707-012-0172-9]

[97] Tian F, Gui XL, Zhang XJ, Yang JW, Yang P, Yu S. Privacy-Preserving approach for outsourced spatial data based on POI distribution. Chinese Journal of Computer, 2014,37(1):123−138 (in Chinese with English abstract).

[98] Sadilex A, Kautz HA, Bigham JP. Finding your friends and following them to where you are. In: Proc. of the 5th Int'l Conf. on Web Search and Data Mining. New York: ACM Press, 2012. 723−732. [doi: 10.1145/2124295.2124380]

[99] Mascetti S, Freni D, Bettini C, Wang XS, Jajodia S. Privacy in geo-social networks: Proximity notification with untrusted service providers and curious buddies. The VLDB Journal, 2011,20(4):541−566. [doi: 10.1007/s00778-010-0213-7]

[100] Freni D, Vicente CR, Mascetti S, Bettini C, Jensen CS. Preserving location and absence privacy in geo-social networks. In: Proc. of the 19th ACM Int'l Conf. on Information and Knowledge Management. New York: ACM Press, 2010. 309−318.

[101] Huang RW, Gui XL, Yu S, Zhuang W. Privacy preserving computable encryption scheme of cloud computing. Chinese Journal of Computers, 2011,34(12):1−12 (in Chinese with English abstract).

[102] Yiu ML, Ghinita G, Jensen CS, Kalnis P. Enabling search services on outsourced private spatial data. VLDB Journal, 2010,19(3): 363−384. [doi: 10.1007/s00778-009-0169-7]

[103] Ku WS, Hu L, Shahabi C, Wang HX. A query integrity assurance scheme for accessing outsourced spatial databases. Geoinformatical, 2013,17(1):97−124. [doi: 10.1007/s10707-012-0156-9]

附中文参考文献:

[2] 周傲英,杨彬,金澈清,马强.基于位置的服务:架构与进展.计算机学报,2011,34(7):1155−1171. [doi: 10.3724/SP.J.1016.2011.01155]

[11] 霍峥,孟小峰.轨迹隐私保护技术研究.计算机学报,2011,34(10):1820−1830. [doi: 10.3724/SP.J.1016.2011.01820]

[28] 王璐,孟小峰.位置大数据隐私保护研究综述.软件学报,2014,25(4):693−712. http://www.jos.org.cn/1000-9825/4551.html

[50] 张学军,桂小林,冯志超,田丰,余思,赵建强.位置服务中的查询隐私度量框架研究.西安交通大学学报,2014,48(2):8−13. [doi: 10.7652/xjtuxb201402002]

[78] 林欣,李善平,杨朝会.LBS 中连续查询攻击算法及匿名性度量.软件学报,2009,20(4):1058−1068. http://www.jos.org.cn/1000-9825/3428.html [doi: 10.3724/SP.J.1001.2009.03428]

[88] 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.计算机学报,2011,34(10):1976−1985. [doi: 10.3724/SP.J.1016.2011.01976]

[97] 田丰,桂小林,张学军,杨建伟,杨攀,余思.基于兴趣点分布的空间外包数据隐私保护技术.计算机学报,2014,37(1):123−138.

[101] 黄汝维,桂小林,余思,庄威.云环境中支持隐私保护的可计算加密方法.计算机学报,2011,34(12):1−12. [doi: 10.3724/SP.J.1016.2011.02391]

张学军(1977－),男,宁夏中宁人,副教授,CCF学生会员,主要研究领域为LBS隐私量化与保护.

桂小林(1966－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为云安全,网络与信息安全,物联网,隐私保护.

伍忠东(1968－),男,教授,CCF 高级会员,主要研究领域为信息安全,隐私保护.