

可信群智感知系统研究

曾 豪¹⁾ 张 博¹⁾ 崔禾磊¹⁾ 於志文^{1),2)} 陈亚兴¹⁾
郭 斌¹⁾ 周兴社¹⁾

¹⁾(西北工业大学计算机学院 西安 710072)

²⁾(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要 群智感知作为一种新兴的物联网感知范式,能够在无需额外部署传感器的情况下,利用大众的智能移动设备在多样化应用场景中收集并处理感知数据,展现出卓越的灵活性、广泛的覆盖性和显著的经济性。群智感知系统通常由任务发布者、任务参与者和感知平台组成,三方共同协作以完成感知任务。然而,系统在实际运行中往往面临主观人为因素(如系统内外实体基于自身利益主动发起的攻击行为)和非主观人为因素(如系统内外客观条件所致的影响)的双重威胁,这些因素可能对系统的可信性造成严重破坏,进而阻碍其进一步发展与广泛应用。现有研究综述在群智感知系统的可信性研究方面尚未形成完整且系统的理论体系与框架。针对此现状,本文首先总结了群智感知系统的通用框架,明确划分了各个实体的核心功能并分析其作用,从系统层面、实体层面和数据层面提炼出群智感知系统的九个关键可信特征。其次,本文系统分析了主观与非主观人为因素对群智感知系统可信特征的影响机制,并基于上述三个层面归纳总结了应对这些因素的策略及其应用效果。最后,本文展望了群智感知系统的未来研究方向,围绕系统、实体和数据层面的可信性研究,探讨了如何构建可信群智感知系统,旨在推动其广泛应用与持续发展。

关键词 群智感知;可信计算;隐私保护;数据安全;质量评估

中图法分类号 TP18

DOI号 10.11897/SP.J.1016.2026.02025

A Survey of Trustworthy Crowdsensing Systems

ZENG Hao¹⁾ ZHANG Bo¹⁾ CUI He-Lei¹⁾ YU Zhi-Wen^{1),2)} CHEN Ya-Xing¹⁾
GUO Bin¹⁾ ZHOU Xing-She¹⁾

¹⁾(School of Computer Science, Northwestern Polytechnical University, Xi'an 710072)

²⁾(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)

Abstract As an emerging paradigm for Internet of Things (IoT) sensing, crowdsensing leverages the crowd's smart mobile devices to collect and process sensing data for diverse application scenarios without additional sensor deployments, providing excellent flexibility, extensive coverage, and economic benefits. The crowdsensing system mainly consists of task providers, task participants, and sensing platforms, which work collaboratively to accomplish sensing tasks. However, subjective human factors (such as malicious attack behaviors for personal benefit) and non-subjective human factors (such as external and internal system objective conditions) may impact or disrupt the crowdsensing system, hindering further development and widespread application. Moreover, existing surveys still lack a comprehensive and systematic theoretical framework

收稿日期:2025-11-13;在线发布日期:2026-05-25。本课题得到国家重点研发计划项目(2024YFB4505502)、国家自然科学基金联合基金重点支持项目(U22B2022)和国家自然科学基金面上项目(62372383)资助。曾 豪,博士研究生,主要研究方向为群智感知和隐私计算。E-mail:hao_zeng@mail.nwpu.edu.cn。张 博,博士研究生,主要研究方向为隐私计算和系统安全。崔禾磊(通信作者),博士,教授,主要研究方向为可信群智感知与隐私计算。E-mail:chl@nwpu.edu.cn。於志文(通信作者),博士,教授,主要研究方向为群智感知、普适计算和智能物联网。E-mail:zhiwenyu@nwpu.edu.cn。陈亚兴,博士,副教授,主要研究方向为可信群智感知与数据隐私计算。郭 斌,博士,教授,主要研究方向为普适计算、群智感知和人机物融合群智计算。周兴社,博士,教授,主要研究方向为嵌入式计算和普适计算。

for assessing the trust of the crowdsensing system. In light of this, we first summarize the general framework of the crowdsensing system, outline the core functions of different entities, and define 9 critical features of the trust across the system layer, the user layer, and the data layer. Then, we explore the impacts of subjective and non-subjective human factors on the trust features of the crowdsensing system and systematically summarize the methodological strategies to address these factors from the above three layers respectively. Finally, to promote the further development and widespread application of crowdsensing, we explore how to build a trustworthy crowdsensing system and present future research directions around the trustworthy research of the system layer, user layer, and data layer.

Keywords crowdsensing; trust computing; privacy protection; data security; quality evaluation

1 引 言

群智感知(Crowdsensing)由众包、参与感知等概念发展而来,是一种新兴的物联网感知范式^[1]。相较于传统的基于传感网和物联网的感知方式^[2],群智感知无需额外部署大量传感器设备,而是利用广泛普及的智能移动设备和智能体,在多样化的应用场景中动态地捕获数据,形成规模庞大、随时随地运作且与大众日常生活密切相关的群智感知系统,具有灵活部署、广域覆盖、高效经济等优势^[3]。目前,群智感知系统已被广泛应用于环境质量监测^[4-5]、交通流量监控^[6-7]、健康数据追踪^[8]、室内定位^[9]以及灾后救援^[10]等关键领域。

群智感知系统主要由任务发布者、任务参与者和感知平台三个实体紧密构成^[3]。任务发布者负责设计并发布感知任务,同时提供必要的经济奖励;任务参与者则利用其所持有的智能移动设备或智能体执行指定任务,并将收集到的感知数据上传至感知平台;感知平台则承担任务分配、数据质量评估、激励机制实施等关键职能。这些实体间的高效协同与精密配合,使得群智感知系统能够深度整合并优化社会资源^[11-12]。

然而,在多方利益错综复杂的环境下,群智感知系统中往往潜藏着恶意实体,这些恶意实体基于自身利益主动发起(即由主观人为因素导致)的恶意攻击行为,给系统带来了复杂且严峻的安全隐私挑战^[13]。例如,(1)任务发布者可能设计恶意任务窃取任务参与者的敏感信息(如位置信息和移动轨迹)^[13-17],甚至在得到感知数据后拒绝履行支付报酬的义务^[18-21]。(2)任务参与者可能伪造、窃取感知数据或与任务发布者勾结以获取不正当奖励^[22-26]。

(3)感知平台可能在任务分配、数据质量评估和激励机制过程中偏袒特定实体(任务发布者和任务参与者)从而破坏感知服务的公平性^[27-29]。此外,(4)其他外部实体可能通过窃听和暴力破解等手段^[14-15,17,19,30]攻击群智感知系统的通信模块,获取实体的隐私数据,甚至利用无线电信号、GPS信号等侧信道攻击方式^[31-32]诱导任务参与者前往错误的地理位置。这些恶意行为可能导致数据泄露或篡改,侵害其隐私,甚至引发系统崩溃,最终造成群智感知服务不可用。

除了上述主观人为因素外,群智感知系统还可能受到其他非主观人为因素的影响。例如,(1)任务参与者的专业能力不足可能造成设备操作不规范或感知时长不足等问题^[33-35];(2)设备功能受限可能导致设备无法及时响应任务或因电池等问题中断任务^[36-37];(3)外部环境干扰,如恶劣的天气条件,可能影响任务参与者的积极性和设备运行的稳定性^[3,38]。这些非主观人为因素虽然不包含直接的恶意动机,但它们的存在依然可能对群智感知系统产生不可忽视的影响。

随着群智感知系统应用场景的不断拓展,其所面临的挑战也愈加复杂,尤其是在主观人为因素复杂化以及非主观人为因素多样化的情况下,现有方法策略难以提供全面有效的保护。国内外研究者对此给予了广泛关注,展开了深入调研,并取得了一些重要的综述研究成果。代表性综述诸如:Tong等人^[39]围绕群智感知系统中的任务分配、质量控制、激励机制设计以及隐私保护四个核心问题对现有研究进行了系统性的总结;Liu等人^[40]聚焦于群智感知系统中资源限制和感知服务质量问题对现有研究进行了深入分析,并进一步探讨了如何构建具有成本效益的群智感知系统;Wang等人^[41]对现有隐私

保护策略进行了全面梳理,并将其划分为身份隐私、数据隐私、属性隐私和任务隐私四大类,深入分析了各类隐私保护策略的性能特点;Xiong 等人^[13]以感知数据在感知任务中的生命周期为轴,对其在感知阶段、上传阶段以及交易阶段面临的安全威胁及相应的防御策略进行了归纳和总结;Cheng 等人^[42]围绕群智感知系统在数据感知与任务分配过程中所面临的隐私泄露风险与隐私保护需求,对现有群智感知隐私保护技术进行了分类梳理与定性评估;Zhang 等人^[43]则进一步从位置隐私、身份隐私以及数据隐私三个关键维度出发,对现有隐私保护方法进行了系统梳理与分析;Yang 等人^[44]梳理了生成式人工智能在群智感知系统安全防护与隐私保护中的作用机理与应用潜力。然而,这些综述工作在群智感知系统的可信性研究方面尚未形成完整且系统的理论体系与框架。

从本质上讲,“可信性”^[45]是在传统软件系统的“安全”和“可靠”等概念的基础上发展而来的,其核心内涵在于:一个可信的软件系统能够以预期的方式运行并实现既定目标。在此理念指导下,“可信性”已被引入到可信软件(Trustworthy Software)^[46-47]以及可信机器学习(Trustworthy Machine Learning)^[48-49]等多个重要研究领域。作为一种高度开放的人机协同系统,群智感知系统的可信性不仅继承了传统软件系统的基本可信特征,如可用性、鲁棒性和真实性,还进一步结合其开放协同的交互特性,形成了面向系统层面、实体层面以及数据层面的新型可信特征,包括公平性、可认证性、匿名性、可追溯性、完整性和机密性。由此,可信群智感知系统(Trustworthy Crowdsensing System)是一种在自身设计和实现上值得信任,能够提供符合任务发布者、任务参与者以及感知平台预期的感知服务,确保各项功能的高可用性,并对潜在攻击与故障具有韧性的群智感知系统。然而,想要构建满足上述要求的可信群智感知系统,仍然是当前亟需攻克挑战。

与现有的群智感知系统研究综述不同,本文提炼出群智感知系统需要考虑的九个可信特征,分析并总结了主观和非主观人为因素对群智感知系统可信特征的影响,探讨了现有研究中针对这两类因素的方法策略及其应用效果,并阐述了群智感知系统的未来研究方向,以期构建可信群智感知系统提供思路和借鉴。因此,本文的主要贡献包括以下三个方面:

(1)本文从群智感知系统的通用框架出发,首先划分了各个实体的核心功能并分析其作用。进而为了评估影响群智感知系统可信性的因素,本文从系统、实体和数据三个层面总结了群智感知系统在可信性方面所需要考虑的九个关键特征。

(2)本文深入调研了近年来国内外在群智感知领域的相关文献,将导致群智感知系统不可信的因素分为主观人为因素和非主观人为因素两大类,分析并总结它们各自的产生原因及其对群智感知系统九个可信特征的影响。

(3)本文结合主观人为因素和非主观人为因素对群智感知系统可信性的影响,探讨了现有研究针对主观人为因素和非主观人为因素的方法策略及其应对效果。通过对现有研究的分析和总结,本文分层阐述群智感知系统的未来研究方向,探讨如何构建可信的群智感知系统,旨在推动其广泛应用与持续发展。

2 群智感知系统模型

本节首先从群智感知系统的通用框架出发,明确划分了各个实体的核心功能并分析其作用;随后,凝练出群智感知系统在可信性方面需要考虑的九个关键特征,为后续分析奠定了基础。

2.1 通用框架

群智感知系统主要由任务发布者、任务参与者和感知平台三个实体紧密构成^[3,11,50],通过整合任务参与者的多样化感知能力,实现了对现实世界全方位、精细化的监测与分析。如图1所示,任务发布者首先将具有明确需求目标的感知任务及相应的感知预算(用于经济奖励)发布至感知平台。感知平台利用智能匹配算法,基于任务的要求与任务参与者的技能、位置等因素,精准地将任务分配给最适合的任务参与者。随后,任务参与者在指定的时间内前往指定区域,利用携带的设备(如手机、手环以及手表等)以及专业技能完成感知任务并上传收集到的感知数据。感知平台接收到大量感知数据后,将对感知数据进行融合与分析,从中提取出有价值的信息。最后,感知平台将处理后的感知数据结果及时反馈给任务发布者,同时根据任务发布者设定的感知预算,向任务参与者发放相应的经济奖励。然而,要确保实体间的高效协同运作并非易事,这依赖于各个实体核心功能的精妙设计与集成。这些功能决定了系统能否有效收集、处理并融合来自不同任务

参与者的海量感知数据^[51]。接下来,我们将系统性地划分各个实体的核心功能,分析这些核心功能的作用和协同策略。

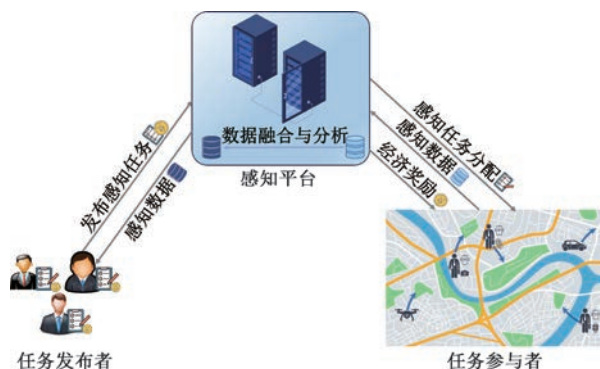


图1 群智感知系统的通用框架及流程

任务发布者的核心功能包括任务管理和通信。

(1)任务管理:负责定义感知任务的具体内容、硬件要求、时间窗口、感知区域和感知预算。根据应用场景,可将感知任务类型分为紧急任务和非紧急任务。例如,监控道路交通流量的任务需实时获取交通流量数据,以便交通管理部门迅速疏导拥堵,因此被视为紧急任务。而市场调研任务仅需任务发布者(产品公司)将问卷作为任务发布到感知平台并允许任务参与者在相对宽松的时间内完成,因此被视为非紧急任务。(2)通信:负责任务的发布与感知数据的获取。它将定义好的感知任务进行格式化和编码,确保任务在传输过程中能够被准确解析。同时,它接收来自感知平台的感知数据,对数据进行解码,恢复原始信息供后续处理使用。通过高效稳定的通信功能,任务发布者能够顺利地将任务发布至感知平台,并及时获取所需的感知数据。

任务参与者的核心功能包括设备管理、数据感知和通信,三者紧密协作,确保任务执行得高效与精准。(1)设备管理:负责实时监控并优化智能设备的运行状态、资源分配及配置。这使得无论是随身携带的手机、手环、手表等智能移动设备,还是智能汽车、机器人、无人机等复杂智能体,都能根据任务具体内容,灵活调配资源,协调各设备间的数据采集与传输,同时关注设备健康,及时发现并预警潜在故障。(2)数据感知:负责从智能移动设备或智能体中收集和感知数据。通过这些设备内部的传感器(如红外温度计、GPS、摄像头等)实时捕捉并解析环境信息,如温度、位置以及图像等,然后经过数据清洗、去噪、压缩等精细处理将感知数据中的噪声和冗余信息去除。(3)通信:负责接收来自感知平台的感知任务,并将任务参与者收集处理的感知数据传输

至平台。它不仅需要准确解析感知平台发送的任务信息(包括任务类型、具体内容以及硬件要求等),而且在传输感知数据前需要进行封装处理,以确保感知数据的完整性。

感知平台的核心功能包括数据存储、任务分配、数据质量评估以及激励机制,这些功能确保了平台的高效运作。(1)数据存储:作为信息中枢,存储和管理任务发布者和任务参与者的基本信息,涵盖身份信息、历史任务记录和活跃程度等,为任务匹配与数据质量评估提供基础。(2)任务分配:负责将感知任务分配给最合适的任务参与者。它敏锐捕捉感知任务的需求多样性与任务参与者的动态性,综合考量感知任务的时间窗口、感知区域以及感知预算,与参与者的兴趣偏好、时空轨迹以及期望的激励回报进行精确匹配,设计出高效且人性化的任务分配策略。(3)数据质量评估:负责筛选高质量的感知数据。鉴于任务参与者的技能和声誉值各不相同,数据质量评估需要对每个参与者的数据质量进行独立评估,剔除低质和冗余数据,确保仅高质量数据得以保留。(4)激励机制:确保任务参与者的积极性。任务参与者数量或声誉不足会影响群智感知服务。因此,感知平台通过采用适当的激励方式(比如经济奖励)鼓励任务参与者积极投入感知任务并提供高质量的感知数据,从而提升群智感知服务的质量。

2.2 可信特征

为了评估影响群智感知系统可信性的因素并构建清晰的可信性分析框架,本小节总结了群智感知系统需要考虑的九个关键可信特征。同时,为了更全面地理解这些可信特征,我们将其分为三个核心层面进行探讨:系统层面、实体层面和数据层面。每个层面所涵盖的可信特征及其定义如下。

2.2.1 系统层面

可用性:群智感知系统采取隐私保护措施(数据加密与噪声干扰等)后仍能正常访问和处理相关数据,感知服务的效率和质量未受到显著影响^[41]。

公平性:群智感知系统在任务分配和激励机制等过程中确保所有任务发布者和任务参与者享有平等的机会和权益,避免任何形式的偏袒^[20,52]。

鲁棒性:群智感知系统应及时识别恶意攻击(如通过注入伪造感知数据以扰乱系统决策的虚假数据注入攻击^[22]、通过发送大量非法请求导致系统超负荷运行的拒绝服务攻击^[18]等),并采取有效的防御措施,从而避免系统崩溃^[53]。

2.2.2 实体层面

可认证性:确保实体(包括任务发布者、任务参与者和感知平台)在访问和操作系统资源时,身份真实、合法且经过授权,防止未授权的实体访问系统数据或执行敏感操作^[30]。

匿名性:通过技术手段确保实体的身份信息(包括实体名称和位置信息等)不被任何实体识别,实现任务信息、感知数据与对应的身份信息的隔离,防止任何试图追踪或关联身份的行为^[26,29,54]。

可溯源性:实时监测实体的行为,当检测到恶意行为时,能够有效追踪和识别恶意行为的发起实体,在必要时揭示恶意实体的真实身份,实现对实体行为的约束和监督^[55]。

2.2.3 数据层面

真实性:确保任务参与者提供的感知数据以及感知平台的存储数据等数据对象来自声称的真实来源,防止任何形式的数据伪造^[56]。

完整性:采取必要措施来防止群智感知系统中的数据对象在收集、传输、存储和处理等过程中被非法篡改或损坏^[18,20]。

机密性:对群智感知系统中的数据对象实施严格的加密措施,确保这些数据在从收集、传输、存储到处理的整个生命周期内均受到保护,防止未经授权的实体通过任何手段进行访问或泄漏^[20,26]。

3 群智感知系统不可信因素分析

本文将导致群智感知系统不可信的因素分为两类:主观人为因素和非主观人为因素。如图2所示,在导致群智感知系统不可信的因素中,主观人为因素是指系统各个实体基于自身利益主动发起的恶意攻击行为,例如拒绝支付报酬以逃避责任的拒绝付款攻击^[18-21]、试图免费获取他人感知数据的搭便车攻击^[18,20,25-26]等;而非主观人为因素则是指除主观人为因素以外的所有因素,这些因素通常由系统内外客观条件所致,而非由实体主观意愿引发的风险,例如任务参与者专业能力不足^[33-35]、外部环境干扰^[3,38]等。本节将分析和总结主观人为因素和非主观人为因素对群智感知系统可信性的影响。

3.1 主观人为因素

在群智感知系统中,主观人为因素主要表现为各类恶意实体(包括任务发布者、任务参与者、感知平台及其他外部实体)在系统运行过程中实施的各种攻击行为。这些攻击行为往往依托于各功能模块

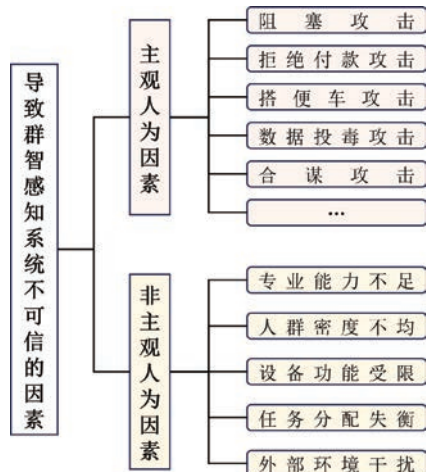


图2 导致群智感知系统不可信的因素分类

被发起,利用功能模块自身的业务逻辑和运行机制实施破坏,进而对群智感知系统的正常运行构成潜在威胁。本小节首先依据这些攻击行为发生所在的功能模块,将其划分为通信模块攻击、任务管理模块攻击、设备管理模块攻击、数据感知模块攻击、数据存储模块攻击、任务分配模块攻击、数据质量评估模块攻击以及激励机制模块攻击,如图3所示,从而刻画攻击行为对系统运行过程的影响。然后,在各个功能模块中探讨各类恶意实体基于其在系统中的角色定位与利益诉求所实施攻击的方式及其背后的动机。最后,我们在表1中对上述攻击行为的发起者及其破坏的可信特征进行了总结。

3.1.1 通信模块攻击

通信模块作为群智感知系统数据传输与交换的核心载体,面临着来自系统内外多方实体的安全威胁。任务发布者、任务参与者、感知平台及其他外部实体均可能针对通信链路或传输内容发起攻击,其攻击动机、实施方式及潜在影响存在显著差异。基于此,我们围绕通信模块中的四类常见攻击,分析不同实体实施这些攻击的目的与方式。

(1)推理攻击(背景知识攻击)^[13,16-17,19,73]:在群智感知系统中,推理攻击通常基于可获得的背景知识,对看似匿名的数据进行分析与推断,从而得到个体的敏感信息。该攻击可由系统内外的多类实体发起,不同实体的实施动机与攻击目标存在显著差异:①任务发布者实施的推理攻击主要服务于情报收集与竞争分析。他们通过精心设计的任务来收集任务参与者的位置数据、移动轨迹等背景信息,以预测任务参与者可能频繁出现的区域;结合参与者历史任务类型与完成记录,推断其技能水平与偏好;进一步通过分析任务提交的时间、地理分布特征,甚至关联

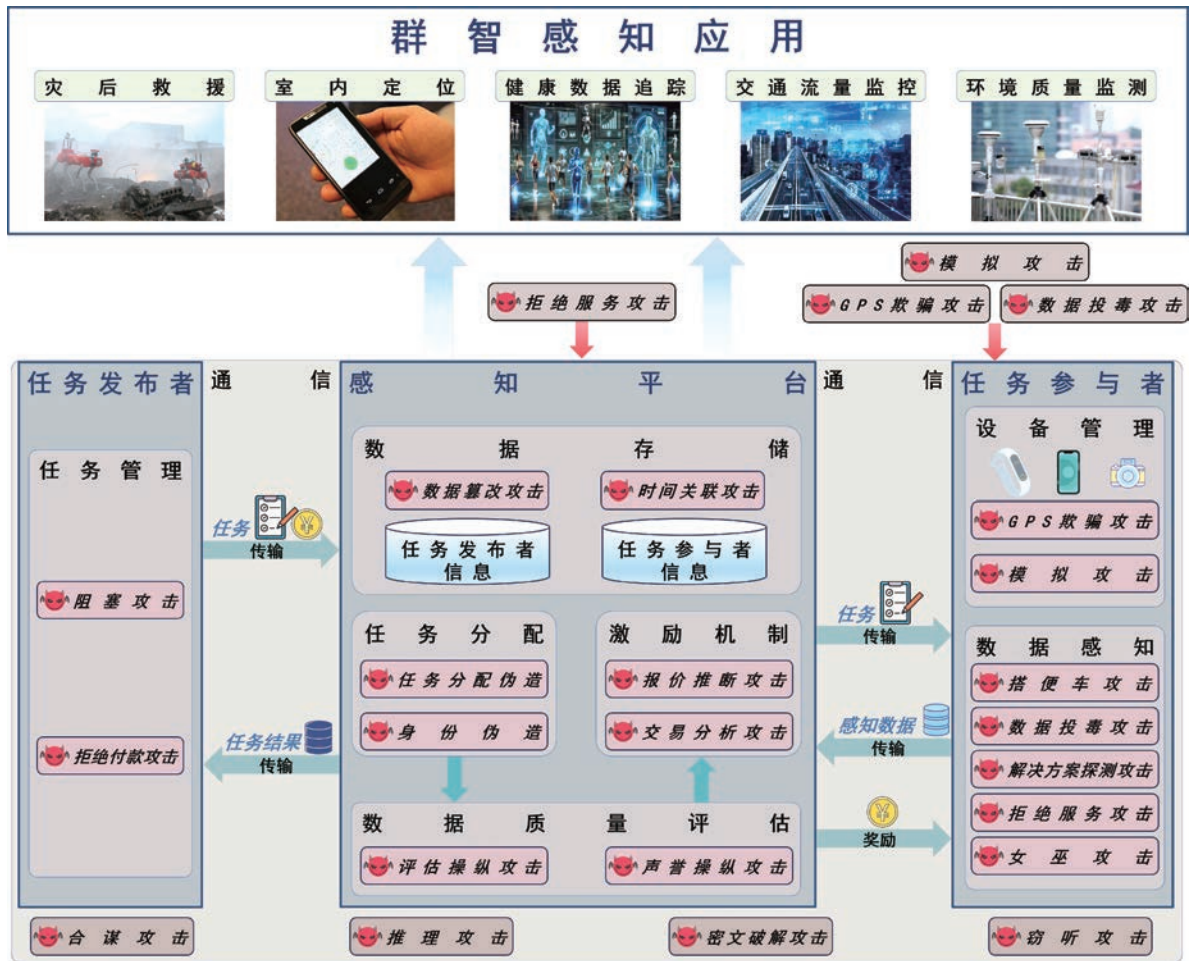


图 3 群智感知系统各模块所面临的潜在攻击

表 1 主观人为因素对群智感知系统可信性的影响分析

主观人为因素	发起者	破坏的可信特征								
		可用性	公平性	鲁棒性	可认证性	匿名性	可溯源性	真实性	完整性	机密性
阻塞攻击 ^[57-59]	任务发布者	●	○	●	○	○	○	○	○	●
拒绝付款攻击 ^[18-21]	任务发布者	●	●	○	○	○	○	○	○	○
搭便车攻击 ^[18,20,25-26]	任务参与者	○	●	○	○	○	○	●	○	○
解决方案探测攻击 ^[21]	任务参与者	○	●	○	○	○	○	●	○	○
女巫攻击 ^[16,26,60-62]	任务参与者	●	●	●	●	○	●	●	○	○
GPS欺骗攻击 ^[31-32,63]	任务参与者,其他外部实体	●	○	○	●	○	○	●	●	●
模拟攻击 ^[25,64]	任务参与者,其他外部实体	●	●	○	●	○	○	●	○	○
数据投毒攻击 ^[22,65-66]	任务参与者,其他外部实体	●	●	○	○	○	○	●	○	○
拒绝服务攻击 ^[18,20,67]	任务参与者,其他外部实体	●	○	●	○	○	○	○	○	○
窃听攻击 ^[14,30]	任务参与者,其他外部实体	○	●	○	○	●	○	●	○	●
合谋攻击 ^[29,55,68-69]	任务发布者,任务参与者感知平台	○	●	○	○	●	●	○	○	●
数据篡改攻击 ^[20,70]	感知平台	○	●	○	○	●	●	○	●	●
时间关联攻击 ^[71]	感知平台	○	●	○	○	●	●	○	○	○
任务分配伪造攻击 ^[28,72]	感知平台	○	●	○	○	○	●	○	○	○
身份伪造攻击 ^[70]	感知平台	○	●	○	●	●	●	○	○	○
报价推断攻击 ^[73]	感知平台	○	●	○	○	●	○	○	○	○
交易分析攻击 ^[74]	感知平台	○	○	○	○	●	●	○	○	●
评估操纵攻击 ^[27,75]	感知平台	○	●	○	○	○	○	○	●	●
声誉操纵攻击 ^[76]	感知平台	○	●	○	○	○	○	○	●	○
推理攻击 ^[13,16-17,19,73]	所有实体	○	○	○	○	●	●	○	○	●
密文破解攻击 ^[14-15,77]	所有实体	○	●	○	○	●	●	○	○	●

注:●表示主观人为因素影响了该可信特征;○表示主观人为因素没有影响该可信特征。

公开的社交媒体活动信息,逐步刻画任务参与者的出行规律、职业兴趣与行为特征。任务发布者之间也可能通过分析彼此的任务发布历史、定价策略与参与人群特征,推断对方的身份或商业策略。②任务参与者实施的推理攻击则更多面向同行竞争。他们通过感知任务中收集到的位置信息和轨迹数据,推测其他参与者可能经常出现的区域或生活规律^[17];在基于竞标任务中收集多轮竞标信息,推断其他参与者的出价策略与行为模式,并据此制定针对性的竞争策略^[73]。任务参与者还可能通过社交关系或协同参与的任务信息推断他人身份与社交网络结构,进一步扩大隐私泄露范围。③感知平台由于掌握全局视角与大量历史数据,可以利用感知数据与位置信息重建参与者的活动轨迹与身份特征,通过分析参与者之间的交互关系构建社交网络,将匿名身份与真实身份进行关联,从而破坏参与者匿名性并获取敏感信息^[16-17]。此外,平台还可能通过长期数据分析推断用户行为模式,用于商业决策或运营优化。④其他外部实体实施推理攻击的目的往往包括隐私窃取、商业情报收集、精准跟踪甚至后续的定向攻击,他们通过爬取公开数据或入侵第三方服务获取群智感知系统中泄露的部分任务信息、位置信息或交互记录,并将其与外部背景知识(如公开地图数据、社交网络信息或历史轨迹数据库)进行关联分析,从而推断任务参与者或任务发布者的敏感信息。当用户意识到匿名性难以保障时,其参与意愿将显著下降,进而对群智感知系统的长期运行与数据质量产生不利影响。

(2)密文破解攻击^[14-15]:在群智感知系统中,密文破解攻击是指攻击者通过直接攻击加密算法或密钥管理机制,绕过系统的密码学防护,将受保护的感知数据还原为明文,从而引发敏感信息的直接泄露。与基于统计关联与概率推断的推理攻击不同,密文破解攻击无需依赖背景知识假设,其攻击结果更为精确且危害更为直接。该攻击可由任务发布者、任务参与者、感知平台以及系统外部实体发起,其实施方式与攻击目的因主体角色不同而存在明显差异。①任务发布者通常因竞争或情报收集动机发起攻击。他们在任务参与者提交加密的感知数据后发起选择关键词攻击,提交特定关键词并观察系统返回的加密结果,进而推断参与者的活动模式与敏感偏好;或在掌握部分明文-密文对的情况下实施选择明文攻击,分析加密机制弱点以推导加密密钥;甚至利用高性能计算资源尝试暴力破解,穷举密钥空间以

解密目标数据。这些攻击一旦成功,将使发布者能够非法获取竞争对手的策略、参与者的轨迹与身份,进而操纵任务分配或实施精准竞争。②任务参与者实施密文破解攻击通常以牟取不当激励或获取竞争优势为目的。攻击者可能针对其他任务参与者上传的加密感知数据进行分析,通过破解其中的位置信息、轨迹数据或环境感知结果,实现身份推测、行为跟踪或能力评估。在掌握足够隐私信息后,攻击者甚至可以生成与合法参与者高度相似的感知数据,用以绕过平台的真实性检测机制,从而骗取奖励或扰乱任务结果。③感知平台作为系统的集中管理者,天然具备更强的密文分析能力。平台在接收加密感知数据后,可能利用已知的部分明文信息(如任务模板、固定字段或历史数据)实施已知明文攻击,或结合字典攻击与统计分析手段推测加密内容,从而恢复参与者的原始感知数据。这种行为虽不一定以恶意破坏为直接目的,但会实质性削弱加密机制对参与者隐私的保护效果,使位置、设备状态甚至身份信息暴露于平台内部,从根本上破坏参与者的隐私假设与匿名性保障。④其他外部实体通常需要先通过窃听攻击获取通信链路中的密文数据,并在离线环境下实施密文破解。对于采用弱加密或配置不当的系统,攻击者可通过频率分析推测加密方式;在更复杂的场景中,则可结合选择关键词攻击或选择明文攻击,分析已知明文与密文之间的对应关系,逐步逼近加密密钥。一旦破解成功,外部攻击者即可批量获取敏感感知数据,用于隐私窃取、身份追踪甚至后续的精准攻击。

(3)窃听攻击^[14,30]:在群智感知系统中,窃听攻击与密文破解攻击是两类在技术路径与威胁本质上存在显著区别的威胁。密文破解攻击侧重于在已获取密文数据后,通过密码分析技术主动破解加密机制以恢复明文,其威胁焦点在于加密算法或密钥本身的强度与可靠性;而窃听攻击主要指攻击者在通信信道上被动地非法截获传输中的数据,其前提是能够访问通信链路,且威胁的焦点在于数据传输过程的机密性。由此可见,窃听攻击常作为密文破解攻击的数据获取前置环节。①任务参与者发起的窃听攻击通常以获取竞争优势或牟取不当激励为目的。攻击者通常利用无线监听、网络嗅探或本地代理等手段,监听未加密或弱加密的通信信道,捕获其他任务参与者在任务执行过程中提交的感知数据或元数据(如任务标识、提交时间与位置特征)。通过持续监听与数据积累,恶意参与者不仅能够推断任

务发布者的任务目标与重点感知区域,还可据此伪造高度相似的感知数据,从而绕过平台的真实性检测机制并骗取奖励。^②其他外部实体实施的窃听攻击则通常具备更强的攻击能力与更广的监听范围。此类攻击者可通过部署恶意接入点、控制网络基础设施或实施中间人攻击,对任务发布者、任务参与者与感知平台之间的通信流量进行大规模监控^[14,19]。即使通信内容经过加密,外部攻击者仍可通过流量分析、通信频率与时序特征推断任务规模、执行周期及参与实体关系,从而间接获取系统运行状态与敏感业务信息;在通信保护不足的情况下,其甚至可直接截获明文数据,造成隐私泄露。

(4)合谋攻击^[23-24,55,68,78]:在群智感知系统中,合谋攻击是一种以多方实体协同实施为特征的攻击形态,通过非法勾结、共享私密信息或协同操作来获取不当利益或实现不正当竞争。其核心特征不在于最终造成的具体损害形式(如隐私泄露或激励操控),而在于这些损害必须依赖多实体之间的共谋与配合才能实现或显著放大。因此,合谋攻击在攻击目的上可能与其他攻击类型存在交叉,但在攻击实施机制与威胁模型上具有独立性。具体而言,①任务发布者可能与感知平台勾结,交换其他任务发布者的敏感信息以获取竞争优势,从而实施针对性的竞价或任务策略^[68];也可能与任务参与者串谋相互提交虚假任务和低质量数据,通过操控声誉值非法提升自身收益^[24];任务发布者之间还可能形成串谋联盟,互相承诺提升声誉或相互支持,以在平台竞争中获得不正当优势^[78]。②任务参与者也可能通过与其他实体串通非法获取利益或破坏系统正常运行,例如任务参与者之间组成串谋联盟并共同操纵投标和拍卖结果^[23],或串通提交相似甚至伪造的感知数据来操纵系统的判定,提高彼此的声誉^[55];任务参与者还可能与感知平台串通,利用平台共享的敏感信息获取其他参与者的身份、位置以及感知数据等关键信息^[68,79]。通过这些精心策划的合谋攻击,恶意的任务发布者能够获得虚假的高声誉并显著增强其在感知平台上的竞争力,恶意的任务参与者能够操控竞价或感知数据获取不当收益,平台从中实现利益输送或谋取不法收益,最终对群智感知系统的稳定运行构成严重威胁。

3.1.2 任务管理模块攻击

任务发布者通过任务管理功能模块在群智感知系统平台上创建并配置感知任务,这是平台业务运行的核心驱动力。然而,该功能模块在赋予任务发

布者较高自主性的同时,也暴露出可被滥用的安全隐患。恶意任务发布者可能利用其在任务定义、参数配置及任务生命周期管理中的权限,恶意构造任务内容或操纵任务发布与结算流程,以极低的实施成本获取不当收益。基于上述攻击动机,任务管理模块主要面临以下两类常见攻击。

(1)阻塞攻击(虚假任务注入攻击)^[57-59]:任务发布者通过发布非法虚假任务诱导任务参与者采集无关的或无效的感知数据。甚至设置无法完成的任务目标来消耗感知平台的资源,占用任务参与者设备的资源(例如电池、传感器、通信带宽和计算资源),从而造成堵塞。通过注入精心设计的任务,任务发布者可以诱导任务参与者提交包含隐私信息的数据,进而推测出任务参与者的身份信息。这样的攻击会干扰系统正常运行,破坏数据质量,并降低任务参与者的积极性。

(2)拒绝付款攻击(虚假报告攻击)^[18-21]:任务发布者在收到任务参与者的感知数据后,恶意声称自己没有收到感知数据或数据质量不达标,甚至通过篡改任务参与者的感知数据来伪造报告,影响感知平台的激励机制,从而拒绝支付报酬。任务发布者在得到感知数据后拒绝支付报酬的恶意行为被称为拒绝付款攻击或者虚假报告攻击。此类攻击通过拒绝支付报酬来降低成本、谋取不正当利益,甚至损害群智感知系统的公平性。

3.1.3 设备管理模块攻击

设备管理模块主要负责对任务参与者使用的智能设备进行认证和状态维护。该模块通过管理设备身份、硬件特征及运行环境等信息,为平台判断用户参与资格、数据来源及激励分配提供依据。然而,恶意任务参与者或者其他外部实体可能通过伪造设备指纹或模拟硬件环境等手段绕过设备认证管理,规避平台对设备型号与能力的校验,从而提交虚假或低质量的感知数据以牟取不当激励。基于上述分析,设备管理模块主要面临以下两类常见攻击。

(1)GPS 欺骗攻击^[31-32,63]:通常由任务参与者或其他外部实体发起,其共同特征是通过伪造或操纵 GPS 信号向系统提供虚假的位置信息。①恶意任务参与者可借助无线电发射器和 GPS 模拟器向感知平台或任务发布者提供虚假的定位数据,通过伪造 GPS 信号使平台误判其处于指定感知区域^[31]或者模拟合法定位信息来截获并篡改其他任务参与者设备接收到的 GPS 信号,从而进一步扩大攻击影响范围^[63]。这种攻击行为具有较强的隐蔽性和破

坏性,不仅会导致感知平台接收到错误的 GPS 信号,还会干扰感知平台的任务分配决策,进而降低整个群智感知系统的数据质量。②其他外部实体可利用无线电发射器和 GPS 模拟器向操纵智能体(智能汽车、机器人以及无人机等)的任务参与者发送强度高于真实信号的伪造 GPS 信号,诱导目标智能体偏离原有路径并按照攻击者预设的轨迹运行^[32]。这种攻击行为不依赖平台内部身份,且通常具备更强的信号覆盖与持续干扰能力,对依赖高精度定位的自动控制系统构成严重威胁。

(2)模拟攻击^[25,64]:通常由任务参与者或其他外部实体发起,其核心目标为冒充合法设备参与感知任务以获取不当收益。①任务参与者通过深度复制目标设备的硬件特征,采用高度相似的设备(如相同型号的手机、手环等智能移动设备),伪装成合法的任务参与者。这种硬件模拟攻击使得任务参与者能够在不拥有规定设备的情况下,假冒合法任务参与者进行数据感知任务。攻击者还可能利用软件层面的漏洞来模拟合法设备的感知数据和行为,比如收集现有的硬件指纹数据并训练自己的模型来模拟硬件行为、对设备上的软件代码进行修改以及使用仿真软件^[64]。通过模拟攻击,任务参与者冒充合法设备参与感知任务并提交虚假数据,以骗取平台的奖励,进而干扰和降低了感知数据的质量,对群智感知系统构成威胁。②其他外部实体通过窃听任务参与者与感知平台之间的通信,解析数据格式和协议,并在此基础上模拟合法任务参与者的行为。这些恶意实体可利用获取到的硬件信息(如 MAC 地址、设备型号等)选取相似或相同的硬件设备进行模拟,伪装成合法任务参与者参与感知任务,从而窃取数据或操纵任务结果。

3.1.4 数据感知模块攻击

数据感知模块是群智感知系统获取真实世界信息的核心环节,负责感知数据的采集、处理与上报。然而,任务参与者及其他外部实体可能在经济利益驱动、不正当竞争或恶意干扰等动机作用下,针对数据感知过程发起攻击,刻意操纵或破坏感知数据。基于上述攻击动机,数据感知模块主要面临以下五类常见攻击行为。

(1)数据投毒攻击(虚假数据注入攻击)^[22,57,65-66,80-81]:在群智感知系统中,数据投毒攻击是指攻击者通过持续或阶段性地注入精心构造的虚假感知数据来干扰数据聚合过程,从而破坏整体数据质量^[65]。该攻击可由任务参与者或其他外部实体发起,其实施方

式与攻击能力因主体角色不同而存在差异。①任务参与者实施数据投毒攻击通常以牟取不当激励或操纵任务结果为目的。攻击者往往并非持续提交异常数据,而是在较长时间内提供高质量、符合统计特征的感知数据以积累较高声誉值,随后在关键任务或特定时段突然注入伪造的感知数据^[80]。攻击者还可能根据平台采用的数据聚合机制与异常检测策略,精心设计投毒数据的幅度与分布,使其在不触发检测阈值的前提下最大化聚合误差^[22,66]。通过此类精心策划的攻击,任务参与者不仅能够注入不真实、伪造或误导性的数据,破坏系统的数据质量,还能借此机会获取不正当利益,对群智感知系统的整体安全构成威胁。②其他外部实体通常不直接篡改已有任务参与者的感知数据,而是利用群智感知系统的开放性,批量引入一组恶意任务参与者作为攻击载体。这些参与者按照统一或协同的攻击策略上传经过精心设计的感知数据,从而在空间、时间或数值分布上形成系统性偏差^[66,82]。相较于单个任务参与者的投毒行为,外部实体可通过多点协同显著放大攻击影响,使聚合结果在全局范围内产生持续性偏移并规避基于单点异常或声誉评估的防御机制。

(2)拒绝服务攻击^[18,20,67]:在群智感知系统中,拒绝服务攻击是指攻击者通过占用或耗尽系统关键资源,导致合法请求被阻塞或延迟,最终破坏系统的正常运行。这类攻击既可能由系统内部的任务参与者发起,也可能来自系统外部实体,其攻击路径与破坏方式存在明显差异。①任务参与者发起的拒绝服务攻击通常以不当获取任务机会或激励为目的。攻击者主要利用平台任务分配的缺陷,在其自身计算、感知或执行能力有限的情况下接受大量感知任务,阻碍了其他任务参与者获取和执行任务。攻击者甚至在接受任务后故意不执行或延迟执行,导致任务无法按时完成,进而造成整个系统的效率大幅下降,甚至面临崩溃的风险^[67]。②其他外部实体实施的拒绝服务攻击则通常以瘫痪系统服务为目标。攻击者通常向感知平台发送大量非法请求,迅速占用计算、存储或通信资源,导致服务器超负荷运行,无法处理系统内部实体的请求。在此情况下,系统将无法及时响应任务发布、任务分配或数据上传等正常请求,导致系统内部实体无法访问关键服务,甚至引发大范围服务中断^[18,20]。

(3)搭便车攻击^[18,20,25-26]:任务参与者在感知任务开始后,迅速提交部分或虚假的数据,尽管他们并未完成整个任务流程,却仍要求获得相应报酬^[20]。

更为恶劣的是,部分任务参与者甚至窃取其他任务参与者的日志系统中真实事件的完整内容,包括事件字段的值和签名,然后重复提交这些感知数据以骗取报酬^[25]。任务参与者利用此类攻击更快地获取报酬,而无需投入大量时间和资源去真正完成任务。

(4)解决方案探测攻击^[21]:在激励机制透明度较高的群智感知系统中(尤其是在基于区块链的群智感知系统^[18]中,所有奖励发放记录均公开可见),解决方案探测攻击成为一种更具针对性与隐蔽性的高级欺诈手段。其本质是攻击者利用激励机制逻辑的公开性与确定性,通过逆向工程手段解析“任务要求-数据质量-奖励回报”之间的隐含映射关系,进而生成能通过验证的伪造数据以骗取奖励。在此基础上,攻击者利用生成模型(如扩散模型、GAN等)生成满足评估规则但并非真实感知的伪造数据,并通过不断试探与优化,使其在不显著影响聚合结果的前提下仍能获得高额奖励。与搭便车攻击不同,解决方案探测攻击针对的是对数据质量要求更高的任务,它并非提交不完整或随机伪造的数据,而是通过伪造符合评估规则的数据来骗取奖励。该攻击对系统的威胁主要体现在两点:一方面,感知平台会在不知情的情况下对大量伪造数据进行奖励分发,导致激励机制被利用,破坏系统公平性;另一方面,伪造数据虽不明显扭曲聚合结果,但长期累积会降低数据真实性,进而侵蚀系统的决策基础与用户信任,影响系统长期稳定运行。

(5)女巫攻击^[16,26,60-62]:任务参与者创建大量虚假账户,操纵多个设备充当独立的任务参与者来发送相似的感知数据,从而提高收益以及声誉等。此外,他们可能通过虚假账户提交不真实或误导性的感知数据,影响感知平台的数据质量和分析结果,同时利用对多个虚假账户的控制,迅速垄断任务资源甚至操纵任务的投标^[60],阻止合法任务参与者获取任务,实现对系统资源的恶意抢占。更进一步,他们通过伪造的虚假账户分散其行为轨迹,阻止系统有效识别其真实身份。

3.1.5 数据存储模块攻击

数据存储模块负责对任务发布者与任务参与者的相关信息进行集中存储与管理,是群智感知系统中承载敏感信息和关键状态的核心组件。然而,在“诚实但好奇”或“恶意”假设下,由于感知平台同时掌握数据存储与管理权限,可能出于经济利益、隐私窃取或控制系统运行结果等动机,主动滥用其权限对存储数据实施攻击,从中得到敏感信息并获取额

外收益。基于上述动机,数据存储模块主要面临以下两类常见攻击行为。

(1)时间关联攻击^[71]:感知平台可以通过数据存储模块中记录的时间相关元信息(如数据上传时间戳、存储访问顺序、查询响应时延等)对同一任务发布者或任务参与者在一段时间内的一次或多次数据提交行为进行关联分析,从而推断其敏感属性。即便感知数据内容经过加密或匿名化处理,感知平台仍可通过分析存储日志与访问时间序列之间的统计相关性,并结合历史时间分布模型,推断用户的敏感信息,重构其时空行为模式,最终推断出用户的位置轨迹和身份特征,导致用户位置隐私和行为隐私的严重泄露。

(2)数据篡改攻击^[20,70]:一旦感知平台破解了存储的任务发布者和任务参与者的信息,可能对这些数据进行修改或伪造。平台可能利用存储和管理权限直接修改任务发布者发布的任务信息或任务参与者的位置信息,破坏他们的声誉。

3.1.6 任务分配模块攻击

任务分配模块负责根据任务需求和任务参与者状态完成感知任务的分配。然而,感知平台作为任务分配的实际执行者,可能出于经济利益最大化或合谋牟利等动机,对任务分配结果进行操纵,从而获取不正当收益或间接掌控感知数据的采集来源与流向。基于上述动机,任务分配模块主要面临以下两类常见攻击行为。

(1)任务分配伪造攻击^[28,72]:感知平台可能在分配过程中故意偏袒某些参与者,优先将高价值任务分配给与平台有合谋关系的任务参与者,将有较大风险的任务分配给特定参与者以故意削弱其竞争力,从而影响任务的公平分配。

(2)身份伪造攻击^[70]:感知平台伪造虚假的任务参与者,或者滥用其他真实任务参与者的身份信息,以此为基础伪装成多个不同的参与者。这些伪造的参与者被优先分配高价值感知任务,从中非法获利。此外,感知平台可能冒充任务发布者发布任务,诱导任务参与者提交感知数据,这些数据可能包含位置信息、环境数据等敏感信息,并且可能被感知平台非法收集和使用。

3.1.7 数据质量评估模块攻击

数据质量评估模块负责对任务参与者提交的感知数据进行质量判定,其评估结果直接影响声誉更新和后续的激励机制。然而,感知平台通常对评估标准及评估结果具有完全控制权,在经济利益最大

化或合谋牟利等动机驱使下,可能滥用其权限对数据质量评估过程进行人为操纵。基于上述动机,数据质量评估模块主要面临以下两类常见攻击行为。

(1)评估操纵攻击^[27,75]:感知平台在数据质量评估模块中具有对评估标准与评估结果的完全控制权。感知平台一方面可能与某些任务参与者共享彼此的信息,根据其感知数据合谋修改奖励函数,从而使这些任务参与者获得不正当的奖励^[75]。另一方面,平台甚至可能通过破坏或篡改部分诚实任务参与者的感知数据、伪造评估结果等手段,使数据质量评估结果偏向特定参与者^[27]。

(2)声誉操纵攻击^[76]:感知平台可能通过控制或篡改任务参与者声誉体系的计算与更新规则,对声誉分数进行恶意操纵,从而影响后续激励机制。具体实施上,平台可在声誉计算模型中调整权重参数或更新策略(如加权平均、指数衰减、贝叶斯更新等),使某些诚实参与者的声誉评分被系统性压低;同时,平台也可能引入或操控多个虚假参与者,通过协同互评、虚假反馈或虚假数据提交等方式同步提升合谋参与者的声誉。通过上述操纵手段,平台能够在任务分配与支付决策中偏袒特定参与者,从而获取不正当利益。

3.1.8 激励机制模块攻击

激励机制模块负责根据任务参与者的实际贡献分配奖励。然而,感知平台可能出于经济利益最大化、策略性压价或获取敏感信息等动机,滥用其权限对激励过程进行分析与操纵。基于上述动机,激励机制模块主要面临以下两类常见攻击行为。

(1)报价推断攻击^[73]:感知平台作为激励机制的执行人,对报价信息与结算过程具有完全可观测性。平台可以整合质量评估后的权重、参与者的历史竞标特征以及最终结算反馈数据,采用贝叶斯概率推断、回归建模或差分分析等技术手段,逆向推导参与者的真实感知成本。即便报价过程采用了隐私保护措施,平台仍可通过观察不同质量水平下的报酬变化规律,捕捉用户报价与其物理开销(如能耗、位移)之间的统计关联。该攻击的主要目的在于使平台获取参与者的私有成本信息,从而利用信息不对称实施策略性压价,以接近参与者心理极限的最低激励成本获取高质量感知数据,实现对用户剩余价值的剥削并扩张平台私利。

(2)交易分析攻击^[74]:感知平台分析区块链上的交易事务,试图识别任务发布者和任务参与者的身份。这种信息可以用于获取这些实体的敏感信息并分析他们的活动模式,得到任务完成情况、奖励获取频率等。

3.2 非主观人为因素

在群智感知系统中,非主观人为因素主要由系统内外客观条件所致,而并非由实体主观意图所致。非主观人为因素包括任务参与者的专业能力不足、人群密度不均、设备功能受限、任务分配失衡以及外部环境干扰等。这些因素虽然没有直接的恶意动机,但依然会对系统可信性造成影响。本小节将探讨非主观人为因素的产生原因及其对群智感知系统可信性的影响,并在表2中对这些因素影响的可信特征进行总结。

表2 非主观人为因素对群智感知系统可信性的影响分析

非主观人为因素	影响的可信特征								
	可用性	公平性	鲁棒性	可认证性	匿名性	可溯源性	真实性	完整性	机密性
专业能力不足 ^[33-35]	○	○	○	○	○	○	●	○	○
人群密度不均 ^[83-85]	●	○	○	○	○	○	●	○	○
设备功能受限 ^[36-37]	●	○	○	○	○	○	●	●	○
任务分配失衡 ^[52,86-87]	●	●	○	○	○	○	●	○	○
外部环境干扰 ^[3,38]	●	○	○	○	○	○	●	●	○

注:●表示非主观人为因素影响了该可信特征。

○表示非主观人为因素没有影响该可信特征。

3.2.1 专业能力不足

任务参与者的专业能力不足可能会在数据感知过程中导致任务理解偏差、设备操作不规范、感知时长不足以及非预期行为干扰等问题^[33-35]。这些问题可能导致任务参与者的感知过程不够充分或者感知数据注入噪声,影响感知数据的真实性。

以环境噪声监测任务为例,专业能力不足主要

体现在以下几个方面^[33]:(1)任务理解偏差:任务参与者可能对环境噪声的概念理解存在偏差。在测量指定区域的环境噪声水平时,部分参与者会主动接近存在人群谈话或车辆鸣笛等区域进行感知,而非指定区域的实际环境噪声。这种概念理解的偏差导致感知数据缺乏代表性,影响系统对区域噪声水平的准确评估。(2)设备操作不规范:由于缺乏必要的

设备操作知识,任务参与者可能在数据感知过程中出现不当操作。如在噪声感知过程中频繁晃动移动设备导致产生风噪或碰撞声,或无意中遮挡设备麦克风等情况,这些操作失误都会导致感知数据质量显著下降或失真。(3)感知时长不足:任务说明中若未明确规定感知持续时间,任务参与者会因理解差异而采用不同的感知时长。部分任务参与者可能仅在指定区域感知若干秒,难以反映指定区域实际的环境噪声。此外,感知时长的不统一使得数据难以标准化处理,增加了数据处理的难度。(4)非预期行为干扰:任务参与者在数据采集过程中可能因知识欠缺而产生非预期的行为干扰,如自言自语或哼唱等行为。这些无意识的非预期行为会引入额外的噪声源,影响感知数据的真实性。

3.2.2 人群密度不均

由于地理、经济和社会等因素的共同作用,人群密度通常呈现出显著的不均衡性^[83]。人群密度不均可能会对系统的时空覆盖范围造成影响^[84-85],并且低人群密度区域的任务参与者的数量不足以满足感知任务的要求,从而导致某些重要区域的感知数据出现空缺。这些感知数据的空缺不仅影响数据的真实性,还使得感知平台在数据融合和分析时受到限制,难以全面反映真实情况。

由于任务参与者的分布受到地理区域的限制,群智感知系统在某些区域或时段难以实现预期的覆盖^[84]。这种时空覆盖范围不足的问题主要源于任务参与者在空间和时间上的不均匀分布:一些区域由于地理偏远、交通不便或人流量稀少,无法吸引足够的任务参与者,而任务参与者在日常生活中通常只在特定区域和特定时段活动。这就造成了群智感知系统在部分区域和时段难以获得连续且全面的感知数据,形成了“感知盲区”。当时空覆盖范围受限时,系统的可用性随之受到影响。在依赖于实时感知数据的场景(例如交通流量监控^[6-7]、环境质量监测^[4-5]等)中,往往需要系统在每个时间节点都能够准确获取最新的感知数据,以便快速应对变化。感知数据的缺失或延迟会导致群智感知系统无法及时反馈和响应,削弱群智感知系统对动态环境的响应能力,从而影响系统的可用性。

3.2.3 设备功能受限

群智感知系统通常依赖于多个设备的协作来完成各种感知任务。然而,这些设备通常资源有限,硬件组件存在局限,容易受到电池电量、计算能力和网络带宽等因素的制约^[36],或者在使用过程中出现硬

件故障^[37]。

设备功能受限不仅会影响单个设备的感知效率和精度,也可能影响设备间的协同效应,导致感知数据丢失或延迟。设备资源受限,如电池电量不足、计算能力有限或带宽不足,会直接导致传感器获取的感知数据质量下降或任务执行的延迟。在群智感知系统中,可能需要多个设备协作完成任务,当某些设备由于资源受限无法及时响应或执行任务时,可能导致数据丢失或不完整。而设备硬件故障,如传感器损坏、处理器故障等,可能导致设备无法正常工作或感知数据失真。尤其是在大规模的动态环境中,设备故障的随机性和不可预测性会削弱系统对异常情况的应对能力,进而影响群智感知系统的可用性。

3.2.4 任务分配失衡

在群智感知系统的任务分配中,部分研究往往聚焦于各种优化目标,如最大化感知任务的分配数量、最小化任务参与者的总移动距离、最大化任务参与者的总收益^[39,88-89]。然而,这些研究往往忽视了任务参与者的技能、偏好以及任务的需求。事实上,任务参与者通常更偏向于接近自己位置、收益较高的任务,而任务发布者则更倾向于招募服务质量更高、成本更低的任务参与者。当任务分配策略未能充分考虑这些个体因素时,可能导致感知任务与任务参与者间的匹配关系不稳定,从而造成任务分配失衡^[86-87]。

当任务分配未能合理匹配任务参与者的技能、偏好和感知任务的需求时,感知任务可能会交由缺乏相应技能的任务参与者执行,导致感知数据质量下降。此外,这种不合理的任务分配方式会增加任务参与者的工作负担,致使他们无法有效完成感知任务,进而影响其收益,导致任务参与者感到不公平的待遇,最终引发人员流失^[52]。与此同时,任务分配失衡还会显著降低任务执行的整体效率,尤其是在任务需求紧迫或任务数量庞大的情况下,系统的响应速度会受到显著影响,从而削弱系统的可用性,使系统难以在动态环境中稳定运行^[86]。

3.2.5 外部环境干扰

在群智感知系统中,外部环境干扰通常指的是恶劣天气条件等自然环境因素^[3],这些因素可能显著影响任务参与者的积极性和设备运行的稳定性,导致感知任务的执行效率和感知数据的质量下降。

在暴雨天气下,任务参与者可能因为恶劣天气不愿意执行交通流量监控或排水状况监控等感知任务^[6-7],使得感知任务的执行面临人员不足的问题,

最终影响感知任务的完成情况。此外,暴雨可能对设备的操作也带来负面影响,例如设备中的传感器可能因湿气、泥泞或积水问题发生故障或失效,进一步加剧了感知任务执行的不稳定性。在高温天气条件下,传感器可能因过热而导致电气元件的精度和性能下降^[38],甚至发生故障。在低温环境下,电池寿命会缩短,使得设备的运行时间显著减少,甚至出现设备无法正常启动或频繁关闭的情况,造成感知数据的不连续性,从而影响感知数据的完整性以及系统的可用性。

4 研究进展与分析

我们在主流文献数据库中开展系统性的关键词检索,检索对象覆盖近 15 年(2012~2026)内发表于国际知名会议与期刊的研究成果。在检索过程中,我们以“crowdsensing”或“crowdsourcing”为核心主题词,并与“attack”、“privacy”、“authentication”、“incentive”、“coverage”、“quality”等关键词进行组合检索,从而覆盖群智感知系统在可信性方面的相关研究工作。在此基础上,我们进一步对入选论文的参考文献与被引文献进行滚雪球检索^[90],以补充可能因关键词差异或发表渠道限制而遗漏的重要相关研究。最后,为确保文献的高度相关性,我们通过论文摘要(Abstract)与引言(Introduction)对所有候选文献进行了人工筛选与质量评估,筛选出最具研究价值的文献纳入综述分析。

针对上述主观人为因素和非主观人为因素对群智感知系统可信性的影响,本节将探讨现有研究针对主观人为因素和非主观人为因素的方法策略,分析这些方法策略的应对效果,并分别从系统层面的可用性、公平性和鲁棒性,实体层面的可认证性、匿名性和可溯源性,以及数据层面的真实性、完整性和机密性对这些方法策略进行总结和对比。

尽管现有研究提出的方法策略考虑到了这些可信特征(在 2.2 节中进行了详细定义),但它们在某些可信特征方面可能存在不足之处。因此,我们将各方法策略对这 9 个可信特征的满足情况分为了三类:未考虑/无法满足(○)、初步考虑/部分满足(◐)以及完全满足(●),如表 3 和表 4 所示。具体而言,在真实性方面,◐表示通过某些技术使感知数据接近真实,但无法保证感知数据在采集过程中未经过任何处理;在完整性方面,◐表示能够处理数据中的缺失部分,但无法防止数据被恶意篡改;在匿名性方

面,◐表示仅对实体的声誉值进行加密,而未加密其身份信息;在公平性方面,◐表示仅考虑了任务分配公平性或激励机制公平性,但没有同时满足任务分配和激励机制等多方面的公平性;在鲁棒性方面,◐表示可以抵御部分恶意攻击行为,但难以应对更复杂或未知的攻击。

4.1 针对主观人为因素的方法策略

在群智感知系统实际运行过程中,系统内外实体可能通过多种方式发起恶意攻击,导致系统面临的安全威胁日益严峻,并对系统可信特征造成实质性破坏。为了有效应对这些主观人为因素,我们将从系统层面、实体层面和数据层面对现有研究策略进行分析,探讨这些方法策略在应对主观人为因素方面的效果,并在表 3^[91-106]中对它们所能达到的可信特征进行总结与对比。

4.1.1 系统层面

(1) 可用性

在群智感知系统中引入一系列隐私保护措施虽然能够提升系统的安全性和隐私性,但可能会对系统的运行效率和服务稳定性带来影响。例如,零知识证明和同态加密等隐私计算技术可能消耗大量的计算和通信资源^[107-108],增加感知平台负载;任务参与者的位置信息在经过噪声干扰或加密处理后,可能会导致任务分配不准确。

现有研究提出使用轻量级的隐私保护技术来解决群智感知系统的安全隐私与可用性之间的冲突。Chen 等人^[91]采用确定性签名和轻量级加密编码,支持高效且可验证的声誉共享,并能够与传统群智感知系统兼容。Wang 等人^[88]提出了基于平面拉普拉斯分布的隐私机制来混淆任务参与者和任务指定区域的真实位置,并确保混淆位置的可用性。在此基础上,通过基于阈值的在线任务分配算法为任务参与者分配任务并规划路径。尽管这些隐私保护技术在理论上为用户匿名性和数据机密性提供了有力保障,但其引入的噪声可能影响感知服务的质量。Zheng 等人^[93]结合秘密共享与基于压缩感知的数据恢复算法,在不接触明文数据的前提下实现了对缺失/噪声数据的高精度补全与校准。Gong 等人^[96]提出了基于方波机制的随机化报告技术,并设计了相应的隐私预算分配算法,有效缓解了隐私保护技术引入的噪声对感知服务质量的负面影响。

(2) 公平性

在群智感知系统中,存在诸多不公平现象。例如,感知平台可能设计不公平的激励机制,导致诚实的

表 3 针对主观人为因素的方法策略的总结和对比

文献	技术路线	方法策略	满足的可信特征								
			可用性	公平性	鲁棒性	可认证性	匿名性	可溯源性	真实性	完整性	机密性
[29]	传统加密技术	基于 Pedersen 承诺的隐私保护机制	○	○	○	○	●	●	●	○	○
[55]		基于短群签名的隐私保护流量监控方案	●	○	○	●	●	●	○	●	●
[68]		基于单向哈希链和可搜索加密的数据请求方案	●	○	○	●	○	○	○	●	●
[81]		基于哈希校验的身份认证机制	○	○	○	●	○	○	○	○	○
[91]		基于确定性签名与轻量级加密的可验证声誉共享机制	●	○	○	○	◐	○	○	○	○
[92]		基于群签名的可控匿名机制	○	○	○	○	●	●	○	○	●
[16]	隐私计算技术	采用 Hadamard 乘积的轻量级隐私保护任务匹配算法	●	○	○	○	●	○	◐	●	●
[19]		基于零知识证明的隐私保护数据质量评估与激励机制	○	◐	○	○	●	○	●	○	●
[27]		基于差分隐私的可验证隐私保护真值发现算法	●	◐	○	○	○	○	◐	●	●
[30]		基于隐私保护的多任务数据聚合方案	●	○	○	●	○	○	○	●	○
[64]		基于硬件指纹的物联网设备识别框架	○	◐	◐	●	○	○	●	○	○
[88]		基于拉普拉斯平面的位置保护任务分配机制	●	○	○	○	●	○	○	○	○
[93]		基于秘密共享与压缩感知的隐私保护数据恢复与校准方法	●	○	○	○	●	○	○	○	●
[94]		基于声誉和零知识证明的隐私保护真值发现框架	●	○	○	○	◐	○	◐	○	●
[95]		基于差分隐私的位置保护频谱感知任务框架	●	○	○	○	●	○	○	○	●
[96]		方波机制驱动的隐私预算分配算法	●	○	○	○	●	○	○	○	●
[20]	区块链技术	基于区块链的隐私保护的数据证明(PoD)机制	○	◐	○	○	○	●	◐	●	●
[97]		基于区块链的链下共识与链上轻量级验证的任务分配机制	●	●	○	○	○	●	○	○	○
[98]		基于区块链的隐私个性化任务分配方案	●	◐	○	●	◐	●	○	○	●
[99]		基于区块链的在线激励机制	○	●	○	○	○	●	○	○	○
[100]		基于子链的区块链感知数据提交与验证优化方案	●	○	◐	○	○	●	○	○	○
[101]		基于区块链的轻量化密钥同步与安全通信协议	●	○	◐	○	○	●	○	●	●
[102]		基于区块链的加密时空属性高效比较方法	○	◐	○	○	●	●	○	○	○
[103]		基于区块链的任务参与者选择机制	○	○	○	○	◐	●	●	○	○
[104]		基于区块链智能合约的感知数据交易机制	○	○	○	○	○	●	○	●	●
[32]	机器学习技术	基于 LSTM 的 GPS 欺骗攻击检测方法	●	○	◐	○	○	○	○	○	○
[52]		基于递归与最近邻算法的任务分配算法	●	◐	○	○	○	○	○	○	○
[105]		防止数据毒化攻击的在线质量学习方法	○	○	◐	○	○	○	◐	○	○
[106]		基于深度学习的数据真实性验证方法	○	○	◐	○	○	○	●	○	○

注:●表示方法策略完全满足该可信特征要求,例如,在匿名性中对实体的身份信息进行加密,完全隐匿其身份。

●表示方法策略初步考虑或部分满足该可信特征要求,例如,在匿名性中仅对实体的声誉值进行加密,而没有对其身份信息进行加密保护。

○表示方法策略未考虑或无法满足该可信特征要求。

表 4 针对非主观人为因素的方法策略的总结和对比

文献	目标模块	方法策略	满足的可信特征								
			可用性	公平性	鲁棒性	可认证性	匿名性	可溯源性	真实性	完整性	机密性
[119]	任务分配模块	基于大规模多设备协作的任务卸载与资源分配策略	●	○	○	○	○	○	○	○	○
[120]		基于公平性约束的任务分配策略	●	◐	○	○	○	○	○	○	○
[121]		基于公平性和分配率的多目标优化任务分配策略	●	◐	○	○	○	○	○	○	○
[122]		基于强化学习的任务分配策略	●	◐	○	○	○	○	○	○	○
[123]		基于大模型的任务分配策略	●	◐	○	○	○	○	○	○	○
[124]		基于图卷积神经网络的信任强化评估框架	●	○	○	○	○	○	◐	○	○
[125]		综合考虑任务需求、参与者偏好以及预算约束的任务匹配算法	●	○	○	○	○	○	◐	○	○
[126]		基于流动性预测的多任务分配算法	●	○	○	○	○	○	◐	○	○
[127]	激励机制	基于 Stackelberg 博弈和拍卖的激励机制	●	◐	○	○	○	○	○	○	○
[128]	模块	基于比例公平和博弈理论的激励机制	○	◐	○	○	○	○	○	○	○
[129]		基于深度强化学习的激励机制	●	◐	○	○	○	○	○	○	○
[38]	数据感知模块	基于设备置信度的真值发现算法	●	○	○	○	○	○	◐	○	○
[130]		采用贝叶斯压缩感知的城市信号地图感知系统	●	○	○	○	○	○	◐	◐	○
[131]		基于时空覆盖的多目标优化策略	●	○	○	○	○	○	○	◐	○
[132]		基于环境矩阵和传感器矩阵的数据重建	○	○	○	○	○	○	○	◐	○
[133]		采用自适应集群与动态参数优化相结合的数据感知策略	●	○	○	○	○	○	○	◐	○
[134]		基于深度压缩感知的数据插补框架	○	○	○	○	○	○	○	◐	○
[135]		基于自适应超图的期望最大化真值发现算法	●	○	○	○	○	○	◐	○	○

注:●表示方法策略完全满足该可信特征要求,例如,在公平性中同时满足任务分配和激励机制等多方面的公平性。

●表示方法策略初步考虑或部分满足该可信特征要求,例如,在公平性中仅考虑到了任务分配公平性或激励机制公平性。

○表示方法策略未考虑或无法满足该可信特征要求。

任务参与者在提交感知数据后遭遇拒绝付款攻击,甚至包庇恶意的任务参与者重复提交感知数据骗取报酬^[18]。此外,感知平台可能提供不公平的任务分配,部分任务参与者可能被分配了过多的任务,长期承担高负荷工作可能导致其疲劳,从而降低服务质量;而任务量过少的参与者则难以获得足够的报酬,未能实现其应有的价值回报。这种任务分配失衡现象可能导致任务参与者的收益不平衡,进一步影响系统的公平性^[52]。

现有研究针对任务分配公平性和激励机制公平性展开了研究。Zhang 等人^[52]提出效用公平指数,通过公平感知的任务分配实时为任务参与者规划任务,最大化整体效用并保障任务参与者的公平性。然而,更多的研究则提出了去中心化的群智感知系统来避免对中心化平台的依赖^[20,98-99]。Wu 等人^[98]提出了一种区块链辅助、可验证的个性化隐私保护任务分配策略(VP²-Match)。该策略将个性化任务匹配问题简化为联合范围和子集查询,并通过扩展的对称隐向量加密,在加密的任务参与者信息和任务需求之间实现高效的相等、比较和子集匹配,从而保证了任务参与者和任务发布者之间的双重隐私保护,提升了任务匹配的灵活性,同时确保了系统的公平性。Huang 等人^[20]提出的 BlockSense 群智感知系统依托区块链矿工验证感知数据的质量。矿工需通过工作量证明来获得经济奖励,而任务参与者通过提交高质量的感知数据来获得经济奖励。当任务参与者按照要求完成感知任务后,智能合约会自动给予经济奖励,从而杜绝搭便车攻击或拒绝付款攻击。Fang 等人^[99]提出了基于区块链的在线激励机制,以保障任务发布者与任务参与者之间的经济公平,并动态调整任务发布者与任务参与者的声誉,从而抵御潜在的搭便车攻击或拒绝付款攻击。然而,现有研究通常聚焦于任务分配或激励机制中的某一方面,忽略了二者之间的关联。例如,合理的任务分配策略可以提升任务参与者的积极性,但若激励机制设计不当,可能导致参与者的行为偏离预期目标,从而影响感知任务的执行质量,最终影响系统的公平性。因此,任务分配和激励机制需要协同优化,共同确保系统的公平性。

(3) 鲁棒性

群智感知系统正遭受多种潜在攻击的威胁,具体包括由恶意任务发布者、任务参与者或其他外部实体发动的拒绝服务攻击^[18,67]、数据投毒攻击^[22,82]以及模拟攻击^[25,64]等。这些攻击手段不仅干扰了

系统日常稳定运行,还降低了系统的鲁棒性。

为应对这些威胁,现有研究提出了多种防御策略来增强群智感知系统的鲁棒性^[32,64,100,105]。Sun 等人^[100]提出了基于区块链的群智感知系统来抵御由拒绝服务攻击引起的单点故障问题,并利用子链来减轻主链感知数据提交和交易验证的压力,但是区块链上公开可见的任务发布者和任务参与者间的交易事务可能导致敏感信息泄露^[74]。Zhao 等人^[105]利用在线质量学习算法来学习任务参与者的感知数据的质量,寻找声誉较高的任务参与者,并筛选声誉较低的恶意任务参与者。然而,这种策略并无法确保感知数据的真实性,只是在一定程度上缓解了数据投毒攻击带来的危害^[22]。Xiao 等人^[64]提出了基于硬件指纹的 MCU-Token 身份验证机制,结合硬件指纹和机器学习来生成设备的唯一访问令牌,并将访问令牌与中毒数据混合在一起,防止攻击者使用泄漏的令牌来训练模型。Wang 等人^[32]提出基于长短期记忆(LSTM)机器学习算法的 GPS 欺骗攻击检测方法。该方法利用 LSTM 算法每隔固定时间记录无人机的速度、方向及其与起点的距离,根据这些数据预测无人机的未来飞行轨迹。同时,提前设计若干可能的飞行轨迹,一旦无人机接收到的 GPS 定位信号偏离当前轨迹,就可以在短时间内准确、快速地检测出无人机受到了 GPS 欺骗攻击。尽管这些防御策略在特定场景下能够有效缓解部分攻击,但群智感知系统面临的攻击手段种类繁多且不断演化。同时,现有的防御策略在应对不同攻击场景时的泛化能力有限,难以提供全面的保护。

4.1.2 实体层面

(1) 可认证性

在群智感知系统中,未经身份认证的恶意实体(任务发布者或任务参与者)可能通过系统漏洞提交无效感知任务或虚假感知数据。同时,系统资源可能被滥用,任何实体都可以随意访问敏感信息或执行关键操作,难以进行责任追踪。

为了确保实体行为的可验证,防止未授权的实体访问系统数据或执行敏感操作,现有研究提出了多种身份认证方案。Zhang 等人^[81]利用哈希函数计算实体身份信息的哈希值,并以哈希值校验实现身份认证,确保只有合法实体才能发布任务或参与任务。同时,得益于哈希函数的单向性^[109],感知平台及恶意实体无法通过观察到的哈希值伪造他人身份。与此类似,Zhu 等人^[68]采用单向哈希链来实现轻量级身份认证,确保只有合法实体拥有有效的哈

希链节点以发布或参与任务。此外,基于硬件的身份认证方案也被广泛应用于群智感知系统。安全芯片(例如 Trusted Platform Module)^[110]通过提供硬件级别的密钥管理和身份验证来保障实体的可认证性。生物识别传感器(例如指纹识别)^[111]可以在身份认证过程中确保实体身份的唯一性,有效防止身份伪造等攻击。尽管这些基于硬件的方案能在不同维度保障实体的可认证性,然而在移动设备上实现这些技术仍然面临不少挑战,主要包括可信执行环境与安全芯片的功耗、成本以及生物识别传感器引发的隐私风险。因此,研究的突破口可能在于解决这些硬件在资源受限的移动设备上的功耗和成本问题,同时提升其安全性与兼容性,以推动基于硬件的身份认证在群智感知系统中的大规模应用。

(2) 匿名性

在群智感知系统中,任务发布者和任务参与者的匿名性一旦被破坏,不仅可能导致个人信息的泄露和滥用,还会引发身份盗用和报复行为,显著降低这些实体的积极性。

为了保护任务发布者与任务参与者的匿名性,现有研究普遍采纳了假名技术、差分隐私技术以及区块链技术等。Cheng 等人^[16]利用 Hadamard 乘积和 k-匿名技术来保护任务参与者的位置隐私和身份隐私。他们引入了可信的声誉中心为每个任务参与者分配声誉值和假名,并根据任务结果的反馈来更新这些声誉值和假名,从而确保任务参与者的匿名性得以持续维护。此外,还采用了 Hadamard 乘积和 k-匿名技术来保护任务参与者的位置隐私。Jin 等人^[95]针对频谱感知任务,提出了一个名为 DPSense 的群智感知框架。DPSense 采用了差分隐私技术^[112],通过扰乱任务参与者的移动轨迹来达到位置差分隐私,从而在保护隐私的同时,也确保了系统的整体效率。Yang 等人^[102]在基于区块链的群智感知系统中设计了一种简洁且安全的比较方法,可对加密的空间与时间属性进行高效的子集与范围比较,在实现精确时空匹配的同时,保障任务发布者与任务参与者的双重隐私。然而,这些匿名保护技术仍存在不足:假名技术依赖中心化管理,容易受到拒绝服务攻击引起的单点故障问题影响;差分隐私技术^[112]引入噪声可能导致身份认证准确性下降;基于区块链的方案计算和存储开销较大,难以在资源受限的移动设备上高效运行。

(3) 可溯源性

感知平台发起的攻击通常源于其内部操作,隐

蔽性强且难以外部溯源;而任务参与者通过实施女巫攻击,即伪造多个虚假账户同时参与任务以规避监管,分散其行为轨迹,掩盖真实身份。这些攻击行为破坏了群智感知系统的可溯源性,使得恶意行为难以被准确追踪。

为了保护实体的身份隐私,群智感知系统往往会采用匿名化技术,而此类技术在保障实体身份隐私的同时也增加了实体行为追溯的难度,因此需要在匿名性和可追溯性间进行权衡与优化。Li 等人^[55]通过短群签名^[113]实现了任务参与者的有条件匿名身份验证,允许在发生恶意行为时追踪参与者的真实身份。尽管任务参与者身份对系统而言是匿名的,但系统在检测到数据中毒等恶意行为时,仍可通过追踪特定签名识别恶意任务参与者。Song 等人^[92]为了确保诚实任务参与者的匿名性以及不诚实任务参与者的可追溯性,引入群签名机制为群成员分配群密钥,使实体在提交感知任务或感知数据时能够生成不可关联的匿名签名^[114]。当实体出现恶意行为时,群成员中的授权开放管理者利用预设的溯源密钥,解除特定签名的匿名性并揭露恶意行为发起实体的身份,实现可溯源性。Zeng 等人^[97]提出了基于区块链的去中心化任务分配方案,通过在链下达成全局最优任务分配方案的共识,并利用区块链的去中心化、防篡改和公开透明特性在链上验证任务分配结果的合法性以及实体行为,当检测到恶意行为时,智能合约自动触发溯源流程,并结合不可篡改的链上记录追踪实体身份。

4.1.3 数据层面

(1) 真实性

在群智感知系统中,部分自私的任务参与者可能为谋取更多的利益而故意提交伪造的感知数据,严重威胁到数据的真实性^[106]。更令人担忧的是,感知平台出于自身利益考量,可能会与任务参与者合谋,联手伪造感知数据,进一步加剧数据真实性面临的挑战与风险。

群智感知数据真实性问题已引起广泛关注,现有研究工作利用隐私计算、区块链以及深度学习等技术提出了多种解决方案。Tong 等人^[29]引入 Pedersen 承诺机制对任务参与者的竞标等敏感信息进行保护,在确保隐私不泄露的同时支持后续结果的完整性验证。Gao 等人^[103]提出了基于区块链的群智感知系统 TrustWorker,利用区块链的去中心化、透明性与不可篡改特性使任务参与者的选择过程具备可信保障,从而提供真实可靠的感知数据。Zhou

等人^[106]提出了基于深度学习的数据真实性验证方法,他们基于 ImageNet 等可用数据集^[115],利用旋转、剪切和黑色遮挡等随机操作来修改数据真实性并生成训练所需的伪造数据,实现伪造数据的自动检测。然而,现有方法策略大多是在获得感知数据后筛选伪造数据,而非从源头上防止数据造假行为的发生,使其在面对合谋攻击、女巫攻击以及数据中毒攻击联合的复杂攻击时容易失效。

(2)完整性

感知平台在感知任务和感知数据等关键信息的传输与处理过程中占据主导地位。然而,出于利益驱动,平台有可能采取非法手段,诸如篡改任务请求、感知数据或数据质量评估结果,进而严重损害数据的完整性^[27]。

当前研究正积极探索以数字签名、区块链以及算术电路为主的技术来确保群智感知中数据的完整性。Yan 等人^[30]通过数字签名来确保感知任务在传输过程中不被篡改,同时,通过数据收集阶段生成的哈希值和数据聚合阶段使用的数字签名来保证感知数据在传输过程中的完整性。An 等人^[104]受到区块链不可篡改和透明特性的启发,将感知任务以智能合约的形式发布。智能合约固有的不可篡改特性在源头上遏制了感知任务被篡改的风险^[116]。同时,他们通过验证链上数据摘要是否正确来检查获取的(加密)感知数据是否被篡改。Xu 等人^[27]通过基于算术电路的公开验证技术^[117]来验证平台的数据质量评估中获取的感知数据是否完整以及最终返回的结果是否被篡改。

(3)机密性

感知任务和感知数据等关键信息在传输和处理过程中,恶意实体可能会拦截通信过程中的信息,或者伪装成合法实体对敏感数据进行篡改或窃取,对感知任务和感知数据的机密性造成威胁。

为确保数据机密性,常见策略包括使用对称加密或代理重加密来保护感知数据^[41],但这些策略在保护数据隐私的同时,往往难以兼顾数据质量的验证。为此,现有研究逐渐转向隐私计算技术。Zhao 等人^[19]提出了感知数据质量评估的零知识证明模型,该模型在不泄漏感知数据内容的情况下有效地检验了数据是否满足任务发布者的要求。Cheng 等人^[94]设计了基于声誉的隐私保护真值发现框架 PRTD。PRTD 采用 Paillier 算法来保护感知数据隐私,并利用 Pedersen 承诺来保护声誉值隐私,最后通过任务参与者的声誉和感知数据聚合推导出准

确的真值,其中真值发现旨在从多个可能存在噪声或偏差的感知数据中推断出最接近真实值的聚合结果。考虑到群智感知系统中通信资源的限制,Ding 等人^[101]提出密钥同步更新算法 TXLKS 和安全通信协议 LCPT,更加适合资源受限的智能移动设备。然而,许多隐私保护方法(如零知识证明、同态加密等)在资源受限的设备上计算开销较大,无法适用于实时性要求较高的场景;而差分隐私^[118]等技术通过添加噪声来保障数据的机密性,可能造成数据精度丢失。

4.2 针对非主观人为因素的方法策略

在群智感知系统中,非主观人为因素通常会影响到数据的真实性、完整性,以及系统的可用性、公平性和鲁棒性,但对数据的机密性以及实体的可认证性、匿名性和可溯源性并没有影响,如表 5 所示。因此,我们将从系统层面和数据层面对现有研究进行分析,深入探讨这些方法策略在应对非主观人为因素方面的效果,并在表 4^[119-135]中对这些方法策略所能达到的可信特征进行总结和对比。

4.2.1 系统层面

(1)可用性

在群智感知系统中,非主观人为因素,如人群密度不均、设备功能受限以及外部环境干扰等,可能对系统的可用性造成影响。人群密度不均会导致系统在部分区域和时段无法获得连续且全面的感知数据,影响群智感知系统的时空覆盖范围^[84-85];设备功能受限可能导致任务参与者无法及时响应和有效执行感知任务^[36];外部环境干扰(如暴雨天气)可能影响任务参与者执行任务的积极性,而无法及时提供感知服务^[3]。

为了解决人群密度不均(尤其是任务参与者稀缺)的问题,现有研究提出了稀疏群智感知(Sparse Crowdsensing)策略^[136-137]。该策略旨在在任务参与者数量较少的情况下,通过优化感知任务分配和数据感知策略,最大化有限任务参与者所能提供的时空覆盖范围,从而实现高效的感知数据采集和覆盖。He 等人^[130]提出了基于稀疏人群感知的城市信号地图感知系统,该系统使用贝叶斯压缩感知^[138]来预测某些感知区域缺失的信号值,并提供信号预测值的置信区间。Dinh 等人^[131]引入了时空覆盖(Spatial-Temporal Coverage)的概念来量化感知区域的面积(空间覆盖)和感知区域的持续时间(时间覆盖)。通过制订多目标优化问题,确定任务参与者(车辆)的最佳感知对象(空气质量)监测频

表 5 可信特征之间存在的冲突与权衡分析

可信特征	存在冲突的可信特征	冲突原因分析	权衡技术方案
可用性	鲁棒性、机密性	为保障群智感知系统的可用性,可能需限制防御机制与数据加密强度,进而可能削弱系统鲁棒性和数据机密性	在群智感知系统中,采用轻量级加密与边缘节点局部防御,动态调整防御强度,并通过神经网络剪枝进行高效异常检测,根据系统负载灵活启用深度攻击检测机制
公平性	匿名性	为保障任务分配和激励机制的公平性,群智感知系统可能需要关联实体行为与身份,从而降低匿名性保护	引入深度学习异常行为检测模型,从海量匿名任务日志自动识别恶意行为,并结合假名声誉机制和零知识证明,在保障身份隐私的前提下实现贡献驱动的公平任务分配与激励机制
鲁棒性	可用性	增强系统鲁棒性可能需要全面部署攻击检测与防御机制,但这会增加系统负载并降低可用性	通过在线/增量学习模型快速识别新兴攻击,配合边缘局部防御与动态防御调节,在群智感知系统中根据负载灵活启用深度检测机制以减少误报和无效检测
可认证性	匿名性	为了实现身份可认证,群智感知系统可能需要部分公开身份信息,从而影响匿名性保护	在群智感知系统中,通过图神经网络挖掘参与者行为关联,发现潜在合谋行为,同时采用假名声誉和零知识证明,实现身份合法性验证而不泄露真实身份
匿名性	公平性、可认证性、可溯源性、真实性	为了保护任务发布者和参与者的匿名性,系统难以基于身份进行公平任务分配,恶意实体的行为难以溯源,且无法验证感知数据的真实性	采用可控匿名机制,在正常任务执行阶段保持匿名,在检测到恶意行为或争议时由授权实体撤销匿名
可溯源性	匿名性、机密性	为实现可溯源性,系统可能需要关联任务提交记录与参与者身份,从而限制实体匿名性和数据机密性	通过区块链加密存储群智感知行为日志,并结合安全多方计算实现隐私保护下的行为审计,恶意行为确认后可条件解密进行实体溯源
真实性	匿名性、机密性	为实现数据真实性验证,可能需要暴露部分身份或数据来源信息,从而影响实体匿名性和数据机密性	通过真值发现算法处理加密冲突数据,并利用承诺机制、匿名签名和零知识证明,实现匿名环境下的数据真实性验证,无需泄露参与者身份或数据内容
完整性	机密性	为确保数据完整性,系统可能需要访问部分明文或元数据,从而限制数据机密性	采用分级加密配合 Merkle 树和零知识证明,实现密文感知数据的完整性验证,并通过神经网络进行篡改检测和异常模式识别
机密性	可用性、可溯源性、真实性、完整性	端到端加密提升了数据机密性,但增加计算开销降低系统响应速度,同时隐藏数据来源使真实性难以验证,密文状态下细粒度篡改检测受限,恶意行为难以追溯	在群智感知系统中,采用轻量加密和压缩感知降低数据传输开销,并通过分级加密策略对敏感信息进行保护,仅最小必要信息用于验证与溯源

率,以最大化时空覆盖范围、最小化成本并平衡车辆负载,从而在各种复杂时空条件下提供稳定和可靠的感知服务,提升群智感知系统的可用性。

为了解决设备功能受限和外部环境干扰导致的任务响应不及时问题,现有研究在群智感知系统架构方面采用边缘计算^[139]来降低延迟、提高任务响应速度,在系统策略方面设计激励机制^[12]来提升任务参与者的积极性。Zhou 等人^[119]利用边缘计算技术将感知范式从集中式基础设施扩展到分布式网络边缘,减少了可有可无的网络跳数并降低了传输延迟。边缘计算通过将感知任务和感知数据从感知计算平台转移到更靠近任务参与者的边缘节点(如边缘服务器或网关)进行处理,从而加快感知任务响应速度并减少网络传输延迟。Yang 等人^[127]指出可以通过设计激励机制让任务参与者获得满意的奖励来补偿其资源消耗,该策略也可以用来补偿其因外部环境干扰而导致的更高资源消耗(例如电池快速耗尽和网络流量增加)。然而,激励机制在应对复杂多变的外部环境时,可能无法动态调整奖励策略,导

致任务参与者的积极性波动较大。

(2)公平性

在群智感知系统中,任务分配和激励机制的设计对系统的公平性至关重要,而系统的公平性则是维持任务参与者积极性和感知服务长期稳定运行的关键因素^[140]。然而,由于感知平台在任务分配时未能充分考虑任务参与者的技能、偏好和位置等因素,可能会导致任务分配失衡^[86-87]。这种失衡表现为任务过度集中分配给少数任务参与者,而其他参与者则因任务稀缺或不匹配而处于闲置状态,从而引发后者对任务分配公平性的质疑,还会削弱其积极性,从而影响整个系统的稳定运行。为了保障群智感知系统的公平性,除了优化任务分配策略外,设计合理的激励机制也是关键,通过合理的奖励分配来激发任务参与者的积极性。基于此,现有研究主要从任务分配和激励机制两个方面探索如何保障群智感知系统的公平性。

现有研究提出了多种策略来提升群智感知系统中的任务分配公平性,以减少任务参与者之间的收

益差异和任务分配不均衡问题。Chen 等人^[120]设计了工人公平成本(Worker Fairness Cost)指标,通过计算任务参与者应得的经济奖励与实际分配的经济奖励之间的差异,旨在最小化所有任务参与者之间的最大公平成本。Basik 等人^[121]提出了两阶段分配模型,用于确保任务参与者在执行众包配送任务(如在线购物和按需本地配送)时的诚实性,同时兼顾任务分配的公平性和完成率。Shi 等人^[122]利用强化学习策略,适应高度动态的大规模任务分配场景,克服了传统算法的短视性问题。此外,许多研究也在探索自适应任务分配模型^[87,140],通过结合任务参与者的技能、偏好和位置等动态特征,提升任务分配的灵活性与公平性,同时构建了多目标优化框架以在公平性、整体效率和成本之间实现平衡。Guo 等人^[123]利用大语言模型对任务发布者的需求与任务参与者的偏好进行解析与整合,使参与者能够直观理解任务分配逻辑并提升分配过程的透明性,从而实现高效且公平的任务分配。这些策略不仅确保了任务分配的公平性,还关注群智感知系统的整体效能,从而增强了任务参与者的积极性并保障了系统的长期稳定运行。

此外,激励机制的设计对于提升群智感知系统的公平性同样至关重要。为了确保任务参与者在不同策略下能够获得合理的经济奖励并激发他们的积极性,现有研究尝试引入多种方法来优化激励机制。Lu 等人^[128]将比例公平引入激励机制,旨在减少对感知平台的过度干预,尤其在面对理性和自私的任务参与者时,能够更好地平衡参与者的策略选择。通过这种方法,群智感知系统能够在最大化社会效益的同时,以最小的成本保持系统的公平性。Wang 等人^[129]提出了基于深度强化学习的激励机制,综合考虑任务参与者的贡献、设备资源和感知任务等因素。该机制能够根据任务参与者的历史表现和技能偏好动态调整激励,进一步提升任务参与者的积极性并优化系统的公平性。由此可见,激励机制的研究越来越注重自适应和动态调整,从而在复杂多变的感知环境中保障系统的公平性。

4.2.2 数据层面

(1) 真实性

由于任务参与者的专业能力、人群密度、设备功能、任务分配以及外部环境等非主观人为因素的影响,感知数据常常面临失真或不准确的问题,从而降低其真实性。为应对这些非主观人为因素带来的挑战,现有研究提出了多种技术与策略,其中真值发

现^[141]和任务匹配优化^[3]是关键的研究方向。真值发现通过整合多个任务参与者的感知数据,推导出接近真实的感知数据,有效应对了专业能力不足、设备功能受限和外部环境干扰等问题;而任务匹配优化则根据感知任务的需求、任务参与者的技能、偏好以及设备资源,为每个感知任务分配最合适的任务参与者,从而最大化任务参与者的能力与资源利用,减轻因人群密度不均或任务分配失衡对数据真实性的影响。

真值发现通过整合不同任务参与者的感知数据来推导出接近真实的感知结果,极大地缓解了由于任务参与者的专业能力不足、设备功能受限以及外部环境干扰等非主观人为因素导致的数据真实性下降问题。例如,Chen 等人^[38]在温度感知任务中提出了基于手机状态特征的真值发现方法。该方法将易于获取的手机状态特征作为输入,生成带有置信度的环境温度预测值。同时构建了真值发现模型,将多个带有置信度的预测结果进行聚合,以得出更为真实的环境温度值,从而有效提升了感知数据的真实性。然而,任务参与者通常面临时间限制和成本约束而只能完成部分感知任务,这导致现实场景中的感知数据集往往呈现出高度稀疏性。针对大多数真值发现方法在处理稀疏数据集时表现不佳的问题,Wang 等人^[135]提出了基于自适应超图的期望最大化真值发现算法(HGEM)。该算法通过利用超图的独特拓扑结构,对稀疏数据集进行更精细的建模,从而显著提升了在任务参与者声誉评估和感知对象真值推断方面的准确性,更有效地适应了不同数据稀疏度的场景。

任务分配优化的核心目标是根据任务的需求、任务参与者的技能、偏好和设备资源,合理匹配感知任务和参与者,以确保任务高效完成并满足质量要求,保障感知数据的真实性。Yin 等人^[125]提出了针对多对一任务分配问题的优化方案,旨在解决具有不同质量要求和预算限制的任务如何高效分配给不同技能和偏好的任务参与者。该方法通过考虑质量下限、预算上限以及任务参与者技能水平的不同,设计了稳定的匹配机制,为每个任务合理分配最合适的参与者,确保任务既能满足质量要求,又不超出预算限制,从而实现资源的高效利用。Zhang 等人^[126]提出基于流动性预测的群智感知多任务分配算法,通过模糊逻辑系统来分析任务参与者的历史轨迹,从而准确预测其未来的流动性。基于流动性预测结果,他们设计了全局启发式搜索算法将感知任务分

配给时空特征重叠度较高的任务参与者。Zhan 等人^[124]提出了基于图卷积神经网络的信任强化评估框架来优化任务执行的效果。该框架综合考虑工作人员的技能、声誉和位置等,通过图卷积网络有效地构建任务参与者之间的关系,为每个感知任务招募最合适的任务参与者来协作执行复杂的感知任务,确保感知数据的真实性。

(2)完整性

设备功能受限^[36-37]和外部环境干扰^[3,38]往往会导致感知数据在采集、处理和传输过程中出现丢失,从而破坏数据的完整性。例如,由于电池电量不足或存储空间受限,设备可能无法完整记录或传输感知数据,导致关键数据信息的缺失;网络信号不佳或带宽限制可能引发数据包丢失;智能体的高速运动和网络连接的不稳定性导致感知数据在传输过程中面临较高的丢包率。

现有研究主要采用插值法、边缘计算和深度学习等多种技术手段,致力于解决动态环境中感知数据丢失问题。Kong 等人^[132]提出了一种基于插值法的数据重建方法,通过最小化重建矩阵与真实环境矩阵之间的误差,有效修复丢失的数据,从而尽可能还原完整的感知数据。同时,他们深入分析了多种常见的数据丢失模式,如随机丢失、块丢失和连续丢失等,针对不同的丢失模式优化重建算法。Liu 等人^[133]针对车载感知系统中的数据丢失问题,结合边缘计算技术,提出了一种自适应集群与动态参数优化相结合的双重策略。该方法通过动态调整车辆间的集群结构,确保通信质量较好的车辆优先分组,从而减少因车辆移动和网络不稳定性带来的数据丢失风险。此外,在线感知参数调整机制能根据网络状况实时优化数据采集参数,进一步减少不必要的数据传输,有效规避丢包问题。Chang 等人^[134]针对环境质量监测中的感知数据丢失问题提出了一种基于深度压缩感知的数据插补框架,通过压缩感知技术有效减少数据冗余,再结合深度神经网络从部分感知数据中推断缺失的数据。然而,这些方法在面对大规模部署和实时处理时,往往存在较高的计算复杂度和资源消耗,限制了其在广泛应用中的可行性。

4.3 对比分析与小结

结合上述,我们进一步对现有方法策略进行对比分析,以便更清晰地呈现不同方法策略的适用场景与局限性。针对主观人为因素的方法策略,我们在表 3 中进行了总结和对比,并以技术路线为维度

进行分类,系统比较了传统加密、隐私计算、区块链与机器学习等技术路线在可信特征上的权衡关系;鉴于非主观人为因素通常由系统内外客观条件引起且与特定系统模块直接相关,我们在表 4 中按任务分配、数据感知以及激励机制等目标模块进行分类,并对现有方法策略进行了总结与对比;最后,我们在表 5 中系统梳理了群智感知系统中九个可信特征之间的冲突关系,并对不同可信特征冲突的原因及相应权衡技术方案进行了分析和总结。

表 3 涵盖了传统加密技术、隐私计算技术、区块链技术与机器学习技术,并从可用性、公平性、鲁棒性、可认证性、匿名性、可溯源性、真实性、完整性与机密性九个可信特征对这些技术实现的方法策略进行评估:(1)传统加密技术(如哈希校验、群签名)^[81,113]适用于对实时性要求高、参与节点资源受限的轻量级身份认证与消息完整性保护,能够在较低开销下提供较强的可认证性或匿名性保障,但在复杂数据流转与多方协作场景中,单纯依赖加密难以实现端到端的隐私保护,其机密性与匿名性能力也较弱。(2)隐私计算技术(如零知识证明、差分隐私)^[107-108]在匿名性与机密性上具备显著优势,能够在群智感知的开放参与环境中有效降低用户隐私泄露风险,适合对敏感数据(如位置、行为轨迹、健康信息等)有严格保护需求的场景;但其计算与通信开销较高,难以直接应用于资源受限的移动终端或对实时性要求强的任务(如突发事件感知、实时交通监测),并且在参数配置不当时可能引入额外的准确性损失。(3)区块链技术^[103-104]通过去中心化账本与共识机制实现多方协作中的公平性与可溯源性,能够有效支撑群智感知系统中的数据来源追溯与审计需求,适用于需要透明审计、长期可追溯的感知场景;但其共识机制带来的时延、存储冗余与能耗开销较大,在高频数据上传或实时感知任务中存在明显瓶颈,并且链上数据不可篡改的特性可能导致隐私数据面临长期暴露风险,需要结合链下存储与访问控制机制共同设计。(4)机器学习技术(如 LSTM、深度学习)^[32,106]在识别异常行为与验证数据真实性方面具有自适应能力,但其性能高度依赖训练数据的质量,且在群智感知系统中容易受到数据投毒、模型中毒等攻击影响。

表 4 总结和对比了任务分配模块、激励机制模块与数据感知模块中的现有方法策略,这些方法策略并未将恶意攻击行为作为主要考量对象,而是面向群智感知系统的关键功能模块优化。具体而言,(1)在任务分配模块中,基于多目标优化的方法^[121,125]

能够在公平性与可用性之间实现可控权衡,但其模型构建与参数调优过程较为复杂,通常适用于优化目标明确、约束条件可形式化描述的场景;基于强化学习与深度强化学习的方法^[122,124]可通过持续交互自适应优化任务分配,在一定程度上缓解动态行为带来的分配偏差,有助于提升长期运行系统中结果的真实性,但其训练成本高、收敛较慢;基于大模型的方法^[123]在理解用户意图和复杂任务描述方面具有优势,可降低因语义误解引入的非真实性风险。(2)在激励机制模块中,基于 Stackelberg 博弈的方法^[127]能激励真实参与,但博弈求解复杂,适合参与者理性且数量适中的场景;基于比例公平的方法^[128]实现简单,但可能无法充分激励高质量贡献,适合对公平性要求高的场景。(3)在数据感知模块中,现有研究常采用贝叶斯压缩感知^[130]与矩阵重建技术^[132]解决数据缺失与不完整问题,适用于感知节点稀疏或覆盖不均的场景。这些方法能够利用数据的稀疏性或低秩结构进行重构,但在大规模高维数据场景下收敛速度与计算开销仍是瓶颈。另一些研究采用真值发现技术^[38,135]从多源数据中提取高精度观测值,从而有效应对传感器精度波动和噪声干扰导致的不真实风险。

表 5 系统分析了群智感知系统中九个可信特征之间的冲突原因与权衡方案。分析表明,这些特征并非相互独立,而是存在复杂的权衡:可用性与鲁棒性、机密性之间存在性能与安全的权衡,防御机制和加密操作会影响系统响应速度;公平性与匿名性之间存在身份验证与隐私保护的权衡,公平分配需要身份信息但匿名性要求隐藏身份;匿名性与可认证性、可溯源性、真实性之间存在隐私保护与责任追究的权衡,匿名保护会削弱身份验证、行为追踪和数据来源确认能力;机密性与可用性、可溯源性、真实性、完整性之间存在加密强度与系统功能的权衡,端到端加密增强安全性但增加计算开销并阻碍数据共享与验证。针对这些冲突,我们在表 5 中提出了融合传统加密技术、隐私计算技术与非安全隐私技术(如机器学习、真值发现、压缩感知等)的综合权衡方案,例如采用轻量级加密与边缘节点局部防御来平衡可用性与鲁棒性,利用深度学习模型从匿名日志中检测异常行为以兼顾公平性与匿名性,通过可控匿名机制在正常执行时保持匿名而在检测到恶意行为时撤销匿名以平衡匿名性与可溯源性,结合区块链加密存储与安全多方计算实现隐私保护的行为审计以平衡可溯源性与机密性。

由此可见,表 4 所列方法策略侧重于对群智感知系统核心功能模块的优化,在提升系统可用性与公平性以及保障数据真实性与完整性方面发挥了基础性支撑作用;然而,在群智感知系统实际运行过程中,系统内外实体可能通过多种方式发起恶意攻击,上述机制往往难以单独应对由恶意实体发起的攻击行为。因此,仍需与表 3 中面向主观人为因素的防御策略协同设计与联合部署,才能实现群智感知系统可信性的整体提升。需要注意的是,即便如此,这些权衡技术方案仍无法确保群智感知系统中所有可信特征在同一时间得到完全满足。因此,在系统的可信性设计与研究中,需要根据具体应用场景综合分析各可信特征之间的冲突与优先级,并在实际部署过程中动态调整策略以实现最优折中。

5 未来研究方向

随着群智感知系统应用场景的不断拓展,系统面临的挑战日益复杂,尤其是非主观人为因素的多样化以及主观人为因素的复杂化,使得现有的方法策略难以提供全面有效的保护^[142]。在此背景下,群智感知系统的可信性研究显得尤为关键。可信性意味着系统自身的设计和实现值得信任,能够持续稳定地提供符合实体主观期望的服务,确保高度的可用性,并具备强大的抵御潜在攻击和故障的能力。然而,针对群智感知系统的可信性研究,迄今为止尚未形成一套完整且系统的理论体系和框架^[13]。因此,在构建如图 4 所示的可信的群智感知系统时可能面临着诸多挑战。例如,如何在确保数据机密性的同时提高系统的可用性?如何平衡实体匿名性与可认证性的需求?如何抵御复杂多变的攻击?这不仅需要技术上的创新,还需要在系统设计上做出精巧的权衡。鉴于此,我们将从系统层面、实体层面和数据层面出发,阐述群智感知系统的未来研究方向,探讨如何构建可信的群智感知系统。

5.1 系统层面的可信研究

群智感知系统不仅受到非主观人为因素(如参与者专业能力、设备功能等)的影响,还面临着来自主观人为因素(如合谋攻击、女巫攻击等)的威胁。因此,群智感知系统在运行过程中既需要适应参与者能力与设备条件随时间和环境变化所带来的动态不确定性,又需要有效应对恶意攻击行为在策略、规模与协同方式上的多样化、隐蔽化及持续演化特征。在此背景下,群智感知系统的未来研究在系统层面

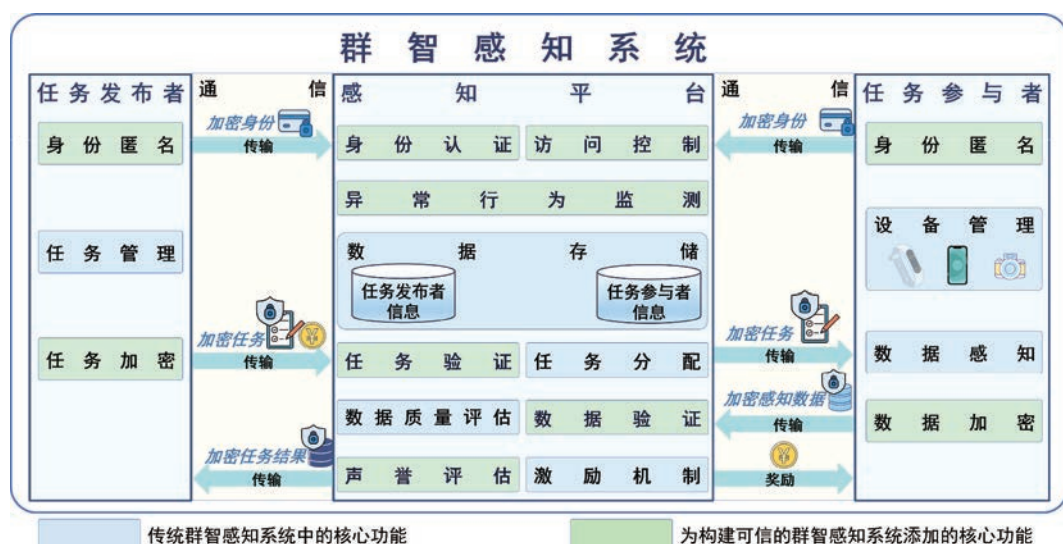


图4 可信群智感知系统架构

可关注以下挑战。

(1)如何在去中心化架构下实现公平的任务分配与激励机制？在现有群智感知系统中，任务分配与激励机制通常依赖中心化平台进行统一决策与管理。然而，中心化架构在实际应用中面临单点失效和平台可信假设过强等问题，且容易引发参与者对任务分配和激励机制公平性的质疑^[97]。为降低对可信第三方的依赖，去中心化架构下的任务分配与激励机制设计逐渐成为一种重要研究方向。在去中心化环境中，缺乏全局视图和统一控制节点导致任务分配需在信息不完备与异步交互条件下完成；同时，恶意实体可能通过虚假身份、虚假数据等攻击行为来破坏公平性。针对上述问题，未来研究可从以下技术路径展开探索：一是采用区块链与智能合约实现任务分配与激励机制，通过规则化合约保障过程透明，但需解决智能合约的可扩展性与链上成本问题^[20,97,143-145]；二是构建去中心化身份与声誉体系，通过历史行为累积声誉值并用于任务分配与激励机制，但该方式易受早期恶意节点共谋、身份伪造等攻击影响^[68,146-147]。不同路径在系统可用性和公平性之间存在内在权衡：区块链智能合约虽可提升公平性，但其链上存储、共识通信以及交易确认带来的延迟与开销可能降低系统可用性与参与者体验；去中心化声誉体系虽可提供长期行为约束，但在动态参与与匿名性较高的环境中，声誉更新的准确性与抗操纵性难以保障。因而，未来研究可进一步探索多路径融合与协同优化方案，例如：在链下完成大部分计算与匹配任务，通过链上哈希证明或轻量级共识进行结果验证，以兼顾公平性与可用性；同时，结合

差分隐私、同态加密或安全多方计算等隐私保护技术，降低信息泄露风险。

(2)如何构建自适应攻击检测与可解释防御框架？群智感知系统的开放性使其容易成为长期隐蔽攻击的目标^[148]。攻击者通常不会采取单次、明显的破坏行为，而是通过长期潜伏、分布式协同与策略迭代，逐步破坏感知数据、操纵声誉体系或渗透任务分配过程，使得传统基于规则或静态阈值的检测方法难以在早期阶段识别并阻断。因此，群智感知系统需要构建能够持续监测并动态响应的攻击检测机制，以便在攻击初期发现异常并防止其扩散。同时，在长期、隐蔽攻击场景中，攻击检测的可解释性尤为关键^[149]。系统管理者通常需要了解攻击发生的证据链条、攻击策略与关键触发特征，才能对参与者声誉、任务分配规则或验证策略进行有针对性的修正^[150]，仅有“异常/正常”的判定无法支撑有效的溯源、取证与防御策略调整。在此背景下，生成式人工智能（通常由大模型驱动）可作为攻击检测与溯源的核心驱动器；其一，具备对多源感知数据进行语义理解与跨模态融合的能力，能够从网络流量^[111]、任务提交日志、任务参与者行为序列等多维信息中学习更复杂的攻击模式，并在新型攻击出现时通过少样本学习或在线更新快速适应，从而提升检测的泛化能力与自适应性。其二，可将检测过程转化为可解释的形式^[151]，输出包括关键特征、异常因果链以及攻击策略分析的结构化解释，支持对攻击来源、协同路径和策略演化的追踪。其三，基于大模型生成的解释结果可以进一步驱动防御策略的自动化更新，例如根据溯源结果调整声誉权重或重新分配任

务。未来研究可探索大模型在攻击检测中的增量学习、可解释推理与证据链构建能力,并结合可验证日志(如区块链记录^[18,20])与隐私保护技术^[152],为群智感知系统构建自适应攻击检测与可解释防御框架。

5.2 实体层面的可信研究

在群智感知系统中,实体层面的可信研究对于保障实体的可认证性、匿名性以及可溯源性至关重要。群智感知系统通常通过假名技术^[16]等策略实现身份匿名,以保护实体隐私;但匿名机制必须与感知平台的身份认证功能相结合,确保仅经认证的实体能够参与系统。实体身份往往与其所携带的智能移动设备绑定,随着设备规模持续增长,网络攻击面不断扩大,实体层面面临的挑战也愈加严峻。其中最为核心的问题在于如何在满足匿名性的同时实现可认证性,并有效抵御身份伪造攻击^[70]和女巫攻击^[60-61]等安全风险。因此,群智感知系统在实体层面未来可围绕以下挑战开展研究。

(1)如何构建去中心化且可问责的实体身份管理框架?在群智感知系统中,实体身份管理既要保障参与者的匿名性与隐私,又要确保身份可认证、行为可追溯,以有效抵御身份伪造、女巫攻击等威胁。传统中心化身份管理依赖单点信任的感知平台,既容易成为攻击目标,也可能导致权限滥用,因此亟需构建去中心化且可问责的身份管理框架。该框架的核心难点在于:一方面需要在去中心化环境下实现身份的可认证与可撤销,避免匿名性被恶意利用;另一方面需要在隐私保护与可追责之间取得权衡,例如过度匿名会削弱追责能力,而过度可追溯又会侵蚀隐私。未来研究需正视上述内在权衡:基于区块链的身份存证^[116,143,153]与智能合约审计^[154]能提供去中心化的凭证管理与不可篡改的审计轨迹,但链上存储与共识机制会引入延迟、成本与可扩展性瓶颈;零知识证明^[26]与匿名凭证^[155]可在不暴露身份信息的情况下完成合法性验证,但其计算与交互开销可能限制在资源受限设备上的可用性,并增加追溯时的复杂度;可信执行环境(TEE)^[110,156]可强化密钥保护与身份生成的可信根,但其依赖特定硬件、存在侧信道风险,可能导致设备兼容性问题。这些技术往往在隐私强度、问责能力、性能开销三者间形成此消彼长的关系。因此,未来研究可进一步将身份管理与声誉评估、激励机制协同设计,通过对实体行为的持续审计与声誉反馈实现动态授权与追责,从而在隐私保护、身份认证与运行效率之间实现更全面的权衡。

(2)如何设计实体合谋行为的检测与防护机制?在群智感知系统中,实体之间可能存在恶意串通行为,这些行为通过伪造、篡改或重复提交数据来破坏数据评估、声誉评估和激励机制,因此需要在隐私保护的前提下识别并抑制实体合谋行为。该机制面临的关键难点在于:合谋行为具有隐蔽性、动态性与跨任务协作特征,单一维度的异常检测难以有效识别;同时,隐私保护与合谋检测存在内在冲突,过强的匿名或加密会削弱对协同行为的关联分析能力,而过度追踪又可能侵蚀隐私并影响参与意愿。未来研究可以采用图神经网络^[157]与异常检测^[158]等方法对实体间协同关系进行建模,从行为关联、时空模式与任务结果一致性等多维特征中识别异常协作群体;引入可解释的多维声誉评估与行为关联分析,以降低误判率并提高可解释性;采用差分隐私^[118]或安全多方计算^[159]等隐私计算技术支持在加密或噪声化数据上进行联合行为分析。为了在隐私保护、抗合谋能力与系统效率之间实现更合理的权衡,可进一步将合谋检测与身份管理、激励机制及任务分配协同设计,通过对可疑实体实施动态惩罚或降低任务权重,并结合声誉评估与激励机制形成闭环。

5.3 数据层面的可信研究

感知平台的数据存储作为信息中枢,负责存储和管理任务发布者与任务参与者的基本信息及感知数据等。这些数据通常会经过加密或加噪处理,从而保障数据的机密性并抵御潜在的篡改或密文破解攻击^[70,77]。感知平台的数据验证功能会将这些数据在加密或加噪的情况下进行聚合评估,验证其完整性和真实性,抵御搭便车攻击^[25]等。然而,结合现有研究发现,同态加密^[104]以及差分隐私^[118]等技术虽然具有较高的隐私保护能力,但是当它们在资源有限的移动设备上应用时面临着巨大计算负担和通信开销的问题。因此,群智感知系统在数据层面仍面临若干挑战,未来可围绕以下挑战开展研究。

(1)如何设计轻量级同态加密算法以在资源受限设备上实现实时数据保护?在群智感知系统中,参与者的感知数据往往涉及位置和身份等敏感信息,若直接上传明文将导致隐私泄露风险;同时,系统需要对数据进行聚合、统计或学习等操作以支持任务决策,因此需要一种既能保护数据隐私又能支持在密文上计算的加密机制。同态加密^[160]作为典型的“在密文上计算”的技术,能够在不暴露原始数据的情况下实现数据聚合与分析,因此在数据层面具有重要价值。然而,同态加密本质上依赖大整数

或多项式环运算,导致计算与存储开销显著高于传统加密方式^[161],在资源受限的移动设备上会带来能耗、延迟与通信压力;同时,若为降低开销而简化参数或运算结构,又可能削弱安全性或同态能力,从而无法满足后续聚合与分析需求。未来研究一方面可以设计适配群智感知数据特征的轻量同态加密框架,通过降低密文维度、采用低成本数学结构或可验证计算等方式减轻设备负担;另一方面可结合边缘计算^[162]与可信执行环境^[156,163],将部分同态运算或密文管理迁移到资源更充足的边缘节点,并通过密文压缩、分层加密与动态参数调整在不同场景中平衡安全强度与计算开销,从而实现资源受限设备上的实时数据保护与系统可用性保障。

(2)如何整合联邦学习与群智感知以在隐私保护下进行模型训练?群智感知系统依赖大量参与者采集的分布式感知数据,这些数据往往具有敏感性且难以集中存储与处理,因此模型训练需要在保障用户隐私的前提下进行。联邦学习作为一种在本地保留数据、仅上传模型更新的分布式学习范式,能够在一定程度上缓解数据泄露风险并降低集中式数据管理的压力,与群智感知场景天然契合。然而,群智感知中任务参与者设备能力、任务类型与数据分布高度异构,导致模型收敛慢且易出现偏差;移动终端计算与通信资源有限,传统联邦学习的频繁通信与本地训练开销难以承受;隐私增强机制(如差分隐私^[164]或同态加密^[160])会引入噪声或计算负担,从而在隐私保护与模型精度之间形成不可避免的权衡。未来研究可以考虑通过将部分聚合任务下放到边缘节点并采用模型压缩、稀疏更新等手段降低通信成本;结合差分隐私^[164]、安全多方计算^[159]或轻量加密方案实现可控隐私保护;并引入异常更新检测、可信参与者筛选与激励机制协同提升系统鲁棒性与长期参与意愿,从而在群智感知环境中构建高效、可信的隐私保护训练框架。值得注意的是,这些技术路径之间存在内在耦合,例如提升隐私保护可能降低模型精度、降低通信开销可能增加聚合偏差,因此需要在统一的系统框架下进行协同优化,以在群智感知环境中实现高效、可信且可持续的隐私保护训练。

6 总 结

群智感知系统的可信性研究整体上仍处于探索阶段,正由面向单一问题和局部可信特征的研究,逐

步向覆盖系统层、实体层和数据层的可信性框架演进。然而,现有综述在群智感知系统的可信性研究方面尚未形成完整且系统的理论体系与框架。随着群智感知系统应用场景的不断拓展,其所面临的挑战也愈加复杂,尤其是在非主观人为因素多样化以及主观人为因素复杂化的情况下,现有方法策略难以提供全面有效的保护。基于此,本文首先从群智感知系统的通用框架出发,提炼了群智感知系统可信性研究中需要关注的关键特征;随后深入梳理了主观与非主观人为因素对不同层面可信特征的影响机理及现有应对策略;最后,本文从去中心化架构的公平任务分配与激励机制、自适应攻击检测与可解释防御框架以及实体合谋行为检测与防护机制等方面指出群智感知系统可信性研究的发展趋势和未来研究方向,旨在通过隐私计算、区块链和大模型等关键技术的有机融合在系统层面、实体层面与数据层面之间实现动态权衡与整体优化,以推动可信群智感知系统的构建。

致 谢 本课题得到国家重点研发计划项目(2024YFB4505502)、国家自然科学基金联合基金重点支持项目(U22B2022)和国家自然科学基金面上项目(62372383)资助。衷心感谢各位专家在审稿过程中提供的建议和帮助!

参 考 文 献

- [1] Liu Y. Crowd sensing computing. Communications of the CCF, 2012,8(10):38-41(in chinese)
(刘云浩. 群智感知计算. 中国计算机学会通讯, 2012,8(10): 38-41)
- [2] Lin H, Li C, Yang J, et al. CP-IoT: A cross-platform monitoring system for smart home//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2024:1-18
- [3] Liu Y, Guo B, Wang Y, et al. TaskMe: Multi-task allocation in mobile crowd sensing//Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing. Heidelberg, Germany, 2016:403-414
- [4] Wu D, Xiao T, Liao X, et al. When sharing economy meets IoT: towards fine-grained urban air quality monitoring through mobile crowdsensing on bike-share system. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2020,4(2):1-26
- [5] Abidi I, Nangia I, Aditya P, et al. Privacy in urban sensing with instrumented fleets, using air pollution monitoring as a

- usecase//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2022:1-18
- [6] Guo B, Chen H, Yu Z, et al. FlierMeet: A mobile crowdsensing system for cross-space public information reposting, tagging, and sharing. *IEEE Transactions on Mobile Computing*, 2014, 14(10):2020-2033
- [7] Jiang Z, Zhu H, Zhou B, et al. CrowdPatrol: A mobile crowdsensing framework for traffic violation hotspot patrolling. *IEEE Transactions on Mobile Computing*, 2023, 22(3): 1401-1416
- [8] Mukherjee S, Weikum G, Danescu-Niculescu-Mizil C. People on drugs: Credibility of user statements in health communities//Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining. New York, USA, 2014: 65-74
- [9] Wu C, Yang Z, Liu Y. Smartphones based crowdsourcing for indoor localization. *IEEE Transactions on Mobile Computing*, 2015, 14(2):444-457
- [10] Wu Y, Wang Y, Hu W, et al. Resource-aware photo crowdsourcing through disruption tolerant networks//Proceedings of the IEEE International Conference on Distributed Computing Systems. Nara, Japan, 2016:374-383
- [11] Guo B, Wang Z, Yu Z, et al. Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Computing Surveys*, 2015, 48(1):1-31
- [12] Wu Y, Zeng J, Peng H, et al. Survey on incentive mechanisms for crowd sensing. *Journal of Software*, 2016, 27(8): 2025-2047(in chinese)
(吴垚, 曾菊儒, 彭辉等. 群智感知激励机制研究综述. 软件学报, 2016, 27(8):2025-2047)
- [13] Xiong J, Bi R, Tian Y, et al. Security and privacy in mobile crowdsensing: Models, progresses, and trends. *Chinese Journal of Computers*, 2021, 44(9):1949-1966(in chinese)
(熊金波, 毕仁万, 田有亮等. 移动群智感知安全与隐私: 模型、进展与趋势. 计算机学报, 2021, 44(9):1949-1966)
- [14] Ni J, Zhang K, Yu Y, et al. Providing task allocation and secure deduplication for mobile crowdsensing via fog computing. *IEEE Transactions on Dependable and Secure Computing*, 2018, 17(3):581-594
- [15] Zhang C, Zhao M, Zhu L, et al. Enabling efficient and strong privacy-preserving truth discovery in mobile crowdsensing. *IEEE Transactions on Information Forensics and Security*, 2022, 17:3569-3581
- [16] Cheng Y, Ma J, Liu Z, et al. A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks. *IEEE Transactions on Dependable and Secure Computing*, 2022, 20(3):1771-1788
- [17] Zhang Q, Wang T, Tao Y, et al. Trajectory privacy protection method based on differential privacy in crowdsensing. *IEEE Transactions on Services Computing*, 2024:1-16
- [18] Li M, Weng J, Yang A, et al. CrowdBC: a blockchain-based decentralized framework for crowdsourcing. *IEEE Transactions on Parallel and Distributed Systems*, 2018, 30(6):1251-1266
- [19] Zhao B, Tang S, Liu X, et al. PACE: Privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing. *IEEE Transactions on Mobile Computing*, 2020, 20(5):1924-1939
- [20] Huang J, Kong L, Cheng L, et al. BlockSense: Towards trustworthy mobile crowdsensing via proof-of-data blockchain. *IEEE Transactions on Mobile Computing*, 2022, 23(2):1016-1033
- [21] Mao Y, Dang Z, Wang H, et al. Solution probing attack against coin mixing based privacy-preserving crowdsourcing platforms. *IEEE Transactions on Dependable and Secure Computing*, 2024, 21(5):4684-4698
- [22] Fang M, Sun M, Li Q, et al. Data poisoning attacks and defenses to crowdsourcing systems//Proceedings of the Web Conference. Ljubljana, Slovenia, 2021:969-980
- [23] Xiao M, Jin W, Li M, et al. Collusion-resistant worker recruitment in crowdsourcing systems. *IEEE Transactions on Mobile Computing*, 2021, 22(1):129-144
- [24] Li W, Wen M, Su Z, et al. Collusion detection and trust management for indoor navigation system with crowdsourcing. *IEEE Transactions on Dependable and Secure Computing*, 2022, 20(4):2913-2924
- [25] Yuan B, Wu Y, Yang M, et al. SmartPatch: Verifying the authenticity of the trigger-event in the IoT platform. *IEEE Transactions on Dependable and Secure Computing*, 2022, 20(2):1656-1674
- [26] Koutsos V, Damle S, Papadopoulos D, et al. AVeCQ: anonymous verifiable crowdsourcing with worker qualities. *IEEE Transactions on Dependable and Secure Computing*, 2024:1-18
- [27] Xu G, Li H, Xu S, et al. Catch you if you deceive me: Verifiable and privacy-aware truth discovery in crowdsensing systems//Proceedings of the ACM Asia Conference on Computer and Communications Security. Taipei, China, 2020:178-192
- [28] Li Y, Li H, Mei B, et al. Fairness-guaranteed task assignment for crowdsourced mobility services. *IEEE Transactions on Mobile Computing*, 2024, 23(5):5385-5400
- [29] Tong F, Zhou Y, Wang K, et al. A privacy-preserving incentive mechanism for mobile crowdsensing based on blockchain. *IEEE Transactions on Dependable and Secure Computing*, 2024, 21(6):5071-5085
- [30] Yan X, Ng W W, Zhao B, et al. Fog-enabled privacy-preserving multi-task data aggregation for mobile crowdsensing. *IEEE Transactions on Dependable and Secure Computing*, 2023, 21(3):1301-1316
- [31] Masood A, Lakew D S, Cho S. Security and privacy challenges in connected vehicular cloud computing. *IEEE Communications Surveys & Tutorials*, 2020, 22(4):2725-2764

- [32] Wang S, Wang J, Su C, et al. Intelligent detection algorithm against UAVs' GPS spoofing attack//Proceedings of the IEEE International Conference on Parallel and Distributed Systems. Hong Kong, China, 2020:382-389
- [33] Budde M, Schankin A, Hoffmann J, et al. Participatory sensing or participatory nonsense? Mitigating the effect of human error on data quality in citizen science. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2017,1(3):1-23
- [34] Mairitha N, Mairitha T, Lago P, et al. CrowdAct: Achieving highquality crowdsourced datasets in mobile activity recognition//Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2021,5(1):1-32
- [35] Harding M, Knowles B, Davies N, et al. HCI, civic engagement & trust//Proceedings of the Annual ACM Conference on Human Factors in Computing Systems. Seoul, Republic of Korea, 2015:2833-2842
- [36] Liu J, Luo K, Zhou Z, et al. ERP: Edge resource pooling for data stream mobile computing. IEEE Internet of Things Journal, 2019,6(3):4355-4368
- [37] Wang E, Zhang M, Yang B, et al. Large-scale spatiotemporal fracture data completion in sparse crowdsensing. IEEE Transactions on Mobile Computing, 2024,23(7):7585-7601
- [38] Chen D, Shi X, Song X, et al. Phone-based ambient temperature measurement with a new confidence-based truth inference model. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2023,6(4):1-18
- [39] Tong Y, Zhou Z, Zeng Y, et al. Spatial crowdsourcing: A survey. The VLDB Journal, 2020,29:217-250
- [40] Liu J, Shen H, Zhang X. A survey of mobile crowdsensing techniques: A critical component for the internet of things//Proceedings of the IEEE International Conference on Computer Communication and Networks. Waikoloa, USA, 2016:1-6
- [41] Wang Y, Yan Z, Feng W, et al. Privacy protection in mobile crowd sensing: A survey. World Wide Web, 2020,23(1):421-452
- [42] Cheng X, He B, Li G, et al. A survey of crowdsensing and privacy protection in digital city. IEEE Transactions on Computational Social Systems, 2023,10(6):3471-3487
- [43] Zhang S, He N, Li Z, et al. A survey on mobile crowd sensing: Concepts, applications, technologies, and future directions. IEEE Internet of Things Journal, 2025,12(24):52090-52109
- [44] Yang Y, Zhang B, Guo D, et al. Generative AI for secure and privacy-preserving mobile crowdsensing. IEEE Wireless Communications, 2024,31(6):29-38
- [45] Zhang H, Chen L, Zhang L. Research on trusted network connection. Chinese Journal of Computers, 2010,33(4):706-717(in chinese)
(张焕国,陈璐,张立强. 可信网络连接研究. 计算机学报, 2010,33(4):706-717)
- [46] Yu Y, Huang Y, Chen H. Redundancy mechanism and reliability analysis of trusted software system based on component. Computer Systems and Applications, 2018,62(11):66-71(in chinese)
(郁湧,黄宇鑫,陈浩. 基于构件的可信软件系统冗余机制及可靠性分析. 计算机系统应用, 2017,62(11):66-71)
- [47] Liu B, Li G, Zhang H, et al. The gap between trustworthy AI research and trustworthy software research: a tertiary study. ACM Computing Surveys, 2024,57(3):1-40
- [48] Wang J, Li H, Wang H, et al. Trustworthy machine learning: Robustness, generalization, and interpretability//Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Long Beach, USA, 2023:5827-5828
- [49] Bayram F, Ahmed B S. Towards trustworthy machine learning in production: An overview of the robustness in MLOps approach. ACM Computing Surveys, 2025,57(5):1-35
- [50] Liu Y, Guo B, Wu W, et al. Multitask-oriented participant selection in mobile crowd sensing. Chinese Journal of Computers, 2017,40(8):1872-1887(in chinese)
(刘琰,郭斌,吴文乐等. 移动群智感知多任务参与者优选方法研究. 计算机学报, 2017,40(8):1872-1887)
- [51] Wang T, Jin X, Lu C, 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)
- [52] Zhang J, Jiang T, Gao X, et al. An online fairness-aware task planning approach for spatial crowdsourcing. IEEE Transactions on Mobile Computing, 2022,23(1):150-163
- [53] Cai C, Zheng Y, Du Y, et al. Towards private, robust, and verifiable crowdsensing systems via public blockchains. IEEE Transactions on Dependable and Secure Computing, 2019,18(4):1893-1907
- [54] Liang Y, An J, Hu X, 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)
- [55] Li M, Zhu L, Lin X. Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing. IEEE Transactions on Services Computing, 2019,14(6):1902-1913
- [56] Hamad S A, Sheng Q Z, Zhang W E, et al. Realizing an internet of secure things: A survey on issues and enabling technologies. IEEE Communications Surveys & Tutorials, 2020,22(2):1372-1391
- [57] Zhang Y, Simsek M, Kantarci B. Empowering self-organized feature maps for ai-enabled modeling of fake task submissions to mobile crowdsensing platforms. IEEE Internet of Things

- Journal, 2020,8(3):1334-1346
- [58] Chen Z, Simsek M, Kantarci B. Region-aware bagging and deep learning-based fake task detection in mobile crowdsensing platforms//Proceedings of the IEEE Global Communications Conference. Taipei, China, 2020:1-7
- [59] Zhang Y, Simsek M, Kantarci B. Ensemble learning against adversarial AI-driven fake task submission in mobile crowdsensing//Proceedings of the IEEE International Conference on Communications. Dublin, Ireland, 2020:1-7
- [60] Lin J, Li M, Yang D, et al. Sybil-proof online incentive mechanisms for crowdsensing//Proceedings of the IEEE Conference on Computer Communications. Honolulu, USA, 2018:2438-2446
- [61] Sucasas V, Mantas G, Bastos J, et al. A signature scheme with unlinkable-yet-accountable pseudonymity for privacy-preserving crowdsensing. *IEEE Transactions on Mobile Computing*, 2019,19(4):752-768
- [62] Jin X, Gong Z, Jiang J, et al. RCTD: Reputation-constrained truth discovery in sybil attack crowdsourcing environment//Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Barcelona, Spain, 2024:1313-1324
- [63] Jansen K, Schafer M, Moser D, et al. Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA, 2018:1018-1031
- [64] Xiao Y, He Y, Zhang X, et al. From hardware fingerprint to access token: Enhancing the authentication on IoT devices//Proceedings of the Network and Distributed System Security Symposium. San Diego, USA, 2024:1-18
- [65] Li T, Chen Y, Zhang R, et al. Secure crowdsourced indoor positioning systems//Proceedings of the IEEE Conference on Computer Communications. Honolulu, USA, 2018:1034-1042
- [66] Zheng Z, Li Z, Huang C, et al. Data poisoning attacks and defenses to LDP-based privacy-preserving crowdsensing. *IEEE Transactions on Dependable and Secure Computing*, 2024,21(5):4861-4878
- [67] Yang K, Zhang K, Ren J, et al. Security and privacy in mobile crowdsourcing networks: Challenges and opportunities. *IEEE Communications Magazine*, 2015,53(8):75-81
- [68] Zhu L, Li M, Zhang Z. Secure fog-assisted crowdsensing with collusion resistance: From data reporting to data requesting. *IEEE Internet of Things Journal*, 2019,6(3):5473-5484
- [69] Duan Z, Li W, Zheng X, et al. Mutual-preference driven truthful auction mechanism in mobile crowdsensing//Proceedings of the IEEE International Conference on Distributed Computing Systems. Dallas, USA, 2019:1233-1242
- [70] Zhang K, Liang X, Lu R, et al. Exploiting mobile social behaviors for sybil detection//Proceedings of the IEEE Conference on Computer Communications. Hong Kong, China, 2015:271-279
- [71] Niu B, Chen Y, Wang Z, et al. Eclipse: Preserving differential location privacy against long-term observation attacks. *IEEE Transactions on Mobile Computing*, 2022,21(1):125-138
- [72] Shi D, Tong Y, Zhou Z, et al. Learning to assign: Towards fair task assignment in large-scale ride hailing//Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Virtual, Singapore, 2021:3549-3557
- [73] Wang Z, Li J, Hu J, et al. Towards privacy-driven truthful incentives for mobile crowdsensing under untrusted platform. *IEEE Transactions on Mobile Computing*, 2021,22(2):1198-1212
- [74] Biryukov A, Tikhomirov S. Deanonymization and linkability of cryptocurrency transactions based on network analysis//Proceedings of the IEEE European Symposium on Security and Privacy. Stockholm, Sweden, 2019:172-184
- [75] Wang E, Cai J, Yang Y, et al. Trustworthy and efficient crowdsensed data trading on sharding blockchain. *IEEE Journal on Selected Areas in Communications*, 2022,40(12):3547-3561
- [76] Li M, Zhu L, Zhang Z, et al. Anonymous and verifiable reputation system for e-commerce platforms based on blockchain. *IEEE Transactions on Network and Service Management*, 2021,18(4):4434-4449
- [77] Yuan D, Li Q, Li G, et al. PriRadar: A privacy-preserving framework for spatial crowdsourcing. *IEEE Transactions on Information Forensics and Security*, 2019,15:299-314
- [78] Kuang L, Zhang H, Shi R, et al. A spam worker detection approach based on heterogeneous network embedding in crowdsourcing platforms. *Computer Networks*, 2020,183:1-11
- [79] Zhang C, Zhu L, Xu C, et al. Location privacy-preserving task recommendation with geometric range query in mobile crowdsensing. *IEEE Transactions on Mobile Computing*, 2021,21(12):4410-4425
- [80] Ma L, Liu X, Pei Q, et al. Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. *IEEE Transactions on Services Computing*, 2018,12(5):786-799
- [81] 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*, 2019,18(3):1245-1260
- [82] Li Z, Zheng Z, Guo S, et al. Disguised as privacy: Data poisoning attacks against differentially private crowdsensing systems. *IEEE Transactions on Mobile Computing*, 2022,22(9):5155-5169
- [83] Rula J P, Bustamante F E. Crowdsensing under (soft) control//Proceedings of the IEEE Conference on Computer Communications. Hong Kong, China, 2015:2236-2244
- [84] Xie X, Yang Y, Fang Z, et al. coSense: Collaborative urban-

- scale vehicle sensing based on heterogeneous fleets. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2018,2(4):1-25
- [85] Yang Y, Fang Z, Xie X, et al. Extending coverage of stationary sensing systems with mobile sensing systems for human mobility modeling. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2020, 4(3):1-21
- [86] Yucel F, Yuksel M, Bulut E. QoS-based budget constrained stable task assignment in mobile crowdsensing. *IEEE Transactions on Mobile Computing*, 2021,20(11):3194-3210
- [87] Dai C, Wang X, Liu K, et al. Stable task assignment for mobile crowdsensing with budget constraint. *IEEE Transactions on Mobile Computing*, 2021,20(12):3439-3452
- [88] Wang H, Wang E, Yang Y, et al. Privacy-preserving online task assignment in spatial crowdsourcing: A graph-based approach//*Proceedings of the IEEE Conference on Computer Communications*. London, UK, 2022:570-579
- [89] Zhang C, Luo X, Liang J, et al. POTA: Privacy-preserving online multi-task assignment with path planning. *IEEE Transactions on Mobile Computing*, 2024,23(5):5999-6011
- [90] Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering//*Proceedings of the International Conference on Evaluation and Assessment in Software Engineering*. London, UK, 2014:1-10
- [91] Chen X, Xie M, Meng X, et al. CPRPS: A cross-platform reputation privacy sharing for speed-up quality data collection in mobile crowdsensing. *IEEE Transactions on Information Forensics and Security*, 2026:1-15
- [92] Song M, Hua Z, Zheng Y, et al. Enabling reliable and anonymous data collection for fog-assisted mobile crowdsensing with malicious user detection. *IEEE Transactions on Mobile Computing*, 2026,25(1):1414-1430
- [93] Zheng Y, Zhou M, Wang S, et al. SecDR: Enabling secure, efficient, and accurate data recovery for mobile crowdsensing. *IEEE Transactions on Dependable and Secure Computing*, 2024,21(2):789-803
- [94] Cheng Y, Ma J, Liu Z, et al. A privacy-preserving and reputationbased truth discovery framework in mobile crowdsensing. *IEEE Transactions on Dependable and Secure Computing*, 2023,20(6):5293-5311
- [95] Jin X, Zhang R, Chen Y, et al. DPSense: Differentially private crowdsourced spectrum sensing//*Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Vienna, Austria, 2016:296-307
- [96] Gong Z, Zhang J, Wang H, et al. A privacy-preserving scheme with high utility over data streams in mobile crowdsensing. *IEEE Transactions on Information Forensics and Security*, 2025,20:5372-5385
- [97] Zeng H, Cui H, Zhang X, et al. DCrowd: Decentralized mobile crowdsensing via proof of task assignment blockchain. *IEEE Transactions on Dependable and Secure Computing*, 2025,22(6):6281-6295
- [98] Wu H, Dudder B, Jiang S, et al. VP²-Match: Verifiable privacy-aware and personalized crowdsourcing task matching via blockchain. *IEEE Transactions on Mobile Computing*, 2024, 23(10):9913-9930
- [99] Fang X, Cai H, Sheng B, et al. A blockchain-based secure and fair online incentive mechanism for crowdsensed data trading. *IEEE Transactions on Information Forensics and Security*, 2025,20:9372-9386
- [100] Sun W, Xue K, Li M, et al. FishboneChain: A scalable and liquidity-guaranteed crowdsourcing platform based on multiple child chains. *IEEE Transactions on Dependable and Secure Computing*, 2025,22(6):6566-6579
- [101] Ding Z, He D, Qiao Q, et al. A lightweight and secure communication protocol for the IoT environment. *IEEE Transactions on Dependable and Secure Computing*, 2024, 21(3):1050-1067
- [102] Yang X, Qi S, Zhou J, et al. Invisible, yet trusted: Blockchainempowered privacy-preserving spatio-temporal task matching in crowdsourcing with efficient public verification. *IEEE Transactions on Mobile Computing*, 2026:1-16
- [103] Gao S, Chen X, Zhu J, et al. TrustWorker: A trustworthy and privacy-preserving worker selection scheme for blockchainbased crowdsensing. *IEEE Transactions on Services Computing*, 2022,15(6):3577-3590
- [104] An B, Xiao M, Liu A, et al. Secure crowdsensed data trading based on blockchain. *IEEE Transactions on Mobile Computing*, 2021,22(3):1763-1778
- [105] Zhao Y, Gong X, Lin F, et al. Data poisoning attacks and defenses in dynamic crowdsourcing with online data quality learning. *IEEE Transactions on Mobile Computing*, 2021, 22(5):2569-2581
- [106] Zhou Z, Liao H, Gu B, et al. Robust mobile crowd sensing: when deep learning meets edge computing. *IEEE Network*, 2018,32(4):54-60
- [107] Cai C, Xu L, Zhou A, et al. Toward a secure, rich, and fair query service for light clients on public blockchains. *IEEE Transactions on Dependable and Secure Computing*, 2022,19(6):3640-3655
- [108] Moon J, Yoo D, Jiang X, et al. THOR: Secure transformer inference with homomorphic encryption//*Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Taipei, China, 2025:3765-3779
- [109] Abdullahi S M, Wang H, Li T. Fractal coding-based robust and alignment-free fingerprint image hashing. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 2587-2601
- [110] Segall A. Trusted platform modules: why, when and how to use them. *Institution of Engineering*, 2016:1-400
- [111] Bezawada B, Bachani M, Peterson J, et al. Behavioral fin-

- gerprinting of IoT devices//Proceedings of the Workshop on Attacks and Solutions in Hardware Security. Toronto, Canada, 2018:41-50
- [112] Dwork C. Differential privacy//Proceedings of the International Conference on Automata, Languages and Programming. Venice, Italy, 2006:1-12
- [113] Boneh D, Boyen X, Shacham H. Short group signatures//Proceedings of the International Cryptology Conference. Santa Barbara, USA, 2004:41-55
- [114] Zhao Y, Yang X, Feng Q, et al. Anonymous credential protocol based on SM2 digital signature. *Journal of Software*, 2024,35(7):3469-3481(in chinese)
(赵艳琦,杨晓艺,冯琦等.基于SM2数字签名的匿名凭证协议. *软件学报*,2024,35(7):3469-3481)
- [115] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, USA, 2016:770-778
- [116] Wood G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 2014:1-32
- [117] Song W, Wang B, Wang Q, et al. Publicly verifiable computation of polynomials over outsourced data with multiple sources. *IEEE Transactions on Information Forensics and Security*, 2017,12(10):2334-2347
- [118] Wang D, Ren J, Wang Z, et al. Privacy-preserving streaming truth discovery in crowdsourcing with differential privacy. *IEEE Transactions on Mobile Computing*, 2021, 21(10):3757-3772
- [119] Zhou Z, Liao H, Gu B, et al. Robust mobile crowd sensing: When deep learning meets edge computing. *IEEE Network*, 2018,32(4):54-60
- [120] Chen Z, Cheng P, Chen L, et al. Fair task assignment in spatial crowdsourcing. *Proceedings of the VLDB Endowment*, 2020,13(12):2479-2492
- [121] Bask F, Gedik B, Ferhatosmanoglu H, et al. Fair task allocation? in crowdsourced delivery. *IEEE Transactions on Services Computing*, 2021,14(4):1040-1053
- [122] Shi D, Tong Y, Zhou Z, et al. Learning to assign: Towards fair task assignment in large-scale ride hailing//Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining. Virtual, Singapore, 2021:3549-3557
- [123] Guo X, Peng M, Hao X, et al. AgentSense: LLMs empower generalizable and explainable web-based participatory urban sensing//Proceedings of the Web Conference. Dubai, United Arab Emirates, 2026:1-13
- [124] Zhan Z, Wang Y, Duan P, et al. Enhancing worker recruitment in collaborative mobile crowdsourcing: A graph neural network trust evaluation approach. *IEEE Transactions on Mobile Computing*, 2024,23(10):10093-10110
- [125] Yin X, Chen Y, Li B. Task assignment with guaranteed quality for crowdsourcing platforms//Proceedings of the IEEE/ACM International Symposium on Quality of Service. Vilanova i la Geltru, Spain, 2017:1-10
- [126] Zhang J, Zhang X. Multi-task allocation in mobile crowd sensing with mobility prediction. *IEEE Transactions on Mobile Computing*, 2023,22(2):1081-1094
- [127] 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
- [128] Lu J, Liu H, Jia R, et al. Incentivizing proportional fairness for multi-task allocation in crowdsensing. *IEEE Transactions on Services Computing*, 2024,17(3):990-1000
- [129] Zhao N, Pei Y, Liang Y C, et al. Deep-reinforcement-learningbased contract incentive mechanism for joint sensing and computation in mobile crowdsourcing networks. *IEEE Internet of Things Journal*, 2024,11(7):12755-12767
- [130] He S, Shin K G. Steering crowdsourced signal map construction via bayesian compressive sensing//Proceedings of the IEEE Conference on Computer Communications. Honolulu, USA, 2018:1016-1024
- [131] Dinh T A N, Nguyen A D, Nguyen T T, et al. Spatial-temporal coverage maximization in vehicle-based mobile crowdsensing for air quality monitoring//Proceedings of the IEEE Wireless Communications and Networking Conference. Austin, USA, 2022:14491454
- [132] Kong L, Xia M, Liu X Y, et al. Data loss and reconstruction in sensor networks//Proceedings of the IEEE Conference on Computer Communications. Turin, Italy, 2013:1654-1662
- [133] Liu L, Wang L, Lu Z, et al. Cost-and-quality aware data collection for edge-assisted vehicular crowdsensing. *IEEE Transactions on Vehicular Technology*, 2022,71(5):5371-5386
- [134] Chang Q, Tao D, Wang J, et al. Deep compressed sensing based data imputation for urban environmental monitoring. *ACM Transactions on Sensor Networks*, 2023,20(1):1-21
- [135] Wang P, Jiao D, Yang L, et al. Hypergraph-based truth discovery for sparse data in mobile crowdsensing. *ACM Transactions on Sensor Networks*, 2024,20(3):1-23
- [136] Wang L, Zhang D, Wang Y, et al. Sparse mobile crowdsensing: Challenges and opportunities. *IEEE Communications Magazine*, 2016,54(7):161-167
- [137] Wang E, Tian Z, Yang Y, et al. Data-driven similarity-based worker recruitment towards multi-task data inference for sparse mobile crowdsensing//Proceedings of the IEEE/ACM International Symposium on Quality of Service. Orlando, USA, 2023:1-10
- [138] Ji S, Xue Y, Carin L. Bayesian compressive sensing. *IEEE Transactions on signal processing*, 2008,56(6):2346-2356
- [139] Chen X, Pu L, Gao L, et al. Exploiting massive D2D collaboration for energy-efficient mobile edge computing. *IEEE Wireless Communications*, 2017,24(4):64-71

- [140] Guo B, Liu Y, Wang L, et al. Task allocation in spatial crowdsourcing: current state and future directions. *IEEE Internet of Things Journal*, 2018, 5(3):1749-1764
- [141] Li Y, Gao J, Meng C, et al. A survey on truth discovery. *ACM SIGKDD Explorations Newsletter*, 2016, 17(2):1-16
- [142] Feng W, Yan Z, Zhang H, et al. A survey on security, privacy, and trust in mobile crowdsourcing. *IEEE Internet of Things Journal*, 2017, 5(4):2971-2992
- [143] Shao Q, Jin C, Zhang Z, et al. Blockchain: Architecture and research progress. *Chinese Journal of Computers*, 2018, 41(5):969-988(in chinese)
(邵奇峰, 金澈清, 张召等. 区块链技术: 架构及进展. *计算机学报*, 2018, 41(5):969-988)
- [144] Yang K, Dutta S. Secure and efficient task matching with multikeyword in multi-requester and multi-worker crowdsourcing//*Proceedings of the IEEE/ACM International Symposium on Quality of Service*. Tokyo, Japan, 2021:1-6
- [145] Yao X W, Yang X T, Li Q, et al. UMIM: Utility-maximization incentive mechanism for mobile crowd sensing. *IEEE Transactions on Mobile Computing*, 2024, 23(5):6334-6346
- [146] He Y, Li M, Li H, et al. A blockchain based incentive mechanism for crowdsensing applications. *Journal of Computer Research and Development*, 2019, 56(3):544-554(in chinese)
(何云华, 李梦茹, 李红等. 群智感知应用中基于区块链的激励机制. *计算机研究与发展*, 2019, 56(3):544-554)
- [147] Deng Q, Zuo Q, Li Z, et al. Privacy-preserving bilateral reputation evaluation in blockchain based crowdsensing. *Journal of Computer Research and Development*, 2024, 62(11):2681-2692(in chinese)
(邓清勇, 左清华, 李哲涛等. 群智感知应用中基于区块链的激励机制. *计算机研究与发展*, 2024, 62(11):2681-2692)
- [148] Bilot T, Jiang B, Li Z, et al. Sometimes simpler is better: A comprehensive analysis of state-of-the-art provenance-based intrusion detection systems//*Proceedings of the USENIX Security Symposium*. Seattle, USA, 2025:7193-7212
- [149] Cheng Z, Lv Q, Liang J, et al. Kairos: Practical intrusion detection and investigation using whole-system provenance//*Proceedings of the IEEE Symposium on Security and Privacy*. San Francisco, USA, 2024:3533-3551
- [150] Li S, Dong F, Xiao X, et al. Nodlink: an online system for finegrained apt attack detection and investigation//*Proceedings of the Network and Distributed System Security Symposium*. San Diego, USA, 2024:1-18
- [151] Aly A, Mansour E, Youssef A. OCR-APT: Reconstructing APT stories from audit logs using subgraph anomaly detection and LLMs//*Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Taipei, China, 2025:261-275
- [152] Yao A C. Protocols for secure computations//*Proceedings of the IEEE Symposium on Foundations of Computer Science*. Chicago, USA, 1982:160-164
- [153] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 2008:1-9
- [154] Xiao Y, Zhang N, Li J, et al. Privacyguard: Enforcing private data usage control with blockchain and attested off-chain contract execution//*Proceedings of the European Symposium on Research in Computer Security*. Guildford, UK, 2020:610-629
- [155] Li P, Lai J, Wu Y. Accountable attribute-based authentication with fine-grained access control and its application to crowdsourcing. *Frontiers of Computer Science*, 2023, 17(1):1-14
- [156] Jang J S, Kong S, Kim M, et al. SeCReT: Secure channel between rich execution environment and trusted execution environment//*Proceedings of the Network and Distributed System Security Symposium*. San Diego, USA, 2015:1-15
- [157] Zhou A, Xu X, Raghunathan R, et al. KnowGraph: Knowledge-enabled anomaly detection via logical reasoning on graph data//*Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Salt Lake City, USA, 2024:168-182
- [158] Wang C, Muller R, Song R, et al. From threat to trust: Exploiting attention mechanisms for attacks and defenses in cooperative perception//*Proceedings of the USENIX Security Symposium*. Seattle, USA, 2025:7387-7406
- [159] Jiang Z, Ye P, He S, et al. Lotto: Secure participant selection against adversarial servers in federated learning//*Proceedings of the USENIX Security Symposium*. Philadelphia, USA, 2024:343-360
- [160] Li Z, Gui X, Gu Y, et al. Survey on homomorphic encryption algorithm and its application in the privacy-preserving for cloud computing. *Journal of Software*, 2017, 29(7):1830-1851(in chinese)
(李宗育, 桂小林, 顾迎捷等. 同态加密技术及其在云计算隐私保护中的应用. *软件学报*, 2017, 29(7):1830-1851)
- [161] Cho W, Hanrot G, Kim T, et al. Fast and accurate homomorphic softmax evaluation//*Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. Salt Lake City, USA, 2024:4391-4404
- [162] Ganjavi R, Sharafat A R. Edge-assisted public key homomorphic encryption for preserving privacy in mobile crowdsensing. *IEEE Transactions on Services Computing*, 2023, 16(2):1107-1117
- [163] Ivanov A, Rothenberger B, Dethise A, et al. SAGE: software-based attestation for GPU execution//*Proceedings of the USENIX Annual Technical Conference*. Boston, USA, 2023:485-499
- [164] Gu X, Li M, Xiong L. DP-BREM: Differentially-private and byzantine-robust federated learning with client momentum//*Proceedings of the USENIX Security Symposium*. Seattle, USA, 2025:3065-3082



ZENG Hao, Ph. D. candidate. His research interests are crowdsensing and privacy computing.

ZHANG Bo, Ph. D. candidate. His research interests are privacy computing and system security.

CUI He-Lei, Ph. D. , professor.

His research interests are trustworthy crowdsensing and privacy computing.

Background

The proliferation of smartphones, cloud computing, Internet of Things (IoT), and wireless communication systems drives the rapid development of crowdsensing. As an emerging paradigm for IoT sensing, crowdsensing leverages the crowd's smart mobile devices, such as smartphones, to collect and process sensing data for diverse application scenarios without additional sensor deployments, providing excellent flexibility, extensive coverage, and economic benefits.

The crowdsensing system mainly consists of task providers, task participants, and sensing platforms, which work collaboratively to accomplish sensing tasks. However, subjective human factors (such as malicious attack behaviors for personal benefit) and non-subjective human factors (such as external and internal system objective conditions) may impact or disrupt the crowdsensing system, hindering further development and widespread application. Existing surveys mainly discuss one of the specific aspects of crowdsensing systems, such as task assignment, incentive mechanisms, privacy protection, and security threats, lacking a comprehensive and systematic theoretical framework for assessing the trust of crowdsensing system. Critical gaps remain in designing trustworthy crowdsensing systems that are capable of providing services consistent with entities' subjective expectations, ensuring high availability, and possessing the ability to withstand potential failures and attacks.

YU Zhi-Wen, Ph. D. , professor. His research interests are crowdsensing, ubiquitous computing, and Smart IoT.

CHEN Ya-Xing, Ph. D. , associate professor. His research interests are trustworthy crowdsensing and privacy computing.

GUO Bin, Ph. D. , professor. His research interests are ubiquitous computing, mobile crowd sensing, and HCI.

ZHOU Xing-She, Ph. D. , professor. His research interests are embedded computing and pervasive computing.

To tackle this problem, in this paper, we first summarize the general framework of the crowdsensing system, outline the core functions of different entities, and define 9 critical features of the trust across the system layer, the user layer, and the data layer. Then, we conduct an in-depth review of recent domestic and international literature in the field of crowdsensing, categorizing the factors that undermine the trust of the crowdsensing system into subjective human factors and non-subjective human factors. We analyze the causes of these factors and their impacts on the 9 critical trust features of the crowdsensing system. Considering the impacts of both subjective and non-subjective human factors, we discuss the methodological strategies employed in existing studies to address these factors and summarize their application effects from the system layer, user layer, and data layer. Furthermore, we explore how to build a trustworthy crowdsensing system and present future research directions around the trustworthy research of the system layer, user layer, and data layer. This work aims to promote the further development and widespread application of crowdsensing, providing insights and references for building trustworthy crowdsensing systems.

This work was supported in part by the National Key R&D Program of China (No. 2024YFB4505502) and the National Natural Science Foundation of China (No. U22B2022, 62372383).