文章编号:2096-1472(2025)10-0036-06
DOI:10.19644/j.cnki.issn2096-1472.2025.010.008

面向移动群智感知的隐私交易保护方案研究

周桂龙,张 洁

(南京邮电大学计算机学院,江苏 南京 210023)
✉ 1750295898@qq.com; zhangjie@njupt.edu.cn

摘 要:在移动群智感知领域,用户数据隐私安全正面临着来自多方面的攻击,为了有效加强隐私保护,提出了一种隐私交易保护方案。该方案通过集成多层次加密技术、匿名凭证系统以及用户激励机制,旨在有效保护用户隐私的同时,促进用户积极参与。实验显示,2 核心手机认证及伪名生成平均耗时 8s,4 核心设备性能更佳,使用 TOR 时延迟约 10s。在 100 个活跃任务中,私有信息检索协议 3.5s 内完成,证实了方案的高效性和实用性,显著优于现有方法。

关键词:移动群智感知;隐私保护;隐私交易;激励机制;数据安全;匿名凭证
中图分类号:TP309.2 **文献标志码**:A

Research on Privacy-Preserving Transaction Scheme for Mobile Crowd Sensing

ZHOU Guilong, ZHANG Jie

(*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*)
✉ 1750295898@qq.com; zhangjie@njupt.edu.cn

Abstract: In the domain of mobile crowd sensing, user data privacy faces multifaceted security threats. To enhance privacy protection effectively, this study proposes a privacy-preserving transaction scheme. By integrating multi-layer encryption techniques, an anonymous credential system, and user incentive mechanisms, the scheme aims to safeguard user privacy while promoting active participation. Experimental results demonstrate that dual-core phone authentication and pseudonym generation require an average of 8 seconds, with quad-core devices delivering superior performance. When using TOR, the latency is approximately 10 seconds. In scenarios with 100 active tasks, the Private Information Retrieval protocol completes within 3.5 seconds, confirming the scheme's efficiency and practicality while significantly outperforming existing methods.

Key words: mobile crowd sensing; privacy protection; privacy transaction; incentive mechanism; data security; anonymous credentials

0 引言(Introduction)

在大数据时代,数据隐私交易[1]的重要性日益凸显。移动群智感知(Mobile Crowd Sensing, MCS)[2]作为一种新兴范式,利用传感设备的普及,在环境监测[3]、智能交通[4-5]及辅助医疗[6]等领域展现了广阔的应用前景。然而,MCS 用户需贡献带有时空标签的数据,这些数据可能泄露位置、健康状况等敏感信息,甚至形成用户画像[7],增加隐私风险。传统假设用户完全信任系统的模式已不再适用。如何保护隐私,提高数据可用性并确保公平性,成为研究热点。

尽管隐私保护能促进用户参与,但外在激励仍是关键[8]。已

收稿日期:2024-11-18

有研究提出货币奖励[9]、社交机制[10]等激励形式,并探索其在MCS中的应用[11-12]。然而,如何在隐私保护下公平激励用户,尤其是在用户动态参与的场景中,仍存在挑战[13]。同时,匿名性虽保护隐私,却增加了对抗性用户及其恶意行为的检测难度。

为应对以上挑战,本研究设计了一种兼具隐私保护和激励公平性的MCS架构,扩展了SPPEAR[14]的安全特性并改进奖励机制,实现了高效的隐私保护与广泛用户参与,并通过形式化分析验证了方案的安全性与实用性。

1　相关工作(Related work)

为了解决以上问题,本研究的贡献如下:移动群智感知的安全性和隐私性已引起广泛关注[15-16],多项研究致力于通过匿名化用户贡献的数据[17-18]以及模糊化位置信息[19]来保护用户隐私。此外,其他研究还采用了泛化[20]或扰动[21]的方法,即有意降低用户提交给移动群体感知系统的信息质量和数量。然而,虽然这些技术在一定程度上增强了用户隐私保护,但它们并未涵盖隐私保护的全部范围。例如:仅通过参与某些感知任务就可能透露用户敏感信息,如其家庭的大致位置[22-23]。此外,强有力的隐私保护需要在移动群体感知系统中的实体不可信的情况下仍然有效,即这些实体可能试图获取并推断用户的隐私信息。

AnonySense[17]是一个通用的安全与隐私保护框架,适用于任务调度和报告。报告通过无线接入点提交,同时利用混合网络使提交的数据与其来源脱钩。然而,它使用群签名来加密保护报告,因而易受Sybil攻击的影响。尽管AnonySense能够驱逐恶意用户,过滤其虚假贡献,但这需要对合法报告进行去匿名化处理。这一过程不仅成本高昂,还会侵犯合法参与者的匿名性。相比之下,本研究提出的系统通过一个高效的撤销机制避免了恶意用户,并在不侵蚀合法用户隐私的情况下筛选出恶意输入。

群签名方案通过限制用户认证的速率来防止匿名滥用,具体表现为在给定时间间隔内设定一个预定义的阈值k[24]。超过此阈值则被视为不当行为,结果是用户的去匿名化和撤销。然而,这种技术无法捕捉其他类型的恶意行为,如恶意用户通过在时间间隔内提交$(k-1)$个虚假样本来污染数据。在此方面,本研究的方案与恶意行为无关,并通过授权令牌和具有不重叠有效期的假名来防止此类匿名滥用。

PEPSI[18]阻止未授权实体查询感知任务结果,并提供了可证明的安全性。它采用了集中式解决方案,主要关注数据查询的隐私性,即仅关注感兴趣实体而不考虑问责机制和隐私保护的激励机制。PEPPeR[25]则保护信息查询节点的隐私(因此并不关注信息贡献节点),通过将节点发现过程与用于查询这些节点的访问控制机制分离开来。PRISM[26]则专注于感知应用的安全部署,并未考虑隐私问题。

在PoolView中,移动客户端在共享私密测量值之前进行扰动。为了防止利用用户数据相关性的推理攻击,GANTI等[27]提出了一种模糊模型。该方案的新颖之处在于,虽然无法获得用户的私密数据,但仍可准确计算这些数据的统计信息。PoolView仅考虑数据流的隐私,因此不考虑恶意用户的问责机制。

YAO等[28]提出了一种面向移动群智感知应用的隐私保护数据报告机制。该机制的直觉是通过切断数据与参与者之间的联系来保护用户隐私。然而,与本论文相反,该方案仅专注于隐私问题,因此未考虑激励机制和恶意用户的问责机制。

CHRISTIN等[29]提出了一种基于信誉的机制,用于评估用户贡献数据的可信度,超出了本研究的讨论范围。类似地,SHIELD[30]利用机器学习技术检测并筛选恶意用户提交的错误数据,这些用户试图通过污染数据收集过程来操控移动群体感知系统。在本研究中,本研究假设存在这样一个能够评估匿名用户总体贡献的机制。

在移动群智感知领域,大量工作集中于激励用户参与的机制[9,11,31]。这些研究利用了拍卖、动态定价、货币优惠券、服务配额和信誉度等机制。然而,它们并未考虑用户隐私,因此可能通过将用户身份与其贡献数据联系起来而泄露敏感信息。赵国峰等[32]提出了一种通过根据隐私暴露程度给予用户报酬来增强隐私保护的方法:随着用户隐私暴露的增加,系统会提供更好的服务和报酬作为补偿。

2　隐私交易保护方案(Privacy-preserving transaction scheme)

2.1　场景模型与威胁模型

本研究考虑了包含以下实体的通用移动群智感知系统。

任务发起者又称信息消费者,为发起数据收集活动的组织或个人,通过招募用户并分发感知任务来进行数据收集。任务发起者发起感知任务和活动。每个任务本质上是对用户需要使用的传感器、感兴趣区域和任务生命周期的具体说明。感兴趣区域是参与用户必须贡献数据的本地区域,可以通过地图上形成多边形的坐标显示定义,或通过标注的地理区域隐式定义。用户又称信息生产者,操作具有感知能力的移动设备和导航模块的用户。设备具备发射接收机,可以通过无线局域网或蜂窝网络(如5G)进行通信[33]。后端基础设施支持感知任务全生命周期的系统实体:它们负责注册和认证用户,收集并聚合用户贡献的报告,最后将结果以各种形式传播给所有感兴趣的相关方。

移动群智感知系统可能会遭受外部和内部攻击者的滥用。外部攻击者是与系统没有任何关联的实体,因此其破坏能力有限。它们可以窃听通信,试图收集用户活动信息。它们还可能通过贡献未经授权的样本或重放合法用户的样本来操纵数据收集过程。然而,使用简单的加密和访问控制机制可以轻松减轻这类攻击。内部攻击者是系统的合法参与者,但表现出恶意行为。本研究不仅指具有恶意意图的操作员,还包括被入侵的设备,如运行恶意版本的移动群体感知应用程序。这类攻击者可以在数据收集过程中提交虚假但经过认证的报告,目的是扭曲系统对感知现象的感知,从而降低感知任务的效用。

在完整的移动群智感知场景中,如图1所示,用户在设备上下载移动客户端,收集并传输感知信息。群组管理器负责设备注册并颁发匿名凭证,通过授权令牌授权设备参与任务。身

份提供者认证设备并协调任务参与，伪名认证机构为用户提供匿名的短期凭证(伪名)，以确保数据完整性和真实性。报告服务存储和处理提交的数据，并发放用于奖励的收据。撤销机构负责取消违规设备的匿名性。各实体通过最小化信息共享和职责分离来确保隐私保护，使用 SAML 断言建立信任，并通过 TLS 通道保障通信安全。为了避免网络标识符泄露，设备可通过 TOR(The Onion Router)[34] 网络进行交互。

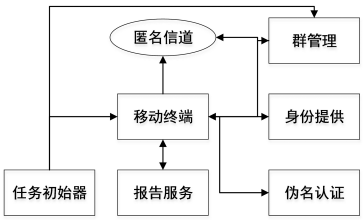


图 1 移动群体感知场景中的数据隐私交易

Fig. 1 Data privacy-preserving transaction in mobile crowd sensing scenario

2.2 移动群智感知隐私交易保护

为了实现移动群智感知隐私交易保护，本研究设计了一套多层次的架构，包含任务发起者、用户设备、后端基础设施等实体，各实体通过基于加密的安全通信协议进行交互。

首先，任务发起者定义感知任务的区域、时间期限及传感器使用规范，并通过群管理者向用户分配任务。任务发起者利用 ECDSA 签名算法确保任务描述的真实性，群管理者通过群签名机制为用户设备分配群公钥和私钥。

在设备认证流程中，设备凭借签名密钥和授权令牌向身份提供者进行身份验证，并从个人认证中心接收伪名。伪名是将匿名身份与公钥相关联的证书。首先，移动客户端生成一系列密钥对，并据此创建同等数量的证书签名请求。随后，客户端将这些证书签名请求提交给个人认证中心，以获取相应的伪名。在设备未通过认证前，个人认证中心会向身份提供者发出安全断言标记语言认证请求。该请求通过个人认证中心的私钥进行签名，并采用身份提供者的公钥进行加密。根据安全断言标记语言的要求，请求中包含一个用于会话管理的随机生成的临时标识符。之后，设备将该请求转发给身份提供者。

接下来，身份提供者对认证请求进行解码和解密，验证个人认证中心的签名并开始认证流程。这一认证过程基于群签名技术，身份提供者向设备发送一个以时间戳或随机数形式呈现的挑战。设备则利用其签名密钥对挑战进行群签名，并提交从群签名密钥分发者处获得的令牌。身份提供者使用群签名公钥验证挑战。一旦认证成功，身份提供者将生成一个安全断言标记语言认证响应，该响应通过身份提供者的私钥签名并用个人认证中心的公钥加密。响应内容包括临时标识符和认证声明，声明设备已通过群签名方案成功进行匿名认证，并包含授权令牌和设备的访问权限。

最后，设备将安全断言标记语言断言提交给个人认证中心，个人认证中心对其进行解密并验证签名及字段信息。一旦交易完成，设备即通过认证并获得有效的伪名。每个伪名都设定了时间有效性，明确了其可用期限，即伪名的生命周期。个人认证中心发行的伪名具有不重叠的生命周期，以避免恶意用户同时暴露多个身份，从而实施身份伪造攻击[35]。

在用户贡献感知任务的过程中，设备通过签署其贡献的样本并附加相应的伪名来参与。每个样本 s_i 由式(1)表示：

$$s_i = \{v \parallel t \parallel (\mathrm{loc}) \parallel \sigma_{\mathrm{PrvKey}} \parallel C_i\} \tag{1}$$

其中：v 是感知现象的值，t 是时间戳，σ_{PrvKey} 是使用伪名 C_i 中包含的公钥对应的私钥生成的数字签名，覆盖所有样本字段，而 loc 字段包含设备当前的位置坐标。

当接收到样本时，接收服务器会验证其签名和时间戳，以及伪名的时间有效性。如果样本被认定为真实，接收服务器将为设备准备一个收据 r_i，由式(2)给出：

$$r_i = \{\mathrm{receiptid} \parallel \mathrm{region}_i \parallel \mathrm{taskid} \parallel \mathrm{time} \parallel \sigma_{RS}\} \tag{2}$$

其中：σ_{RS} 是接收服务器的数字签名，region_i 是包括提交 s_i 中指定的 loc 的区域。

在任务完成后，系统会根据用户的贡献对其进行报酬。如果报酬机制要求，每个任务描述会指定用户将共享报酬金额 B。报酬的分配基于用户的贡献程度，即提交的数据样本数量。使用夏普利值来公平地量化每个用户的报酬，其计算如式(3)所示：

$$\varphi_i(v) = \frac{1}{\lfloor N \rfloor !} \sum_{\Pi} [v(P_i^{\Pi} \cup i) - v(P_i^{\Pi})] \tag{3}$$

其中：求和是在所有可能的用户排列 Π 上计算的，P_i^{Π} 是排列 Π 中用户 i 之前的用户集合。夏普利值的无偏估计器可以简化计算过程，如式(4)所示：

$$\varphi_i(v) = \frac{1}{k} \sum_{\Pi} [v(P_i^{\Pi} \cup i) - v(P_i^{\Pi})] \tag{4}$$

其中：k 是随机选择的用户子集的数量。

为了进一步细化报酬机制，本研究定义了值函数，它不仅基于用户提交的数据数量，还考虑了他们贡献的空间分散。具体来说，值函数由式(5)给出：

$$v(S) = H(\boldsymbol{R}_S) \cdot \sum_{i \in S} \boldsymbol{R}_i \tag{5}$$

其中：$\boldsymbol{R}_S$ 是一个向量，定义了联盟 S 为每个区域贡献的样本数量，而 $H(\boldsymbol{R}_S)$ 是香农熵，用于衡量样本在不同区域的分布均匀性，其计算如式(6)所示：

$$H(\boldsymbol{R}_S) = -\sum p_i \cdot \log(p_i) \tag{6}$$

其中：p_i 是联盟 S 在区域中的样本 i 比例。当所有区域接收到相同数量的样本时，$H(\boldsymbol{R}_S)$ 等于 1，此时联盟的价值 $v(S)$ 就是参与用户为任务贡献的样本总和。如果一个联盟在某些区域的样本数量过多，那么 $H(\boldsymbol{R}_S)$ 将趋向于 0，从而 $v(S)$ 将等于样本总和的一小部分。这种报酬协议必须建立在数据验证机制之上，以确保只有可信的用户贡献才能获得报酬。

2.3 隐私保护安全性分析

所提方案的通信通过安全通道传输层安全协议进行，确保了通信的保密性和完整性。此外，每个系统实体都拥有一个认证的数字证书。在方案中，群签名密钥分发者是策略决策点，它针对设备参与特定感知任务的资格发出授权决策。身份提供者是策略执行点，它基于授权令牌授权设备参与。

恶意设备可能会注入错误的报告以污染数据收集过程。

例如:考虑一个交通监控任务,其中实时交通地图是基于用户提交的位置和速度报告构建的。通过滥用它们的匿名性或如果可能的话,通过发起身份伪造攻击,不当行为的用户可以对道路网络的拥堵水平施加虚假的感知。依赖于群签名来验证用户报告的方案[17]容易受到滥用:检测是否由同一设备生成的两份报告需要打开所有报告的签名,而不考虑生成它们的设备。除了成本高昂之外,这种方法还侵犯了合法用户的隐私。

本方案中通过使用授权令牌克服了这一挑战:它们表明设备已针对特定任务进行了认证,并接收了具有不重叠生命周期的伪名。这样,个人认证中心可以证实先前发行的伪名的时间有效性,并且在设备请求时,为其提供不与先前发行的伪名重叠的新伪名。因此,对抗性设备不能表现出身份伪造行为,因为它们不能同时使用多个伪名。尽管如此,重复使用伪名以加密保护多个报告,是以隐私换取开销的权衡。

所使用的私有信息检索方案防止了好奇的群签名密钥分发者推断出用户希望参与的任务。此外,设备在不透露其身份的情况下向身份提供者进行认证。最后,伪名允许设备匿名且不相关联地证明它们提交的样本的真实性。通过使用多个伪名并通过 TOR 与报告服务器交互,设备可以实现增强的报告不可链接性。此外,TOR 防止系统实体和蜂窝网络服务提供商基于网络标识符对设备进行匿名化。从本质上讲,通过端到端加密和 TOR,本研究的系统防止了网络服务提供商从参与感知任务中获得任何额外信息。

所使用的密码学原语确保违规用户不能否认其行为。更具体地说,在注册阶段执行的交互式协议保证了签名密钥仅被设备所知,因此,确保了不可抵赖性。此外,数字签名是用仅设备所知的密钥生成的,从而实现了不可否认性。

本方案可以在不必然披露其身份的情况下驱逐违规设备。为了实现对不当行为的移动客户端的永久驱逐,注册阶段可以通过涉及网络运营商的认证方法进行增强。本研究考虑在半信任环境中运行。特别是,个人认证中心可能会被破坏,并为未经身份提供者认证的设备发行证书。如果发生这种情况,个人认证中心将不拥有任何发行伪名的安全断言标记语言断言,因此,它可以因不当行为而受到责任追究。此外,身份提供者不能错误地认证未注册的设备:它不能伪造包含在安全断言标记语言断言中的授权令牌。因此,个人认证中心将拒绝发行伪名,从而身份提供者将被追究责任。此外,安全断言标记语言认证响应由身份提供者进行数字签名,因此不能被恶意设备伪造或篡改。

恶意报告服务器试图利用完全撤销协议进行用户匿名化的特殊情况是不当行为的一个特例。为了减轻这种情况,本研究要求在启动解决和撤销协议之前,向决议机构提供强有力的不当行为迹象。恶意用户不能伪造收据,因为它们是由报告服务器签名的。此外,它们被绑定到特定任务,因此不能被用来从其他任务中获得奖励。勾结的恶意用户可能会交换收据。然而,所有收据在提交后都被任务协调器作废,因此,它们不能被“双重消费”。由报告服务器生成的收据由任务协调器验证,它们都不知道用户的长期身份。因此,激励机制保护了用户匿名性。

3　实验与分析(Experiment and analysis)

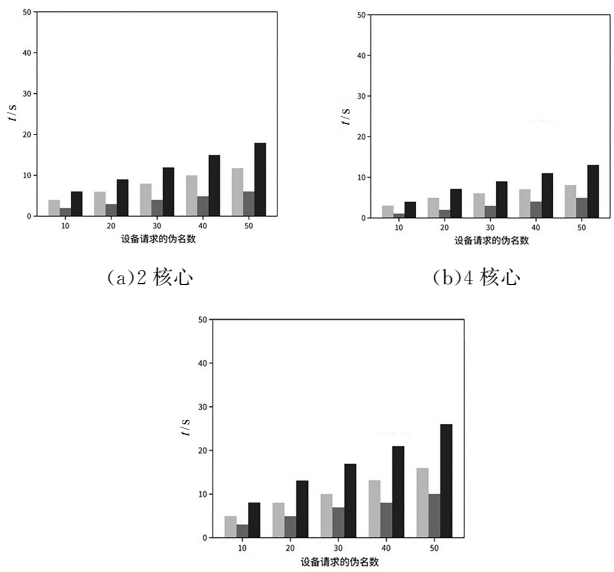
3.1　实验设置

为了测试身份提供者、群签名密钥分发者、个人认证中心和决议机构被部署在具有双核心 2.0 GHz CPU 的独立虚拟机上。本研究在两个虚拟机上分布了个人认证中心提供的服务,以进行本研究的可靠性评估。本研究使用 OpenSSL 库进行密码学操作,即椭圆曲线数字签名算法和传输层安全协议,以及 JDBC 库来实现群签名方案。本研究将感知应用程序部署在不同配置的 Android 智能手机上,包括具有 4 核心/1 GB RAM 和 2 核心/1 GB RAM 的手机。本研究使用 Jmeter 来模拟多个设备同时访问基础设施。

在样本提交和验证方面,本研究采用了在 224 位素数域(secp224k1 曲线)上计算的椭圆曲线数字签名算法,从而实现了 112 位的安全级别。

3.2　实验设置

图 2 展示了在两部移动设备上认证和获取伪名协议的性能。其中图 2(a)展示了 2 核心情况,图 2(b)展示了 4 核心的情况,图 2(c)展示了 4 核心且有 TOR 的情况。在这次评估中,设备从一组 10 个中请求一个授权令牌。本研究展示了执行算法的不同步骤所需的时间,平均值为 50 次观察结果。对于 2 核心手机,获得认证和十个伪名所需的时间大约为 8s。随着设备请求更多的伪名,这个时间线性增加:对于 50 个伪名,认证协议在 22s 内执行完毕。在身份提供者端,基于群签名的认证需要 4s。对于 4 核心设备,协议所需的时间显著减少。当使用 TOR 时,本研究会经历额外的网络延迟。TOR 引入了大约 10s 的延迟,从而将 50 个伪名的认证时间提高到 23s。即使在大量的任务周期中,这样的伪名数量也能提供足够的隐私。



(a)2 核心　　(b)4 核心

(c)4 核心(有 TOR)

图 2　认证协议评估

Fig. 2 Certification protocol assessment

图 3 评估了实现的私有信息检索方案:本研究展示了在 4 核心设备上获取一个授权令牌(针对一个任务)所需的时间,作为活跃任务数量的函数。随着系统中活跃任务数量的增加,这

个延迟轻微增加。即使在一组 100 个活跃任务中，私有信息检索协议也在大约 3.5s 内执行完毕。

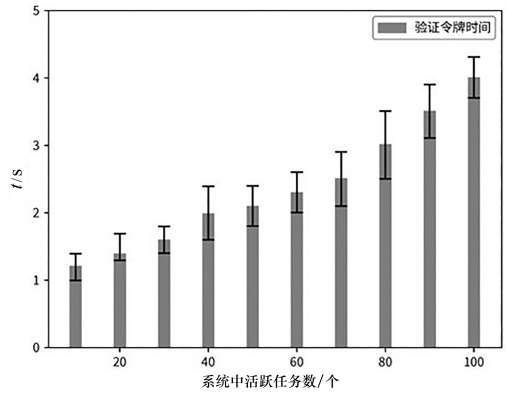


图 3 令牌获取时间

Fig. 3 Token acquisition time

3.3 基础设施端评估

图 4 显示了单个设备撤销所需的时间，作为数据库中伪名数量的函数。决议机构向个人认证中心查询设备用于请求伪名的授权令牌。检索到令牌后，决议机构要求群签名密钥分发者将其转换为设备的长期标识符。然后，群签名密钥分发者使所有与令牌对应的分配器失效，并通知身份提供者。因此，个人认证中心撤销了所有设备伪名。这两个处理延迟分别计为在个人认证中心和群签名密钥分发者上花费的时间。

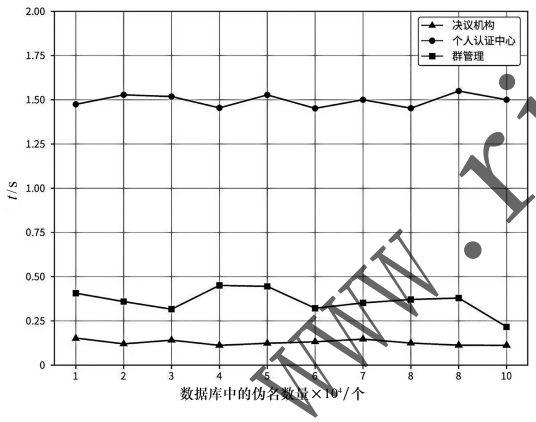


图 4 设备撤销评估

Fig. 4 Device revocation assessment

假设所有设备具有相同的请求策略来生成伪名集。这最大化了数据库集的熵。每个假定的设备获得了 10 个令牌，用于请求每个令牌的 10 个伪名，从而给出了整体比例 1 个设备：10 个令牌：100 个伪名。图 4 中的箱线图显示了在 100 次运行中平均的结果，伪名集从 10 000 个线性增加到 100 000 个项目。系统的性能不受集大小的显著影响。平均而言，撤销一个设备需要 2.3s。

4 结论(Conclusion)

本研究提出的隐私交易保护方案通过多层次架构有效解决了移动群智感知中隐私保护和用户激励的双重挑战。该方案基于匿名凭证和加密技术，既保证了用户贡献数据的隐私性，又在数据交易过程中提供了公平的奖励机制。此外，通过引入反向拍卖和伪名认证机制，方案确保了在不泄露用户身份的情况下对恶意用户的追责，从而提升了系统的安全性和可操作性。实验与理论分析表明，该方案不仅在效率上具备实际可行性，还能在面对恶意攻击时提供高度的隐私保护。未来工作将进一步优化激励机制与隐私保护的平衡，为更广泛的移动群智感知应用提供支持。

参考文献(References)

[1] 刘峰，杨杰，李志斌，等. 一种基于区块链的泻用型数据隐私保护的安全多方计算协议[J]. 计算机研究与发展，2021，58(2)：281-290.

[2] SISZ Z，SOURI A. Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things[J]. Transactions on emerging telecommunications technologies，2024，35(4)：e4217.

[3] GOSAIN I，GUPTA A，MONGIA A，et al. A Survey of incentive mechanism in MCS：types and characteristics[C]// IEEE. 2023 IEEE World AI IoT Congress (AIIoT). New York：IEEE，2023：613-619.

[4] GISDAKIS S，MANOLOPOULOS V，TAO S，et al. Secure and privacy-preserving smartphone-based traffic information systems[J]. IEEE transactions on intelligent transportation systems，2014，16(3)：1428-1438.

[5] SEDAR R，KALALAS C，VAZQUEZ-GALLEGO F，et al. A comprehensive survey of V2X cybersecurity mechanisms and future research paths[J]. IEEE open journal of the communications society，2023，4：325-391.

[6] RAN J R，CHEN B. A comprehensive roadmap for transforming healthcare from hospital-centric to patient-centric through healthcare Internet of Things (IoT)[J]. Engineered science，2024，30：1175.

[7] ZHAO P，YANG Z，ZHANG G. Personalized and differential privacy-aware video stream offloading in mobile edge computing[J]. IEEE Transactions on cloud computing，2024，12(1)：347-358.

[8] LI M，MA M，WANG L，et al. Quality-Improved and Delay-Aware incentive mechanism for mobile crowdsensing with social concerns：a stackelberg game approach[J]. IEEE transactions on computational social systems，2024：1176-1178.

[9] KRONTIRIS I，ALBERS A. Monetary incentives in participatory sensing using multi-attributive auctions[J]. International journal of parallel，emergent and distributed systems，2012，27(4)：317-336.

[10] DI B，WANG T，SONG L，et al. Incentive mechanism for collaborative smartphone sensing using overlapping coalition formation games[C]// IEEE. 2013 IEEE Global Communications Conference (GLOBECOM). Atlanta：IEEE，2013：1705-1710.

[11] AUXILIA M，RAJA K. Dynamic access control model for cloud computing[C]// IEEE. 2014 Sixth International

Conference on Advanced Computing (ICoAC). Piscataway, NJ:IEEE, 2014:47-56.
[12] KOUTSOPOULOS I. Optimal incentive-driven design of participatory sensing systems[C]// IEEE. Proceedings IEEE INFOCOM. Turin:IEEE, 2013:1402-1410.
[13] WU E,PENG Z. Research Progress on Incentive Mechanisms in Mobile Crowdsensing[J]. IEEE Internet of Things journal, 2024,11(14):24621-24633.
[14] GISDAKIS S,GIANNETSOS T,PAPADIMITRATOS P. SPPEAR: security & privacy-preserving architecture for participatory-sensing applications[C]// ACM. Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks. New York: ACM, 2014: 39-50.
[15] CHRISTIN D. Privacy in mobile participatory sensing: Current trends and future challenges[J]. Journal of systems and software, 2016,116:57-68.
[16] KAPADIA A,KOTZ D,TRIANDOPOULOS N. Opportunistic sensing: Security challenges for the new paradigm [C]// IEEE. 2009 First International Communication Systems and Networks and Workshops. Piscataway, NJ: IEEE, 2009:1-10.
[17] SHIN M,CORNELIUS C,PEEBLES D,et al. AnonySense: A system for anonymous opportunistic sensing[J]. Pervasive and mobile computing, 2011,7(1):16-30.
[18] DE CRISTOFARO E,SORIENTE C. Extended capabilities for a privacy-enhanced participatory sensing infrastructure (PEPSI)[J]. IEEE transactions on information forensics and security, 2013,8(12):2021-2033.
[19] BOUTSIS I,KALOGERAKI V. Privacy preservation for participatory sensing data[C]// IEEE. 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom). Piscataway,NJ:IEEE, 2013:103-113.
[20] KAZEMI L,SHAHABI C. TAPAS: Trustworthy privacy-aware participatory sensing[J]. Knowledge and information systems, 2013,37:105-128.
[21] AOKI S,KOBAYASHI H,IWAI M,et al. Perturbation with general tendency for mobile community sensing[C] // IEEE. Proceedings of IEEE 2nd Int. Conf. Mobile Services. Piscataway,NJ:IEEE, 2013:23-30.
[22] GIANNETSOS T,GISDAKIS S,PAPADIMITRATOS P. Trustworthy people-centric sensing: Privacy, security and user incentives road-map[C]// IEEE. 2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET). Piscataway,NJ:IEEE, 2014:39-46.
[23] BONEH D,BOYEN X,SHACHAM H. Short group signatures[C]// Springer. Annual International Cryptology Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004:41-55.
[24] CAMENISCH J,HOHENBERGER S,KOHLWEISS M, et al. How to win the clonewars: efficient periodic n-times anonymous authentication[C]// ACM. Proceedings of the 13th ACM Conference on Computer and Communications Security. New York:ACM, 2006:201-210.
[25] DIMITRIOU T,KRONTIRIS I,SABOURI A. PEPPeR: A querier's privacy enhancing protocol for participatory sensing[C]// Springer. Security and Privacy in Mobile Information and Communication Systems. Berlin,Heidelberg:Springer, 2012:93-106.
[26] DAS T, MOHAN P, PADMANABHAN V N, et al. PRISM: platform for remote sensing using smartphones [C]// ACM. Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services. New York:ACM, 2010:63-76.
[27] GANTI R K, PHAM N, TSAI Y E, et al. PoolView: stream privacy for grassroots participatory sensing[C]// ACM. Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems. New York: ACM, 2008:281-294.
[28] YAO Y,YANG L T,XIONG N N. Anonymity-based privacy-preserving data reporting for participatory sensing [J]. IEEE Internet of Things journal, 2015,2(5):381-390.
[29] CHRISTIN D,ROBKOPF C,HOLLICK M,et al. IncogniSense: an anonymity-preserving reputation framework for participatory sensing applications[J]. Pervasive and mobile computing, 2013,9(3):353-371.
[30] GISDAKIS S,GIANNETSOS T,PAPADIMITRATOS P. SHIELD: A data verification framework for participatory sensing systems[C]// ACM. Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. New York:ACM, 2015:1-12.
[31] WU H T,ZHENG Y,ZHAO B,et al. An anonymous reputation management system for mobile crowdsensing based on dual blockchain[J]. IEEE Internet of Things journal, 2021,9(9):6956-6968.
[32] 赵国锋,吴昊,王杉杉,等. 车联网 POI 查询中的位置隐私和查询隐私联合保护机制[J]. 电子与信息学报, 2024,46(1):155-164.
[33] 徐璠,吴慧慈,陶小峰. 5G 网络空间安全对抗博弈[J]. 电子与信息学报, 2020,42(10):2319-2329.
[34] 郑献春,王瑞,闫皓楠,等. 基于分布式爬虫的高性能 Tor 网络内容监控系统[J]. 信息安全学报, 2023,8(1): 144-153.
[35] 张宏俊,李鹏,叶昊,等. 基于区块链数据用户角色模型的印章数据加密安全系统. 江苏省:CN202410418367.9[P]. 2024-06-14.

作者简介:

周桂龙(1999-),男(汉族),宿迁,硕士生。研究领域:隐私保护。
张 洁(1981-),女(汉族),徐州,高级工程师,博士。研究领域:无线通信,移动网络。本文通信作者。