Software Engineering and Applications 软件工程与应用, 2023, 12(6), 826-831
Published Online December 2023 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2023.126080

Hans汉斯

群智感知网络中轨迹隐私保护方法安全性分析

王心怡，廖祎玮，张志敏，纪　雷，赵国生

哈尔滨师范大学计算机科学与信息工程学院，黑龙江 哈尔滨

收稿日期：2023年10月9日；录用日期：2023年12月4日；发布日期：2023年12月13日

摘　要

随着科技与经济的快速发展和移动智能设备层出不穷极大地推动了群智感知(Crowdsensing, CS)网络的发展。其中，轨迹隐私保护方法是群智感知隐私保护研究的热点问题，虽然轨迹隐私保护方法多样，但在具有大规模参与者的群智感知网络中仍存在隐私保护不当的问题。因此，本文对群智感知轨迹隐私保护方法的安全性进行分析，对研究者开展群智感知轨迹隐私保护研究具有重要意义。首先，本文对群智感知轨迹隐私保护面临的安全问题进行详细的阐述。接着归纳总结了现有群智感知轨迹隐私保护方法包括假数据、匿名、抑制和扰动等方法的研究现状和存在的问题。最后，对群智感知轨迹隐私保护方法未来研究方向总结与展望。

关键词

轨迹隐私，隐私保护方法，群智感知

Security Analysis of Trajectory Privacy Protection Methods in Crowdsensing Networks

Xinyi Wang, Yiwei Liao, Zhimin Zhang, Lei Ji, Guosheng Zhao

College of Computer Science and Information Engineering, Harbin Normal University, Harbin Heilongjiang

Received: Oct. 9th, 2023; accepted: Dec. 4th, 2023; published: Dec. 13th, 2023

Abstract

With the rapid development of technology and economy and the emergence of mobile intelligent devices, the development of crowdsensing networks has been greatly promoted. Among them, trajectory privacy protection methods are a hot topic in the research of crowdsensing privacy protection. Although there are various methods for trajectory privacy protection, there is still a

文章引用: 王心怡, 廖祎玮, 张志敏, 纪雷, 赵国生. 群智感知网络中轨迹隐私保护方法安全性分析[J]. 软件工程与应用, 2023, 12(6): 826-831. DOI: 10.12677/sea.2023.126080

problem of improper privacy protection in crowdsensing networks with large-scale participants. Therefore, this paper analyzes the security of the trajectory privacy protection methods of crowdsensing, which is of great significance for researchers to conduct research on the trajectory privacy protection of crowdsensing. Firstly, this article provides a detailed explanation of the security issues faced by the privacy protection of crowdsensing trajectories. Then, the research status and existing problems of existing crowdsensing trajectory privacy protection methods, including false data, anonymity, suppression, and perturbation methods, were summarized and summarized. Finally, a summary and outlook on the future research directions of crowdsensing trajectory privacy protection methods.

Keywords

Trajectory Privacy, Privacy Protection Methods, Crowdsensing

1. 引言

群智感知网络利用大量普通参与者的感知设备收集感知数据，对数据进行采集、处理和分析[1]。它的核心在于通过吸纳广泛的参与者，将分散的信息和知识汇聚成整体，形成具有价值的资源和产出，推动社会创新和发展。由于群智感知网络感知设备的普遍性和参与者位置移动的灵活性，完美的解决了传统传感器感知网络维护成本高且覆盖范围受限使得感知任务的完成效果和效率都大打折扣的问题，同时互联网的发展更是加快了群智感知的研究与应用。

群智感知虽然为社会带来了巨大的发展与机遇，但在执行任务过程中参与者仍存在隐私泄露的问题[2]。当参与者参与感知任务时，需要上传参与者的个人隐私信息并将它提交给感知平台，其中包括参与者执行任务时的位置序列即参与者的轨迹信息，而在这个过程中极容易遭到外部攻击者的攻击，因此，参与者轨迹会面临极大的隐私泄露风险。外部攻击者可以根据参与者对某些位置的访问频率推测出轨迹位置中的重要位置区域比如医院、工作单位、学校等来推测被攻击者的职业人际关系等等，严重威胁了参与者的隐私同时影响参与者参与感知活动的积极性进而危害行业发展。因此，本文首先总结了群智感知轨迹隐私保护面临的安全问题，然后分析现有群智感知轨迹隐私保护方案的研究现状，最后总结和展望群智感知轨迹隐私保护方法未来的研究方向。

2. 群智感知轨迹隐私保护面临的安全问题

群智感知网络中主要包含三个实体分别是参与者、感知平台和任务发布者[3]。如图 1 所示，任务发布者发布任务请求到感知平台，感知平台将任务发布给每个参与者，参与者上传感知数据到感知平台通过感知平台将感知数据发送任务发布者。在参与者上传感知数据到感知平台时，外部攻击者可能会窃取参与者的隐私信息，造成隐私泄露。参与者上传的感知数据中包含参与者的数据、身份和位置信息，其中参与者的位置隐私保护中的轨迹隐私保护得到广泛关注，通过对这些轨迹数据的分析和挖掘结果可以研究出个人的行为模式等敏感信息，因此目前群智感知中参与者的轨迹隐私保护得到了广泛的关注。

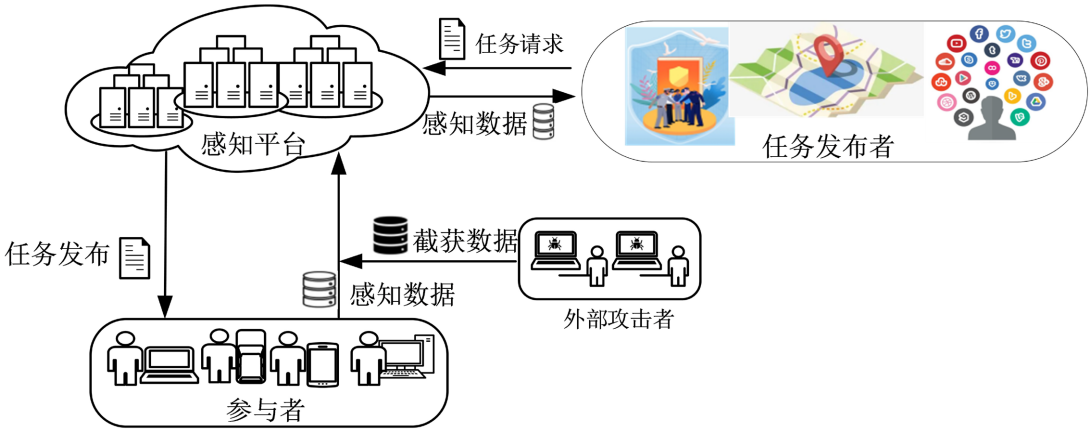

Figure 1. Crowdsensing privacy threats
图 1. 群智感知隐私威胁

群智感知网络中参与者需要上传感知数据用于后续的数据挖掘过程，由于传输链路的不稳定，恶意攻击者极容易在传输过程中截获数据，通过分析参与者上传的轨迹数据获取参与者的隐私信息。当前的轨迹隐私保护主要面临着以下几种安全问题。

(1) 参与者轨迹频繁访问经过某一位置点，导致参与者隐私泄露。攻击者掌握参与者一定的历史轨迹，这些历史轨迹上的频繁访问的轨迹点很可能暴露其兴趣偏好、家庭住址等个人隐私信息。例如某天参与者的轨迹点集中的地方是某一兴趣班，可以由此推断出这个参与者的兴趣爱好。

(2) 频繁经过具有特殊意义的语义位置点导致的参与者隐私泄露。例如，参与者长时间访问某一超市这一具有具体语义信息的位置点，那么攻击者可以根据其访问的频率判断参与者的家庭住址等信息。

(3) 参与者背景信息与轨迹之间的关联导致的参与者隐私泄露。攻击者掌握一定的背景知识，依据背景知识推测出参与者特定的兴趣区域。例如，某人每天晚上在某一时间段有 90%的概率时间段从地点 A 出发到地点 B，那么通过时间和地理位置信息，攻击者很容易判断出该参与者可能先去吃饭再去散步，导致参与者的行为习惯被泄露。

3. 群智感知轨迹隐私保护保护方法

目前，群智感知轨迹隐私保护方法受到了广泛的关注。总的来看，群智感知轨迹隐私保护方法可以概括为假数据、匿名、泛化和抑制隐私保护技术。

3.1. 基于假数据的轨迹隐私保护方法

假数据轨迹隐私保护技术是在待发布的真实轨迹中添加一定量的假轨迹，使攻击者无法判断真实轨迹信息，以此保护轨迹隐私[4]。You 等人[5]提出了两种能够产生假轨迹的方案，分别通过生成与真实轨迹运行模式相同的轨迹和旋转真实轨迹生成假轨迹与真实轨迹混淆，但算法运行效率较低，在群智感知大规模轨迹数据的情况上并不适用。Dai J 等人[6]提出了一种分割假轨迹的轨迹隐私保护方法，在真实轨迹上随机采样生成假轨迹点组成满足隐私要求的假轨迹来混淆真实轨迹，但是这种方法仍存在这算法运行效率较低的问题。刘向宇等人[7]使用网格划分方法将真实轨迹和敏感轨迹混合隐藏具有较高的运行效率。李凤云等人[8]利用车辆自适应时间窗口算法对车辆轨迹进行分组选择，通过混淆算法将需要保护的车辆轨迹与周围车辆轨迹辆混合发布从而达到隐私保护的目的。

综上所述，目前的假数据轨迹隐私保护技术主要通过生成与原始轨迹相似的轨迹对原始轨迹进行隐私保护，但是添加假数据的与原有轨迹差异太小，攻击者可以根据参与者历史信息推测出有价值的信息。

添加的假数据与原有轨迹差异程度太大，又降低了轨迹的可用性。此外，由于假数据轨迹隐私保护技术在原始轨迹上添加了大规模的假轨迹数据在要求实时性高的群智感知网络中并不适用。

3.2. 基于匿名的轨迹隐私保护方法

轨迹匿名技术，可以将轨迹隐匿在一定的范围内，使得隐匿后轨迹与原轨迹无法分辨。Tan 等人[9]提出了基于 k 匿名的语义匿名化模型，找到 k-1 个兴趣点的敏感区域，根据敏感区域的敏感特性对轨迹进行模糊处理，保证了较高的隐私保护水平但可用性较低。Chen 等人[10]通过考虑不同路段上阈值的变化，构建一个考虑道路网络信息的自适应阈值集。然后，针对输出的匿名轨迹数据集，利用微分隐私下匿名位置距离的拉普拉斯机制对其进行微扰，提高了轨迹的不可分辨性。宋成等人[11]选择 k-1 个噪声用户与真实用户组成 k 匿名组，实现用户身份和轨迹的隐私保护。这种方法虽然达到了较高的隐私保护效果但是降低了轨迹的可用性。Gao 等人[12]提出了轨迹混淆的差异位置隐私保护机制，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化到目标混淆子区域，最后在目标混淆子区域进行拉普拉斯采样，得到混淆轨迹点，减少了 20%以上的数据质量损失。

综上所述，当前轨迹匿名技术隐私保护方案，主要通过构建匿名轨迹集实现对轨迹的隐私保护，但是在实际应用中匿名集的构建应根据参与者不同匿名需求不同进行改变。此外为了方便后续对轨迹的处理和利用，轨迹隐私保护需要着重考虑轨迹可用性问题，即如何选择合适的匿名区域，在保护参与者轨迹隐私的同时减少轨迹的失真度。相较于在真实轨迹中加入假轨迹的方法中攻击者可能存在着一定概率获取参与者的真实轨迹，基于匿名的轨迹隐私保护方法将轨迹点扰动到一定范围内，即使攻击者可以获得轨迹信息，但由于对发布轨迹进行一定程度上的隐匿该方法仍保证较高的隐私保护水平。但是基于匿名的轨迹隐私保护技术的匿名的范围难以准确掌控，所以基于匿名的轨迹隐私保护方法常需要与其他技术联合使用来提高轨迹的可用性。

3.3. 基于抑制的轨迹隐私保护方法

基于抑制的轨迹隐私保护方法，是根据参与者的实际需求选择性的发布轨迹数据。例如：参与者认为自己一天的轨迹中，超市、餐厅这一地理位置相对于医院是不敏感的，那么在发布这位参与者的轨迹时，不发布医院这一位置点，但是发布超市这一位置点。在这个轨迹的发布过程中，轨迹时不完整的，轨迹失真较大，因此采用抑制方法需要构建隐私保护度和轨迹失真度的平衡函数以保证良好的效果。Lan 等人[13]将扰动与抑制方法结合提出了一种结合划分兴趣区域和驻留点提取的隐私保护方法，通过在驻留点添加 Laplace 噪声来保护轨迹隐私。汪逸飞等人[14]通过计算某一时空轨迹点的信息熵值构建代价函数，抑制局部时空轨迹点来保护用户轨迹隐私。

综上所述，采用基于抑制的轨迹隐私保护方法，相较于基于假数据和基于匿名的轨迹隐私保护方法，虽然在一定程度上提高了参与者轨迹的可用性，但是基于抑制的轨迹隐私保护方法依赖于抑制轨迹点的判断方法。在进行抑制轨迹点的判断过程中，如果存在着某些较为重要的轨迹点没有被抑制，会导致隐私保护水平下降。同时抑制部分轨迹点也存在着轨迹的时间序列遭到破坏的问题，无法保证轨迹的准确性。此外，虽然对当前发布的轨迹点进行抑制，但是若攻击者拥有足够多的背景知识时依然可以获取参与者隐私信息即基于抑制的轨迹隐私保护方法无法抵御基于背景知识的攻击，因此在研究中常将轨迹抑制技术与其他技术结合使用。

3.4. 基于扰动的轨迹隐私保护方法

扰动的思想是对位置添加随机噪声生成扰乱位置，由于随机噪声可以人为控制，所以更适合应用于需要较高可用性的轨迹发布场景。差分隐私技术是最典型的基于扰动的隐私保护方法。差分隐私是通过

加噪手段，将数据扰动到一定范围内，由于扰动的范围可以通过隐私预算控制，所以灵活性较高。差分隐私按照处理数据的位置，可以分为集中式差分隐私和本地差分隐私。集中式差分隐私，由第三方服务器统一对待保护数据进行处理，这就要求第三方服务器可信性，而本地化差分隐私，将数据处理分散到参与者自身在自身处理，避免不可信第三方造成的隐私泄露问题。因此，集中式差分隐私常采用拉普拉斯机制等添加噪声的方法来进行隐私保护，本地化差分隐私常采用随机响应方法来进行隐私保护。

吴云乘等人[15]针对根据时序位置和地理拓扑推测参与者的隐私偏好的问题，提出了将地理拓扑关系采用无向图表示，根据无向图节点之间的关系设置隐私级别，有效的避免了攻击者根据关联知识获取参与者隐私的问题。刘凯等人[16]首先使用 DBSCAN 算法对数据分析清除噪音点，然后结合状态转移矩阵利用差分隐私方法对轨迹点进行差分隐私扰动。李洪涛等人[17]从路网拓扑关系的角度出发对路段敏感程度进行级别划分，通过差分隐私位置保护机制实现位置隐私保护。陈思等人[18]将机器学习方法与差分隐私方法结合提出了一种基于差分隐私的轨迹隐私保护方案，有效解决了攻击者掌握一定背景知识的问题。

综上所述，现有的基于扰动的轨迹隐私保护方法常与机器学习方法结合使用，为了达到个性化的隐私保护需求，部分研究者采用聚类、网格划分等方法判断频繁停留区域，判断不同隐私级别，然后泛化实现参与者的隐私保护。与基于假数据的轨迹隐私方法对比由于扰动方法主要采用添加噪声的方法进行隐私保护使得方法的运行效率普遍较高。与基于匿名的轨迹隐私方法相比扰动方法可以通过设施隐私预算来控制扰动的大小有效的提高了轨迹的可用性。与基于抑制的轨迹隐私保护方法对比扰动方法可以在一定程度上抵抗攻击者的背景知识攻击。因此基于扰动方法在轨迹隐私保护中得到了研究者的广泛应用。

4. 群智感知轨迹隐私保护方法未来研究方向

目前轨迹隐私保护技术研究在各个方面虽然取得了一定的进展，但是都存在一定的局限性，现有参与者轨迹隐私保护方法存在着以下问题。

(1) 差异化隐私保护：现有轨迹进行差分隐私保护采用单一的隐私预算，未考虑参与者不同轨迹位置点敏感度不同，以灵活地适应不同隐私需求，无法为每个用户提供个性化的隐私保护机制，导致保护不足和过保护问题。

(2) 隐私保护不够全面：轨迹数据在时间和空间维度上具有相关性，现有的研究仅考虑轨迹数据的空间属性没有考虑轨迹的时间属性，使隐私保护不充分。

(3) 可用性和效用问题：隐私预算是一项影响预算资源的重要参数，资源分配不合理会导致平台成本较高。此外，采用较高的隐私预算，隐私保护程度会下降，但会提高数据的准确性。而采用较小的隐私预算会有较高的隐私保护程度，但会导致数据准确性下降。

随着群智感知网络的不断发展，参与者的轨迹隐私保护问题将会得到更大的关注。针对上述问题，群智感知轨迹隐私保护方法未来的研究方向如下。

(1) 在未来的群智感知参与者轨迹隐私保护过程中，为了提高参与者参与感知活动的积极性，应更注重参与者的背景信息，构建根据参与者的不同敏感背景构建隐私模型，采取个性化的隐私保护。

(2) 针对轨迹隐私保护不够全面和发布轨迹不准确的问题，在进行参与者轨迹隐私保护时考虑根据轨迹的多属性问题，进行多方面的考量使得敏感区域判定更准确。同时可以结合深度学习和强化学习等方法提高发布轨迹质量。

(3) 目前群智感知轨迹隐私保护研究虽然保证了较高的隐私保护水平但是轨迹的可用性较低，在未来的研究中可以通过构建轨迹隐私保护水平与轨迹可用性平衡函数来达到轨迹隐私保护与可用性的平衡。

(4) 当前随着群智感知大规模参与者的出现，群智感知轨迹隐私保护方法的运行效率问题也应得到关注，即可以考虑如何通过构建更高性能的轨迹隐私保护算法来实现运行效率的提升。

5. 结语

随着移动群智感知的快速发展，更多的参与者参与到感知任务中，群智感知中参与者的隐私保护得到广泛的关注。群智感知参与者轨迹隐私保护方法是参与者位置隐私保护的研究重点。本文从群智感知参与者轨迹隐私保护的角度出发，首先概括了参与者可能面临的轨迹隐私安全问题，其次总结了群智感知轨迹隐私保护方法研究现状，说明了当前群智感知轨迹隐私保护方法存在的问题。最后，根据目前的方法存在的问题对群智感知轨迹隐私保护方法未来研究方向进行了展望，为未来的研究提供参考。

基金项目

黑龙江省高等教育教学改革研究一般研究项目(SJGY20220351)和 2023 年度省规划办重点课题(GJB1423438)。

参考文献

[1] Zhang, J., Yang, F., Ma, Z., *et al*. (2020) A Decentralized Location Privacy-Preserving Spatial Crowdsourcing for Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, **22**, 2299-2313. https://doi.org/10.1109/TITS.2020.3010288

[2] 熊金波, 毕仁万, 田有亮, 刘西蒙, 马建峰. 移动群智感知安全与隐私: 模型、进展与趋势[J]. 计算机学报, 2021, 44(9): 1949-1966.

[3] 李利, 何欣, 韩志杰. 群智感知的隐私保护研究综述[J]. 计算机科学, 2022, 49(5): 303-310.

[4] Li, S., Shen, H. and Sang, Y. (2020) A Survey of Privacy-Preserving Techniques on Trajectory Data. In: Shen, H., Sang, Y., Eds., *Parallel Architectures, Algorithms and Programming*. Springer, Cham, 461-476. https://doi.org/10.1007/978-981-15-2767-8_41

[5] You, T.H., Peng, W.C. and Lee, W.C. (2007) Protecting Moving Trajectories with Dummies. 2007 *International Conference on Mobile Data Management*, Mannheim, 1 May 2007, 278-282. https://doi.org/10.1109/MDM.2007.58

[6] Dai, J. and Hua, L. (2015) A Method for the Trajectory Privacy Protection Based on the Segmented Fake Trajectory under Road Networks. 2015 2*nd International Conference on Information Science and Control Engineering*, Shanghai, 24-26 April 2015, 13-17. https://doi.org/10.1109/ICISCE.2015.12

[7] 刘向宇, 陈金梅, 夏秀峰, 等. 防止暴露位置攻击的轨迹隐私保护[J]. 计算机应用, 2020, 40(2): 479-485.

[8] 李凤云, 郭昊, 毕远国, 等. 基于路径混淆的实时轨迹隐私保护方法[J/OL]. 计算机工程与应用, 2023: 1-8. https://kns.cnki.net/kcms/detail/11.2127.TP.20221108.1458.006.html

[9] Tan, R., Tao, Y., Si, W., *et al*. (2020) Privacy Preserving Semantic Trajectory Data Publishing for Mobile Location-Based Services. *Wireless Networks*, **26**, 5551-5560. https://doi.org/10.1007/s11276-019-02058-8

[10] Chen, H., Li, S. and Zhang, Z. (2020) A Differential Privacy Based (k-ψ)-Anonymity Method for Trajectory Data Publishing. *Computers, Materials & Continua*, **65**, 2665-2685. https://doi.org/10.32604/cmc.2020.010965

[11] 宋成, 程道晨, 倪水平. 个性化差分隐私的 k 匿名轨迹隐私保护方案[J]. 北京邮电大学学报, 2023, 46(3): 109-114.

[12] Gao, Z., Huang, Y., Zheng, L., *et al*. (2022) Protecting Location Privacy of Users Based on Trajectory Obfuscation in Mobile Crowdsensing. *IEEE Transactions on Industrial Informatics*, **18**, 6290-6299. https://doi.org/10.1109/TII.2022.3146281

[13] Lan, W., Lin, Y., Bao, L., *et al*. (2020) Trajectory-Differential Privacy-Protection Method with Interest Region. *Journal of Frontiers of Computer Science & Technology*, **14**, 59-72.

[14] 汪逸飞, 罗永龙, 俞庆英, 刘晴晴, 陈文. 基于信息熵抑制的轨迹隐私保护方法[J]. 计算机应用, 2018, 38(11): 3252-3257.

[15] 吴云乘, 陈红, 赵素云, 梁文娟, 吴垚, 李翠平, 张晓莹. 一种基于时空相关性的差分隐私轨迹保护机制[J]. 计算机学报, 2018, 41(2): 309-322.

[16] 刘凯, 韩益亮, 郭凯阳, 吴日铭, 汪晶晶. 基于密度的噪声应用空间聚类算法的差分隐私轨迹保护机制[J]. 科学技术与工程, 2022, 22(25): 11091-11096.

[17] 李洪涛, 任晓宇, 王洁, 等. 基于差分隐私的连续位置隐私保护机制[J]. 通信学报, 2021, 42(8): 164-175.

[18] 陈思, 付安民, 苏铠, 孙怀江. 基于差分隐私的轨迹隐私保护方案[J]. 通信学报, 2021, 42(9): 54-64.