移动群智感知安全与隐私:模型、进展与趋势

熊金波[1)] 毕仁万[1)] 田有亮[2)] 刘西蒙[3)] 马建峰[4)]

[1)](福建师范大学计算机与网络空间安全学院 福州 350117)

[2)](贵州大学计算机科学与技术学院 贵阳 550025)

[3)](福州大学数学与计算机科学学院 福州 350108)

[4)](西安电子科技大学陕西省网络与系统安全重点实验室 西安 710071)

摘 要 移动群智感知作为一种新兴的物联网感知范式,通过激励现代化智能感知设备获得高质量的感知数据,从而高效地完成大规模且复杂的社会感知任务并服务人类社会.移动群智感知系统由感知用户、感知平台和服务提供商组成,在感知任务执行过程中,感知数据经历感知、上传和交易三个阶段,各阶段均面临多种多样的数据安全和隐私泄露风险,危害感知用户隐私和感知数据安全.首先介绍移动群智感知的系统模型、实际应用场景并给出主要安全研究方法,以感知数据参与感知任务的生命周期为轴线,讨论在感知数据生命周期的三个阶段所面临的安全与隐私威胁;在上述威胁基础上,分别从三个阶段系统阐述现有的数据安全与隐私保护解决方案;最后,从隐私度量、隐私框架、隐私保护和隐私计算等方面探讨进一步的发展趋势与研究方向.

关键词 移动群智感知;数据安全;隐私保护;差分隐私;博弈模型

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2021.01949

Security and Privacy in Mobile Crowdsensing: Models, Progresses, and Trends

XIONG Jin-Bo[1)] BI Ren-Wan[1)] TIAN You-Liang[2)] LIU Xi-Meng[3)] MA Jian-Feng[4)]

[1)](*College of Computer and Cyber Security, Fujian Normal University, Fuzhou* 350117)

[2)](*College of Computer Science and Technology, Guizhou University, Guiyang* 550025)

[3)](*College of Mathematics and Computer Science, Fuzhou University, Fuzhou* 350108)

[4)](*Shaanxi Key Laboratory of Network and System Security, Xidian University, Xi'an* 710071)

Abstract Having emerged as a novel intelligent perception paradigm of the Internet of Things, mobile crowdsensing (MCS) is capable of handling large-scale and complex social sensing tasks and service applications in human society by motivating modern intelligent sensing devices to provide high-quality sensing data. With the exploding growth of smart devices, MCS has made a rapid progress in recent years, and has greatly enriched various applications and services in smart city, such as intelligent transportation, connected healthcare, smart energy, ambient monitoring, etc. An MCS system is mainly composed of sensing users, sensing platforms and service providers. In the duration of a sensing task, the relevant sensing data goes through three stages: data sensing, data uploading and data trading. Each stage is faced with a variety of risks that could endanger sensing users' privacy and sensing data security. The existing works mainly discuss the security and privacy of MCS from one stage or one particular security problem, lacking an overall and systematic

收稿日期:2020-09-12;在线发布日期:2021-05-28.本课题得到国家自然科学基金(61872088,62072109,U1905211,U1804263,61772008,61702105,61872090)、福建省自然科学基金(2019J01276)、贵州省科技支撑重大项目(20183001)、贵州省公共大数据重点实验室开放课题(2019BDKFJJ004)、陕西省网络与系统安全重点实验室开放课题(NSSOF1900104)资助.**熊金波**,博士,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为移动群智感知安全与隐私保护.E-mail:jbxiong@fjnu.edu.cn.**毕仁万**,博士研究生,中国计算机学会(CCF)学生会员,主要研究方向为安全深度学习与隐私.**田有亮**(通信作者),博士,教授,博士生导师,主要研究领域为密码学与信息安全.E-mail:youliangtian@163.com.**刘西蒙**,博士,研究员,博士生导师,主要研究领域为密码学与人工智能安全.**马建峰**,博士,教授,博士生导师,中国计算机学会(CCF)会士,主要研究领域为密码学、计算机网络、信息安全.

perspective. Without comprehensively addressing the security and privacy issues, the continuous developments of MCS could be hindered. This paper introduces a system model and real application scenarios of MCS, followed by the main security research methods. Taking the lifecycle of sensing data participating in the sensing task as the axis, we discuss the security and privacy threats in all three stages of the sensing data lifecycle. Targeting these threats, we elaborately describe the existing security and privacy protection solutions from data security, location privacy and identity privacy. We give the further developing trends and research directions of MCS to conclude the paper, such as individual dynamic privacy measurement, adaptive privacy-preserving framework, blockchain-based secure key management, multi-meta privacy protection and integrated privacy computing, etc.

Keywords mobile crowdsensing; data security; privacy protection; differential privacy; game theory model

1 引 言

以信息化和智能化为典型特征的智慧城市正得到以美、欧为代表的发达国家政府和产业界的高度重视. 同时,我国由多部委联合发布的《关于促进智慧城市健康发展的指导意见》明确提出到 2020 年建成一批特色鲜明的智慧城市,智慧城市建设已上升为国家战略. 然而,随着第四次工业革命的深入,现代城市空间的立体延伸、功能的深度耦合以及场景的开放多变对城市精准管理提出了新挑战. 移动群智感知(Mobile CrowdSensing,MCS),将移动感知和众包思想相结合,是一种新颖的物联网感知范式,也是智慧城市中一种全新的信息传播方式和信息服务模式[1]. 大量具备感知能力的移动智能感知终端协同完成某一泛在智慧型深度社会感知任务,在更广阔的范围和更复杂的环境下构建 MCS 网络,为用户提供个性化服务[2]. 随着第五/六代(5th/6th-Generation,5G/6G)移动通信网络的高速发展和物联网应用的普及,智能设备的数量和市场规模呈井喷式增长,为 MCS 系统提供了更加多样化、异构的感知数据采集来源[3]. 相对于需要专门安装传感设备进行数据采集的传统传感器网络,MCS 不仅节省大量人力和物力成本,参与感知任务的感知用户更具有动态性和实时性等契合“大数据”特点的良好属性. MCS 的快速发展将极大地丰富智慧城市的各种应用和服务,推动实现“万物互联、智慧互通”,现已广泛应用于医疗、工业、政务、社区服务、教育以及出行等领域[4-6]. 智慧城市各类应用服务与 MCS 的契合关系如图 1 所示.

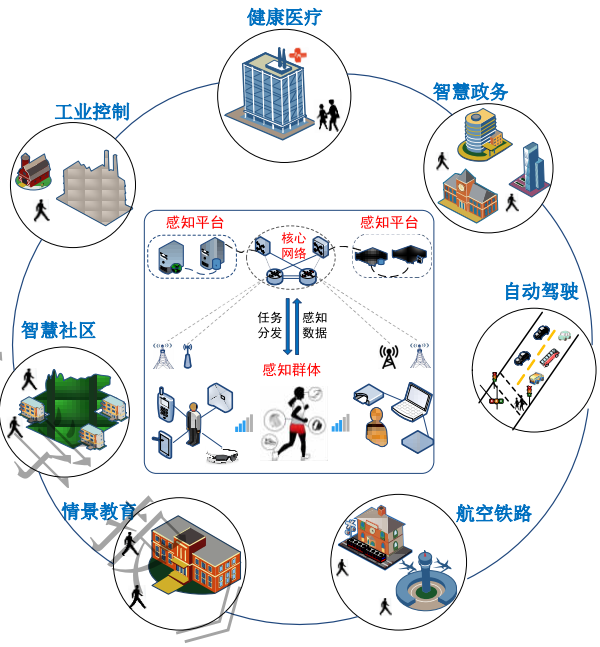

图 1 移动群智感知范式与智慧城市应用服务的契合关系

在 MCS 服务范式中,感知数据在感知阶段、上传阶段和交易阶段面临着不同的安全和隐私挑战[7]. 在数据感知阶段,感知用户需要消耗计算、存储和通信带宽等资源来采集感知数据以获取相应的激励报酬和奖赏[8-10],感知平台则需要部署合理的任务资源分配策略,以合理的代价获得更高质量的数据[11-12];同时,不同的感知用户对于同一感知任务具有不同的认知和参与态度,且感知用户的身份、位置、场景等信息是动态变化的,感知平台如何在尽可能少地泄露用户隐私的前提下实现对感知数据质量的正确评估以及隐私度量和量化隐私泄露风险是当前的一大隐私挑战[13-14]. 在数据上传阶段,感知用户为了契合任务场景,选择上传的数据往往包含位置和属性等隐私信息,随着管理权转移至感知平台,感知数据容易遭受数据窃取攻击、感知平台非授权转发及数据移动性管理困难等严重问题[15]. 在数据交易阶段,理性的感知平台和云服务提供商为了追求

各自最大的利益，容易遭受恶意共谋攻击，使得敏感数据、任务报价等隐私信息发生泄露[7]，从而陷入囚徒困境.

因此，如何应对并克服感知数据全生命周期内感知用户的隐私泄露及隐私度量、数据质量和隐私保护的均衡、上传和交易阶段的恶意攻击等安全和隐私问题是 MCS 系统发展的重大阻碍和技术壁垒，受到国内外学术界和产业界的广泛关注，并取得了较多的研究成果.

Vergara-Laurens 等人[16]从任务处理和报告处理两方面对 MCS 环境中隐私保护机制的基础算法进行分类，并分别讨论了各个算法的普适应用场景；Liu 等人[17]针对 MCS 服务中存在大量冗余数据的问题，从降低资源成本和提高服务质量两方面综述当前的研究进展，并总结目前的挑战与技术难题；Restuccia 等人[18]针对 MCS 数据信息质量问题，从真值发现框架、真值发现算法以及隐私保护真值发现算法三方面归纳总结现有研究成果，并指出对于隐私保护真值发现算法的研究还处于起步阶段. 与已有的 MCS 隐私保护研究综述不同，本文以感知数据参与感知任务的生命周期为轴线，对感知数据分别在感知阶段、上传阶段及交易阶段所面临的安全威胁和对应的解决方案与实现机制进行系统地归纳与评述，并总结出进一步的发展趋势与研究方向，以期为相关科研人员准确把握 MCS 安全与隐私领域最新研究动态和未来发展方向提供借鉴.

本文第 2 节介绍 MCS 系统模型与实际应用；第 3 节描述 MCS 系统中的安全研究方法与威胁模型；第 4 节针对各阶段安全与隐私威胁，系统综述国内外相关研究现状以及解决方案；第 5 节指出 MCS 安全与隐私的发展趋势与未来研究方向；第 6 节总结全文.

2　系统模型与实际应用

2.1　系统模型

MCS 系统模型主要由感知用户、感知平台和服务提供商三部分组成，如图 2 所示[7]. 由感知用户的移动智能终端（如智能手机、平板电脑、可穿戴设备、车载感知设备等）和移动传感设备作为基本感知单元，它们采集到感知数据后，通过移动互联网或 5G/6G 网络协作所构建的 MCS 网络上传给感知平台，实现动态的任务分配和数据采集；感知平台获得任务响应和上传数据后，进一步与云服务提供商完成数据交易和报酬回馈，服务提供商对交易的数据进行处理并将任务结果反馈给请求用户，以完成大规模、复杂多样化的 MCS 服务过程.

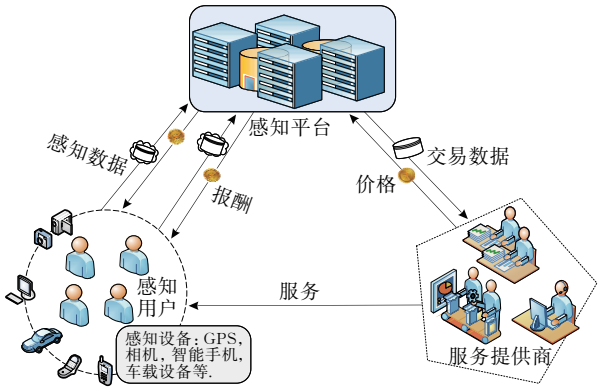

图 2　移动群智感知系统模型

感知用户. 是智能移动终端、可穿戴、车载等感知设备的使用对象，通过移动互联网、5G/6G 网络与感知平台进行交互，在完成身份认证后，实现 MCS 感知任务的分配、协调和参与，并将所采集到的感知数据进行隐私保护处理后上传至感知平台.

感知平台. 作为感知用户与服务提供商的中介，是由一台或多台靠近感知用户端的诚实且好奇的数据微中心. 感知平台可以由雾节点或者边缘计算节点来承载，需要采用合理的激励机制促使更多的感知用户参与任务，并对感知用户上传的感知数据进行分类、聚合以及建模等处理；最后将处理后的感知数据提供给云服务提供商，获得与数据质量相匹配的任务报酬.

服务提供商. 作为感知数据的请求者，通过与感知平台进行交互，完成感知数据的安全交易. 服务提供商可以由云服务器来承载，根据与感知平台交易所得的感知数据集合，挖掘其中的价值信息，然后服务于发起感知服务请求的社会组织或个体，最终为智慧城市管理、环境持续监控、自动驾驶汽车、智能家居、健康医疗、协同计算等提供 MCS 服务.

2.2　实际应用

作为新型智慧物联网感知范式，MCS 服务与应用十分广泛，下面从智慧交通、社会服务和环境监测三个方面简要介绍 MCS 的实际应用.

在智慧交通方面，通过 MCS 实施道路路况检测（道路坑洼、工地噪音）、智能寻找停车位[19]、公共设施保修（如消防栓、交通信号灯、井盖等）和实时交通导航和监测等应用. 例如，ParkNet 使用 GPS 和车门超声波传感器检测空停车位，并共享检测结

果[20];PAS(Prediction-based Actuation System)系统[21]通过 MCS 预测城市中潜在的车辆路线和乘车请求的概率,在有限的预算下实现最优的传感覆盖质量,为智慧城市中的拼车业务提供一个成本低、维护方便、机动性强、运行时间长的驱动系统.

在社会服务方面,主要包含社交网络、社会感知等应用.例如,腾讯提供基于关系距离的好友推荐机制;海量物联网 MCS 设备可以建立物与人之间的通信网络,促使物联网发展为社交物联网[22],用户可以根据主观意愿在网络中设置隐私和安全等级,通过传感器接受并执行特定任务,选择与其他对象进行交互,从而扩展用户社交网络[23];PetaJakarta 项目通过 MCS 范式采集了大量社会媒体数据,进而绘制出洪水地图系统[24],提供预警服务.

在环境监测方面,主要借助移动智能手机及其互联的智能终端进行数据采集.例如,配备智能手机的移动人群采集空气污染(如二氧化碳、氮氧化物)数据,云服务提供商负责收集和汇总这些数据,并绘制空气污染地图[25].基于 MCS 范式研发校园噪声检测与渲染系统,由移动客户端与云服务提供商执行交互,支持任务分配、噪音检测和噪音地图绘制等任务,采用 MySQL 存储和管理用户、任务、噪音数据等[26].

此外,MCS 还广泛应用于网联健康医疗、智能电力、工业 4.0、自动驾驶、智慧农业等诸多领域.

3 安全方法与威胁模型

安全与隐私是 MCS 系统的基本属性,这需要安全研究方法和隐私威胁分析来提供有力的隐私保障.在本节中,首先给出主要的安全研究方法,然后针对 MCS 系统中感知数据参与感知任务的不同生命周期,分感知、上传和交易三个阶段论述其面临的各类安全与隐私威胁.感知数据各阶段的特征与主要安全威胁如表 1 所示.

表 1 移动群智感知数据生命周期各阶段的特征与安全威胁

生命周期阶段	主要特征	数据安全与隐私威胁	主要安全研究方法
数据感知阶段	消耗资源大、用户属性动态变化、感知类型多样、用户主观因素复杂等	虚假数据攻击、女巫攻击、位置攻击、感知任务关联攻击	差分隐私、模糊泛化、同态加密
数据上传阶段	感知任务动态性、场景迁移、数据管理权与所有权分离	中间节点攻击、女巫攻击、位置攻击、背景知识攻击	安全多方计算、同态加密
数据交易阶段	非安全信息静态博弈、恶意交易、囚徒困境、各方追求利益最大化	积分关联攻击、共谋攻击、时间关联攻击	博弈论方法

3.1 主要安全研究方法

(1)安全多方计算.MCS 服务中多方交互的场景不可避免.当无可信第三方时,安全多方计算模型[27]可以在一个良好定义的通用框架中提供隐私保护机器学习,并利用秘密共享技术安全训练线性回归、逻辑回归和神经网络模型.各方仅知晓其输入和输出信息,以保证完全零知识.然而,零知识通常需要复杂的计算协议,实现较困难.在安全性要求不苛刻的情况下,利用安全多方计算建立一个安全模型是可行的.

(2)差分隐私.差分隐私指在待发布数据中添加某种分布的噪声,以保护移动群智感知数据隐私[28].还可以使用泛化方法对某些敏感属性进行模糊处理,如 K-匿名[29]、L-多样性等,直到第三方无法区分个体,从而使数据无法恢复,以保护数据隐私.然而,这些方法的核心是对数据进行加噪和泛化处理,涉及数据可用性、准确性和隐私之间的权衡,且数据传输过程存在较多攻击威胁.

(3)同态加密.MCS 数据在平台进行汇集、统计后,通常借助机器学习、深度学习等大数据分析、聚合技术以获得高精度的统计参数或者高性能的服务模型[30].在明文上直接操作无疑将造成用户信息的直接泄露,同态加密、秘密共享等方案则可以基于困难问题设计相应的密文操作方案,通过加法、乘法等同态性质做到与明文操作结果一致.与差分隐私保护不同,不管是数据还是模型参数,都不会被直接传输,也不会被其他方进行数据推测攻击.因此,泄露原始数据的可能性很小.但是其较高的安全性能在一定程度上加重了部分计算开销以及通信开销[31].

(4)博弈论方法.通过结合经济学理论中的博弈思想[7,32],针对不同的交互应用场景,可以根据信息的知晓程度构建完全/不完全信息博弈模型,亦可按执行顺序分为静态博弈、动态博弈以及重复博弈模型研究多实体间的囚徒困境问题,进而寻求 MCS 中各合作方之间诚实行为的约束条件和影响因素,同时实现各合作方的利益最大化[33].

3.2 威胁模型

本小节围绕 MCS 数据生命周期的三个阶段,详细阐述各阶段可能遇到的威胁和攻击类型,图 3 展示了这些类型的整体结构.

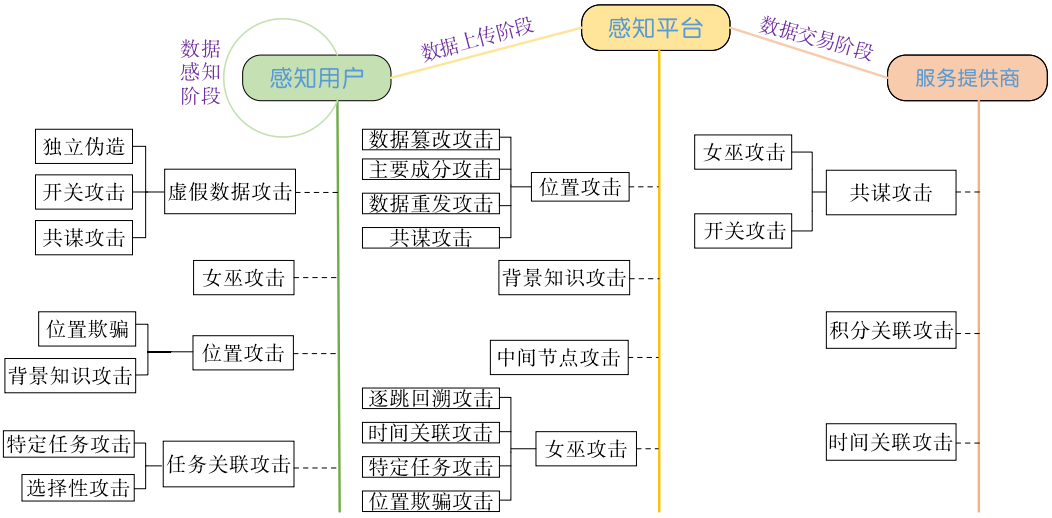

图 3　移动群智感知数据生命全周期各阶段可能的威胁模型

3.2.1　数据感知阶段

在数据感知阶段，感知用户须结合感知任务的场景属性采集相匹配的感知数据，因此感知用户的身份、位置、时间、情境等信息属性是动态变化的，且感知用户对于感知任务具有不同的认知程度和参与态度，面临虚假数据攻击、女巫攻击、位置攻击和任务关联攻击等较为复杂的数据安全威胁与隐私泄露风险.

(1) 虚假数据攻击[34]. ① 独立伪造. 恶意用户篡改感知数据真实值，伪造数据来攻击感知平台；② 开关攻击. 敌手对感兴趣的感知任务会在初始阶段首先表现为诚实用户，再获取较高的信誉积分后提交虚假数据干扰并攻击感知平台；③ 共谋攻击. 恶意用户相互共谋，故意提交虚假数据，造成严重的感知数据攻击；感知用户与不可信服务器之间共谋，通过提供其位置信息和时间信息与不可信服务器提供的其他感知用户的众多通信会话内容等信息，并利用剔除、拟合等手段来获取其他感知用户的敏感信息.

(2) 女巫攻击[35]. 恶意用户发动女巫攻击，通过利用多个女巫标识的 IP 地址参与感知任务，通过提交相似数据来贪婪获取较高的报酬奖励；或者通过生成多份女巫标识的虚假数据攻击感知平台. 若感知用户之间存在交互过程，则敌手就可以利用不同的女巫身份通过相互投票来获取更高的信誉积分，参与更多的感知任务攻击，获取更多的利益，严重威胁感知平台.

(3) 位置攻击. ① 位置欺骗[34]. 敌手可通过监听信道追踪感兴趣的感知任务，利用第三方程序的假位置伪装成可靠来源，提交虚假数据攻击感知平台；② 背景知识攻击[17]. 敌手利用已获取的一些感知用户的活动轨迹、周围环境等背景信息来预测用户在某个时间段可能会出现的位置区域，从而窃取更多的隐私信息.

(4) 任务关联攻击[36]. ① 特定任务攻击. 敌手为了锁定攻击目标，尝试向服务器请求一个只有少数感知用户才会接受的任务，敌手所获得的返回结果中会有很高的概率包含攻击目标的具体敏感信息；② 选择性攻击. 敌手通过选择控制多个相关任务分配而不是请求单个任务，利用多个请求任务之间的相关性，将任务分配给一个或有限几个感知用户，使得该任务在几个感知用户之间彼此相连，从而获取更多的敏感信息.

3.2.2　数据上传阶段

在感知数据上传阶段，由感知平台随机动态地发布感知任务，感知用户为了契合任务场景，选择上传的数据会包含自身的位置和属性等信息，容易导致位置攻击、背景知识攻击，随着数据的管理权转移至感知平台，会引起感知平台容易遭受数据窃取攻击、感知平台非授权转发等严重问题.

(1) 位置攻击[37]. ① 逐跳回溯攻击. 敌手通过反向逐跳追踪信号来源来确定感知用户的位置，即敌手使用三角定位法确定信号来源点位置后，立刻转移到该点并继续对信号进行监听，多次重复上述过程，敌手就可以获取感知用户的具体位置信息；② 时间关联攻击[38]. 敌手通过分析来自同一感知用户在一段时间内一个或多个位置的上传信息，从而获取感知用户的活动轨迹，在最坏的情况下，敌手获取到感知用户的一个提交信息就能推断出感知用户的位置、身份等敏感信息；③ 特定任务攻击[36]. 敌手在感知用户参与感知任务过程中或者上传数据过程中监听窃取用户的位置、身份等敏感信息；④ 位置

欺骗[34]. 敌手可通过信道监听并追踪感兴趣的感知任务,利用第三方程序的虚假位置来伪装成可靠来源,提交虚假数据攻击感知平台.

(2)背景知识攻击[17]. 在感知数据上传阶段,敌手利用已获取的关于感兴趣的感知用户的背景知识来推测并窃取隐私数据;或者敌手通过获取到的背景知识推断在数据上传的某个时间段某感知用户出现在某个匿名区域,即使感知用户以匿名的方式发布消息,敌手仍能通过已获取的时间位置信息匹配出相应的结果,从而窃取感知用户的隐私.

(3)中间节点攻击[37]. ① 数据篡改攻击. 在俘获中间节点数据后,敌手通过对捕获的节点数据进行恶意修改、直接删除,通过向节点数据中注入大量虚假信息等手段,伪装自己的真实身份并上传低质量的感知数据,使感知平台得到不完整的查询或聚合结果,严重扰乱感知平台;② 主要成分攻击. 在俘获节点数据后,尽管感知用户的隐私数据已经经过随机扰乱技术处理,敌手仍能通过求平均或剔除噪音函数等方式对真实数据进行拟合,获取近似真实值,从而窃取感知用户的隐私信息;③ 数据重发攻击. 敌手进行重复转发捕获的节点数据,使网络通信量大大增加,影响网络的正常运转,同时打乱了节点转发的时序,加大感知平台对数据完整性验证的难度;④ 共谋攻击[34]. 敌手通过攻击中间节点并俘获节点后,与本地感知用户共谋,获取本地感知用户提供的关于位置、时间、感知任务要求等具体信息,进而对俘获节点的感知数据进行剔除拟合,从而获取其他感知用户的身份敏感信息和第三方所需的感知信息.

(4)女巫攻击[35]. 在数据上传过程中,恶意感知用户发动女巫攻击是指通过利用多个女巫标识的IP地址参与感知任务,通过提交相似数据来贪婪获取较高的报酬奖励. 若感知用户之间存在交互过程,相遇节点存在互相推荐公钥以及可信度评分问题,敌手都可以利用不同的女巫身份通过相互举荐刷分来获取更高的可信度,参与更多的感知任务攻击,严重影响感知系统性能.

3.2.3 数据交易阶段

在感知数据交易阶段,感知平台与服务提供商之间可能存在共谋攻击等诸多恶意交易行为,从而导致利益损失;同时,交易过程还将发生积分关联攻击、时间关联攻击等导致泄露交易双方的身份、数据、报价等隐私信息.

(1)共谋攻击[34]. 在数据交易阶段,敌手与感知平台或服务提供商共谋,在感知用户与感知平台或者服务提供商的交互过程中,感知平台或服务提供商通过向敌手提供与感知用户的通信会话信息,敌手提供已获取感知用户的背景知识,进一步挖掘感知用户的敏感信息,形成恶意的交互过程.

(2)积分关联攻击[34]. ① 女巫攻击. 恶意敌手使用女巫标识的多重身份通过互相投票来获取较高的信誉积分,从而获取更多的报酬;② 开关攻击. 敌手通过信道窃听、侧信道攻击获取交易的具体信息,通过伪装自己为可靠来源,获得一定的信誉积分后,开始提交虚假数据影响感知平台的数据聚合结果,降低感知数据的质量.

(3)时间关联攻击[37]. 攻击者通过分析交易阶段中同一感知用户在特定时间段内的一次或多次交互信息,获取参与者的敏感信息. 最严重的情况就是一次信息交互就能泄露感知用户的隐私信息.

4 研究进展与分析

本节将针对上述各阶段的威胁模型,结合近年来国内外的最新研究工作,对感知数据生命周期各阶段的安全与隐私保护方法进行分析与评述.

4.1 数据感知阶段

感知阶段的主体是移动智能终端,主要围绕终端采集数据的质量、终端所属用户的身份信息和移动位置等数据的安全与隐私问题展开研究. 本节详细从安全威胁、安全技术方法及其优缺点等方面对相关安全与隐私保护方案进行系统的梳理与分析,如表2所示.

表2 数据感知阶段综合分析

问题分类	文献	安全与隐私威胁	所用方法与策略	方案优势	方案局限性
数据安全	[18]	独立伪造,开关攻击	真值发现算法评估感知数据的QoI,选择高质量数据上传	有效提高用户上传数据的可靠性	不能抵抗共谋攻击,计算效率低下
	[39]	独立伪造,共谋攻击	匿名分组后通过差分隐私加噪保护数据安全	实现数据源匿名的数据有效分类	不能抵抗多假名攻击
位置隐私	[40]	背景知识攻击,位置欺骗	马尔科夫链模拟感知用户行为,构建用户和敌手之间的零和随机博弈	抵抗背景知识敌手自适应的攻击策略	对转发节点处理数据能力要求高
	[41]	背景知识攻击,女巫攻击	采用多假名机制和实体身份验证	抵抗女巫攻击,有效解决用户问责问题	通信时延较大

（续　表）

问题分类	文献	安全与隐私威胁	所用方法与策略	方案优势	方案局限性
身份隐私	[35]	特定任务攻击，选择性攻击，女巫攻击	主观隐私偏好等级划分感知数据安全强度，双层神经网络学习用户行为	动态有效地生成用户特征信息，符合用户隐私意愿	缺乏有效的隐私度量方式，且需要额外的平台训练开销
	[42]	特定任务攻击，选择性攻击	随机匿名绑定用户身份信息，动态更新用户信誉值	有效隔离感知数据与用户真实身份信息	通信轮数多，不适合实时MCS应用场景
	[43]	共谋攻击，开关攻击	构建感知用户联盟，联盟身份聚合数据	实现联盟用户奖励的公平有效分配	缺乏联盟标准和方法
	[44]	特定任务攻击，选择性攻击	构建感知用户联盟，联盟身份聚合数据	提高联盟匿名强度	需要额外的联盟构建预算
	[45]	特定任务攻击，共谋攻击	垄断和寡头的经济理论	多设备协作模块化，避免任务关联攻击	设备间协同实现比较困难

4.1.1　数据安全

在数据感知阶段，防御感知用户通过提交低质量或虚假数据，从而影响感知平台最终的数据聚合质量，现有方案主要从恶意用户、用户共谋等方面考虑数据安全问题. 在MCS中，Restuccia等人[18]提出信息质量(Quality of Information，QoI)定义及其实施框架. 从QoI约束条件的定义出发，经过感知数据收集、QoI评估、QoI执行，到QoI约束条件的定义组成QoI闭环. 系统先进行约束条件定义再收集数据，根据真值发现算法对感知数据进行QoI评估，然后选出有效数据上传到系统，系统在识别约束条件后再对上传的感知数据进行QoI执行，从而保证感知数据满足约束条件下的有效性和可靠性. 相比于传统服务质量(Quality of Service，QoS)侧重于服务器和通信链路的安全问题，QoI闭环更加侧重于考虑感知用户的主观数据安全问题，具有很强的灵活性，但计算开销大、效率较低. 针对传统数据采集的随机响应方案中存在个别用户或多个用户相互共谋提交虚假数据，进而影响感知数据聚合和分类质量的问题，Sei等人[39]提出S2M(Single to Randomized Multiple Dummies)和结合贝叶斯的S2M两种方法，不同于传统方案由感知值生成伪装值，而是生成一组伪装值供匿名上传，聚合器根据上传的加噪数据生成评估类别表(也称为交叉制表或多维直方图)，重构数据类别的真实分布，采用均方误差(Mean Square Error，MSE)和詹森-香农(Jason Shannon，JS)散度度量数据的精确性，从而实现数据质量与隐私保护的平衡.

从上述工作来看，该阶段数据安全问题的可靠隐私手段主要是差分隐私和匿名技术. 然而，通过向数据添加噪音降低数据的敏感度，虽然可以实现较强的隐私保护，但会造成数据失真. 因此，如何实现数据有效性和隐私保护之间的平衡仍然是一个开放问题.

4.1.2　位置隐私

在数据感知阶段，位置隐私主要体现在用户进行感知数据采集时的时空变换以及与平台频繁通信等导致的关联性位置隐私泄露. Liu等人[46]指出通过减少MCS周期中的投标和分配步骤来增强MCS应用程序的位置隐私保护，该方案具有较小的通信开销，且双方可经过博弈选取最佳防御策略. 考虑到恶意敌手可以结合上下文动态调整攻击策略，进而识别智能手机用户的位置相关隐私问题，Wang等人[40]采用马尔可夫模型来捕捉感知数据上下文之间的转换，将用户与敌手之间的交互竞争描述为零和随机博弈，在纳什均衡点获得感知用户的最佳防御策略. 尽管能够有效防御背景知识攻击，但该方案实现复杂且对转发节点的处理能力要求较高. Chen等人[41]提出基于感知用户密度的位置隐私保护方案，利用多假名机制解决低密度感知用户参与场景下的防御薄弱问题；通过引入实体身份验证服务器，避免多假名机制下的女巫攻击，同时也可解决用户问责问题. 但在该方案中，多假名授权中心、身份验证服务器和密钥管理服务器之间的通信时延较大，不适用于实时性要求较高的MCS应用场景.

综上所述，现有研究工作主要采用博弈和匿名技术解决该阶段的位置隐私问题，从上下文动态、用户密度关联信息、假名机制等方面隐藏用户位置特征相关的敏感信息. 但上述方法对于具体用户的认证过程较为复杂，且攻击者仍可发起关联攻击获取用户的隐私信息. 因此，对于数据感知阶段而言，如何对移动状态下采集数据的感知用户轨迹隐私进行识别与度量，设计适应移动智能终端的轻量级位置与轨迹隐私保护框架也是未来的研究热点.

4.1.3　身份隐私

在数据感知阶段，身份隐私主要围绕感知用户由于任务与身份信息关联以及感知数据与身份信息关联导致的隐私信息泄露问题展开论述. 联合匿名机制、移动节点的信任度和声誉管理服务器实现匿名用户的可信管理[42]是一种新颖的方法，感知用户利用随机数匿名绑定任务和身份信息，服务器对感

知数据进行计算评估，并将评估结果签名加密后返回给用户，最后感知用户将反馈结果上传至服务器，服务器进行结果正确性验证和用户信誉值更新. 在整个过程中，服务器不能同时获取用户的身份特征信息和感知数据，从而保护了用户隐私[47]，但该方案仍然具有较长的时延，效率不高. Niu 等人[35]提出了一种感知用户身份安全识别机制，感知用户根据自己的隐私偏好划分感知数据的隐私等级，并通过差分隐私保护隐私等级高的数据，采用双层神经网络来学习用户的行为方式，生成用户身份特征数据库，从而有效实现用户身份的安全识别，该方案可以抵御恶意用户通过多个女巫标识 ID 参与任务，但缺乏有效的隐私度量方法，且神经网络训练增加了平台的计算开销. 为了克服用户共谋问题，一种用户联盟策略的思想[43-44]被提出，允许用户在同一广义身份下合作提供他们的数据，提高了 K-匿名用户隐私保护强度，但缺乏有效建立联盟的标准和方法. Dimitriou 等人[45]使用任务服务器、拍卖服务器与数据处理服务器协作完成感知任务，通过匿名机制和任务不可连接性使中标人能够在数据与身份无关联的情况下获得合理奖励，从而有效防御敌手通过任务关联攻击感知用户，该方案能够保证感知用户在拍卖过程的所有阶段(从投标到奖励)获得隐私保障，适用于典型的 MCS 应用.

从上述方案可以看出，相关工作主要通过匿名、信誉机制、身份安全验证以及多服务器协作等手段进行身份隐私保护，尽管一定程度上实现了感知数据与用户身份属性信息的分离，但大多数方案实现难度大、效率较低. 值得关注的是，将隐私保护融合神经网络[35]的思想比较新颖，紧密结合人工智能技术，如何有效利用机器学习[27]、深度学习、强化学习、联邦学习和元学习等模型与算法设计感知数据隐私度量与隐私保护方法值得深入探究.

4.2 数据上传阶段

在感知用户将感知数据从移动智能终端上传到感知平台的过程中，由于通信网络的不安全性和中间节点的脆弱性，从而极易造成感知数据和用户隐私的泄露. 数据上传阶段的工作总结如表 3 所示.

表 3 数据上传阶段综合分析

问题分类	文献	安全威胁	所用方法与策略	方案优势	方案局限性
数据安全	[36]	主要成分攻击，逐跳回溯攻击	用户分割并转发数据给相邻节点，阈值触发数据上传行为	有效防止数据被篡改或伪造	转发节点可靠性缺乏评估机制，通信和计算开销较大
	[48]	主要成分攻击，女巫攻击，数据篡改攻击，共谋攻击	用户采用秘密共享方式分割数据并转发给可信节点	有效评估节点的可靠性，有效隔离数据源与数据的关联	数据分割数量依赖可靠节点数量，且时延较大
	[49]	主要成分攻击，数据重发攻击，数据篡改攻击	评估授权节点的可靠性，分类加密转发数据	选择有效的传输路径实现不同等级的数据安全保护	推荐公钥和相遇节点的可靠性评估增加系统实现难度
位置隐私	[50]	时间关联攻击，特定任务攻击	采用局部敏感哈希算法将用户位置信息散列映射至匿名空间	有效实现用户位置信息的散列和匿名保护	缺乏用户可靠性认证，不能抵抗女巫攻击
	[51]	背景知识攻击，位置欺骗	采用空间网格匿位分割和加噪扰乱数据	调节网格加噪程度实现用户主观隐私保护等级	缺乏隐私度量，额外的网格生成预算
	[52]	时间关联攻击	用户乱序组合行动轨迹的若干位置信息并上传	隐私保护强度符合用户主观意愿，有效隔离位置信息与时间的关联	缺乏用户可靠性认证，不适用于位置关联性任务
	[53]	主要成分攻击，时间关联攻击	采用非对称加密数据，动态在线节点完成数据转发和上传	有效消除数据源与任务的时间关联，节点动态性强	对转发节点处理能力要求高，缺乏可靠性评估机制
身份隐私	[54]	女巫攻击，时间关联攻击	平台对用户进行身份认证和数据验证	有效保护用户身份和数据隐私	不能抵抗背景知识攻击
	[55]	数据篡改攻击，主要成分攻击	采用双线性映射对身份信息批量签名，匿名验证用户感知数据	轻量级保护用户身份和感知数据隐私	不支持公开信道下的数据传输

4.2.1 数据安全

上传阶段的数据安全问题主要包含感知数据被截取和篡改、转发节点不可信以及上传环境动态变换等. 现有解决方案主要基于数据分割、中间节点可信评估以及数据完整性验证三个方面设计安全防御策略，从而最大限度确保数据的机密性与完整性. Hu 等人[36]提出基于数据分割保护感知数据安全的方案，用户将数据分割并转发给 k 个相邻节点，并设置转发跳数阈值，达到阈值时触发各转发节点将分片信息直接传送给感知平台的行为，有效防止服务器将具体的感知用户和感知数据相关联，该方案可以有效抵御数据伪造和篡改攻击，但具有较大的计算开销和通信开销. 进一步地，Wu 等人[48]在文献[36]的基础上，从数据质量和社会贡献两个维度对

转发节点进行可信评估，用户将数据分割并采用秘密共享方式发送给评估可靠的节点，各节点上传数据后，感知平台再验证数据的完整性，从而隐藏了原始数据和源标识的关联，并且可以有效防御各节点篡改数据或相互共谋获取较多数据片；然而，该协议分割数据片的数量与可信节点的个数有关，当可信节点数过少时极易泄露用户的敏感信息，且具有较长的时延. 类似地，Tang 等人[56]提出基于数据分割、秘密共享和两阶段转发相结合的延迟感知隐私保护(Delayed Perception Privacy Protection，DAPP)传输方案，用户采用多假名 ID 机制将分割后的感知数据上传给感知平台，且为了防止敌手通过属性信息来链接多个假名或将假名与真实身份关联，该方案利用 ID 哈希链生成动态假名，且允许源节点在哈希链中使用同一个密钥.

此外，Sun 等人[57]提出基于两层雾异构的数据安全传输方案，两层雾分别为动态下层和静态上层，用户将数据同态加密后上传到下层雾节点，该节点负责身份认证和数据验证，聚合数据后上传给上层雾节点，上层雾节点再对原始数据进行冗余筛查和分析计算；该方案将验证过程和计算过程隔离处理，从而确保用户数据的安全. Gisdakis 等人[58]通过传输层安全协议(Transport Layer Security，TLS)、敏感信息检索技术(Sensitive Information Retrieval，SIR)和安全断言标记语言(Security Assertion Markup Language，SAML)实现感知数据的安全上传和实体之间的安全通信. Wu 等人[49]针对节点颁发密钥的可靠性问题提出面向感知数据隐私保护的动态信任关系(Dynamic Trust Relationships Aware Data Privacy Protection，DTRPP)方案，在 DTRPP 中，节点需要对推荐公钥节点的可靠性进行动态评估，结合时延大小以及其他节点对该节点的评价判断相遇节点的行为特征，获取节点的累计信任值，保证节点授权公钥的真实可靠性，从而最大限度地减少数据内容的泄露. 根据不同的保密要求对数据进行分类，根据数据分类、中继节点的信任程度和中心度，选择合适的转发中继方案，实现数据转发的灵活性和有效性，但对相遇节点可信度的评估实现具有较大难度，可以考虑通过共识机制来实现节点信任的及时更新.

综上所述，现有方案主要通过数据分割和加密技术来实现感知数据的安全上传与完整性验证. 首先，上述方案基本依赖于可信计算技术，但可信计算技术不仅缺乏有效的度量方法，而且还存在动态适应性较差、物理成本较高、缺乏安全协议支持等问题；其次，随着感知数据的激增，密钥的管理与分发开销也是一大难题；最后，在感知数据的上传过程中，经常出现拥堵、节点丢失等影响数据正常上传的现象. 因此，如何设计高效的感知数据隐私上传机制也是值得深入研究的课题.

4.2.2　位置隐私

该阶段的位置隐私问题主要由于感知用户具有较强的移动性，感知数据在上传过程中极易泄露用户位置等相关的敏感信息. Khuong 等人[50]提出利用局部敏感哈希算法(Locality Sensitive Hashing，LSH)，将用户位置数据散列到至少包含 k 个用户的高维区间，并将位置接近的用户映射在同一个覆盖空间中，从而确保在感知平台不可信的情况下，保护感知用户上传数据时的位置隐私；但该方案缺乏对感知用户的有效认证，不能抵御女巫攻击. 针对通过网络信道截获感知数据上传时的位置信息或利用背景知识推测用户位置信息的攻击，Agir 等人[51]提出用户自适应的位置隐私保护方案，系统通过为用户设置个性化隐私阈值，生成匹配隐私等级的网格单元数量，用户挑选出与其对等的数据量进行加噪处理并上传给感知平台；尽管该方案可以抵御背景知识攻击，但缺乏有效的隐私度量方法，且网格单元的动态生成增加了系统实现难度. Chen 等人[52]针对不可信感知平台和监听者对感知用户位置信息的攻击，提出允许感知用户参与构建位置信息的方案，感知用户在报告自己的位置信息之前核查隐私保护强度是否符合意愿，进而选择是否报告位置信息，并从其位置轨迹中自主选择若干个位置，乱序组合后上传给感知平台，从而消除上传地点和上传时间的关联性；尽管该方案具有较强的灵活性，但缺乏对用户的认证，且不适用于位置关联的任务. 此外，Lin 等人[59]基于 BBS+(Blaze，Bleumer，and Strauss)签名[60]和代理重加密[61]提出雾辅助的隐私保护 MCS 框架，用户在上传数据时将位置信息映射至两个独立矩阵中，可信第三方对上传报告的用户身份进行验证，从而有效抵御女巫攻击. 在 MCS 中，利用节点移动性来保护移动节点位置隐私的方法能够让用户使用非对称加密方法加密数据并分配给多个动态的在线中间节点进行转发，确保恶意节点无法通过跟踪路径来确定源节点，同时确保敌手无法通过时间关联和任务关联攻击源节点[53]；但该方案仅涉及对中间节点是否在线的询问，缺乏对移动节点的信任评估与管理[62].

综上所述，位置隐私保护相关工作主要结合差分隐私、签名认证、公钥加密、可信节点评估等方法进行分析，提出相应的安全防御和管理策略，从而

确保感知平台的正常运行,并且提高感知系统的整体性能.然而,现有方案仍然缺乏有效的位置隐私动态度量机制、随任务变化或场景适应的低开销隐私预算评估方法以及有效抵抗共谋攻击和不可信节点腐蚀的方法,这些仍然是亟需关注和突破的挑战问题.

4.2.3 身份隐私

在数据上传阶段,感知用户的身份信息与感知数据的关联性也极易造成用户隐私信息泄露,目前的研究工作主要实现对用户身份的有效认证,解决用户问责问题.在智慧医疗方面,由于医疗数据的特殊性,既要严格保护患者的隐私信息,又要保证数据真实可靠,保障科学研究统计的正确性.针对这一问题,Li 等人[63]提出基于密钥协议的生物认证方案,通过哈希函数、模糊提取器、一次性验证的 Diffie-Hellman 密钥协议实现患者隐私信息的机密性和完整性.Chen 等人[54]结合匿名性、不可链接性和消息认证提出隐私保护方案,用户使用假名上传加密后的医疗信息,平台对用户进行身份认证和数据验证,从而有效保护用户隐私信息.针对医疗数据,Liu 等人[55]提出基于改进 CL-AS(Certificateless Aggregate Signature)签名算法的方案,感知用户将身份信息通过安全信道上传给可信第三方进行注册,随后采用双线性映射对数据进行签名,感知平台将用户的签名信息进行聚合,从而实现对用户的匿名批量验证;该方案采用匿名方法批量验证所有用户的隐私数据,从而保证了感知数据的安全可靠性和感知用户身份信息的机密性,并基于 CDHP(Computational Diffie-Hellman Problem)困难问题,在随机谕言模型中证明了所提方案的安全性.随后,Zhang 等人[64]指出方案[55]存在两种类型的签名伪造攻击,合理而严谨的概率分析表明将该方案的安全性规约到 CDHP 是无效的,该匿名批量验证方案存在瑕疵,为未来设计安全方法提供了借鉴.

综上所述,现有研究工作主要利用映射、签名、多假名机制、数据加密和扰动的方法来保护用户身份隐私.整体而言,现有工作对于用户身份隐私的内涵和涉及的因素还不够全面,对于感知用户的身份隐私信息还缺乏轻量级且高效的隐私度量与隐私保护方法.

4.3 数据交易阶段

针对数据交易阶段存在的数据安全与隐私威胁,主要分感知用户与感知平台、感知平台与服务提供商两个方面考虑,其研究现状总结如表 4 所示.

表 4 数据交易阶段综合分析

交互双方	文献	安全威胁	所用方法与策略	方案优势	方案局限性
感知用户与感知平台	[34]	共谋攻击,女巫攻击,开关攻击	将感知数据聚类成若干分组,过滤评估质量低的数据组	有效提高数据聚合的准确度	缺乏普适有效的数据可靠性等级评估机制
	[65] [66]	独立伪造	本地差分隐私添加噪声,加权聚合噪声数据	有效提高数据聚合结果的准确性	数据加噪权重依赖于历史记录,不具有迁移特性
	[67]	女巫攻击,共谋攻击	两台不共谋的云服务器接收数据和执行真值发现过程	不需要用户在线参与,实现密文下的数据交易	真值发现过程需要多轮迭代计算,效率低
	[68]	共谋攻击 背景知识攻击	时间戳分组聚合用户加噪数据,过滤低质量分组数据	具有用户自适应隐私预算,降低云服务器存储开销	多组件协同过程实现复杂
	[69]	共谋攻击	采用分布式多级节点代理发布数据	具有用户自适应性,避免不可信平台泄露隐私	需要额外的多级节点选择预算
	[70]	时间关联攻击,共谋攻击	用户上传模糊距离代替真实位置,根据最小化模糊距离筛选用户	有效保护了用户的真实位置信息,自适应用户位置隐私保护强度	缺乏有效的隐私度量方法
	[71]	女巫攻击,位置欺骗	根据用户加密位置信息和信誉值筛选用户	有效保护用户特征信息,且避免用户问责	引入可信第三方需要额外的系统开销
	[72]	共谋攻击,时间关联攻击,女巫攻击	引入半可信第三方随机分组用户,采用组合策略寻找特定任务的最低竞价用户	有效抵抗用户共谋扰乱竞价问题,用户选择具有可伸缩性	缺乏保护用户真实身份隐私机制
感知平台与服务提供商	[73]	共谋攻击	构建不完全信息重复博弈	有效抵抗感知平台与服务提供商的恶意共谋	重复博弈的计算和通信开销较大
	[74]	开关攻击 共谋攻击	构建 Stackelberg 博弈,采用深度卷积神经网络加速学习用户行为和感知数据	兼容不同分布密度的感知用户,用户自适应选择感知设备和感知任务	主观因素较多,博弈均衡不稳定
	[75]	共谋攻击	非共谋的协同服务器共同接收并存储用户数据	兼容不同隐私偏好的感知用户参与感知任务	仅能抵抗部分服务器共谋,访问控制策略增加资源开销

4.3.1　感知用户与感知平台

现有的研究方案主要从以感知用户为中心的隐私激励和以感知平台为中心的数据聚合、任务分配算法等方面设计相应的安全防护技术和策略，从而最大限度确保数据的可靠性和安全性.

(1) 隐私激励. 感知用户与感知平台之间考虑设计合适的激励机制，可以使更多高质量的感知用户积极主动参与任务，并提供高质量的数据，减少平台资源消耗的同时保证用户数据的隐私安全. 针对这一问题，目前相关激励机制的研究工作主要包含减少平台资源支出的激励机制[43,76-77]和最大化用户收益的激励机制[9,66,78-80]. 针对用户共谋以获取较高酬劳的问题，Alsheikh 等人[43]提出根据感知用户个人贡献支付相应报酬的激励机制，感知用户通过添加随机噪声自主选择对数据的匿名程度，随后由多个感知用户通过 D2D(Device to Device)通信形成联盟上传数据，相比于等额报酬支付，感知平台根据感知数据准确性和任务完成质量情况来定义用户个人贡献并支付相应的报酬，同时对提交虚假数据的感知用户进行惩罚. He 等人[78]结合经济学理论与博弈方法，提出了可以在多项式时间内计算出瓦拉均衡点(Walrasian Equilibrium，WE)、最大化感知用户与服务提供商收益的激励方案. 文献[76-77]等通过贪婪算法、蜂群算法等优化感知平台的资源支出，合理分配任务，激励更多的感知用户参与任务. 针对感知用户由于隐私泄露致其保守参与任务的问题，带有隐私泄露补偿的单向组合拍卖机制能够在感知平台可信的情况下，允许用户提交归一化的数据隐私泄露值，感知平台根据用户的隐私泄露程度和数据精度返回最终的报酬奖励和差分隐私预算值[65]. 进一步地，Jin 等人[66]在单向组合拍卖机制中考虑了投标信息的安全性，提出使用差分隐私保护用户的投标信息，从而确保竞标的公平性和安全性. 文献[80-81]等利用 VCG(Vickery Clarke Groves)拍卖和反向拍卖机制及其改进算法来激励高质量的感知用户参与感知任务[82].

(2) 数据聚合[83]. 针对感知数据聚合过程中感知数据的安全问题，Xiong 等人[28]提出隐私保护数据聚合方案，用户采用差分隐私机制向数据添加噪声，并采用同态加密技术加密后上传密文，即使在部分传感数据泄露的情况下，差分隐私机制仍能保证感知用户隐私安全. Zhou 等人[34]提出集成感知数据的空间相关性、感知数据与数据源相关性的新框架，通过聚类合并算法(初始聚类和合并集群)将虚假数据和正常数据聚类到不同的组中，并通过感知用户的声誉信息和上下文对每个集群进行可信度评估，抛弃评级较低的组以确保整体数据的安全可靠，该框架可以有效抵御恶意用户攻击和共谋攻击，但缺乏有效的数据可信度等级划分机制. Chen 等人[41]提出兼容高密度和低密度感知用户参与场景的方案，该方案利用多假名机制克服参与者密度低的脆弱性，并为每个假名设置一个计数器来限制用户样本的总上传量；用户利用 Paillier 同态加密感知数据后上传给感知平台，感知平台再对用户 ID 进行身份认证，从而避免女巫攻击，同时也解决了用户的问责问题. 在具有不同感知能力水平的用户参与的群智感知场景中，Zheng 等人[67]提出密态真值发现(Cryptography based Truth Discovery，CATD)架构，CATD 采用两台非共谋的云服务器进行协作，一台云服务器充当连接感知用户和感知平台的媒介，另一台云服务器则协助完成 TD 算法的迭代过程，整个真值发现过程不需要用户在线参与，从而确保用户的感知值和权重安全；此外，服务提供商生成近似真值密文，虽然可以抵御敌手与平台的共谋，但是方案实现比较复杂且 TD 需要多轮迭代计算开销. 相比之下，Jin 等人[65]提出提升数据精度的加权聚合方法，数据的加权值正比于用户历史任务的完成质量，同时对加权后的聚合数据添加噪声后发送给服务提供商以确保数据安全[66]. Huo 等人[68]提出基于可信雾节点的实时流数据聚合框架，该框架由自适应 w-event 隐私分析算法、智能分组机制和过滤机制三个组件组成，第一个组件负责综合考虑窗口大小和数据质量来自适应地调整隐私预算；第二个组件基于 K-means 算法改进长短期记忆算法(Long Short Term Memory，LSTM)，实现不同时间戳的智能聚类分组以提高隐私保护的能力；第三个组件负责过滤低质量数据以提高数据的可用性；最后，雾服务器只向云服务器发送聚合后的过滤数据以减轻云服务器的计算存储负担. 为了防止聚合后的感知数据泄露用户的隐私信息，Wang 等人[69]研究在不可信感知平台下实时众包统计数据的安全发布问题，提出基于分布式代理的隐私保护框架，感知用户和不可信平台之间引入多级代理，用户可以随机选择一个代理并使用匿名技术传输数据，而不是直接将数据上传到感知平台，从而保护用户的身份与位置等隐私信息.

(3) 任务分配[84]. 针对 MCS 任务分配过程中的隐私泄露问题，Wang 等人[70]首次提出个性化的隐

私保护任务分配框架，在提供个性化位置隐私保护的同时能够有效分配任务，感知用户按照个人隐私级别选择模糊距离代替实际距离上传给感知平台，提出概率赢家选择机制(Probabilistic Winner Selection Mechanism，PWSM)最小化用户模糊距离信息的总行程，还提出 Vickrey 支付决策机制(Vickrey Payment Determination Mechanism，VPDM)，根据每个参与者的移动成本和隐私水平筛选合适的用户，但缺乏有效的隐私度量方法. Ni 等人[71]提出基于信任管理的隐私保护方案，基于感知用户地理位置和信誉值设计一种位置匹配机制帮助感知平台精确分配感知任务，同时保护用户的真实位置信息；通过扩展代理重加密和 BSS＋签名，实现感知用户的特征信息保护，同时解决用户的问责问题，但是也显著增加了系统的计算开销. Xiong 等人[9]提出基于边缘计算且以感知任务为导向的用户选择激励机制(Sensing Task-oriented User Selection Incentive Mechanism，TRIM)，试图在 MCS 中构建一种以任务为中心的设计框架，有效地解决了感知任务需求最大化和多样化问题. 由于感知任务和移动用户在空间和时间域上具有动态关联性，一种基于可扩展分组的隐私保护方案利用拉格朗日插值来扰乱组内参与者的竞价，引入一个或者多个半可信第三方(聚合器)对参与者进行分组，从而保护参与者的隐私信息，并利用组合策略查找分组中每个感知任务的最低竞价用户，从而抵御用户间的共谋，该方案可以实现可伸缩的选择，并能确保感知用户投标的安全性和公平性[72].

综上所述，在用户和感知平台之间进行的数据聚合和任务分配过程中，都存在用户隐私信息泄露问题. 现有方案主要利用加密、差分隐私技术保护用户隐私，并且引入第三方协调数据交易过程，但聚合算法主要从特征信息和数据精度两方面进行评估，缺乏综合有效的隐私度量方法，加解密计算开销较大，差分隐私会造成数据的失真等，如何根据不同的应用场景设计轻量级有效的隐私保护方案仍然是当前的研究重点. 此外，随着移动边缘计算的快速发展与广泛应用，可信或者半可信的边缘节点拥有较强的计算与存储能力，MCS 系统可充分利用边缘节点的灵活性、移动性、边缘性等特征. 因此，MCS 在新型边缘计算应用的安全与隐私保护问题也是未来值得研究的课题.

4.3.2 感知平台与服务提供商

针对这两者之间存在的隐私泄露问题，现有的研究方案主要从博弈方法、分类集群、引入半可信实体等方面设计相应的隐私保护方案.

感知平台和服务提供商均为半可信的理性实体，由于双方为寻求利益最大化而极易陷入恶性交易，容易导致囚徒困境问题. 为此，Ma 等人[73]从博弈方法的角度出发，建立服务提供商与感知平台交易的博弈模型，针对“囚徒困境”问题提出不完全信息重复博弈方法，计算囚徒困境下服务提供商与感知平台的帕累托最优均衡点，从而避免服务提供商与感知平台的恶意共谋；然而，该方案的重复博弈大幅增加了系统的计算开销和通信开销，效率较低. Xiao 等人[74]提出基于深度 Q-网络(Deep Q-network，DQN)的安全 MCS 方案，将服务提供商与感知用户之间的交互表述为 Stackelberg 博弈，服务提供商作为领导者决定并广播每个感知任务的支付策略；每个用户作为跟随者，根据支付策略选择相应感知能力的智能设备；基于 DQN 的 MCS 系统采用深度卷积神经网络，凭借高维状态空间和动作集加速学习过程，从而更有效地防御用户的自私行为和共谋攻击；同时，该方案不需要在动态 MCS 博弈下知道感知用户的分布密度，以减少对低密度感知用户的隐私损害. 与基于 Q-learning[74]的策略相比，基于神经网络的学习训练能更好的预测感知用户的行为和感知数据的聚合值. 文献[81]和[73]均从博弈方法的角度出发，将通信交互的两个实体建模为博弈双方，通过一次博弈或重复博弈计算双方的最优策略，从而确保系统在很长一段时间内维持良好的性能，直到出现新的影响因素打破这种平衡. 针对智能物联网医疗应用程序中的患者数据安全，Luo 等人[75]提出隐私保护的实用框架，将基于秘密共享的 Slepian-Wolf 编码应用于该框架，采用多台云服务器协作构建分布式数据库以抵御感知平台与某些服务器的恶意共谋，并支持精确的秘密共享修复，从而确保数据的完整可靠；此外还提出一种访问控制策略，确保只有符合特定特征的服务提供商才能访问患者数据，但是多云服务器协同也意味着较大的物理成本.

从上述工作看，感知平台与服务提供商均为半可信的理性实体，其不诚实行为均为追求自身利益最大化. 要确保服务提供商与感知平台间的公平有效交易，需要最大限度的使双方利益最大化，防止陷入恶意循环交易. 针对这一问题，目前已有的研究中，博弈模型的思想是比较有效的，但仍存在较大的局限性和单一性，可以结合强化学习、深度学习等对

博弈策略的过程进行动态建模和更新学习，增加方案的鲁棒性.

5　发展趋势

目前，MCS 是一种契合物联网“万物互联、智慧互通”背景的新型移动感知服务范式，结合 5G/6G 技术成为建设智慧城市的重要组成部分. 在以人为核心的智慧城市中，用户的服务体验效果将以极大的导向力驱动市场变化，非常符合 MCS 用户作为该系统的载体角色[85]. 同时，MCS 应用采集的感知数据携带大量与感知用户相关的敏感信息，使得感知用户需要承担个人隐私泄露的巨大风险. 同时，MCS 也作为一种全新的智能感知计算模式，具有和以往传统网络不一样的新型特性，传统网络背景下的隐私保护研究成果难以直接应用于 MCS 中.

一方面，围绕 MCS 范式中感知数据生命周期的三个阶段，数据感知阶段作为数据采集的源头，由于用户对个人隐私的愈加重视，其关注的主要矛盾逐渐转移至自身隐私信息的保护需求与任务报酬之间的权衡. 对于数据上传阶段，海量感知数据、感知用户资源受限、网络类型异构等将导致服务响应延时、计算效率低下、恶意敌手攻击等系统开销和数据安全问题. 对于数据交易阶段，交互实体方的目的均为追求自身利益的最大化，如何寻找良好的约束机制或隐私保护框架，为感知用户的隐私数据提供延伸式的保护更是下一步的研究重点. 另一方面，针对感知数据本身逐渐呈多源化且具有异构特性的趋势，因行业竞争、数据规范安全等因素无法直接交换和共享数据，导致数据挖掘技术缺乏类型丰富的数据集对象，无法深层次挖掘数据价值，阻碍了 MCS 服务的进一步发展. 由此，下面从五个方面阐述 MCS 未来的研究趋势.

(1) 个性化的隐私动态度量与保护

在 MCS 范式中，针对不同感知用户对隐私需求不同，集中式的隐私保护框架存在着隐私保护效率以及数据效用低下的问题，重点考虑场景动态迁移下异构源数据的隐私程度，并结合当前时空状态下感知用户所具有的身份属性、敏感属性等，能够个性化地度量用户隐私需求[86]. 为了实现个性化的隐私保护，首先基于场景动态变化背景的隐私属性对用户进行分类、量化，可以根据对隐私需求的定量分析，制定出对应不同用户主观隐私等级的划分方案，提高隐私保护的资源利用效率；进一步探究隐私保护效率和数据可用性之间的平衡，基于感知数据的隐私程度差异设计保护机制，通过利用匿名、加密、扰动等技术为相应等级的隐私保护对象匹配最佳的隐私保护策略，最终实现用户隐私需求的动态度量，并提供相应的个性化隐私保护方案.

(2) 自适应的隐私保护框架

MCS 范式利用边缘计算体系结构[87]是“万物互联、智慧互通”大数据背景下的必然趋势，在一定程度上缩短了感知用户与云端服务器的距离. 通过大量的协同分布式边缘节点，数据的上传和交互量将随着移动设备的激增而呈现指数级增长，进一步地，数据在进行隐私保护处理与传输的效率与设备资源受限之间的矛盾更加突出. 为此，需要重点关注感知过程中的感知环境、时空、行为特征等因素以及感知数据的隐私风险程度，考虑用户自适应的隐私数据上传策略以及轻量级的高效隐私保护框架，帮助用户做出理性的策略选择，提高实时数据采集效率的同时更合理地消耗设备资源，大大提高智能物联网设备用户的隐私效用.

(3) 基于区块链的 MCS 密钥管理

MCS 感知数据的采集载体主要是各类移动物联网智能设备，通过无线传感网络或 5G/6G 进行数据传输. 然而，在感知数据隐私保护过程中，数据加密、身份认证以及访问控制等均涉及到密钥的分发与管理. 由于网络环境的动态性、异构性，密钥的安全性常常会因不可信的基站等存在巨大风险. 现有工作大多是面向基站角色的分布式密钥管理方案，会给传感器造成额外、沉重的管理开销；此外，还面临感知数据不断激增的现状，轻量级、适应动态特性且可靠性高的 MCS 密钥管理系统亦是一个重要研究方向. 区块链技术[88-89]作为目前验证信息有效性的强有力工具，其去中心化的本质特征可以很好地解决对第三方管理机构的依赖性，同时区块内信息高度透明且不易篡改数据的优点提供密钥安全性和独立性的保障. 因此，结合区块链技术解决上述问题势必成为未来该方向发展的一个重要突破口[90].

(4) 场景适应的多元化延伸式隐私保护

MCS 服务环境在场景动态变换的情况下会受到各种外界因素的影响，如拥有不同攻击能力的敌手、边缘节点以及云服务提供商的潜在不诚实行为、任务场景的动态迁移等，需要重点关注感知数据在上传以及后续交易过程的多阶段隐私泄露风险问题，信息论、概率论以及博弈论等基础理论的结合是理想的研究方向. 例如基于博弈论，引入理性攻击

者,可以对各参与方实体获得最大化收益的行为策略选择进行博弈分析,寻找场景适应的最大约束条件和博弈均衡点,在约束条件下可以保证各参与方做出诚实行为,构建良性的 MCS 服务网络,为场景适应的多元化延伸式隐私保护提供保障.

(5)"孤岛式"感知数据的融合隐私计算

针对不同企业、智能终端之间试图直接交换各自用户数据以获得更大数据集进行深度学习模型训练的过程中存在的隐私数据泄露问题,相关研究开展可以借鉴联邦学习[91-92]、联邦迁移学习[93]、元学习[94]、强化学习[95]、隐私计算[96]思路等,再融合深度学习理论,对横向联邦学习、纵向联邦学习以及联邦迁移学习等相关应用场景进行实例化的剖析.具体地,结合同态加密、差分隐私以及秘密共享技术等,探索深度学习模型隐私训练过程中的逆向参数传递、数据干扰、梯度更新的合理方案[31];另外,多源异构数据的隐私计算也是一大重点,涉及到数据秘密共享、数据特征对齐和云端数据安全聚合等方面;最后,可以考虑对低维空间特征迁移的实例化应用研究,探寻行之有效的用户个性化隐私保护模型的自适应调整策略,帮助 MCS 用户进一步提升服务体验且提供用户迫切需要的隐私保障.

6 结束语

快速发展的物联网及智慧物联网已经上升到国家战略,MCS 作为一种全新的智慧物联网感知范式,得到迅速发展,引起学术界和工业界的广泛关注,为泛在深度社会感知提供全新的信息服务模式.在参与感知任务过程中,感知数据往往包含感知用户的个人身份、位置、访问模式等诸多隐私信息,如何对这些信息进行隐私度量、安全威胁分析和隐私保护等相关研究还处于起步阶段,尚未建立一套完整的理论体系,从理论体系的建立到关键技术的实际应用还有很长的距离.

本文首先描述了 MCS 的基本概念和系统模型,接着介绍了主要的安全研究方法并以感知数据参与感知任务的全生命周期为轴线,从数据感知、上传、交易三个阶段给出隐私威胁模型;然后根据感知数据生命周期的三个阶段,囊括了数据安全、位置隐私与身份隐私三个方面,对国内外最新研究工作的基本思想、工作原理等进行系统分析、归纳与总结,并分别指出了各种技术方法的优缺点和存在的问题;最后,从个性化的隐私动态度量与保护、自适应的隐私保护框架、基于区块链的 MCS 密钥管理、场景适应的多元化延伸式隐私保护、"孤岛式"感知数据的融合隐私计算等方面指出 MCS 安全与隐私的发展趋势和未来研究方向.

参 考 文 献

[1] Ganti R, Ye F, Lei H. Mobile crowdsensing: Current state and future challenges. IEEE Communications Magazine, 2011, 49(11): 32-39

[2] Yang S, Han K, Zheng Z, et al. Towards personalized task matching in mobile crowdsensing via fine-grained user profiling //Proceedings of the IEEE Conference on Computer Communications. Honolulu, USA, 2018: 2411-2419

[3] Zhang C, Zhu L, Xu C, et al. Reliable and privacy-preserving truth discovery for mobile crowdsensing systems. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1245-1260

[4] He M, Ni J, Liu D. Private, fair, and verifiable aggregate statistics for mobile crowdsensing in blockchain era// Proceedings of the IEEE/CIC International Conference on Communications in China. Chongqing, China, 2020: 160-165

[5] Zhang J, Yang F, Ma Z, et al. A decentralized location privacy-preserving spatial crowdsourcing for Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(4): 2299-2313

[6] Tang J, Fu S, Liu X, et al. Achieving privacy-preserving and lightweight truth discovery in mobile crowdsensing. IEEE Transactions on Knowledge and Data Engineering (Early Access), 2021, 1. DOI: 10.1109/TKDE.2021.3054409

[7] Xiong J, Ma R, Chen L, et al. A personalized privacy protection framework for mobile crowdsensing in IIoT. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4231-4241

[8] Xu C, Si Y, Zhu L, et al. Pay as how you behave: A truthful incentive mechanism for mobile crowdsensing. IEEE Internet of Things Journal, 2019, 6(6): 10053-10063

[9] Xiong J, Chen X, Yang Q, et al. A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing. IEEE Transactions on Network Science and Engineering, 2020, 7(4): 2347-2360

[10] Liang Yan, An Jian, Hu Xian-Zhi, et al. Research on incentive mechanism with privacy-preserving in mobile crowd sensing. Chinese Journal of Computers, 2020, 43(12): 2414-2432(in Chinese)
(梁艳, 安健, 胡先智等. 群智感知中支持隐私保护的激励机制研究. 计算机学报, 2020, 43(12): 2414-2432)

[11] Wang L, Yu Z, Zhang D, et al. Heterogeneous multi-task assignment in mobile crowdsensing using spatiotemporal correlation. IEEE Transactions on Mobile Computing, 2019, 18(1): 84-97

[12] Wu D, Yang Z, Yang B, et al. From centralized management to edge collaboration: A privacy-preserving task assignment framework for mobile crowd sensing. IEEE Internet of Things Journal, 2021, 8(6): 4579-4589

[13] Ma Rong, Chen Xiu-Hua, Liu Hui, et al. Research on user privacy measurement and privacy protection in mobile crowdsensing. Netinfo Security, 2018, 18(8): 64-72(in Chinese)
(马蓉, 陈秀华, 刘慧等. 移动群智感知中用户隐私度量与隐私保护研究. 信息网络安全, 2018, 18(8): 64-72)

[14] Ding S, He X, Wang J, et al. Multiobjective optimization model for service node selection based on a tradeoff between quality of service and resource consumption in mobile crowd sensing. IEEE Internet of Things Journal, 2017, 4(1): 258-268

[15] Xiong J, Liu H, Jin B, et al. A lightweight privacy protection scheme based on user preference in mobile crowdsensing. Transactions on Emerging Telecommunications Technologies, 2021, 32(5): 1-16

[16] Vergara-Laurens I, Jaimes L, Labrador M, et al. Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. IEEE Internet of Things Journal, 2017, 4(4): 855-869

[17] Liu J, Shen H, Zhang X, et al. A survey of mobile crowdsensing techniques: A critical component for the Internet of Things//Proceedings of the 25th International Conference on Computer Communication and Networks. New York, USA, 2016: 1-6

[18] Restuccia F, Ghosh N, Bhattacharjee S, et al. Quality of information in mobile crowdsensing: Survey and research challenges. ACM Transactions on Sensor Networks, 2017, 13(4): 1-43

[19] Shi F, Wu D, Arkhipov D, et al. ParkCrowd: Reliable crowdsensing for aggregation and dissemination of parking space information. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(11): 4032-4044

[20] Suhas M, Tong J, Nikhil K, et al. ParkNet: Drive-by sensing of road-side parking statistics//Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services. New York, USA, 2020: 123-136

[21] Chen X, Xu S, Han J, et al. PAS: Prediction-based actuation system for city-scale ridesharing vehicular mobile crowdsensing. IEEE Internet of Things Journal, 2020, 7(5): 3719-3734

[22] Bi R, Chen Q, Chen L, et al. A privacy-preserving personalized service framework through Bayesian game in social IoT. Wireless Communications and Mobile Computing, 2020, 2020:1-13. DOI: 10.1155/2020/8891889

[23] Shafi J, Waheed A. S-IoT: A new platform for online social networks using IoT//Proceedings of the 1st International Conference on Computer Applications & Information Security. Riyadh, UAE, 2018: 1-6

[24] Ogie R, Clarke R, Forehead H, et al. Crowdsourced social media data for disaster management: Lessons from the PetaJakarta.org project. Computers, Environment and Urban Systems, 2019, 73: 108-117

[25] Vahdat-Nejad H, Asef M. Architecture design of the air pollution mapping system by mobile crowd sensing. IET Wireless Sensor Systems, 2018, 8(6): 268-275

[26] Guo X, Wang M, Liu X, et al. Design and development of campus noise detection and rendering system based on mobile crowdsensing//Proceedings of the IEEE International Conference on Consumer Electronics-Taiwan. Yilan, China, 2019: 1-2

[27] Payman M, Peter R. ABY3: A mixed protocol framework for machine learning//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. New York, USA, 2018: 35-52

[28] Xiong J, Ma R, Chen L, et al. Achieving incentive, security, and scalable privacy protection in mobile crowdsensing services. Wireless Communications and Mobile Computing, 2018, 2018: 1-12. DOI: 10.1155/2018/8959635

[29] Liu C, Tian Y, Xiong J, et al. Towards attack and defense views to k-anonymous using information theory approach. IEEE Access, 2019, 7: 156025-156032

[30] Huang K, Liu X, Fu S, et al. A lightweight privacy-preserving CNN feature extraction framework for mobile sensing. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1441-1455

[31] Xiong J, Bi R, Zhao M, et al. Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles. IEEE Wireless Communications, 2020, 27(3): 24-30

[32] Xiong J, Zhao M, Bhuiyan M, et al. An AI-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of IoT. IEEE Transactions on Industrial Informatics, 2021, 17(2): 922-933

[33] Zhang D, Tian Y, Wang L, et al. Cooperative game model of delegation computing: Verifier separated from calculators//Proceedings of the IEEE Conference on Computer Communications Workshops. Toronto, Canada, 2020: 62-67

[34] Zhou T, Cai Z, Wu K, et al. FIDC: A framework for improving data credibility in mobile crowdsensing. Computer Networks, 2017, 120: 157-169

[35] Niu X, Ye Q, Zhang Y, et al. A privacy-preserving identification mechanism for mobile sensing systems. IEEE Access, 2018, 6: 15457-15467

[36] Hu L, Shahabi C. Privacy assurance in mobile sensing network: Go beyond trusted servers//Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops. Mannheim, Germany, 2010: 613-619

[37] Zeng Ju-Ru, Chen Hong, Peng Hui. Privacy preservation in mobile participatory sensing. Chinese Journal of Computers, 2016, 39(3): 595-614(in Chinese)
(曾菊儒, 陈红, 彭辉. 参与式感知隐私保护技术. 计算机学报, 2016, 39(3): 595-614)

[38] Niu B, Chen Y, Wang Z, et al. Eclipse: Preserving differential location privacy against long-term observation attacks. IEEE

Transactions on Mobile Computing (Early Access), 2020: 1. DOI: 10.1109/TMC.2020.3000730

[39] Sei Y, Ohsuga A. Differential private data collection and analysis based on randomized multiple dummies for untrusted mobile crowdsensing. IEEE Transactions on Information Forensics and Security, 2017, 12(4): 926-939

[40] Wang W, Zhang Q. A stochastic game for privacy preserving context sensing on mobile phone//Proceedings of the IEEE Conference on Computer Communications. Toronto, Canada, 2014: 2328-2336

[41] Chen J, Ma H, Zhao D, et al. Participant density-independent location privacy protection for data aggregation in mobile crowd-sensing. Wireless Personal Communications, 2018, 98: 699-723

[42] Wang X, Cheng W, Mohapatra P, et al. ARTSense: Anonymous reputation and trust in participatory sensing// Proceedings of the IEEE Conference on Computer Communications. Turin, Italy, 2013: 2517-2525

[43] Alsheikh M, Jiao Y, Niyato D, et al. The accuracy-privacy trade-off of mobile crowdsensing. IEEE Communications Magazine, 2017, 55(6): 132-139

[44] Xiong Jin-Bo, Ma Rong, Niu Ben, et al. Privacy protection incentive mechanism based on user-union matching in mobile crowdsensing. Journal of Computer Research and Development, 2018, 55(7): 1359-1370(in Chinese)
(熊金波, 马蓉, 牛犇等. 移动群智感知中基于用户联盟匹配的隐私保护激励机制. 计算机研究与发展, 2018, 55(7): 1359-1370)

[45] Dimitriou T, Krontiris I. Privacy-respecting auctions and rewarding mechanisms in mobile crowd-sensing applications. Journal of Network and Computer Applications, 2017, 100: 24-34

[46] Liu B, Zhou W, Zhu T, et al. Invisible hand: A privacy preserving mobile crowdsensing framework based on economic models. IEEE Transactions on Vehicular Technology, 2017, 66(5): 4410-4423

[47] Liu Hui, Bi Ren-Wan, Xiong Jin-Bo, et al. Fog-aided identity privacy protection scheme for sensing users in mobile crowd sensing. Chinese Journal of Network and Information Security, 2019, 5(6): 75-84(in Chinese)
(刘慧, 毕仁万, 熊金波等. 移动群智感知中基于雾节点协作的感知用户身份隐私保护. 网络与信息安全学报, 2019, 5(6): 75-84)

[48] Wu D, Fan L, Zhang C, et al. Dynamical credibility assessment of privacy-preserving strategy for opportunistic mobile crowd sensing. IEEE Access, 2018, 6: 37430-37443

[49] Wu D, Si S, Wu S, et al. Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. IEEE Internet of Things Journal, 2018, 5(4): 2958-2970

[50] Khuong V, Zheng R, Gao J, et al. Efficient algorithms for *K*-anonymous location privacy in participatory sensing// Proceedings of the IEEE Conference on Computer Communications. Orland, USA, 2012: 2399-2407

[51] Agir B, Papaioannou T, Narendula R, et al. User-side adaptive of location privacy in participatory sensing. GeoInformatica, 2014, 18(1): 165-191

[52] Chen X, Wu X, Li X, et al. Privacy-preserving high-quality map generation with participatory sensing//Proceedings of the IEEE Conference on Computer Communications. Toronto, Canada, 2014: 2310-2318

[53] Chen Q, Zheng S, Weng Z, et al. Leveraging mobile nodes for preserving node privacy in mobile crowd sensing. Wireless Communications and Mobile Computing, 2018, 2018: 1-11

[54] Chen C, Yang T, Chiang M, et al. A privacy authentication scheme based on cloud for medical environment. Journal of Medical Systems, 2014, 38(11): 143

[55] Liu J, Cao H, Li Q, et al A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. IEEE Internet of Things Journal, 2019, 6(2): 1321-1330

[56] Tang D, Ren J. A novel delay-aware and privacy-preserving data-forwarding scheme for urban sensing network. IEEE Transactions on Vehicular Technology, 2016, 65(4): 2578-2588

[57] Sun G, Sun S, Sun J, et al. Security and privacy preservation in fog-based crowd sensing on the Internet of Vehicles. Journal of Network and Computer Applications, 2019, 134: 89-99

[58] Gisdakis S, Giannetsos T, Papadimitratos P, et al. Security privacy and incentive provision for mobile crowd sensing systems. IEEE Internet of Things Journal, 2016, 3(5): 839-853

[59] Lin X, Ni J, Shen X, et al. Location privacy protection in mobile crowdsensing. Privacy-Enhancing Fog Computing and Its Applications, 2018: 55-66

[60] Au M, Susilo W, Mu Y, et al. Constant-size dynamic *k*-times anonymous authentication. IEEE Systems Journal, 2013, 7(2): 249-261

[61] Ateniese G, Fu K, Green M, et al. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Transactions on Information and System Security, 2006, 9(1): 1-30

[62] Hu J, Lin H, Guo X, et al. DTCS: An integrated strategy for enhancing data trustworthiness in mobile crowdsourcing. IEEE Internet of Things Journal, 2018, 5(6): 4663-4671

[63] Li X, Wen Q, Li W, et al. Secure privacy-preserving biometric authentication scheme for telecare medicine information systems. Journal of Medical Systems, 2014, 38 (11): 139

[64] Zhang Y, Shu J, Liu X, et al. Comments on "A Large-Scale Concurrent Data Anonymous Batch Verification Scheme for Mobile Healthcare Crowd Sensing". IEEE Internet of Things Journal, 2019, 6(1): 1287-1290

[65] Jin H, Su L, Xiao H, et al. INCEPTION: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems//Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York, USA, 2016: 341-350

[66] Jin H, Su L, Ding B, et al. Enabling privacy-preserving incentives for mobile crowd sensing systems//Proceedings of the 36th IEEE International Conference on Distributed Computing Systems. Nara, Japan, 2016: 344-353

[67] Zheng Y, Duan H, Wang C, et al. Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2475-2489

[68] Huo Y, Yong C, Lu Y. Re-ADP: Real-time data aggregation with adaptive w-event differential privacy for fog computing. Wireless Communications and Mobile Computing, 2018, 2018: 1-13

[69] Wang Z, Pang X, Chen Y, et al. Privacy-preserving crowd-sourced statistical data publishing with an untrusted server. IEEE Transactions on Mobile Computing, 2018, 18(6): 1356-1367

[70] Wang Z, Hu J, Lyu R, et al. Personalized privacy-preserving task allocation for mobile crowdsensing. IEEE Transactions on Mobile Computing, 2019, 18(6): 1330-1341

[71] Ni J, Zhang K, Xia Q, et al. Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing. IEEE Transactions on Mobile Computing, 2020, 19(6): 1317-1331

[72] Li T, Jung T, Li H, et al. Scalable privacy-preserving participant selection in mobile crowd sensing//Proceedings of the IEEE International Conference on Pervasive Computing and Communications. Kona, USA, 2017: 59-68

[73] Ma R, Xiong J, Lin M, et al. Privacy protection-oriented mobile crowdsensing analysis based on game theory//Proceedings of the IEEE Trustcom/BigDataSE/ICESS. Sydney, Australia, 2017: 990-995

[74] Xiao L, Li Y, Han G, et al. A secure mobile crowdsensing game with deep reinforcement learning. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 35-47

[75] Luo E, Bhuiyan M, Wang G, et al. PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems. IEEE Communications Magazine, 2018, 56(2): 163-168

[76] Xiong H, Zhang D, Chen G, et al. ICrowd: Near-optimal task allocation for piggyback crowdsensing. IEEE Transactions on Mobile Computing, 2016, 15(8): 2010-2022

[77] Wang Z, Huang D, Wu H, et al. QoS-constrained sensing task assignment for mobile crowd sensing//Proceedings of the IEEE Global Communications Conference. Austin, USA, 2014: 311-316

[78] He S, Shin D, Zhang J, et al. An exchange market approach to mobile crowdsensing: Pricing, task allocation, and Walrasian equilibrium. IEEE Journal on Selected Areas in Communications, 2017, 35(4): 921-934

[79] Yang D, Xue G, Fang X, et al. Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones. IEEE/ACM Transactions on Networking, 2016, 24(3): 1732-1744

[80] Hu T, Yang T, Hu B, et al. A data quality index based incentive mechanism for smartphone crowdsensing//Proceedings of the IEEE/CIC International Conference on Communications in China. Chengdu, China, 2016: 1-6

[81] Liu Y, Li H, Zhao G, et al. Reverse auction based incentive mechanism for location-aware sensing in mobile crowd sensing//Proceedings of the IEEE International Conference on Communications. Kansas City, USA, 2018: 1-6

[82] Zhang X, Yang Z, Sun W, et al. Incentives for mobile crowd sensing: A survey. IEEE Communications Surveys & Tutorials, 2015, 18(1): 54-67

[83] Wang Tao-Chun, Jin Xin, Lü Cheng-Mei, et al. Privacy preservation method of data aggregation in mobile crowd sensing. Journal of Computer Research and Development, 2020, 57(11): 2337-2347(in Chinese)
(王涛春，金鑫，吕成梅等. 移动群智感知中融合数据的隐私保护方法. 计算机研究与发展，2020，57(11)：2337-2347)

[84] Long Hao, Zhang Shu-Kui, Zhang Yang, et al. Task distribution algorithm based on community in mobile crowd sensing. Journal on Communications, 2019, 40(10): 42-54 (in Chinese)
(龙浩，张书奎，张洋等. 移动群智感知中基于社区的任务分发算法. 通信学报，2019，40(10)：42-54)

[85] Yang Shuo, Wu Fan, Chen Gui-Hai. On designing most informative user selection methods for mobile crowdsensing. Chinese Journal of Computers, 2020, 43(3): 409-422 (in Chinese)
(杨朔，吴帆，陈贵海. 移动群智感知网络中信息量最大化的用户选择方法研究. 计算机学报，2020，43(3)：409-422)

[86] Xiong Jin-Bo, Wang Min-Shen, Tian You-Liang, et al. Research progress on privacy measurement for cloud data. Journal of Software, 2018, 29(7): 1963-1980(in Chinese)
(熊金波，王敏燊，田有亮等. 面向云数据的隐私度量研究进展. 软件学报，2018，29(7)：1963-1980)

[87] Lin L, Liao X, Jin H, et al. Computation offloading toward edge computing. Proceedings of the IEEE, 2109, 107(8): 1584-1607

[88] Zhang C, Zhu L, Xu C, et al. PRVB: Achieving privacy-preserving and reliable vehicular crowdsensing via blockchain oracle. IEEE Transactions on Vehicular Technology, 2021, 70(1): 831-843

[89] Lin C, He D, Kumar N, et al. HomeChain: A blockchain-based secure mutual authentication system for smart homes. IEEE Internet of Things Journal, 2020, 7(2): 818-829

[90] Tian Y, Wang Z, Xiong J, et al. A blockchain-based secure key management scheme with trustworthiness in DWSNs. IEEE Transactions on Industrial Informatics, 2020, 16(9): 6193-6202

[91] Yang Q, Liu Y, Chen T, et al. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): 1-19

[92] Kang J, Xiong Z, Li X, et al. Optimizing task assignment

for reliable blockchain-empowered federated edge learning. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1910-1923

[93] Liu Y, Kang Y, Xing C, et al. A secure federated transfer learning framework. IEEE Intelligent Systems, 2020, 35(4): 70-82

[94] Li Fan-Zhang, Liu Yang, Wu Peng-Xiang, et al. A survey on recent advances in meta-learning. Chinese Journal of Computers, 2021, 44(2): 422-446(in Chinese)
(李凡长, 刘洋, 吴鹏翔等. 元学习研究综述. 计算机学报, 2021, 44(2): 422-446)

[95] Liu Y, Wang H, Peng M, et al. An incentive mechanism for privacy-preserving crowdsensing via deep reinforcement learning. IEEE Internet of Things Journal, 2021, 8(10): 8616-8631

[96] Li F, Li H, Niu B, et al. Privacy computing: Concept, computing framework, and future development trends. Engineering, 2019, 5(6): 1179-1192

XIONG Jin-Bo, Ph. D., professor, Ph. D. supervisor. His main research interests include mobile crowdsensing security and privacy protection.

BI Ren-Wan, Ph. D. candidate. His main research interest is deep learning security and privacy.

TIAN You-Liang, Ph. D., professor, Ph. D. supervisor. His main research interest is cryptography and information security.

LIU Xi-Meng, Ph. D., professor, Ph. D. supervisor. His main research interest is cryptography and artificial intelligence security.

MA Jian-Feng, Ph. D., professor, Ph. D. supervisor. His main research interests include cryptography, computer network and information security.

Background

Thanks to the increasingly developed technologies of cloud computing, edge computing, Internet of Things and 5th generation mobile communications, mobile crowdsensing (MCS), a novel intelligent society perception paradigm joining mobile awareness with crowdsourcing advancements, provides a brand-new approach of information transmission and services for smart city.

Massive mobile intelligent perceptive terminals cooperate to facilitate a deep social perception task for providing personalized user services. With the exploding growth of smart devices, MCS has made a rapid progress in recent years, and has greatly enriched various applications and services in smart city. In MCS, however, sensing data encounters various challenges of data security breaches and privacy disclosures during the entire lifecycle of the sensing task. The existing works mainly discuss the security and privacy of MCS from one stage or one particular security problem, lacking an overall and systematic perspective. Without comprehensively addressing the security and privacy issues, the continuous developments of MCS could be hindered.

To tackle this problem, in this paper, we ingeniously introduce a system model of MCS, and illustrate multiple security methods and threat models corresponding to the three different lifecycle stages of sensing data. Furthermore, we elaborately describe the existing security and privacy protection solutions and discuss the developing trends and research directions of MCS. This work aims to provide references for researchers to accurately identify the latest research trends and future developments in the security and privacy in MCS.

This research is supported by the National Natural Science Foundation of China under Grant No. 61872088, No. 62072109, No. U1905211, No. U1804263, No. 61772008, No. 61702105, and No. 61872090, the Natural Science Foundation of Fujian Province under Grant No. 2019J01276, the Science and Technology Major Support Program of Guizhou Province under Grant No. 20183001, the Guizhou Provincial Key Laboratory of Public Big Data Research Fund under Grant No. 2019BDKFJJ004, the Opening Project of Guangxi Key Laboratory of Trusted Software under Grant No. KX202042, the Opening Project of Shaanxi Key Laboratory of Network and System Security under Grant No. NSSOF1900104, the Opening Project of Guangdong Provincial Key Laboratory of Data Security and Privacy Protection under Grant No. 2017B03031004-12.