计算机科学
COMPUTER SCIENCE

个性化位置隐私保护技术综述

曹腾飞, 尹润天, 朱亮, 许长桥

引用本文

曹腾飞, 尹润天, 朱亮, 许长桥. 个性化位置隐私保护技术综述[J]. 计算机科学, 2025, 52(5): 307-321.

CAO Tengfei, YIN Runtian, ZHU Liang, XU Changqiao. Survey of Personalized Location Privacy Protection Technologies [J]. Computer Science, 2025, 52(5): 307-321.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240600067

个性化位置隐私保护技术综述

曹腾飞[1,2,3]　尹润天[1,3]　朱　亮[4]　许长桥[2]
1 青海大学计算机技术与应用学院　西宁 810016
2 网络与交换技术全国重点实验室　北京 100876
3 青海省智能计算与应用实验室　西宁 810016
4 郑州轻工业大学计算机与通信工程学院　郑州 450002

摘　要　随着移动网络和智能设备的普及,用户的地理位置信息被大量采集和利用,从而使数据隐私面临严峻挑战。在此背景下,用户不仅期望能得到有效的隐私安全保障,也对服务体验的质量提出了更高的要求。然而,保护用户位置隐私通常需要限制或模糊位置信息的精确性,这与提供个性化服务所需的高精度位置数据存在冲突。因此,如何在保护位置隐私和满足用户个性化需求之间进行权衡,成为了一个关键的科学问题。这一问题涉及到数据安全、用户体验和商业利益等多个领域,对于加强隐私保护、增强用户信任以及提升用户服务体验质量具有至关重要的作用。综述了近年来个性化位置隐私保护的研究进展。首先,分析了隐私泄露的原因和常见的攻击手段;接着,总结了位置隐私保护技术的定义及分类;然后,根据用户的个性化需求,探讨了如何在保障用户隐私偏好的基础上提供更适宜的位置隐私保护措施;最后,对个性化位置隐私保护技术的未来研究趋势进行了总结和展望。

关键词:个性化;基于位置服务;位置隐私保护;用户偏好;隐私保护技术
中图分类号　TP393

Survey of Personalized Location Privacy Protection Technologies

CAO Tengfei[1,2,3],YIN Runtian[1,3],ZHU Liang[4] and XU Changqiao[2]
1 College of Computer Technology and Applications,Qinghai University,Xining 810016,China
2 National Key Laboratory of Network and Switching Technology,Beijing 100876,China
3 Qinghai Provincial Laboratory of Intelligent Computing and Applications,Xining 810016,China
4 School of Computer and Communication Engineering,Zhengzhou University of Light Industry,Zhengzhou 450002,China

Abstract　With the proliferation of mobile networks and smart devices,users' geographical location information is being extensively collected and utilized,posing severe challenges to data privacy. In this context,users not only expect to receive effective security safeguards,but also demand higher quality service experiences. However,protecting users' location privacy often requires limiting or blurring the precision of location information,which conflicts with the high-precision location data needed to provide personalized services. Therefore,how to balance location privacy protection and meeting users' personalized needs has become a critical scientific issue. This issue involves multiple domains such as data security,user experience,and commercial interests,and plays a crucial role in enhancing privacy protection,strengthening user trust,and improving the quality of user service experiences. This paper reviews the recent research progress in personalized location privacy protection. Firstly,it analyzes the causes of privacy breaches and common attack methods. Subsequently,it summarizes the definition and classification of location privacy protection technologies. Then,based on users' personalized needs,it discusses how to provide more suitable location privacy protection measures while ensuring users' privacy preferences. Finally,it summarizes and looks forward to the future research trends in personalized location privacy protection technologies.

Keywords　Personalization,Location-based service,Location privacy protection,User preference,Privacy protection technology

到稿日期:2024-06-07　返修日期:2024-11-12
基金项目:青海省应用基础研究项目(2024-ZJ-708);国家自然科学基金(62101299,62461052,62225105);网络与交换技术全国重点实验室(北京邮电大学)开放课题(SKLNST-2023-1-19)
This work was supported by the Qinghai Province Applied Basic Research Project (2024-ZJ-708),National Natural Science Foundation of China (62101299,62461052, 62225105) and Open Foundation of State key Laboratory of Networking and Switching Technology(Beijing University of Posts and Telecommunications)(SKLNST-2023-1-19).
通信作者:曹腾飞(caotf@qhu.edu.cn)

1 引言

在当今的数字化时代，随着移动互联网、物联网和大数据技术的不断发展，越来越多的位置数据被收集和利用，为用户提供了各种个性化服务。目前，智能手机已经成为必不可少的物品，相应的带有定位功能的应用软件也得到了大力发展。此外，基于位置的服务(Location-based Service，LBS)为现在的生活提供了很大的便利，已经逐步影响到出行、社交网络服务、广告投放等生活的方方面面。根据皮尤研究中心[1]的数据，2013 年 74%的移动用户享受了 LBS，到 2015 年用户数达到了 90%。从时间上来说，2016 年移动用户在移动应用程序上花费的时间约为 9000 亿小时，比 2015 年增加了 1500 亿小时，而到 2020 年，这个时长已经增加到了惊人的 3.5 万亿小时[2]。全球移动通信系统协会《2025 年移动经济报告》指出，截至 2025 年初，全球移动互联网用户达 47 亿，总移动连接数达 89 亿。

随着 LBS 在日常生活中的广泛应用，相关的安全和隐私问题也日益成为焦点。用户在请求服务时，需要向 LBS 服务提供商提供自己的位置信息。在这个过程中，用户的位置信息被频繁获取和处理，然而用户很难确保自己位置信息的安全性，这为 LBS 服务提供商轻易获取和可能泄漏用户的位置信息埋下了隐患。实际上，已有调查显示，LBS 服务提供商在处理用户位置信息时可能会有意或无意地导致信息外泄[3]。因此，确保第三方服务提供商的可信性是至关重要的，只有可信的服务提供商承担数据保护责任时，用户的位置信息才能得到妥善保护。

传统 LBS 系统如图 1 所示，它由移动用户、GPS 定位系统、通信网络、LBS 服务提供商 4 部分构成。

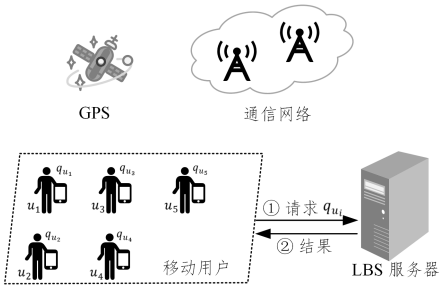

图 1 LBS 系统的基本结构

Fig. 1 Basic structure of LBS system

为了让系统更好地了解用户的需求和喜好，用户可以通过无线网络向 LBS 提供商提交自己的真实位置信息，并期望从服务提供商处得到相关的兴趣点(Point of Interest，POI)，从而为用户提供可靠的服务。基于位置的服务根据信息的传输和处理时间，分为实时和非实时两种服务类型。实时服务指的是系统能够立即响应用户的位置变化，并提供即时且相关的信息或服务，被广泛应用于交通信息服务、紧急救援和社交服务等领域。而非实时服务则不需要立即处理位置信息，可以在一定时间后进行处理或更新。例如，用户预约第二天的打车服务涉及的起点和终点等位置信息虽然属于 LBS 的范畴，但并不是实时处理的。此外，非实时服务还可以通过分析用户的位置历史数据，预测用户的生活习惯或行为模式，从而提供更为个性化的服务，如根据用户的行为趋势预测其未来可能的位置，并据此提供预先的信息或服务。

在 LBS 系统中，除了常用的 GPS 定位外，还可以利用移动通信网络的基站来进行位置定位。这种基站定位方法通过测量用户设备与多个基站之间的信号延迟或信号强度来确定用户的位置，一般应用于室外环境，难以提供较为精确的位置信息。对于室内环境，蓝牙定位技术通过使用蓝牙信标发射的信号进行位置定位，依赖于接收到的信号强度来精确定位。这种方法能够提供高精度的室内位置信息，极大地提高了室内导航的准确性。此外，Wi-Fi 定位技术能够很好地适应室内外两种环境，通过测量设备与多个 Wi-Fi 接入点之间的信号强度来确定位置，同样能够提供精确的位置信息，也非常适用于需要高精度室内定位的场景。目前，用户需求不断提高，结合多种定位技术，利用它们的互补优势，可以为用户提供连贯且精确的定位服务，从而增强 LBS 系统的整体性能和用户满意度。

随着技术的快速发展和 LBS 的普及，位置数据的收集和利用越来越频繁，这带来了对用户隐私安全和数据敏感性的直接挑战。用户的位置信息若被泄露，可能导致恶意攻击者窃取其位置和身份信息，构成巨大的安全威胁。由此，个性化位置隐私保护技术应时而生，其针对用户需求定制隐私保护方案，强调在保护个人隐私的同时，提升服务的个性化和精准度。因此，发展个性化位置隐私保护技术迫在眉睫，它对加强隐私保护、增强用户信任和提升用户服务体验质量具有至关重要的作用。

本文第 2 章对位置隐私泄露存在的问题进行了分析并介绍常用的攻击手段；第 3 章针对攻击方法，概述了位置隐私保护领域的一些关键技术，并分析总结了各种技术的优缺点；第 4 章对国内外个性化位置隐私保护领域的相关文献进行深入分析研究；第 5 章总结了个性化位置隐私保护存在的挑战以及未来可能的研究方向；最后总结全文。

2 位置隐私问题分析

随着信息化时代的发展，数据信息已成为人们工作和生活中不可或缺的资源。人们越来越依赖第三方应用程序提供的服务，这些应用程序通常会收集用户的位置信息。研究显示，位置信息与个体的习惯、活动和社交关系密切相关，这使得位置信息极具敏感性。由于位置信息可能被恶意使用，对公众造成威胁，因此在享受应用程序服务的同时，保护个人隐私安全成为一个亟待解决的问题。

在物联网和工业的快速发展背景下，设备的精确定位显得尤为重要，事实上，这已成为第六代移动网络发展的关键目标之一。随之而来的是，移动设备上的位置隐私泄露风险逐渐加大。在社交网络中，用户常通过移动社交应用程序持续监测自己的位置和社交环境，以获得精确且高质量的基于位置的个性化服务。通常情况下，应用程序通过访问移动设备中的定位[4]模块来获取位置信息。为保护位置隐私，一些方法旨在控制对定位模块的访问权限。然而，一些调查研究指出，即便不访问位置数据，应用程序还是可以通过分析设备中的嵌入式传感器所收集的数据，如触摸屏输入和运动状态等[5-6]，来

推断出用户的私人信息。为了避免个人隐私泄露,用户需要保持警惕并审查自己使用的应用程序是否合法和安全[7]。

本章首先对位置隐私泄露问题进行深入分析,并指出其可能带来的隐私风险;然后介绍了攻击者常用的攻击手段,通过了解攻击的本质特点,更好地采取有效的预防和对抗措施,确保用户的位置隐私不被泄露。

2.1 位置隐私泄露

位置隐私泄露是指在使用移动设备或其他终端设备时,用户的真实地理位置信息被直接或间接地泄露出去。央视揭露了一个苹果手机涉嫌侵害机主的个人隐私问题:在机主使用 LBS 时,他们的住所、上班地点,甚至每天去的地方以及停留时长,均会被准确记录下来。如果这些敏感的位置数据被泄露,不仅会严重侵犯用户的个人隐私,还可能影响到个人和公共的安全。特别是在军事或保密关键领域,位置信息的泄露可能对国家安全构成严重威胁。

大量应用服务的出现,虽然满足了用户的多样化需求,但用户在享受网络服务带来的便利的同时,也可能面临隐私泄露的风险。特别是在使用涉及位置信息的服务时,需要传输的数据中不仅包括当前位置和行动轨迹等信息,还可能涵盖用户的生活习惯、消费偏好、社交关系、政治倾向等敏感信息。

在移动社交网络中,包括脸书、微博等平台都允许用户进行位置共享,例如位置签到、地理位置标签和地理位置语义评论等方式,这些操作可能会将用户的具体位置信息透露给其他网络用户,给用户带来巨大的危害,不法分子会通过网络欺凌、骚扰、诈骗等手段对用户实施社交威胁。此外,医疗隐私泄露可能引起严重的医疗事故。针对医疗服务的一项调查发现,联合健康集团等医疗服务供应商利用社交媒体信息和个人病例数据来评估医疗保健风险并确定保险费率[8],这一做法引发了用户对隐私泄露问题的极大担忧,他们担心这可能导致无法获得公正合理的保险费率;个人信息的泄露也会对用户的工作造成不利影响,企业在招聘员工之前也会利用社交网络对应聘者进行甄别。

在日常生活中使用导航、打车、订餐等软件时,用户都需要向服务商提供位置信息。如果这些信息被泄露,攻击者可能会通过恶意收集挖掘出用户的敏感信息,例如年龄、住址、健康等信息[9]。除了直接共享位置信息外,也存在着位置推理攻击,某些与位置无关的词语也可能由于使用模式的不同而揭示与地点有关的信息。当使用这些词汇的用户包括透露位置和不透露位置的用户时,后者的位置隐私泄露的风险也会增加[10]。在未来移动网络中,位置隐私将面临更大的风险。亚毫米波传输作为毫米波技术的一个分支,具有高频率和短波长的特性,能够提供更高的空间分辨率,从而实现更精准的定位。这种高精度的定位能力在军事、自动驾驶等领域有着广泛应用。然而,这种定位技术也可能导致传统的隐私保护方法失效,因为即使对数据进行模糊处理,攻击者也可能通过其他方式轻易地还原出用户的精确位置。此外,攻击者可以利用亚毫米波传输技术提供的高精度位置数据进行更精确的定位和跟踪,从而更容易实施针对个人的隐私攻击。因此,位置隐私泄露是当前和未来移动网络中需要重点考虑的一个关键问题[11]。

2.2 位置隐私攻击手段

攻击者通常以网络为媒介,窃取用户的隐私。无线传感器网络(Wireless Sensor Networks,WSN)作为一个高度分布式的网络,能够很好地满足攻击者的需求。它由传感器节点(Sybil)和汇聚节点(Sink)组成,能够实现智能感知、远程检测等功能。由于 WSN 的性质,对手很容易跟踪数据包的移动轨迹并获得 Sink 的位置,通过推断汇聚点的方向并选择正确路径进行跟踪,发动方向攻击[12]。此外,在 WSN 中存在着 Sybil 攻击,这种攻击方式能够伪造大量虚假的传感器节点,从而欺骗整个网络,破坏、扰乱其运行。车载自组织网络(Vehicle Ad-Hoc Networks,VANETs)作为未来智能交通系统的核心组成部分,旨在提高车辆之间及车辆与基础设施之间的通信效率和服务质量[13]。在这种网络中,车辆能够动态地加入或离开网络,形成高度灵活的通信拓扑结构,从而实现信息交换和资源共享。这种网络的运作依赖于车辆的移动性和特定的路由协议,支持智能交通管理和车辆安全控制,为城市交通管理和驾驶体验提供了新的实现方案。然而,这种网络也面临着 Sybil 攻击的风险,其中恶意车辆可能会入侵路侧单元(Roadside Unit,RSU),并模拟多个虚假的车辆行为[14]。

攻击者不仅可以收集 WSN 中的信息,还可以收集社交网络中的关系信息,通过分析用户在社交网络中的活动以及与通讯列表中其他人之间的关系,发动社交网络分析攻击,以挖掘用户的隐私信息和行踪。由于背景信息来源丰富,因此,地理社交网络签到服务中的位置发布引发了严重的隐私问题[15]。其中有 3 个因素会影响个人签到行为,即地理信息、人员流动模式和用户偏好。对手可以根据用户的签到历史来推断用户的隐藏位置[16]。

攻击者除了利用社交活动、访问记录、教育背景等外部背景知识,也可以利用用户自身的背景知识进行背景知识攻击,以增加攻击的针对性和有效性。尽管 K-匿名群中的敏感属性不完全一致,但攻击者仍有很大概率通过已知的背景获得其隐私信息。针对这个问题,Yan 等[17]提出了一种抵御背景知识攻击的服务相似性位置 K-匿名隐私保护方法,在选择 K-匿名集时使用位置熵对攻击者的背景知识进行量化,以生成熵最大的 K-匿名集。Liu 等[18]提出了一种隐私攻击-关系背景攻击,攻击者使用目标的关系背景集为目标的隐藏属性构建推理模型。该攻击策略通过构建具有特定数据偏见的模型架构,使系统优先关注与目标密切相关的局部特征模式,进而有效推导出原本被隐藏的敏感属性。

从地理空间上分析,攻击者可以从位置点与用户移动轨迹两方面进行隐私侵犯。

基于位置的攻击侧重于实时获取目标个人的具体地理位置,而移动用户随时随地享受环境感知的功能(例如,找到附近的餐馆,或从地图软件中监控实时交通)都离不开基于位置的服务[19]。然而,当提供 LBS 时,位置披露通常涉及到个人生活方式或访问过的地方等敏感信息,因此埋下了严重的安全隐患。在种攻击方式下,对手可以对 LBS 连续查询[20]进行攻击,通常对位置进行注入(Location Information Attack,LIA)攻击[21],不受信任的用户向匿名器注入虚假位置,从而产生隐私泄露风险。

基于用户历史轨迹的攻击，通过分析用户过去的移动轨迹来获取更深层次的地理位置信息。研究发现，针对微博、Facebook这样的直接位置分享，以及微信这样的间接位置分享，都能暴露出一部分人的真实兴趣点[22]。研究人员为防止重识别攻击，提出了增强型虚拟位置选择算法，但是对手可以在分析LBS历史数据的基础上，通过长期统计攻击(Long-term Statistical Attack，LSA)和区域统计攻击(Regional Statistical Attack，RSA)来获取用户的隐私内容，使得对用户的隐私保护失效[23]。为防止上述攻击，Murakami等[24]提出让用户尽可能少地提供相关敏感信息，这样对手可用的训练数据量就会非常小，从而难以推断用户的信息。但是，在现实情况下，基于马尔可夫链模型的位置隐私攻击仍然可以威胁到用户的隐私安全。

此外，攻击者能够在不依赖于时间和空间的情况下，对目标进行链接攻击。攻击者既可以利用用户自身的背景知识，也可以利用外部背景知识，如社交活动、访问的网站、教育背景以及公共数据库等信息，通过链接攻击分析用户的真实信息，从而进行非法活动。众测应用要求个人与其他人共享本地和个人的传感数据，以产生有价值的知识和服务。然而，仅仅通过简单地抑制敏感上下文的方法，并不能有效防止攻击者利用用户行为中的时空相关性进行攻击[25]。针对基于位置混淆的机制，使用伪装区域来实施。对手通过分类不同来源的数据，仍然能够获得期望信息[26]。

攻击者也可以发起推理攻击，利用公开数据或统计信息，结合所掌握的少量已知信息，来推测未公开的敏感数据。这种攻击技术广泛适用于各类数据环境，尤其在大数据分析和机器学习模型中显得非常有效，因为它可以通过不敏感的信息挖掘出深层的隐私数据[27-28]。推理攻击通常采用统计推断、模式识别和决策树分析等方法执行。为防止这类攻击，可以采取数据匿名化及增强数据加密等保护措施。

除了上述攻击方法，攻击者为了能够更隐蔽地渗透系统并实施攻击，还可能采用同质化攻击手段，通过伪装成系统内的合法实体或设备，并利用相似或近似的特征进行攻击[29]。Pan等[30]针对道路网络场景下怎样保护个性化隐私免受敏感同质性攻击的问题，提出了一种(K，L，P)匿名模型，并基于个性化隐私需求，提出了一种名为 P^3RN 的混淆算法用于在道路网络上生成混淆集合。Liu等[31]采用基于区块链的匿名化方法，来解决位置语义引起的同质性攻击[32]。

保护用户的位置隐私安全，已经成为一个迫切的需求。了解位置隐私泄露方式、安全威胁和对手常用的攻击手段，才能更好地制定保护方案，防止用户隐私数据泄露。常见的位置隐私攻击方法如表1所列。除了上述攻击，还有许多其他类型的攻击，如维特比攻击[33]、侧信道攻击[34]、知识学习攻击[35]等。通过这些攻击手段，不法分子可能会获取到用户的大量隐私信息，从而严重威胁到用户的生命财产安全。

表1 攻击类型总结

Table 1 Summary of attack types

攻击方法	概述	先验知识	访问哪些信息	成功率
基于网络的攻击[12-14]	监控网络流量来推断用户位置	否	用户发送的数据	中等
社交网络分析攻击[15-16]	分析用户在社交网络上的活动推断位置	是	用户社交网络	中等
背景知识攻击[17-18]	利用背景知识与其他公开可得的数据进行关联来推断位置信息	是	匿名位置数据、各种外部数据源	中等
基于位置的攻击[19-21]	获取目标设备物理信息实施攻击	是	设备信息、程序、协议、API	高
基于历史轨迹的攻击[22-24]	分析用户过去的活动轨迹来推断位置	是	历史位置信息	高
链接攻击[25-26]	利用背景知识推断位置信息	是	背景知识	高
推理攻击[27-28]	利用已知的信息预测未公开的敏感信息	是	公开信息	中等
同质化攻击[30-32]	分析用户位置数据的敏感性和均匀性	是	不同时间和位置的数据信息	高

3 位置隐私保护：关键技术探究

为了保障用户的位置隐私安全，研究人员提出了一系列相关技术，旨在对抗攻击者的侵扰。目前，主要采用差分隐私、干扰、K-匿名和加密等技术，以防止用户位置隐私的泄露。本章首先概述位置隐私保护技术的不同架构与评估指标，然后对位置隐私保护的一些关键技术进行介绍。

3.1 位置隐私保护技术架构与评估指标

根据位置隐私保护技术的数据处理、隐私保护和系统管理等方面的不同特点，可以将位置隐私保护架构分为集中式、分布式和混合式。表2总结了3种位置隐私保护架构的优缺点。

表2 隐私保护技术架构分析

Table 2 Privacy protection technology architecture analysis

架构	优点	缺点
集中式架构	集中管理，便于控制和维护；处理效率高	中心服务器可能成为单点故障；存在被攻击的风险
分布式架构	去中心化，避免单点故障	管理和维护复杂；处理效率可能较低
混合式架构	平衡客户端和中心服务器间的负载；灵活性高	系统参数众多，设计和实现复杂

集中式架构：该架构在移动用户和LBS服务提供商之间部署了一个第三方可信的中心服务器，该服务器作为中介，负责集中处理所有位置数据和隐私保护任务。首先将用户的位置信息发送到中心服务器，然后中心服务器对这些信息进行隐私保护处理，最后将处理后的信息转发给LBS服务提供商以响应用户的查询请求。

分布式架构：该架构中位置数据的处理和隐私保护任务分布在多个移动用户或设备上。这些用户或设备通过协作协议共同工作，有效降低了单点故障的风险。用户之间通过加密和安全通信协议进行数据交换，确保数据传输的安全性。随后，将获得的查询请求转发给LBS服务提供商。LBS服务提供商接收并处理这些查询请求，最终将处理后的数据结果集返回给发起查询的用户。

混合式架构：该架构结合了集中式和分布式架构的优点。数据首先在移动用户的本地设备上进行初步处理，然后发送到中心服务器进行进一步的隐私保护处理。最后，中心服务器将处理后的用户查询请求转发给LBS服务提供商。

在探讨位置隐私保护的不同架构时，我们还需要全面评估各种技术的性能。为此，我们将从隐私保护强度、数据可用

性、计算开销和通信开销4个关键维度出发,介绍相关的评估指标。

隐私保护强度:评估技术在防止用户位置信息被未授权访问或泄露方面的能力的关键指标。高隐私保护强度意味着在面对各种攻击和数据分析时,用户的真实位置信息仍然难以被识别或推断,充分保障了用户位置隐私安全。

数据可用性:评估在保护用户隐私的同时,系统或服务能够提供有用和准确信息的程度。数据可用性越高,表明用户在享受隐私保护的同时,仍能获得满意的服务效果,确保了隐私保护与服务质量之间的平衡。

计算开销:评估实施隐私保护技术所需的计算资源和处理能力的标准。这一指标通常关注算法的时间复杂度、空间复杂度以及处理数据所需的计算能力。计算开销越低,表明技术能够在资源受限的环境中高效运行,确保隐私保护技术的实际可行性和用户友好性。

通信开销:评估实施隐私保护技术所需的通信资源和数据传输量的标准。它主要关注隐私保护过程中数据传输的效率和成本,包括数据包的大小、传输频率以及网络带宽的占用情况。通信开销越低,表明技术能够在低网络负载和低通信成本的情况下,有效地保护位置隐私,确保隐私保护技术在实际应用中的可持续性和经济性。

3.2 基于差分隐私的位置隐私保护技术

差分隐私技术通常在中心服务器上实施,通过引入特定的噪声来扰动数据,以确保隐私保护的一致性和有效性。该技术能有效抵抗背景知识攻击。用户可以根据实际需求设定隐私预算,在位置隐私保护和数据可用性之间进行权衡。此外,可以根据数据的敏感程度调整参数,以调整隐私保护级别。然而,选择适当的隐私预算和噪声分布仍然是一项挑战。差分隐私的实现需要考虑隐私保护强度、数据可用性和数据处理效率3个方面。随着数据隐私保护需求的不断增加,差分隐私技术将会得到更广泛的应用,表3给出了差分隐私相关的公式定义。

表3 差分隐私公式的定义

Table 3 Definition of differential privacy formula

名称	公式定义	备注
ε-差分隐私	$Pr[f(D_1)\in S]\leqslant \exp(\varepsilon)\times Pr(f(D_2)\in S]$	D_1和D_2是数据集合(D是原始数据集,D^*是扰动数据集),f
δ-差分隐私	$Pr[f(D)\in S]\leqslant \exp(\varepsilon)\times Pr[f(D^*)\in S]+\delta$	是查询函数,S是结果空间,Pr表示概率,ε和δ是隐私参数
敏感度	$Sens(f)=\max[D_1,D_2][\lvert f(D_1)-f(D_2)\rvert]$	取绝对值后求最大值作为敏感度
噪音特性	$P(x)=\frac{1}{2\varepsilon}\exp\left(-\frac{\lvert x\rvert}{\varepsilon}\right)$	拉普拉斯分布噪音服从的概率密度函数

利用差分隐私技术,Wang等[36]提出了一种基于希尔伯特曲线的差分隐私位置保护方案,在希尔伯特曲线映射的一维空间用户位置上添加拉普拉斯噪声。该方案可以防止具有背景信息的对手的攻击,具有很强的隐私保护力度。Zhang等[37]提出了一种基于差分隐私技术的位置服务隐私保护算法。该方法可以对地理位置信息服务的请求进行有效的保护,能抵御同质化攻击、背景知识攻击、推理攻击等。Li等[38]提出了一种基于马尔可夫模型的差分隐私位置保护方法,该方法不仅满足了差分隐私的要求,有效地保护了位置隐私,而且数据可用性高,时间复杂度低。

3.3 基于干扰的位置隐私保护技术

基于干扰的技术可以将用户的真实位置与一些虚假位置混合在一起,让攻击者无法确定用户的真实位置。根据用户的身份与地理位置的差异,这类技术通常分为假名技术、假位置技术和位置混淆技术。

假名技术在中心服务器上实施,管理和维护假名与用户真实身份之间的映射关系。为用户分配无法跟踪的标记,要求用户拥有多个假名且不得长期使用相同假名,以防止数据主体真实身份泄露。该技术可根据不同应用场景调整假名,灵活应对隐私保护需求,但可能增加资源消耗和通信开销。在车载自组织网络中,假名技术被广泛应用。Saini等[39]提出了一种上下文感知假名更改方案,减少了假名链接,实现了较低的跟踪成功率和较高的匿名集合熵。Ullah等[40]提出了一种自适应分组和假名改变策略,通过分组匿名屏蔽用户真实位置信息,但会导致LBS服务中断,并产生通信开销。Memon等[41]提出了基于混合区域认证协议的道路网络位置隐私化名变更策略,以解决智能交通系统中缺乏安全通信协议的问题。

假位置技术允许用户在其设备上生成虚假的位置信息,然后将这些假位置发送到中心服务器进行下一步处理。这种方法操作简单,在用户提交查询信息时,使用虚假位置对用户的位置信息进行干扰,从而降低用户被恶意追踪的风险。然而,使用该技术可能会影响实际的定位功能,导致某些应用程序无法正常使用。该类技术一般通过距离偏移、区域划分、设定保护级别3个步骤来实现。

距离偏移:通过对实际位置坐标进行随机或规定的偏移,来生成一个相近但不精确的新位置。$P(x,y)$是真实位置,$P'(x',y')$是偏移后的位置,d是一个可以根据实际需求设定或利用概率分布生成的随机距离,θ通常从$[0,2\pi)$范围内均匀选择。

$$x'=x+d*\cos(\theta) \tag{1}$$

$$y'=y+d*\cos(\theta) \tag{2}$$

区域划分:在假位置技术中,通常将地图划分成若干个区域,将用户的精确位置隐藏在一个更大的区域内,只向外提供这个区域的信息,每个区域用一个代表点来代表。RP是代表点集合,$distance(P,p)$指真实位置P与代表点p之间的距离。

$$P'=\operatorname{argmin}(P \text{ in } RP)(distance(P,p)) \tag{3}$$

保护级别:通常会设定一个保护级别,用于控制用户真实位置被泄露的概率。δ是容差,ε是隐私参数。

$$Pr[d\leqslant\delta]\geqslant 1-e^{-\varepsilon} \tag{4}$$

考虑攻击者可能具有一定背景知识的情况,Wang等[42]结合地理位置语义与查询概率,确保了隐私安全与查询结果的准确性。哑元位置技术也属于假位置技术的范畴,它通过

增加虚拟定位实现 K-匿名。如图 2 所示，用户在寻找酒店时，将 $K-1$ 个哑元位置与真实位置一起发送给服务提供商，增加了攻击者判断真实位置的难度。该技术开销小，服务质量高，但隐私保护力度有限。

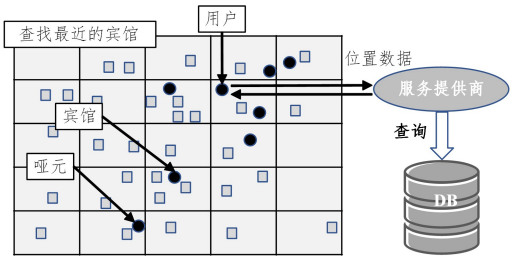

图 2 哑元位置技术的工作流程

Fig. 2 Dummy location technology workflow

位置混淆技术[43]通过在多个节点上分布式实现，其核心在于通过降低定位的精度来提高用户的隐私保护水平。这种技术具有较高的灵活性，能够根据应用的具体隐私需求调整混淆的程度，因此适用于多种应用场景，包括社交网络的位置分享和室内外导航等。特别是在不需要高度精确位置信息的场合，其效果更显著。然而，在实际应用中，平衡隐私保护与位置精度往往较为困难，而且可能需要较大的计算资源和复杂的算法支持。该技术参考了添加噪声的思想，在定位过程中加入了一种随机干扰，使用户的位置信息变得混乱和模糊，从而保护用户的位置信息。Gao 等[44]提出了一种基于轨迹模糊的差分位置隐私保护机制。该机制首先基于滑动窗口算法提取停留点作为轨迹特征，然后通过指数机制将每个停留点模糊到目标模糊子区域，最后在目标模糊子区域进行拉普拉斯采样，得到被模糊的位置点，以此加强隐私保护程度。

3.4 基于 K-匿名的位置隐私保护技术

K-匿名技术通常在中心服务器上实施，其核心理念是通过将每条记录与至少 $K-1$ 条具有完全相同准标识符属性的其他记录合并，从而在数据集中创建一个匿名组。这样，就使得在合并后的数据集中，攻击者无法通过准标识符直接关联识别出单个记录，从而有效地保护了用户的隐私。K-匿名技术通过对数据进行概括化和抽象化处理，选择性地不公开某些敏感信息，从而减少由链接攻击引起的隐私泄漏。这些措施共同提高了数据的安全性，有效降低了隐私泄漏的风险。该技术的优点是可以在保护隐私的同时保持数据的可用性，适用于各种数据类型和应用场景。然而，它可能会降低数据的精度，并且可能会被攻击者通过其他手段进行同质化攻击和背景知识攻击。

在车联网中，如果允许对手监视全局消息流并识别查询来源，则位置隐私保护将变得完全无效。对此，Buccafurri 等[45]提出了一个分布式和分层的模型，来解决上述问题。为防止节点的行为欺骗、服务摇摆等威胁，Yang 等[46]提出了一种可信的去摆动 K-匿名方案。Xing 等[47]加入云服务器作为确信第三方，并将用户与服务提供商的直接通讯隔绝开来，实现对用户位置信息的隐藏。

3.5 基于同态加密的位置隐私保护技术

同态加密技术允许用户在其设备上对数据进行加密，然后将加密后的数据发送到中心服务器进行处理。它是一种特殊的密码转换技术，不仅支持基本的加密操作，还允许对密文进行多种功能计算，即先计算后解密等效于先解密后计算。这个特性在信息安全方面具有重要意义，利用同态加密技术可以在对多个密文进行计算之后再解密，而无需每次都解密每个密文，从而避免高昂的计算成本。

定义一个运算符 Δ 对应的加密算法 E 为同态加密函数，同态加密满足 $E(x\Delta y)=E(x)\Delta E(y)$。发送方对明文 m 进行同态加密，得到密文 $c=E(m)$；接受方在得到密文 c 后，使用同态解密函数 D 进行解密，即 $D_k(c)=f^{-1}(E_k(c))$，其中 k 为密钥。同态加密技术的优势在于，即使数据处于加密状态，也能够对其进行分析和计算，从而保障了数据的可用性和安全性。这一特点使得同态加密成为移动众测的理想选择，因为它允许在不暴露原始数据的情况下，广泛地收集和利用位置或个人信息。但是，该技术会对计算性能产生较大的开销，加密和解密过程可能较为耗时，操作复杂。为解决任务分配过程中的隐私安全问题，Zheng 等[48]提出了一种加密网格匹配方案，为众测过程的各个实体提供隐私保护服务。但是，将隐私保护添加到位置服务会导致计算复杂。Jain 等[49]为了降低计算成本，提出了轻量级隐私保护的基于位置服务的推荐协议，结合希尔伯特曲线、共生矩阵的协同过滤推荐器和可切换同态加密来推荐服务。

表 4 总结了本文所调研文献中，作者在位置隐私保护领域常用的一些保护技术，并对不同技术的架构、性能评估以及优缺点进行了分析。

表 4 隐私保护技术总结

Table 4 Summary of privacy protection technologies

技术名称	技术架构	优点	缺点	性能评估			
				隐私保护强度	数据可用性	计算开销	通信开销
差分隐私[36-38]	集中式	强大的隐私保障；能够实现数据资源的最大利用；定制隐私级别	会对模型可用性和准确性造成一定程度的影响；难以选择最优参数	较高	中等	中等	中等
假名技术[39-41]	集中式	不同数据集中的记录在经过假名化处理后仍可关联，不会泄露数据主体；简单易操作	需要管理大量的假名，导致额外的资源投入和很大的通信开销	中等	较高	较低	中等
假位置技术[42]	混合式	降低追踪风险；操作简单容易	隐私效果较差；影响定位功能	中等	中等	中等	中等
位置混淆技术[43-44]	分布式	灵活性高；适用性广	难以平衡隐私与精度；计算复杂	较高	中等	中等	中等
K-匿名[45-47]	集中式	抵抗链接攻击；易于实现和部署；灵活性高	无法抵抗同质攻击和背景知识攻击	中等	中等	中等	较低
同态加密[48-49]	分布式	支持加密数据计算；适用于云计算；灵活性高	计算效率低；操作复杂	较高	中等	较高	中等

4 个性化位置隐私保护技术分析

数据隐私保护技术的不断创新与发展，为医疗健康、智能交通、社交网络等新型 LBS 服务提供了坚实的安全保障。随着隐私安全性的提升，人们对服务体验的质量也提出了更高的要求。本章将深入探讨个性化位置隐私保护的多个维度。首先，介绍传统的基于位置点和轨迹的保护方法。然后，针对隐私量化以及人工智能技术在这一领域的应用进行探讨，并对数据安全与服务质量之间的平衡问题进行分析。最后，介绍一个通用框架，用于实现个性化位置隐私保护，并详细说明其操作流程。

4.1 基于位置点的个性化位置隐私保护

位置点隐私保护主要是针对用户位置信息中每个单独的位置点进行保护，这些位置点可能包括用户的家庭地址、工作地点等敏感信息。目前，一种被广泛应用的保护方法是利用位置预测机制和假位置选择机制来混淆查询位置，并将这些混淆后的位置连同真实查询位置一起发送到不同的匿名服务器。在考虑到打车服务中可能出现的隐私泄露风险时，Khazbak 等[50]提出了一种基线解决方案。该方案通过位置混淆技术来满足乘客的隐私需求，同时不影响服务的便利性。然而，如果生成的假位置信息描述不充分或随机性不足，可能会影响该方案的效果。针对这一问题，Ma 等[51]提出了一种新的基于差分隐私的道路网络位置不可区分性度量方法，并设计了一种双重混淆算法以提高效率；此外，通过最近邻插值方法，实现了针对不同敏感位置的隐私预算分配，以平衡位置隐私和数据的实用性。

基于位置的服务在车载网络中得到了广泛应用。Xu 等[52]提出一种基于差分隐私的个性化位置隐私保护方案，该方案采用位置混淆和匿名化技术，在不泄露用户实际位置信息的前提下，为用户提供个性化的位置服务。具体流程如图 3 所示。方案中引入了敏感圈的概念，通过比较用户服务请求地点与最近敏感地点之间的距离，来量化用户个性化的隐私需求。此外，依据用户是否位于敏感区域内，为用户在不同位置分配不同的隐私预算，这种分配主要由服务请求位置与敏感位置之间的欧氏距离决定。最后，结合隐私预算和服务质量（Quality of Service，QoS）进行优化，建立了一个多目标优化函数，旨在平衡隐私保护和服务质量。为了解决三维空间中的位置隐私保护问题，Min 等[53]提出了一种两阶段个性化 3D 位置隐私保护机制，通过搜索相邻位置来确定用于隐藏实际位置的保护位置集合，并利用位置偏移置换翻转机制来执行数据隐私保护。该机制生成的虚假位置具有较小的偏移距离，有效改善了隐私与服务质量之间的平衡。

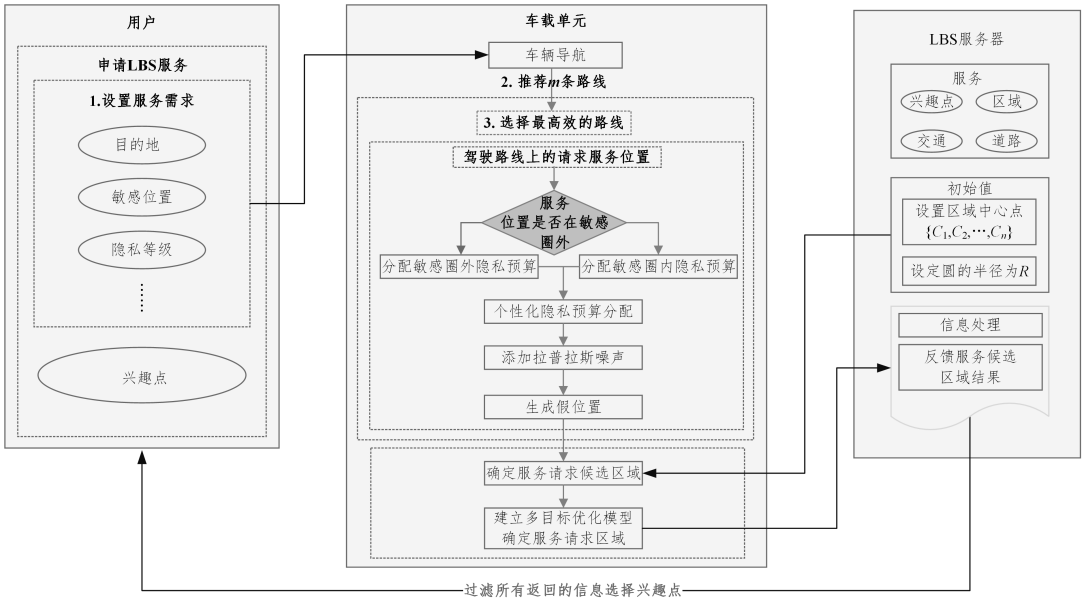

图 3 车联网环境下基于差分隐私的个性化位置隐私保护框架

Fig. 3 Framework of personalized location privacy protection based on differential privacy in vehicular networks

随着互联网的发展，移动众测和空间众包已成为互联网行业中的一个新兴领域。其不仅帮助企业和个人高效地获取专业人力资源，完成复杂或繁琐的任务，也为广大劳动者提供了灵活自主的工作机会。然而，这些活动也可能带来隐私泄露的风险。移动众测的数据采集依赖于移动设备，可能面临设备丢失或数据泄露的风险，且由于移动设备硬件的限制，难以进行细粒度的位置信息混淆处理，从而增加了位置隐私泄露的风险。对此，Wang 等[54]提出了一种面向移动众测的个性化隐私保护任务分配框架，通过概率比较函数（Probability Comparison Function，PCF）来判断哪位工作者更可能靠近任务地点。基于这一函数，进一步引入了一个包含混淆信息和个人隐私级别的概率赢家选择机制，旨在最小化工作者的总出行距离，从而高效保护位置隐私。

空间众包（Spatial Crowdsourcing，SC）被广泛用于地图更新、城市规划、导航服务等领域，其基于地理位置的任务分配特性使得敏感位置存在较高的泄露风险。常见的空间众包隐私保护模型如图 4 所示，主要采取两种隐私保护措施：一种是将数据直接提交给可信的第三方处理；另一种是在工作端直接对隐私进行保护后上传至 SC-服务器。然而，这些方法往往忽视了个性化隐私保护的需求。对此，Fan 等[55]提出一种个性化位置隐私保护的多位置任务分配框架。该框架将每个工作者的实际位置转换为隐私级别决定的圆形区域，并使用

R 树存储位置数据，通过任务修剪策略优化任务分配效率，有效保护隐私安全。此外，Lv 等[56]针对在线最小二分匹配问题，提出了一种基于四叉树截断几何机制的隐私保护方法，通过设计基于四叉树的个性化匹配框架加速距离计算，提高匹配效率。Zhang 等[57]则开发了一个个性化位置隐私保护系统，通过计算位置隐私级别并应用基于指数机制的个性化差分隐私保护机制，有效解决了工作者位置隐私泄露的问题。

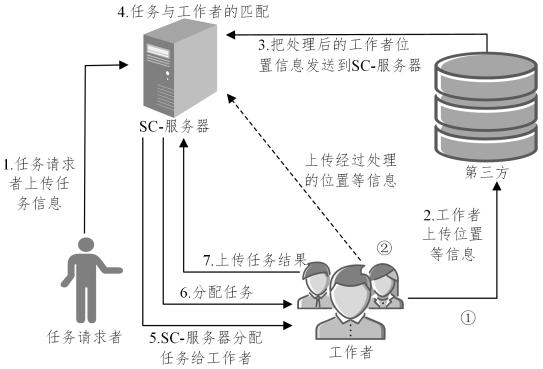

图 4 基于隐私保护的空间众包分配模型

Fig. 4 Privacy-preserving spatial crowdsourcing allocation model

4.2 基于位置轨迹的个性化位置隐私保护

当前，随着网络技术的快速发展和 5G 网络的普及，物联网得到了极大的推动。人们普遍使用的手机、手表等便携式移动通信设备的应用越来越广泛。用户在使用相应的应用程序时，服务提供商通常需要获取位置权限，并实时追踪用户的移动轨迹，这不仅能提高业务价值，还能增强用户体验。

然而，这种对移动轨迹数据的广泛收集和使用也引起了人们的广泛关注，特别是对数据隐私保护方面的担忧。

在轨迹隐私保护研究领域，Wen 等[58]开发了一种优化的个性化轨迹差分隐私机制，通过识别用户的停留点和频繁子轨迹，评估不同位置数据的隐私级别，并分配适当的隐私预算。该机制根据用户的隐私偏好和数据特性动态调整隐私参数，实现个性化隐私保护，但仍具挑战性。该方法主要针对轨迹数据保护，可能不适用于其他类型的数据。另一方面，Zhi 等[59]提出了一种基于面积密度分析的轨迹保护方法，根据用户的停留区域计算停留点，并结合敏感位置的隐私得分情况进行隐私预算分配。此外，Yuqi 等[60]介绍了一种基于个性化本地差分隐私的轨迹合成方法，该方法通过四叉树索引对轨迹点进行编码，利用个性化机制保护隐私，在服务器端估算轨迹点分布以生成和发布新的轨迹数据集。

在用户外出旅行方面，轨迹的隐私保护同样至关重要。Islam 等[61]针对此问题，开发了一个隐私保护模型。该模型提出了一种方法，能够将用户的旅行体验量化成个性化的安全评分，并利用改进的 R-tree 索引技术来存储这些评分。这个过程不依赖于集中式计算，而是基于知识渊博的群众个性化旅行经验，找出用户指定距离阈值内的最安全路线。在 Top-k 相似性查询领域，Yi 等[62]提出了一种基于希尔伯特曲线和同态加密的大规模轨迹数据隐私保护方案，其能够对过滤的 k 条轨迹进行提炼，以获得准确的查询结果。

在轨迹隐私保护中，位置语义扮演了一个极为关键的角色，它关乎到地理位置的含义和重要性，如医院、银行等。位置语义隐私保护技术利用语义知识对位置点[63-64]和轨迹进行处理，以达到保护隐私的目的。Qiu 等[65]提出了一种基于语义感知的移动隐私模型，该模型构建了一个多层次的深度语义树。依靠这个语义树，构建了 K-匿名集，从而为共享的位置信息提供了个性化的隐私保护，并通过迭代这一过程，生成一个可移动语义感知的轨迹。此外，Qiu 等[66]提出了一种基于差分语义广义行为轨迹的移动互联网服务隐私保护方法，其通过形式化用户社会流动性来探索潜在的行为模式，并评估用户行为的不同隐私敏感性。

基于位置轨迹的个性化位置隐私保护领域包含众多技术和方法，这些方法通过分析可能的隐私泄露途径，选用适当的隐私保护技术，并针对用户的个性化隐私需求进行保护，有效地保障了用户的位置隐私。表 5 列出了在基于位置的个性化隐私保护中，针对位置点和轨迹两个方向的一些典型技术方案，同时总结分析了 4.4 小节中关于人工智能技术在个性化位置隐私保护中的应用。

表 5 基于位置的隐私保护技术性能优势分析

Table 5 Performance advantage analysis of location-based privacy protection technologies

类别	技术	方法	文献	优点	缺点	性能评估			
						隐私保护强度	数据可用性	计算开销	通信开销
基于位置点隐私保护	位置混淆	增强解决方案	[50]	满足乘客的隐私要求，不影响服务的便利性	依赖大量的用户历史数据	较高	中等	中等	中等
	位置混淆	双重混淆算法	[51]	隐私保护能力强，安全性高	未考虑速度周围交通状况等，局限性较大	较高	中等	较高	中等
	差分隐私	多属性决策理论	[52]	均衡隐私和服务质量，用户收益高	模型添加属性较少很难应用到现实环境	较高	中等	中等	中等
	位置混淆	两阶段 3D 位置隐私保护	[53]	提高对不同推理攻击的鲁棒性，保证个性化隐私保护	目前仅应用到室内建筑	较高	较低	中等	中等
	差分隐私	概率比较	[54]	保证隐私安全满足真实性、盈利性	仅适用于移动众测	较高	中等	中等	中等
	位置混淆	任务修剪策略	[55]	实用性较高，平均误差较低	仅适用于空间众包	中等	中等	中等	较高
	差分隐私	四叉树截断几何机制	[56]	允许用户直观地选择不同的泛化区域，实现高效匹配	仅适用于空间众包	较高	中等	中等	中等
	差分隐私	指数机制、奖励机制	[57]	有效地平衡位置隐私保护和数据的可用性	仅适用于移动众包	较高	中等	中等	较高

（续表）

类别	技术	方法	文献	优点	缺点	性能评估			
						隐私保护强度	数据可用性	计算开销	通信开销
基于轨迹隐私保护	差分隐私	停留点隐私级别分配	[58]	有效平衡隐私保护和数据效用	适用于轨迹数据的隐私保护	较高	中等	中等	中等
	差分隐私	面积密度分析	[59]	减少隐私预算浪费，保证数据效用	适用于数据信息发布	较高	中等	中等	中等
	差分隐私	四叉树索引	[60]	合成轨迹数据集的时间效率和实用性方面表现良好	合成轨迹的准确性依赖于用户提供的数据	较高	中等	较高	中等
	位置干扰	广义优先算法	[61]	速度快，易实施，安全性高	灵活性不够	较高	较低	中等	中等
	同态加密	时空轨迹相似性度量	[62]	保证查询请求安全，抵抗推理攻击	局限相似性轨迹查询	较高	中等	较高	中等
	K-匿名	构造层次语义树	[65]	自适应能力强，合成轨迹可用性高	依赖于背景知识，操作复杂	中等	中等	中等	较低
人工智能技术	机器学习	K-Means 聚类	[72]	显著提高任务分配效率	仅适用于空间众包	中等	中等	中等	较高
		强化学习	[73]	隐私保护能力强；数据效用高	仅适用于移动众包	较高	较高	中等	中等
	深度学习	LSTM 网络	[74]	预测精度高	适用于船舶航海轨迹	中等	中等	中等	较低
		DQN 技术	[75]	隐私保护能力强；有效抵抗攻击	效率低，稳定性差	较高	中等	较高	中等
	联邦学习	边缘计算	[76]	保障任务分配；提高数据质量	仅适用于空间众包	中等	较高	较高	中等
		凸包优化算法	[77]	有效提高推理精度	依赖于数据质量	中等	较高	中等	中等

4.3 基于隐私量化的个性化位置隐私保护

通过将特定用户的地理位置信息转化为数值型数据集，在确保获取关键信息的同时，实现对地理位置隐私的度量。这一过程的核心目的是构建一套完善的位置隐私评价体系，为用户制定最佳的位置隐私保护策略，以实现个性化的位置隐私保护。下面介绍一些常用的隐私量化指标。

信息熵：用于度量随机变量的不确定性，并在隐私领域中评估隐私风险。具体来说，信息熵越高，随机变量的不确定性越大，相应的隐私风险也就越高。

互信息：对两个随机变量之间相互依赖程度的度量，可用于分析隐私泄漏情况。当两个变量的互信息较大时，表明它们之间的相互依赖程度较高，这可能导致更多的隐私信息被泄露。

决策树：一种可用于分析隐私信息并识别其安全性漏洞的机器学习方法。在匿名数据处理过程中，可以通过构建决策树来识别与敏感信息和身份信息相关的属性，从而更深入地理解数据集的特性。

隐私攻击模型：描述攻击者可能采取的攻击方式和手段的模型，通常包括攻击者的能力、目标和策略。在位置隐私保护中，常见的攻击方式包括基于距离的攻击和基于轨迹的攻击，这些攻击通过分析用户的位置数据来推断用户的身份、行为模式或其他敏感信息。建立攻击模型有助于设计有效的隐私保护机制（Privacy Protection Mechanism，PPM），以避免潜在的隐私泄露风险。

这些常见的隐私量化指标有助于评估隐私风险，分析隐私泄露的可能性，并识别隐私保护措施中的安全漏洞。在道路交通网络中，为了有效保护用户隐私，Zhong 等[67]提出了一种基于敏感度的假名更换机制，通过度量指标来量化每个位置的隐私需求。在敏感性较高的位置，车辆的假名更新频率将更快。这种机制会根据每个车辆的敏感性和假名年龄阈值来制定假名变更策略，从而为每位用户智能地提供个性化的位置隐私保护。

在数据共享发布场景下，针对隐私保护的度量问题，可以参照图 5 展示的模型。该模型结合信息熵和用户隐私偏好，采用一种隐私度量算法，有效解决了应用熵权法度量隐私时可能出现的失真问题，特别适用于数据发布初期，能够量化分析共享数据中的隐私内容。通过设定隐私保护阈值和评估隐私敏感度，基于信息熵与群体隐私偏好的数据共享隐私度量模型实施最优的隐私保护策略，从而在提供数据发布和计算服务时，最大程度地保护用户个人隐私。

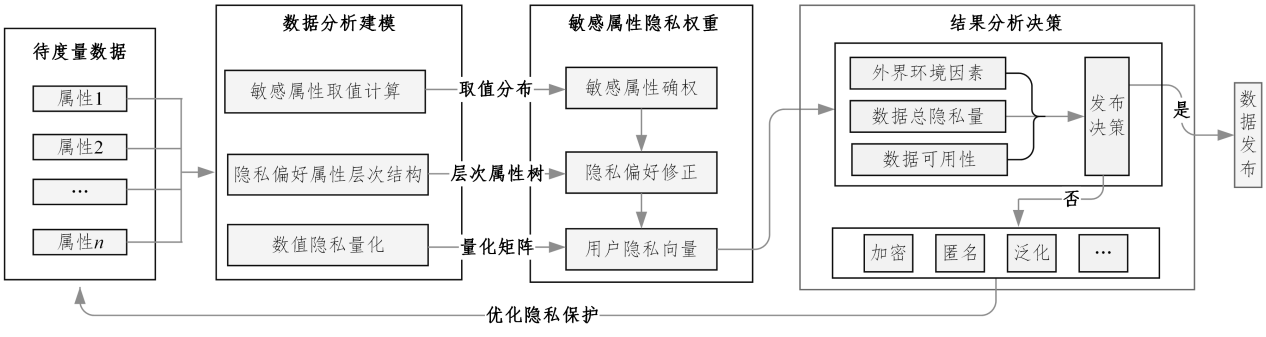

图 5 基于信息熵与群体隐私偏好的数据共享隐私度量模型

Fig. 5 Data sharing privacy measurement model based on information entropy and group privacy preferences

针对移动众测领域数据传输和存储环节的位置隐私安全问题，Wang 等[68]提出了一种融入个性化位置隐私激励的双层移动众感拍卖机制。该机制采用位置混淆技术，使得工作人员可以在移动众测系统中上报混淆后的位置信息，从而保护其个人隐私；同时，引入了隐私预算概念，使得工作人员能够根据自己的意愿决定向平台共享多少位置信息，实现个性化的位置隐私保护。Shen 等[69]提出总的隐私预算会被合理分配到初始设定的敏感位置，通过与初始级别的阈值参数对比，动态调整敏感位置的保护级别，使得在不损害位置隐私的前提下更加灵活地分配隐私预算。另外，Yang 等[70]提出了一个考虑攻击模型的个性化 K-匿名优化算法，该算法在保持 K-匿名性的同时，通过最大化数据集的信息熵来提升隐私保护效果。尽管这种方法能有效防范隐私侵犯，但其计算复杂度较高，需要对每个子集进行熵的计算和调整，因此在处理大规模数据集时可能面临性能挑战。

在隐私保护框架设计方面，目前的研究进展较为缓慢。尽管研究人员提出了多种位置隐私保护机制(Privacy-Preserving Mechanism，PPM)，但每种机制通常在某些方面表现优异，而在其他方面表现较弱。此外，现有研究容易忽略用户移动设备的当前状态，这可能给用户造成不便。Niu 等[71]提出了一个名为 SmartGuard 的通用框架，用于在不同场景下有效利用多个单一的 PPM 来保护位置隐私。该框架通过计算每个隐私策略到理想方案的距离来生成一个度量值，并使用理想隐私策略与非理想隐私策略的距离作为评估标准，据此选择最佳的隐私策略。SmartGuard 可以根据用户的偏好及其移动设备的当前状态，动态地选择最适合的隐私保护策略。

4.4 基于人工智能的个性化位置隐私保护

除了上述一些传统的个性化位置隐私保护方案外，近些年人工智能技术的快速发展，也为个性化位置隐私保护提供了新思路和新方法。利用人工智能技术，根据用户的特定需求和行为模式，动态调整隐私保护策略，以实现更加精准和高效的位置隐私保护。

在机器学习领域，通过构建和训练模型，可以从海量数据中提取有价值的信息，识别复杂模式，并根据这些模式做出预测或决策。这一特性在空间众包任务的分配中得到了应用。Lin 等[72]利用机器学习算法对空间众包任务进行聚类，有效提升了任务分配的成功率，同时为工作人员和任务请求者提供了个性化的位置隐私保护。Bi 等[73]提出了一种基于差分隐私和强化学习的动态隐私测量与保护框架。该框架能够在个性化隐私阈值的约束下，有效地保护感知数据的隐私，并通过执行最优的数据选择策略，最大化数据收益。

在深度学习方面，通过多层神经网络进行特征提取和模型训练。神经网络是一种由多个神经元构成的复杂的非线性数学模型，具有很强的拟合能力，可以很好地拟合复杂的数学模型，从而更好地展示物体之间的内在关系。使用基于长短期记忆(Long Short-term Memory，LSTM)网络的生成模型，能够对原有轨迹数据集中的原始用户轨迹进行补充或预测[74]。DQN(Deep Q-Network)是一种结合了深度学习和强化学习的技术，它通过利用深度神经网络来近似 Q 函数，有效地应对了传统强化学习算法在处理大规模状态和动作空间时遇到的挑战。Pandey 等[75]利用该技术，结合模型的最佳属性，使用户能够获得个性化的位置隐私保护。

此外，具有去中心化、高效、安全等特点的联邦学习近些年逐渐成为研究热点，它使得参与方无需将原始数据发送到中心服务器，只需传输经过训练得到的模型参数。这种分布式处理能够有效地保障用户信息的安全，防止敏感数据的泄露。Sun 等[76]在移动众包场景中提出了一种自适应位置泛化和分组聚合的双边隐私保护方案，该方案以联邦学习为框架，利用边缘计算来减轻云平台和移动设备的数据处理负担，能够自适应保护工人的位置隐私。Huang 等[77]针对消费电子领域中新兴的无设备定位技术对隐私保护的不足进行了研究，并提出了一种利用联邦学习技术的无设备定位隐私保护方法。该方法在通过联邦学习框架保护用户隐私的同时，保持高精度的位置推断能力。

4.5 均衡数据安全与服务质量的研究

数据安全和用户服务质量是技术发展中两个紧密相连的挑战。随着人们对个人信息保护意识的增强以及对数据驱动服务需求的增加，如何在保障数据安全的同时，还能保持或提高服务质量，已经成为学术界关注的核心问题。近些年关于个性化位置隐私保护的研究越来越多，研究者们通常针对特定需求设计相应的隐私保护机制(PPM)。通常，每个 PPM 在隐私保护和资源消耗方面都能取得一定的平衡，但没有一个 PPM 在所有情况下都表现完美。

针对如何平衡数据安全与服务质量的问题，Niu 等[71]充分利用多个单 PPM 进行位置隐私保护，提出了一个名为 SmartGuard 的通用框架。该框架从移动用户的历史数据中收集不同场景下的训练数据，并根据用户的偏好和移动设备的当前状态动态地为用户选择最佳的隐私保护策略。Macha 等[78]研究了数据聚合商在与广告商分享数据之前，如何平衡潜在的隐私风险与广告商的数据效用问题。针对这个问题，他们提出了一种灵活且个性化的框架，用于量化消费者的移动轨迹中的隐私风险。Li 等[79]研究了现有位置隐私保护机制的评估方法，并设计了一个通用评估框架。该框架综合考虑了查询隐私和位置隐私，对移动用户、隐私保护策略及其对手进行了详细的定义和形式化描述。通过性能指标，该框架有效平衡了隐私保护效果和服务实用性。

除了框架设计，一些研究人员特别关注移动用户位置隐私和定位精度的问题，因为定位精度可以直接影响用户的服务体验质量。Apollonio 等[80]对基于位置的服务中的信息质量和用户位置精度进行了权衡，并提出了相应的策略。通过调整参数，该策略能够在服务质量和隐私保护之间取得良好的平衡。Min 等[81]提出了一种语义自适应的地理不可区分性机制，该机制能够对个性化位置隐私保护进行量化，并在隐私保护与服务质量之间实现更好的平衡。结合 4.3 节隐私量化内容，表 6 对数据安全与服务质量权衡量化方法进行了分析总结。

表 6 数据安全与服务质量权衡量化方法分析

Table 6 Analysis of quantitative methods for balancing data security and service quality

量化指标	方法	性能分析	文献
敏感性	基于车辆访问某位置的频率来量化车辆对于每个位置的隐私要求	不仅提供了更强的位置隐私保护，而且考虑了车辆之间的异构性，实现了个性化的位置隐私保护	[67]
隐私预算	引入了隐私预算的概念，让工作者决定向平台披露多少位置信息；拍卖机制	有效而公平地分配感知任务，而且满足个体合理性、真实性和预算平衡性	[68]
	与定制的初始级别阈值参数进行比较，动态调整敏感位置的隐私安全级别	在不损害位置隐私的情况下，分配隐私预算更加灵活	[69]
位置熵攻击模型	提出一种攻击模型下的个性化 K-匿名优化算法	在满足用户隐私保护要求的同时达到最优的服务质量，安全性分析证明了算法的有效性	[70]
量化不同场景下的隐私	建立 SmartGuard 框架，考虑用户偏好和设备状态，动态选择最佳隐私保护策略	针对隐私、能耗和网络带宽方面选择最佳策略，在各种情况下都优于现有的隐私保护机制	[71]
个性化的隐私风险量化	针对消费者的两个潜在隐私成本和广告商的两个潜在利益进行量化分析	灵活地适应不同类型的风险(成本)和效用(收益)，以及不同的可接受的风险效用权衡水平	[78]
位置信息为主要因素	对移动用户、隐私保护策略和对手进行形式化描述；使用性能标准作为度量	考虑对手的先验知识、位置隐私和服务质量，能够应用于快照 LBS 和轨迹 LBS	[79]
隐私值 POI 定位精度	通过调整位置失真参数，在保证服务质量和隐私保护之间取得良好的平衡	通过发送带有不精确位置的查询，能够增强用户的隐私保护，同时仍能提供令人满意的信息质量	[80]
位置不可区分性度量	提出了一种基于语义曲线距离的拉普拉斯噪声机制，以实现差分隐私	在访问不同敏感语义位置时满足用户的个性化隐私需求；有效减少了高度敏感位置的泄露	[81]

4.6 个性化位置隐私保护框架

传统的位置隐私保护方案常常采用加密、假名、匿名化和混淆等技术手段，通过多种不同的隐私保护机制来达到保护用户位置信息的目的。然而，这一方法也存在明显的缺点：统一的隐私保护方案可能导致对用户位置隐私的过度保护或保护不足，这会影响用户的服务体验，难以充分满足用户的个性化需求。

因此，个性化位置隐私保护的重要性日益突现。在确保用户隐私安全的前提下，为用户提供定制化服务成为研究的焦点。如图 6 所示，一个通用的个性化位置隐私保护框架通常包括移动用户和 LBS 服务提供商。这种框架与传统的位置隐私保护不同，在用户发起服务请求时不会直接采取技术手段来保护用户位置信息。相反，它首先对用户的服务请求进行详细分析，考查用户的隐私偏好、兴趣点和敏感点等信息，然后通过敏感性评估、隐私预算的分配以及定制隐私保护等级等措施来为用户制定相应的保护策略。最终，根据这些定制化策略，采用特定的技术手段对用户的位置信息进行保护。这些技术主要将用户的个人数据(如身份码、位置、查询内容等)转变为混淆版本，从而实现对用户位置隐私的个性化保护。

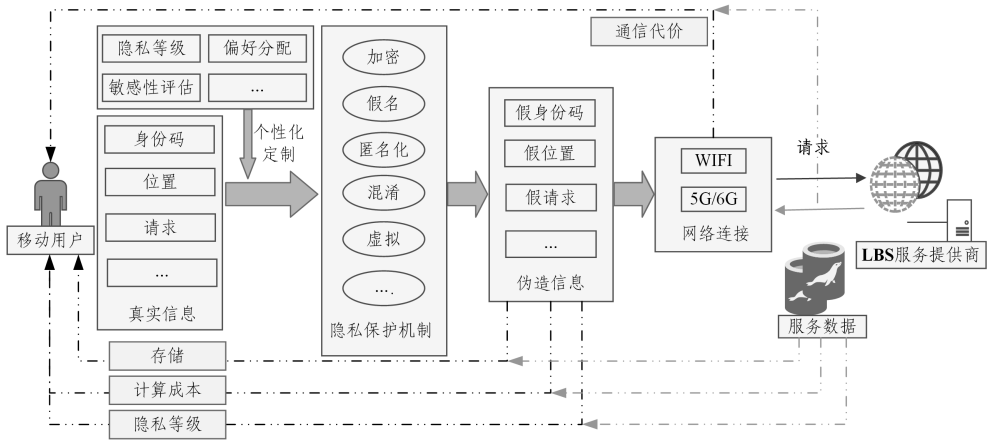

图 6 通用个性化位置隐私保护框架

Fig. 6 Generic personalized location privacy protection framework

5 现存挑战及未来工作展望

本章主要从关注的两个热门领域(不同场景下的个性化位置隐私保护以及法律法规和伦理问题)探讨了在这些领域内所面临的若干挑战和机遇。

1)针对不同场景下的个性化位置隐私保护技术研究

在现代社会，随着城市化进程的加速和交通工具的普及，交通拥堵和交通事故等问题日益突出。因此，导航和交通管理成为城市运行的关键组成部分。未来的研究应当集中在如何为用户提供更智能的动态隐私保护和高效的路径规划服务上。此外，研究的重点还应包括如何在保护个人隐私的前提下，有效利用位置数据进行交通流量分析和预测，以优化交通管理和提高道路使用效率。为了实现这一目标，应该鼓励用户参与隐私保护机制的设计和实施，通过用户反馈和偏好设置等因素，不断优化隐私保护策略。同时，还需要研究如何在多个导航和交通管理平台之间实现统一的隐私保护标准，确保用户在不同平台上的隐私权益得到同等的保护。

在移动社交网络(Mobile Social Network，MSN)中，位置

签到服务日益流行，用户通过签到分享位置，增进社交互动，用户的隐私安全变得愈发重要[82]。服务提供商则通过分析签到数据，洞察用户需求和行为模式，具有重要的商业价值。为保证用户位置信息安全，在不可信服务器环境中，针对基于位置的社交网络，Zhang 等[83]提出了一种时空约束的局部差分隐私轨迹保护方案，专注于特定区域的隐私保护，确保高隐私安全性和数据可用性。Fei 等[84]提出了一种新的无监督方法，用于推断在线社交网络用户的家庭位置，并验证了推断的准确性和可靠性。尽管已有研究提出了基于位置社交网络的位置隐私保护方法，但针对用户个性化体验的研究仍显不足。未来的研究重点应侧重于如何根据不同用户和服务场景，提供定制化的位置共享机制，例如基于好友关系和信任度的灵活控制分享区域和方法，以满足用户的个性化需求。

在广告定位和个性化推荐场景中，个性化位置隐私保护的未来发展应聚焦于以下几个方面。首先，利用人工智能等先进技术，通过更高级的数据处理和加密手段，确保用户的位置数据在传输和存储过程中得到有效保护。其次，增强用户对位置数据的控制权和透明度，使用户能够清晰了解其位置信息的用途，并提供便捷的隐私设置选项，以便用户轻松管理个人位置数据的共享。此外，未来的个性化位置隐私保护还应与法律框架和行业标准紧密结合，确保在收集和使用用户位置数据时严格遵守相关规定，从而在保护用户隐私的同时，促进个性化广告服务的健康发展。

在紧急服务场景中，由于其特殊性和紧迫性，必须采用强大的安全加密技术来确保数据传输的安全性，只有经过授权的紧急服务机构才能访问必要的位置数据。在紧急情况下，用户可能需要提供更多的位置信息以获得及时的帮助，但这也会增加隐私泄露的风险。因此，必须提高隐私保护强度。未来的发展方向包括为用户提供个性化位置隐私保护，以及开发更精准的位置推断技术。即使用户未明确共享位置信息，系统也能通过 Wi-Fi、基站等其他数据源推断用户可能的位置，以提供准确的紧急服务支持。此外，研究还应探索隐私保护度量和假设方案，评估和优化这些技术的实际效果，确保在紧急情况下既能有效保护用户隐私，又能及时提供必要的帮助。

2)法理视角下的个性化位置隐私保护技术研究

随着移动用户数据的快速增长和个性化位置隐私保护服务的普及，保护用户隐私已成为技术开发和政策制定中的紧迫任务。用户在公共领域生成和分享大量关于自己的位置信息，为了确保这些信息的合理使用并对其加以保护，需要在法律和伦理层面提供更好的规范和指导，从而对用户给予更加全面和可靠的隐私保护。Toth 等[85]聚焦于开发个性化学习工具，这些工具不仅关注用户的数据隐私，还充分考虑了道德伦理因素。该工具旨在为不同级别的个性化服务提供透明度和可控性，确保用户能够清楚了解其数据的使用方式，并能够对其进行有效管理。Wang 等[86]提出了一个框架，利用社交媒体帖子中的公共数据来预测个性化隐私偏好。该框架可以作为决策支持系统，协助平台和政策制定者评估隐私政策的影响，从而做出更有效的决策。

在全球化日益加剧的今天，数据跨境流动变得愈发频繁，未来的研究应聚焦于如何确保在不同国家和地区之间进行数据传输时，用户的隐私权益能够得到有效保护。为此，应当关注如何更新和完善隐私法律，以确保这些法律能够有效地保护个人位置数据。此外，需要研究在个性化位置隐私保护中应遵循的伦理标准，如何在技术设计和实施过程中融入伦理要素，从而确保技术的发展和应用不会对个人隐私造成潜在的威胁。

结束语 综合来看，个性化位置隐私保护研究是当前位置隐私保护领域的一个重要方向。通过结合用户的个人偏好和上下文信息，可以更好地保护用户的位置隐私，同时保证位置服务的质量和效果。相关研究中，涉及到了许多关键技术，如位置混淆、轨迹数据处理、差分隐私等。个性化位置隐私保护的研究旨在为用户提供更加个性化、智能化的位置隐私保护方案，从而有效防止位置信息泄露和隐私侵犯。

参 考 文 献

[1] Pew Research Center. Americans Increasingly Use Smartphones for More than Voice Calls, Texting [EB/OL]. www.pewresearch.org/internet/ft_01-27-16_smartphoneactivities/.

[2] JIANG H, LI J, ZHAO P, et al. Location privacy-preserving mechanisms in location-based services: A comprehensive survey [J]. ACM Computing Surveys(CSUR), 2021, 54(1): 1-36.

[3] ENCK W, GILBERT P, HAN S, et al. Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones [J]. ACM Transactions on Computer Systems, 2014, 32(2): 1-29.

[4] ZHAO Y, CHEN J. Vector-indistinguishability: location dependency based privacy protection for successive location data [J]. IEEE Transactions on Computers, 2024, 73(4): 970-979.

[5] MOHAMED R, FARRUKH H, LU Y, et al. iStelan: Disclosing Sensitive User Information by Mobile Magnetometer from Finger Touches [C]// Proceedings on Privacy Enhancing Technologies. 2023: 79-96.

[6] WU Y, SHI C, ZHANG T, et al. Privacy Leakage via Unrestricted Motion-Position Sensors in the Age of Virtual Reality: A Study of Snooping Typed Input on Virtual Keyboards [C]// 2023 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2023: 3382-3398.

[7] HU G, ZHANG B, XIAO X, et al. SAMLDroid: a static taint analysis and machine learning combined high-accuracy method for identifying Android apps with location privacy leakage risks [J]. Entropy, 2021, 23(11): 1489.

[8] ALLEN M. Health Insurers Are Vacuuming Up Details About You - And It Could Raise Your Rates [EB/OL]. www.npr.org/sections/healthshots/2018/07/17/629441555/health-insurers-arevacuuming-up-details-about-you-and-it-could-raise-yourrates.

[9] LI H, ZHU H, DU S, et al. Privacy leakage of location sharing in mobile social networks: Attacks and defense [J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(4): 646-660.

[10] RUSERT J,KHALID O,HONG D,et al. No Place to Hide:Inadvertent Location Privacy Leaks on Twitter[J]. Proc. Priv. Enhancing Technol. ,2019(4):172-189.

[11] FANG D,QIAN Y. 5G wireless security and privacy:Architecture and flexible mechanisms[J]. IEEEVehicular Technology Magazine,2020,15(2):58-64.

[12] WANG J,WANG F Y,CAO Z,et al. Sink location privacy protection under direction attack in wireless sensor networks[J]. Wireless Networks,2017,23:579-591.

[13] VELAYUDHAN N C,ANITHA A,MADANAN M. Sybil attack with RSU detection and location privacy in urban VANETs:An efficient EPORP technique[J]. Wireless Personal Communications,2022,122:3573-3601.

[14] BALARAM A,PUSHPA S. Sybil attack resistant location privacy in VANET[J]. International Journal of Information and Communication Technology,2018,13(4):389-406.

[15] XUE D,WU L F,LI H B,et al. A novel destination prediction attack and corresponding location privacy protection method in geo-social networks[J]. International Journal of Distributed Sensor Networks,2017,13(1):1550147716685421.

[16] XU Z,ZHANG H,YU X,et al. Privacy-Aware Information Sharing in Location-Based Services:Attacks and Defense[J]. IEICE Transactions on Information and Systems,2016,99(8):1991-2001.

[17] YAN G H,LIU T,ZHANG X J,et al. Service similarity-based location k-anonymity method for resisting background knowledge inference attacks[J]. Journal of Xi'an Jiaotong University,2020,54(1):8-18.

[18] LIU S,SINGH L,TIAN K. Information Exposure From Relational Background Knowledge on Social Media[C]// 2020 IEEE International Conference on Data Science and Advanced Analytics(DSAA). IEEE,2020:282-291.

[19] LIN T L,CHANG H Y,LI S L. A location privacy attack based on the location sharing mechanism with erroneous distance in geosocial networks[J]. Sensors,2020,20(3):918.

[20] JIANG H,ZHAO P,WANG C. RobLoP:Towards robust privacy preserving against location dependent attacks in continuous LBS queries[J]. IEEE/ACM Transactions on Networking,2018,26(2):1018-1032.

[21] ZHAO P,LI J,ZENG F. ILLIA:Enabling $ k $-anonymity-based privacy preserving against location injection attacks in continuous LBS queries[J]. IEEE Internet of Things Journal,2018,5(2):1033-1042.

[22] LI H,ZHU H,DU S,et al. Privacy leakage of location sharing in mobile social networks:Attacks and defense[J]. IEEE Transactions on Dependable and Secure Computing,2016,15(4):646-660.

[23] SUN Y,CHEN M,HU L,et al. ASA:Against statistical attacks for privacy-aware users in Location Based Service[J]. Future Generation Computer Systems,2017,70:48-58.

[24] MURAKAMI T. Expectation-Maximization Tensor Factorization for Practical Location Privacy Attacks[C]// Proc. Priv. Enhancing Technol. . 2017:138-155.

[25] MA Q,ZHANG S,ZHU T,et al. PLP:Protecting location privacy against correlation analyze attack in crowdsensing[J]. IEEETransactions on Mobile Computing. 2016,16(9):2588-2598.

[26] DEWRI R. Local differential perturbations:Location privacy under approximate knowledge attackers[J]. IEEE Transactions on Mobile Computing. 2012,12(12):2360-2372.

[27] NIU B,SUN J,CHEN Y. Evaluating the Impact of Adversarial Factors on Membership Inference Attacks[C]// 2023 IEEE Smart World Congress(SWC). Portsmouth,United Kingdom,2023:1-8.

[28] GUNAWAN D,PRIYAWATI D,NUGROHO Y S. Preserving Individual Privacy from Inference Attack in Transaction Data Publishing[C]// 2023 Eighth International Conference on Informatics and Computing(ICIC). Manado,Indonesia,2023:1-6.

[29] YI J,CAO T F,GAO S,et al. Honeypot defense and transmission strategy based on offensive and defensive games in vehicular networks[J]. Chinese Journal of Network and Information Security,2022,8(4):157-167.

[30] PAN X,CHEN W Z,WU L,et al. Protecting personalized privacy against sensitivity homogeneity attacks over road networks in mobile services[J]. Frontiers of Computer Science,2016,10:370-386.

[31] LIU Z P,LIU Q N,MIAO D W. A blockchain anonymity solution to prevent location homogeneity attacks[J]. Concurrency and Computation:Practice and Experience,2022,34(27):e7326.

[32] LI Y J,ZHU Y F,BAI L F. Enhanced location k-anonymity privacy protection scheme based on Geohash[J]. Computer Science,2024,51(9):393-400.

[33] SHAHAM S,DING M,LIU B,et al. Privacy preservation in location-based services:A novel metric and attack model[J]. IEEE Transactions on Mobile Computing. 2020,20(10):3006-3019.

[34] NIU B,CHEN Y,WANG Z,et al. Eclipse:Preserving differential location privacy against long-term observation attacks[J]. IEEE Transactions on Mobile Computing,2020,21(1):125-138.

[35] MA Z,XU S,LIU B. LPP2KL:Online Location Privacy Protection Against Knowing-and-Learning Attacks for LBSs[J]. IEEE Transactions on Computational Social Systems,2022,10(1):234-245.

[36] WANG J,WANG F,LI H. Differential Privacy Location Protection Scheme Based on Hilbert Curve[J]. Security and Communication Networks,2021(1):5574415.

[37] ZHANG Q,ZHANG X,WANG M,et al. DPLQ:location—based service privacy protection scheme based on differential privacy[J]. IET Information Security,2021,15(6):442-456.

[38] LI H,WANG Y,GUO F,et al. Differential privacy location protection method based on the Markov model[J]. Wireless Communications and Mobile Computing,2021(1):4696455.

[39] SAINI I,SAAD S,JAEKEL A. A comprehensive pseudonym changing scheme for improving location privacy in vehicular networks[J]. Internet of Things,2022,19:100559.

[40] ULLAH I,SHAH M A,KHAN A. Adaptive Grouping and

Pseudonym Changing Policy for Protection of Vehicles Location Information in VANETs[C]// 2021 IEEE Symposium Series on Computational Intelligence(SSCI). IEEE, 2021: 1-7.

[41] MEMON I, MEMON H, ARAIN Q A. Pseudonym changing strategy with mix zones based authentication protocol for location privacy in road networks[J]. Wireless Personal Communications, 2021, 116: 3309-3329.

[42] WANG J, WANG C R, MA J F, et al. A fake location selection algorithm based on location semantics and query probability[J]. Journal of Communication, 2020, 41(3): 53-61.

[43] LI L, SHI D, ZHANG X, et al. Privacy preserving participant recruitment for coverage maximization in location aware mobile crowdsensing[J]. IEEE Transactions on Mobile Computing, 2021, 21(9): 3250-3262.

[44] GAO Z G, HUANG Y, ZHENG L, et al. Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6290-6299.

[45] BUCCAFURRI F, DE A V, IDONE M F, et al. A Distributed Location Trusted Service Achieving k-Anonymity against the Global Adversary[C]// 2021 22nd IEEE International Conference on Mobile Data Management (MDM). IEEE, 2021: 133-138.

[46] YANG M, YE B, CHEN Y, et al. A trusted de-swinging k-anonymity scheme for location privacy protection[J]. Journal of Cloud Computing, 2022, 11(1): 2.

[47] XING L, JIA X, GAO J, et al. A location privacy protection algorithm based on double k-anonymity in the social internet of vehicles[J]. IEEE Communications Letters, 2021, 25(10): 3199-3203.

[48] ZHENG X, YUAN Q, WANG B, et al. A Homomorphic Encryption Based Location Privacy Preservation Scheme for Crowdsensing Tasks Allocation[J]. Wireless Personal Communications, 2022, 126(1): 719-740.

[49] JAIN M, SINGH P, RAMAN B. SHELBRS: Location-Based Recommendation Services Using Switchable Homomorphic Encryption[C]// Security, Privacy, and Applied Cryptography Engineering: 11th International Conference, SPACE 2021, Kolkata, India, December 10-13, 2021, Proceedings. Cham: Springer International Publishing, 2022: 63-80.

[50] KHAZBAK Y, FAN J, ZHU S, et al. Preserving personalized location privacy in ride-hailing service[J]. Tsinghua Science and Technology, 2020, 25(6): 743-757.

[51] MA B, WANG X, NI W, et al. Personalized Location Privacy With Road Network-Indistinguishability[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(11): 20860-20872.

[52] XU C, DING Y, ZHAO G, et al. Personalized location privacy protection for location-based services in vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(1): 1163-1177.

[53] MIN M, ZHU H, DING J, et al. Personalized 3D Location Privacy Protection With Differential and Distortion Geo-Perturbation [J]. IEEE Transactions on Dependable and Secure Computing. 2024, 21(4): 3629-3643.

[54] WANG Z, HU J, LV R, et al. Personalized privacy-preserving task allocation for mobile crowdsensing[J]. IEEE Transactions on Mobile Computing, 2018, 18(6): 1330-1341.

[55] FAN Y, LIU L, ZHANG X, et al. MAPP: An efficient multi-location task allocation framework with personalized location privacy-protecting in spatial crowdsourcing [J]. Information Sciences, 2023, 619: 654-678.

[56] LV C, ZHANG L, LI X Y. Personalized Differentially Private Online Minimum Bipartite Matching IN Spatial Crowdsourcing [C]// 2022 8th International Conference on Big Data Computing and Communications(BigCom). IEEE, 2022: 134-143.

[57] ZHANG C, WANG Y, WANG W, et al. A Personalized Location Privacy Protection System in Mobile Crowdsourcing[J]. IEEE Internet of Things Journal, 2024, 11(6): 9995-10006.

[58] WEN R, CHENG W, HUANG H, et al. Privacy preserving trajectory data publishing with personalized differential privacy [C]// 2020 IEEEIntl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking. IEEE, 2020: 313-320.

[59] ZHI W, GONG X, WANG Y. Personalized Differential Privacy Preservation Method for Trajectory Based on Regional Density Analysis[C]// 2023 2nd International Conference on Big Data, Information and Computer Network (BDICN). IEEE, 2023: 43-48.

[60] YUQI O. Trajectory Synthesis Method Based on Personalized Local Differential Privacy[C]// 2023 IEEE 14th International Conference on Software Engineering and Service Science. IEEE, 2023: 230-234.

[61] ISLAM F T, HASHEM T, SHAHRIYAR R. A Crowd-Enabled Approach for Privacy-Enhanced and Personalized Safe Route Planning for Fixed or Flexible Destinations[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 53(11): 10922-10936.

[62] YI K, CHEN Y, SU Y, et al. Towards Efficient Privacy-Preserving Top-k Trajectory Similarity Query[C]// 2023 IEEE International Conference on Mobile Ad Hoc and Smart Systems. IEEE, 2023: 512-520.

[63] MIN M H, YANG S, XU J H, et al. Intelligent Semantic Location Privacy Protection Method in Three-Dimensional Spatial Location Services[J]. Journal of Electronics and Information Engineering, 2024, 46(6): 2627-2637.

[64] MIN M, ZHU H, ZHANG H, et al. Semantic Adaptive Geo-Indistinguishability for Location Privacy Protection in Mobile Networks[J]. IEEE Transactions on Vehicular Technology, 2024, 73(6): 9193-9198.

[65] QIU G, GUO D, SHEN Y, et al. Mobile semantic-aware trajectory for personalized location privacy preservation[J]. IEEE Internet of Things Journal, 2020, 8(21): 16165-16180.

[66] QIU G, TANG G, LI C, et al. DSG-BTra: Differentially Semantic-Generalized Behavioral Trajectory for Privacy-Preserving

Mobile Internet Services[J]. IEEE Internet of Things Journal, 2023,11(7):13029-13038.

[67] ZHONG H,NI J,CUI J,et al. Personalized location privacy protection based on vehicle movement regularity in vehicular networks[J]. IEEE Systems Journal,2021,16(1):755-766.

[68] WANG J,LIU H,DONG X,et al. Personalized Location Privacy Trading in Double Auction for Mobile Crowdsensing[J]. IEEE Internet of Things Journal,2022,10(10):8971-8983.

[69] SHEN Z,HE S,WANG H,et al. A Differential Privacy Budget Allocation Method Combining Privacy Security Level[J]. Journal of Communications and Information Networks,2023,8(1):90-98.

[70] YANG M,WU Y,CHEN Y. A K-anonymity Optimization AlgorithmUnder Attack Model[C]// 2022 IEEE International Conferences on Internet of Things and IEEE Green Computing & Communications. IEEE,2022:357-362.

[71] NIU B,LI Q,WANG H,et al. A framework for personalized location privacy[J]. IEEE Transactions on Mobile Computing, 2021,21(9):3071-3083.

[72] LIN Y,JIANG Y,LI Y,et al. Privacy-preserving batch-based task assignment over spatial crowdsourcing platforms[J]. Computer Networks,2024,241:110196.

[73] BI R,ZHAO M,YING Z,et al. Achieving dynamic privacy measurement and protection based on reinforcement learning for mobile edge crowdsensing of IoT[J]. Digital Communications and Networks,2022,10(2):380-388.

[74] HAN P X,LIU Z B,SUN Z,et al. A novel prediction model for ship fuel consumption considering shipping data privacy: An XGBoost-IGWO-LSTM-based personalized federated learning approach[J]. Ocean Engineering,2024,302:117668.

[75] PANDEY M,KAUR H,BASAK S,et al. Privacy-Preserving Location-Based Services: A DQN Algorithmic Perspective[C]// 2024 International Conference on Advanced Information Networking and Applications (AINA). Cham: Springer Nature Switzerland,2024:384-399.

[76] SUN X,WANG Y,DUAN P,et al. Bilateral Privacy Protection Scheme Based on Adaptive Location Generalization and Grouping Aggregation in Mobile Crowdsourcing[J]. IEEE Internet of Things Journal,2024,11(10):17740-17756.

[77] HUANG H,HUANG T,WANG W,et al. Federated Learning and Convex Hull Enhancement for Privacy Preserving Wi-Fi-Based Device-Free Localization [J]. IEEE Transactions on Consumer Electronics,2024,70(1):2577-2585.

[78] MACHAM,FOUTZ N Z,LI B,et al. Personalized privacy preservation in consumer mobile trajectories [J]. Information Systems Research,2024,35(1):249-271.

[79] LI Y,BAI L,ZHANG Y. Framework of privacy metric for location-based services [C]// 3rd International Symposium on Electrical,Electronics and Information Engineering(ISEEIE 2023). Hangzhou,China:IEEE,2023:120-125.

[80] APOLLONIO F,BEDOGNI L,GORI G,et al. On the Trade-Off Between Privacy and Information Quality in Location Based Services[C]// IEEE 21st Consumer Communications & Networking Conference(CCNC). IEEE,2024:994-997.

[81] MIN M H,ZHU H P,LI S Y,et al. Semantic Adaptive Geo-Indistinguishability for Location Privacy Protection in Mobile Networks [J]. IEEE Transactions on Vehicular Technology,2024, 73(6):9193-9198.

[82] 汪玉洁,刘涛,包象琳,潘正高. 基于社区划分的社交推荐隐私保护方法[J]. 重庆工商大学学报(自然科学版),2024(6):30-38.

[83] ZHANGW,XIE Z,VERA VENKATA SAI A M,et al. A Local Differential Privacy Trajectory Protection Method Based on Temporal and Spatial Restrictions for Staying Detection[J]. Tsinghua Science and Technology,2024,29(2):617-633.

[84] FEI G,LIU Y,HU G,et al. Online Social Network User Home Location Inference Based on Heterogeneous Networks[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(6):5509-5525.

[85] TOTH A. Toward privacy-focused personalization: Designing a learning experience to facilitate privacy-personalization trade-off [C]// 2024 Adjunct Proceedings of the 32nd ACM Conference on User Modeling, Adaptation and Personalization (UMAP). 2024:61-65.

[86] WANG W,LI B. Learning Personalized Privacy Preference From Public Data [C]// ICIS 2023 Proceedings. 2023.

CAO Tengfei, born in 1987, Ph.D, associate professor, Ph. D. supervisor, is a senior member of CCF (No. 34077S). His main research interests include network security and privacy protection technologies.

(责任编辑:柯颖)