计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180080
55(7):1359-1370,2018

移动群智感知中基于用户联盟匹配的隐私保护激励机制

熊金波[1] 马 蓉[1] 牛 犇[2,3] 郭云川[2,3] 林 立[1]
[1](福建师范大学数学与信息学院 福州 350117)
[2](中国科学院信息工程研究所 北京 100093)
[3](信息安全国家重点实验室(中国科学院信息工程研究所) 北京 100093)
(jinbo810@163.com)

Privacy Protection Incentive Mechanism Based on User-Union Matching in Mobile Crowdsensing

Xiong Jinbo[1], Ma Rong[1], Niu Ben[2,3], Guo Yunchuan[2,3], and Lin Li[1]
[1](*College of Mathematics and Informatics*, *Fujian Normal University*, *Fuzhou* 350117)
[2](*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093)
[3](*State Key Laboratory of Information Security* (*Institute of Information Engineering*, *Chinese Academy of Sciences*), *Beijing* 100093)

Abstract As a novel Internet of things (IoT) sensing mode, mobile crowdsensing provides a new way and means for ubiquitous social perception. A large number of sensing data containing sensitive and private information of sensing users is gathered in the mobile crowdsensing, and a great deal of valuable information can be mined, which greatly increases the risk of hacker attacks and private data leakage. While encouraging more sensing users to participate in sensing tasks and providing real data, how to better protect the privacy of sensing data and sensing platform has become a prominent and pressing key issue. In order to solve the above problems, this paper proposes a user-union matching scheme based on the Bloom filter. Before the sensing users upload the sensing data who can choose using the Bloom filter and the binary product of the confusion vector to estimate the similarity, and effectively protect personal privacy information. Meanwhile, aiming at the efficiency of the private set intersection of the sensing data, this study puts forward a light-weight private sensing data set intersection protocol, which can realize private sensing data intersection operation without leakage of any user's real sensing data. Furthermore, we propose a reputation-aware incentive mechanism based on user-union matching, which can effectively control the budget expenditure on the basis of improving the processing efficiency of sensing tasks. Finally, the security analysis shows that the proposed user-union matching scheme is provably secure, and the proposed private sensing data set intersection protocol is secure, and the performance analysis and experimental results show that the proposed reputation-aware incentive mechanism is efficient and effective.

收稿日期:2018-02-01 **修回日期**:2018-05-08
基金项目:国家重点研发计划项目(2016YFB0800700);国家自然科学基金项目(61502489,61502103,61402109);2018年国家级大学生创新创业训练计划(创新训练类)项目(201810394008).
This work was supported by the National Key Rereach and Develpment Program of China (2016YFB0800700), the National Natural Science Foundation of China (61502489, 61502103, 61402109), and the 2018 National Undergraduate Training Programs for Innovation and Entrepreneurship (Innovation Training) (201810394008).
通讯作者:牛犇(niuben@iie.ac.cn)

Key words mobile crowdsensing; union matching; private set intersection; reputation incentive; privacy protection

摘 要 移动群智感知网络作为一种全新的物联网感知模式为实现泛在深度社会感知提供了一种全新的方式和手段.在移动群智感知网络中汇聚了大量蕴含用户敏感、隐私信息的感知数据,并能从中挖掘出大量极具应用价值的信息,这极大地增加了黑客攻击、隐私数据泄露的风险.在激励更多感知用户参与感知任务并提供真实数据的同时如何更好地保护感知数据和感知平台的隐私安全成为一个突出而紧迫的关键问题.针对上述问题,提出一种基于布隆过滤器的用户联盟匹配方案,利用布隆过滤器和二元混淆向量内积计算进行相似度估计,在用户上传感知数据之前可选择进行用户联盟匹配形成感知用户联盟,从而有效保护个人隐私信息;同时针对现有隐私数据交集计算的效率问题提出一种轻量级感知数据交集计算协议,在不泄露任一方真实数据的情况下,实现隐私数据交集运算.最后提出一种基于用户联盟匹配的信誉感知激励机制,在提高感知任务处理效率的基础上有效地控制了预算开支.安全分析表明:所提用户联盟匹配方案是可证明安全的,所提感知数据交集计算协议是安全的.性能分析和实验结果表明:所提出的信誉感知激励机制是高效的.

关键词 移动群智感知;联盟匹配;隐私交集计算;信誉激励;隐私保护

中图法分类号 TP391

随着传感器能力的快速提升以及移动智能终端设备的广泛普及使得移动群智感知网络成为了一种全新的物联网感知模式[1].通过利用大量移动智能终端和移动传感器等普适感知设备采集特定范围内的个体、情景及环境感知数据等,以完成那些仅依靠个体很难实现的大规模、复杂的泛在深度社会感知任务[2].同时,由于其感知数据具有极大潜在价值,使其应用范围不断扩展与延伸.尽管如此,其在多方面也存在新的问题与挑战,尤为突出的是移动群智感知网络的隐私安全问题[3].在移动群智感知网络中,感知用户将感知到的数据实时发送给感知平台,感知平台收集某时间内所参与感知任务的所有感知用户的数据并进行初步数据处理,再与服务提供商进行感知数据交易,并由服务提供商对交易所得到的感知数据进行进一步的分析与处理,后续为用户制定个性化的服务策略以及实现用户行为预测等.在此过程中的感知数据收集和处理会给感知用户的隐私造成威胁.一方面,如果感知用户直接上传隐含敏感信息的感知数据,而不采用适当数据隐私保护技术将可能造成其隐私泄露;另一方面,感知平台对上传后的感知数据进行处理也给感知数据的隐私带来了威胁.因此,感知用户在上传感知数据前如何选择数据隐私保护策略和感知平台对收集到的感知数据如何进行安全的隐私保护计算处理成为群智感知网络发展所面临的严峻挑战之一.如果能够解决感知用户数据和感知平台的隐私保护问题,将减少用户对隐私泄露的顾虑从而保证感知任务所需的感知数据收集质量,提升感知任务的质量和效率,并设计有效的激励机制对感知用户参与感知任务所付出代价进行补偿,以吸引更多用户长期参与其中,将使得移动群智感知任务、感知数据规模更加庞大,其应用进一步得到拓展.

现有研究中,移动群智感知网络的隐私保护方案大多数假设其感知平台完全可信,感知用户在参与感知任务过程中采取隐私保护措施,对每个用户在第 t 次感知任务中提供的真实感知数据选择一个数据隐私保护水平[4-6],数据隐私保护可利用对真实感知数据添加噪声[7-9]、k-anonymity[10-11]等方式,每个用户在不知道其他用户的隐私偏好情况下将隐私保护处理后的数据和数据隐私保护水平上传给感知平台进行聚合[12-13].感知平台从感知用户处收集到所有隐私保护处理后的感知数据集和用户的隐私保护水平之后再交易给服务提供商,虽能起到一定的隐私保护效果,但仍存在着许多尚未解决的 3 个问题:

1) 群智感知网络用户数据量庞大,若每个用户都采用一定的隐私保护方法对真实数据进行处理后再上传,感知平台所收集到的感知数据集的数据真实性和可用性将大打折扣.

2) 大多数方案对感知平台完全可信的假设在实际应用中并不成立,在已有的一些数据聚合方案中常用同态加密[13]的方式实现非完全可信的感知

平台在不知道任一感知用户上传数据的情况下进行隐私数据聚合.但面对庞大的数据量和感知端有限的计算能力,同态加密的计算效率不再满足需求[14].

3) 在移动群智感知网络中,在保护感知用户数据隐私的同时还需考虑合理有效的激励机制构建,要保证感知用户(尤其是信誉好的用户)数量,并在提高感知任务处理效率的基础上有效地对任务预算开支进行控制.

为了解决上述问题,本文提出一种基于用户联盟匹配的信誉感知激励机制,感知用户在上传感知数据前,用户可选择采用布隆过滤器和二元混淆向量内积计算进行相似度估计形成感知用户联盟后再上传感知数据集.感知平台对所收集到的感知(联盟)数据集合进行隐私数据交集计算,综合考虑其计算效率和对数据的隐私保护,利用伪随机函数在不泄露任一(联盟)数据集信息的前提下,协同计算各(联盟)数据集合交集后与服务提供商进行交易获得收益.并通过初始设置感知用户(联盟)的信誉值,在任务分配过程中选择信誉度高的感知用户(联盟)来参与任务处理,并通过设置因子减小感知用户(联盟)的花费代价,能够在提高任务处理效率的基础上有效控制任务预算.本文主要贡献有4个方面:

1) 提出一种基于布隆过滤器的用户联盟匹配方案,采用布隆过滤器和二元混淆向量内积计算进行相似度估计,使得用户可选择在上传数据前形成用户联盟,整个算法不涉及耗时的加密运算,计算开销较小.

2) 针对现有隐私数据交集计算的效率问题,提出一种轻量级感知数据交集计算协议,面对半可信的感知平台,利用伪随机函数对用户(联盟)数据集进行加密和伪随机扰乱后上传到感知平台,再在集合元素的随机函数上求交集.服务提供商可通过伪随机函数的逆过程获得感知数据集合交集.该协议具有较高计算效率,能够满足数据量庞大的群智感知网络的计算需求.

3) 针对现有激励机制在用户选择的随机性、任务处理效率和预算控制方面的不足,提出一种信誉感知激励机制.初始设置感知用户(联盟)的信誉值,在任务分配过程中选择信誉度高的感知用户(联盟)来参与任务处理,并通过设置因子减小感知用户(联盟)的花费代价,可在提高任务处理效率的同时有效控制任务预算开支.

4) 安全分析表明:用户联盟匹配方案是可证明安全的,基于用户联盟匹配的信誉感知激励机制能够满足安全目标,性能分析和实验结果表明所提机制是高效的.

1 相关研究工作

在移动群智感知网络中,普通用户需要主动参与感知任务.然而,用户参与感知任务需要付出一定的代价(例如网络带宽、能耗、费用等消耗),因此需要设计一种合理的补偿激励机制来对用户的消耗代价进行补偿[15-16],以吸引更多用户主动参与到感知任务中来.当前对于移动群智感知网络激励机制已开展一些研究工作,主要可分为以感知平台为中心和以感知用户为中心的2类激励机制模式.以感知平台为中心的激励机制是由感知平台进行任务发布,感知用户根据任务信息自愿选择是否参与任务后由感知平台进行支付报酬.Duan等人[17]将这种以感知平台为中心的激励模式建模为Stackelberg博弈进行进一步研究,综合考虑感知平台和用户仅知道所有用户的感知成本的累积分布函数情况;Han等人[18]研究了移动群智感知网络竞争拍卖激励机制问题,首先感知平台发布一些感知任务,然后感知用户根据他们的感知成本和时间来竞争这些任务,最后感知平台在预算限制下支付给用户感知报酬.另一类以用户为中的激励机制模式是感知用户接收到感知任务信息后提供自身信息及报价,再由感知平台进行选择合适的感知用户参与感知任务.Jaimes等人[19]采用以用户为中心的基于逆向拍卖的动态价格激励机制,进一步考虑了用户基于位置进行感知,而感知平台需要满足覆盖约束和预算约束的情况;文献[20]中把感知任务分成3种不同的类型(即效用值随感知任务大小成正比例变化、效用值随感知任务处理过程成正比例变化以及效用值随任务处理过程成反比例变化),对于每一种任务类型用4种不同的激励机制(Proportion incentive policy, Participation-aware incentive policy, Quality-aware incentive policy, Thrifty incentive policy)计算报酬.其中用户参与激励机制策略PAIP(Participation-aware incentive policy)在选择感知用户时采用随机的方式,没有考虑感知用户自身的特点,这样感知用户在处理任务时目的性不强,在感知任务分配阶段用户的参与率不高,降低了整个任务的完成率,增加了代价花费,从而使任务总预算减少.

此外,感知数据会极大可能地泄露用户的隐私和敏感信息,因此必须设计合理的隐私保护机制在

完成感知数据收集任务的同时能够尽可能保护用户隐私安全. 现有的移动群智感知的隐私保护方案主要关注 3 类方法:

1) 匿名化[4-6,10-11]. 将身份信息移除后再将感知数据上报给感知平台. 这种方法的缺点是无法抵抗背景知识攻击,即仍然可以从匿名化的或其他定位传感器测量值中推断出用户频繁访问的位置以及其他个人信息.

2) 数据加密[13,21]. 使用加密技术将感知数据进行处理变换后上报给感知平台. 这种方法比较安全,但缺点是需要较大的计算开销,需要生成和维护多个密钥,灵活性较差.

3) 数据加扰[7-9]. 对感知数据添加一些噪音后上报给感知平台,添加的噪音需要保证用户个体的隐私信息得到保护,同时依然能够准确地计算出群体信息的统计结果. 但实际情况中噪音的添加往往使得聚合后的数据可用性大打折扣.

综上所述,现有解决移动群智感知网络中的激励机制和隐私保护方案均存在一定问题,现有激励机制在感知用户选择、任务处理效率和预算控制方面存在不足,亟需设计一种可兼顾任务处理效率和预算开支控制,同时保证充足的高信誉用户参与感知任务的激励机制;同时,感知用户所采用的隐私保护方法存在一定安全威胁(例如 k-anonymity 不可抵御背景知识攻击),也缺乏对非完全可信的感知平台的隐私保护研究. 在实现隐私保护的基础上,如何有效减少计算开销、构建轻量级的隐私保护方案也亟待考虑.

2 系统模型、威胁模型和实现目标

为了方便描述本文所提方案与机制,表 1 中列出常用的符号及对应的描述.

Table 1 Symbol and Description

表 1 符号及描述

Parameters	Description
$A,B,\cdots$	User's Attribute Vector
BF_i	User Generated Bloom Filter
z_i	Random Number
θ,η	Prime Number
S	Sensing Dataset
N	The Sum of $r_i\eta-z_i$
E	Confusion Values in Binary Vectors
G	Binary Vectors Inner Product
π	Pseudorandom Permutation
F	Pseudorandom Function
I	Sensing Dataset Intersection
$Thres_i$	Threshold
Q_i	Reputation Value
u_x	the Task Utility Value
c_i	The Cost Function of Participate in the Sensing Task
P_x	The Reward Function of the Sensing Task

2.1 系统模型

在系统模型中,本文考虑一种典型的移动群智感知网络系统架构,包括一个半可信的感知平台、大量参与感知任务的感知用户和参与最终聚合数据交易的服务提供商,如图 1 所示:

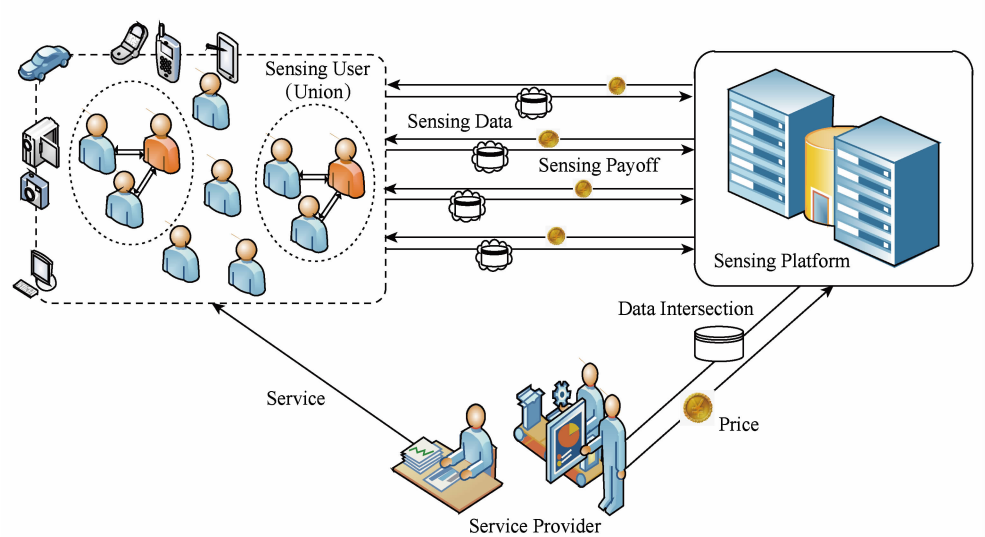


Fig. 1 System model

图 1 系统模型

1) 感知用户是使用移动感知设备(如智能终端设备、可穿戴设备及车载设备等)的社会普通用户,通过有线/无线网络与感知平台进行交互,上传感知数据并最大化获取相应收益.感知用户参与感知任务即可获得相应参与报酬.感知联盟是各感知用户为保护感知数据中蕴含的大量敏感和隐私信息,在上传数据到感知平台之前可在保证自身数据安全前提下进行隐私匹配形成的用户联盟,感知用户在形成感知联盟后再将联盟数据集上传到感知平台中.

2) 服务提供商通过感知平台购买感知数据,用于机器学习、数据可视化、大数据分析等领域,为不同需求的用户提供后续服务.理性的服务提供商希望以合理的价格从感知平台获得可用性较好的数据.

3) 感知平台分别与感知用户和服务提供商进行交互.在基于用户联盟匹配的信誉感知激励机制下,感知平台向移动感知用户发布感知任务,采取信誉感知激励机制吸引更多感知用户(联盟)参与感知任务上传感知数据.之后感知平台对所收集到的数据集进行隐私交集计算将所得结果卖给服务提供商以得到相应报酬.

2.2 安全需求

移动群智感知网络的可靠性和效率取决于通信系统的安全性,其网络越来越复杂,交互性与动态性也越强,也需要更先进的网络技术,同时需要更复杂的安全协议,以应对潜在的安全漏洞与威胁.设计移动群智感知网络隐私保护机制时,在充分考虑通信安全的同时,考虑到恶意攻击者的主要目的是侵犯尽量多的感知用户的隐私数据,为了防止攻击者达到目的,本文需达到3种安全需求:

1) 恶意攻击者即使监听系统中的通信数据流,也无法获取感知用户(联盟)的真实隐私数据.

2) 在联盟匹配过程中即使恶意攻击者试图设定尽可能多的属性和尽可能大的偏好程度发起攻击,但仍不能以此获得较高相似度,成为联盟匹配发起者的最优匹配者.

3) 即使恶意攻击者能够勾结感知平台访问到感知平台所收集的感知数据,他也无法获取感知用户(联盟)的个人真实隐私数据.

2.3 设计目标

在上述的系统模型和安全需求分析下,本文的设计目标是在信誉感知激励机制作用下的移动群智感知网络中提出一种行之有效的隐私保护方案.具体地,要达到2个主要目标:

1) 提出的方案必须满足安全需求.如引言所述,如果在移动群智感知网络中不考虑安全和隐私问题,那么个人用户的隐私数据就会被泄露,就会阻碍移动群智感知网络的进一步发展与应用.因此,提出的方案必须能够满足上述安全需求.

2) 提出的用户联盟匹配方案和感知数据交集计算协议在通信上有较高的效率.虽然感知用户与感知平台之间是通过高带宽低延迟的有线/无线网络通信,但要支持大量感知用户同时发送数据给感知平台,所提方案必须考虑通信效率,这样实时感知的数据才能及时传送到感知平台进行处理.

3 方案构造

3.1 用户联盟匹配方案

在移动群智感知网络中感知用户数据量庞大,若每个感知用户都采用一定的隐私保护方法对真实数据进行处理后再上传,感知平台所收集到的感知数据集中的数据真实性和可用性将大打折扣.为解决这一问题,本文提出一种基于布隆过滤器的用户联盟匹配方案,使得感知用户在上传数据之前通过隐私匹配形成感知用户联盟(联盟中用户数≥2),该联盟用户所形成的感知数据集由3.2节的随机置换处理后上传.在移动群智感知网络中,处于移动终端无线通信(如蓝牙、WiFi等)范围内的任意2个感知用户进行一次信息交互即可完成隐私匹配选择形成感知用户联盟,无需第三方介入.假设 A 和 B 分别是用户联盟匹配的发起者和响应者,本联盟匹配方案主要包括为所有感知用户建立属性向量集合,并设置本匹配方案涉及到的所有参数;感知用户输入自己的属性向量集合,离线生成相应布隆过滤器并输出;输入联盟匹配发起者 A 和响应者 B 的布隆过滤器,将布隆过滤器视为二元向量,计算输出2个二元向量的内积;联盟匹配发起者根据所得二元向量内积,采用基于布隆过滤器的相似度估计公式[22]计算 A 和 B 的属性向量集合相似度,由此确定联盟匹配对象部分,匹配发起者收集与所有响应者的相似度,通过一次通信,联盟匹配发起者可选择相似较高的若干响应者作为联盟匹配对象,形成感知用户联盟(联盟中用户数≥2).用户联盟匹配方案具体流程如图2所示.

① 设置参数.每个用户的智能感知终端首次进行用户联盟匹配时,都需设定其属性向量集合.假设联盟匹配发起者 A 和某响应者 B 的属性向量集合

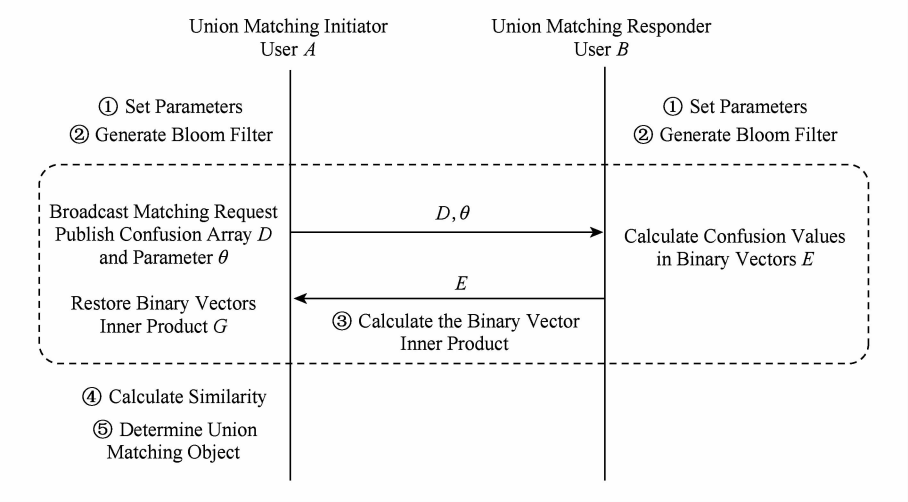


Fig. 2 User-union matching scheme flow diagram

图 2 用户联盟匹配方案流程图

依次记为 $A=\{\langle x_1,a_1\rangle,\langle x_2,a_2\rangle,\cdots,\langle x_{n_A},a_{n_A}\rangle\}$, $B=\{\langle y_1,b_1\rangle,\langle y_2,b_2\rangle,\cdots,\langle y_{n_B},b_{n_B}\rangle\}$,其中属性 x_i 和 y_j 的内容与个数均由 A 和 B 自行设定,且 $n_A\leqslant n$, $a_i,b_j\in[1,l]$. 预先设定常数 n 和 l,要求足以表示用户的所有属性并能区分对每个属性的偏好差异即可. 为了简化联盟匹配问题,假设所有用户对某一个属性的表达方式是唯一的. 另外,令 $m=nl$, A' 和 B' 分别表示 A 和 B 离散后的集合,且 $|A'|=m_A$, $|B'|=m_B$, $s'=|A'\bigcap B'|$, $p(A,B)$ 表示 A 和 B 的相似度函数. 布隆过滤器 (w,m,l,H) 中,参数 w 表示布隆过滤器的长度, m 表示编码的元素个数, l 表示散列函数的个数, H 表示散列函数集合. 散列函数集合 $H=\{h_i\}_{i=0}^{l-1}$ 中的散列函数值域均为 $[0,w-1]$,且相互独立. $BF_{A'}$, $BF_{B'}$ 和 $BF_{\cap}$ 分别表示编码了集合 A', B' 和 $A'\bigcap B'$ 中所有元素的布隆过滤器,其第 $i(0\leqslant i\leqslant w-1)$ 位依次记为 $BF_{A'}[i]$, $BF_{B'}[i]$ 和 $BF_{\cap}[i]$. $t_{A'}$ 和 $t_{B'}$ 分别表示 $BF_{A'}$ 和 $BF_{B'}$ 中 1 的个数.

② 生成布隆过滤器. 根据感知用户设定的属性向量集合,离线生成相应的布隆过滤器. 例如发起者 A 输入 $S=A'$,生成布隆过滤器模块对于每一个 $a'_{ij}=(x_i,f_i(j))\in A'$,把 w 位数组 $BF_{A'}$ 的第 $h(a'_{ij})$ $(0\leqslant i\leqslant l-1)$ 位设为 1,其他位设为 0,生成布隆过滤器 $BF_{A'}$,计算 $BF_{A'}$ 中 1 的个数,记为 $t_{A'}$. 同样地,响应者 B 输入 $S=B'$,生成布隆过滤器 $BF_{B'}$,计算 $BF_{B'}$ 中 1 的个数,记为 $t_{B'}$.

③ 计算二元向量内积. A 输入 $BF_{A'}$,利用素数 $\theta(|\theta|>64\text{ b})$ 和 $\eta(\eta>(w+1)\theta^2)$,以及随机数 $z_i(i=1,2,\cdots,w-1)$ 混淆 $BF_{A'}$ 中的 1 和 0,当 $BF_{A'}[i]=1$ 时,令 $d_i=\theta+z_i+r_i\eta$,否则令 $d_i=z_i+r_i\eta$,以此混淆方式生成数组 $D=\{d_i\}_{i=0}^{w-1}$,并计算所有 $r_i\eta-z_i$ 之和 N 以便最后抵销混淆,输出参数 θ, η, N 和 $D=\{d_i\}_{i=0}^{w-1}$. 其中, η 与 N 保密. A 广播匹配请求,并公开 θ 和 $D=\{d_i\}_{i=0}^{w-1}$. B 为联盟匹配响应者之一,若同意匹配,接收 θ 和 D,把 $BF_{B'}[i]$ 的信息添加到数组 $D=\{d_i\}_{i=0}^{w-1}$ 中,得到数组 $e_i(i=0,1,\cdots,w-1)$. 当 $BF_{B'}[i]=1$ 时, $e_i=\theta d_i$,否则 $e_i=d_i$,最后计算并输出 $e_i(i=0,1,\cdots,w-1)$ 的和值 E;最后向发起者 A 发送 E, $t_{B'}$ 和 $m_B=|B'|$. 当 A 接收到 E, $t_{B'}$ 和 m_B 之后,还原二元向量内积:

$$W=(E+N)\bmod\eta,\qquad G=\frac{W-(W\bmod\theta^2)}{\theta^2},\tag{1}$$

将布隆过滤器 $BF_{A'}$ 和 $BF_{B'}$ 视为二元向量, G 即为二元向量 $BF_{A'}$ 和 $BF_{B'}$ 的内积.

④ 计算相似度. 发起者 A 计算其与响应者 B 的相似度, $\hat{p}(A,B)$ 为多元二维向量集合的相似度函数 $p(A,B)$ 的估计[19]:

$$\hat{p}(A,B)=\frac{2\left[\ln\left(w-\dfrac{Gw-t_{A'}t_{B'}}{w-t_{A'}-t_{B'}+G}\right)\right]}{k(\ln(w-1)-\ln w)(m_A+m_B)},\tag{2}$$

⑤ 确定联盟匹配对象. 发起者 A 和所有响应者 $V_i\in V$ 按上述步骤进行匹配,找到相似较高的若干用户作为联盟匹配对象.

$$V_{\text{match}}=\arg(\max\{p(A,V_i)\}_{i=1}^{\infty}),\tag{3}$$

3.2 感知数据交集计算协议

在感知用户自由选择通过用户联盟匹配方案形成感知用户联盟后还需要对其数据集进行隐私保护,上传到感知平台并由感知平台进行初步数据计算处理如隐私交集计算等,最后将最终结果数据与

服务提供商进行交易.本文所提出的感知数据交集计算协议是一个多方协议,仅在半诚实的感知平台情况下是安全的.在协议中,k 表示计算安全参数(即伪随机置换的密钥长度),而 s 表示统计安全参数.对于 $\lambda \geqslant 1$,本文定义集合 $S^{\lambda}=\{x \parallel 1,2,\cdots,x \parallel \lambda : x \in S\}$ 且 $(S^{\lambda})^{-\lambda}=S$.如果 $F:U \rightarrow V$ 是一个函数,则 $F(S)=\{F(s):s \in S\}$ 表示 F 对集合 S 的评估.本文还用 F^{-1} 表示 F 的逆函数,即 $F^{-1}(F(S))=S$.如果 $\pi:[|S|] \rightarrow [|S|]$ 是一个置换,则集合 $\pi(S)$ 是 S 根据 π(假设元素的自然顺序)排列 S 的元素得到的集合,即 $\pi(S)=\{X_{\pi(i)}:x_i \in S\}$.让 S_i 成为感知用户(联盟)P_i 的感知数据集合.各方协同生成伪随机置换函数 F 的 k 位密钥 K.每一个感知用户(联盟)的随机置换由伪随机函数 $F_k(S_i)$ 分别对集合中的每个元素进行随机化处理,再通过伪随机置换 π 扰乱集合元素顺序,并将置换后的集合发送给感知平台.然后在感知平台集合元素的随机函数上求 $F_k(S_1)$ 到 $F_k(S_n)$ 的交集并将结果存储,以便进行与服务提供商间的数据交易,协议具体流程:

1) 设置和输入:设置 $F:\{0,1\}^k \times U \rightarrow \{0,1\}^{\geqslant k}$ 为伪随机置换,每一方都有一组 $S_i \subseteq U$ 作为输入,而感知平台没有输入.

2) 某一感知用户(联盟)生成一个随机 k 位的密钥 K 并发送给 i,其中 $i \in [2,n]$.

3) 每个感知用户(联盟)$i \subseteq [n]$ 将进行过随机置换的 $T_i=\pi_i(F_k(S_i))$ 数据集发送到感知平台,π_i 是一个伪随机置换.

4) 感知平台计算各数据集交集 $I=\bigcap_{i=1}^{n} T_i$ 并存储.

直观而言,该协议的安全性体现在各方不会收到彼此的消息,其唯一可能的恶意行为是改变他们自己的伪随机置换函数值,这只是改变他们的输入集合.半可信感知平台只接收由于伪随机置换函数的伪随机性而没有显示设置元素的信息的函数值.值得注意的是在协议中每个感知用户(联盟)P_i 调用伪随机函数共 $|S_i|$ 次,而感知平台只执行一个"明文"设定的交集计算而没有加密操作.一旦可以使用任何现有的算法来设置交集,感知用户(联盟)数据集合中几乎线性时间内完成 Hash 表的插入/查找,在大量数据中有较大的效率优势.此外,协议可以异步执行,每一感知用户(联盟)在不同的时间连接,将其感知数据集提交给感知平台,以后再获取输出.

3.3 信誉感知激励机制

该机制初始时为不同的感知用户(联盟)设置不同的信誉值,当感知平台发布感知任务并且感知用户(联盟)竞争参与这些感知任务时,感知平台会根据感知用户(联盟)的信誉值进行选择,优先选择信誉值高的感知用户(联盟)参与任务处理,并且通过因子调节感知用户(联盟)的代价花费.最后对感知用户(联盟)的信誉值进行更新之后,感知用户(联盟)再次进入到下一次的任务竞争中.通过该激励机制在提高感知用户(联盟)参与率和任务完成率的同时,减少感知用户(联盟)的花费,从而节省了总预算.

在感知任务激励过程中,移动群智感知网络主要包括 3 个部分:感知用户(联盟)集 U、任务集 T 和感知平台 ST.任务集 T 包括若干感知任务,每个任务的处理过程是轮流进行的(即在每个任务被执行之前,感知平台 ST 都会向感知用户(联盟)集 U 发布这个任务处理请求),每个感知用户(联盟)会根据任务情况决定是否接受请求来参与感知任务并获得相应报酬.这个过程会重复进行,直到所有的任务都被处理或全部预算用完.

信誉感知激励机制具体工作流程图如图 3 所示:

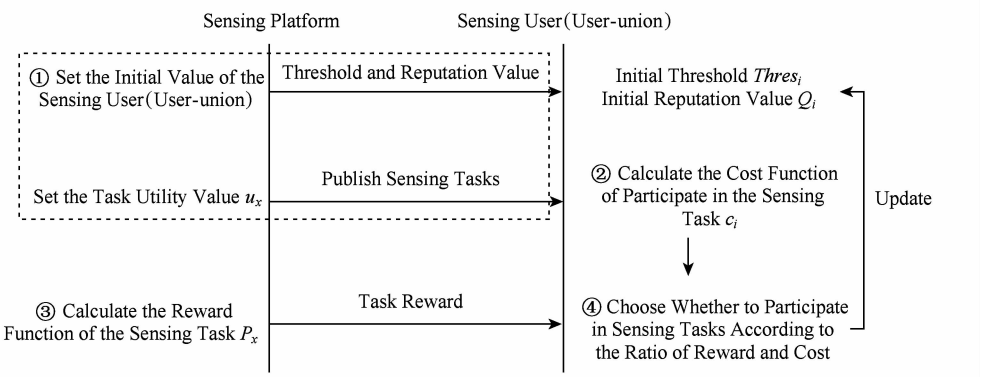


Fig. 3 Reputation-aware incentive mechanism flow diagram

图 3 信誉激励机制流程图

① 当有感知任务要处理时,感知平台 ST 首先把任务集 T 划分为若干任务 $x\subset\{1,2,\cdots,n\}$.并在任务发布区域选取一感知用户(联盟)集 U,对其进行划分 $U_i:i\subset\{1,2,\cdots,n\}$.对每一个感知用户(联盟)$i$ 设置一个独立的阈值 $Thres_i$,该值对其他感知用户(联盟)是保密的,并根据全部感知用户(联盟)的阈值和单个感知用户(联盟)的阈值设置一个信誉值 Q_i:

$$Q_i=\frac{\sum_{i=1}^{n}Thres_i}{Thres_i},\tag{4}$$

同时,针对划分的感知任务的不同,为每一个感知任务设置一个效用值,用 $u_x=f(\xi,\xi_x)$ 表示:

$$u_x=\frac{\xi_x}{\xi}.\tag{5}$$

② 当处理某一感知任务时,感知平台会选取信誉值大的感知用户(联盟)参与感知任务的处理过程.感知用户(联盟)U_i 在处理感知任务 x 时,会付出一定花费代价.针对一个感知任务 x,用 $c_i=f(\xi_x,u_x,Q_i)$ 来表示参与该任务的感知用户(联盟)的代价函数,即感知用户(联盟)的代价受参与的感知任务大小和感知用户(联盟)信誉值影响,与感知任务大小成正比关系,与感知用户(联盟)信誉值成反比关系:

$$c_i=\alpha\xi_x^{u_x}\times 0.5^{Q_i}\beta,\tag{6}$$

其中,α 和 β 是 2 个因子,且 $\alpha+\beta=10$.

③ 感知平台为鼓励更多感知用户(联盟)参与感知任务的处理过程,会在每个感知任务处理后为对应感知用户(联盟)提供报酬.对于感知联盟,将采用 VCG 机制对所得报酬在形成联盟的感知用户中进行分配.本文用 $P_x=f(u_x,n(t),B(t))$ 来表示报酬函数:

$$P_x=\frac{1}{a(n(t)+1)}u_xB(t),\tag{7}$$

其中,a 为正常数.通过这种方式,平台 ST 初始时会提供很高的报酬来鼓励感知用户(联盟)参与任务处理,随着感知用户(联盟)参与的比例越来越高(即 $n(t)$ 值越来越大,最终趋于稳定),报酬会慢慢趋于平稳.

④ 根据处理感知任务 x 时所需的代价 c_i 和平台 ST 对于 x 所支付的报酬 P_x,感知用户(联盟)i 将报酬 P_x 和代价 c_i 的比值与感知用户(联盟)阈值进行比较,如果比值大于阈值,则接受该感知任务处理请求,否则拒绝.最后利用感知用户(联盟)所处理感知任务的效用值来更新其信誉值,并参与竞争下一个感知任务处理请求,直到所有的感知任务全部处理完成或全部预算用完.

4 方案安全性分析

4.1 用户联盟匹配方案安全性分析

4.1.1 联盟匹配发起者的隐私安全

命题 1. 如果方案中的混淆方法[23]是安全的,本用户联盟匹配方案能保护匹配发起者 A 的隐私信息,即响应者不可能知道关于 A 属性集的任何信息.

证明. 对联盟发起者 A 而言,在整个联盟匹配方案中,响应者之一 B 知道所有关于 A 的信息只有参数 θ 和 $D=\{d_i\}_{i=0}^{w-1}$,其中数组 D 是 $BF_{A'}$ 混淆所得.因为,$d_i=\begin{cases}\theta+c_i+r_i\eta, & BF_{A'}[i]=1\\ c_i+r_i\eta, & BF_{A'}[i]=0\end{cases}$,对于 B 和攻击者而言,随机数 c_i 和 $r_i\eta$ 未知,难以区分 d_i 的表示形式,从而无法推测 $BF_{A'}[i]$是否等于 1.此外每一对随机数$(c_i,r_i\eta)_{i=0}^{w-1}$只使用一次且相互独立,因此,即使响应者之一 B 恶意地与发起者 A 进行多次匹配,也难以从所得 D 中推测出敏感信息.综上可知,B 与攻击者无法从所接收到的 θ 和 $D=\{d_i\}_{i=0}^{w-1}$ 推测出联盟匹配发起者 A 的任何属性或相关信息,从而联盟匹配发起者 A 的个人隐私是安全的. 证毕.

4.1.2 联盟匹配响应者的隐私安全

命题 2. 如果方案中的混淆方法[23]是安全的,本用户联盟匹配方案能保护匹配响应者 B 的隐私信息,即匹配发起者 A 除了相似度 p 之外,无法知道关于匹配响应者 B 的属性集的任何信息.

证明. 对匹配响应者 B 而言,联盟匹配发起者 A 仅知道 B 的 E,$t_{B'}$ 和 m_B,其中,$E=\sum_{i=0}^{w-1}e_i$,$e_i=\begin{cases}\theta d_i, & BF_{B'}[i]=1\\ d_i, & BF_{B'}[i]=0\end{cases}$,$t_{B'}$ 为布隆过滤器 $BF_{B'}$ 中 1 的个数,m_B 为 B'的模.显然,由于参数 θ 是公开的,只需知道 e_i,就能推测出 $BF_{B'}[i]$是否为 1.然而,由方案构造可知,除了响应者 B 之外,其他人均不知 e_i 的值,仅知道计算所输出的 E.E 中含有多个 $\theta(z_i+r_i\eta)$和$(z_i+r_i\eta)$,很好地隐藏了 $BF_{B'}$ 的相关信息,所以联盟匹配发起者 A 和攻击者无法从 E 推测出响应者 B 的 $BF_{B'}$,更无法推测出任何关于 B 的属性集的一个属性或其他信息,所以综上联盟匹配响应者 B 的个人隐私是安全的. 证毕.

4.2 感知数据交集计算协议安全性分析

感知数据交集计算协议在2种情况下是安全的:

1) 半诚实的感知平台和诚实的感知用户(联盟);

2) 诚实的感知平台和任何恶意的感知用户(联盟).

在情形1中由协议构造中可知,感知用户(联盟)最终上传到半可信感知平台的数据集是通过随机置换处理所得的数据集 $T_i=\pi_i(F_k(S_i))$,其中 $F:\{0,1\}^k\times U\rightarrow\{0,1\}^{\geqslant k}$ 为伪随机置换函数,π_i 是一个伪随机置换.根据其未知随机性,半可信感知平台和攻击者无法从数据集 T_i 推测出关于真实感知数据集 S_i 的任何信息,因此在该感知数据交集计算协议中感知用户(联盟)上传到感知平台的数据集是安全的.

在情形2中由协议构造可知,在协议进行过程中在各感知用户(联盟)彼此间没有交互不存在恶意勾结行为,对感知用户(联盟)而言,他们唯一可能的恶意行为就是改变其上传数据集的值 T_i,这只是改变他们的输入集合.但由于恶意用户(联盟)对其他的用户(联盟)数据集一无所知,即便改变了其上传数据信息,但在最终感知平台求解数据集交集时,并不会产生较大影响.综上,该感知数据交集计算协议是安全的.

5 性能分析与评价

本节主要从用户(联盟)端和感知平台端的计算开销分析用户联盟匹配方案和感知数据交集计算协议的算法复杂度和通信开销以及在信誉感知激励机制下从感知任务完成比例和感知预算剩余比例2个方面评价其有效性.

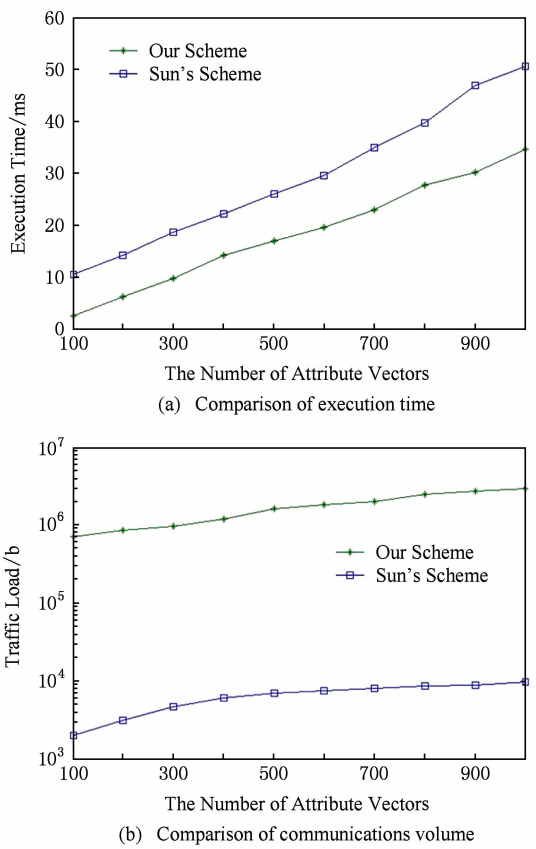
在用户联盟匹配方案中仅涉及用户端的开销,本文从匹配发起者与匹配响应者2方面进行分析,假设在方案中,每个感知用户的属性向量集合包含 n 个属性向量,每个属性的偏好值区间为 $[1,l]$,至多离散 $m(m=nl)$ 个属性向量.散列函数个数为 k,布隆过滤器的长度 $w=1.5km$ b以保证较低的错误率,方案中随机数取256 b.计算开销主要涉及SHA-1(Hash)、模幂(exp)、乘法(mul)和加减法(add/sub).通信开销是指用户接收和发送的以bit为单位的数据.在表2中将本文方案与同是基于布隆过滤器的Sun等人[24]所提出的轻量级隐私信息匹配方案进行,与本方案不同的是Sun[23]方案是利用布隆过滤器进行其时空剖面中共同元素的数量的准确度估计从而进行时空匹配.

Table 2 Performance Comparison of Privacy Information Matching Scheme

表2 隐私信息匹配方案性能对比

Scheme	Matching Participant	Off-line Computing Cost	Online Computing Cost	Traffic Load/b
Sun's Scheme[24]	Initiator		(km)Hash	
	Responder	(km)Hash		w
Our Scheme	Initiator	(km)Hash, $(2w)$mul, $(4w)$add/sub		$256w$
	Responder	(km)Hash	$(2w)$mul, $(4w)$add/sub	320

由表2可看出,本文方案的在线计算开销远小于Sun[24]方案,离线计算开销稍大于Sun[24]的方案,通信开销高于Sun[24]方案.但在移动群智感知网络中对执行时间有着较高要求,本文方案则具有较高的优势,离线计算开销可以预先离线计算,并不占用执行时间,而在线计算开销直接影响执行时间的长短,由图4(a)中明显看出本文方案任务执行时



(a) Comparison of execution time

(b) Comparison of communications volume

Fig. 4 Experimental comparison of matching scheme

图4 匹配方案实验对比图

间比 Sun[24]方案具有明显优势. 此外,在图 4(b)中可看出本文方案需要额外花费通信量传递 Sun[24]方案中未考虑的属性偏好信息,但在移动群智感知网络中采用蓝牙、WiFi 等传输方式,通信时间较短.

在感知数据交集计算协议中涉及用户(联盟)端和感知平台端的计算开销以及通信复杂度. 为描述简单起见,假设用户(联盟)端为 $U=\{A,B\}$,S 为各用户(联盟)的输入集合,A 集合的大小为 v,B 集合的大小为 w,$m=\max(v,w)$. 表 3 将本文所提非加密的感知数据交集计算协议与 Abadi 等人[25]所提出的利用同态加密和多项式插值实现的加密隐私数据交集计算协议进行比较.

Table 3 Performance Comparison of PSI Protocol

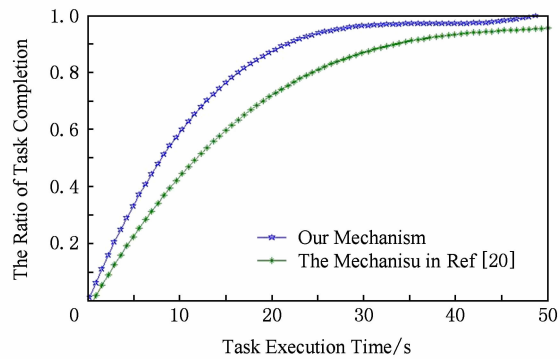
表 3 PSI 协议性能对比

Protocol	Computing Complexity of Sensing User(union)	Computing Complexity of Sensing Platform	Communication Complexity
Abadi's Protocol[25]	$O(m)$exp	$O(v+w)$exp	$O(w+v)$
Our Protocol	$O(m)$sym	$O(v+w)$sym	$O(w+v)$

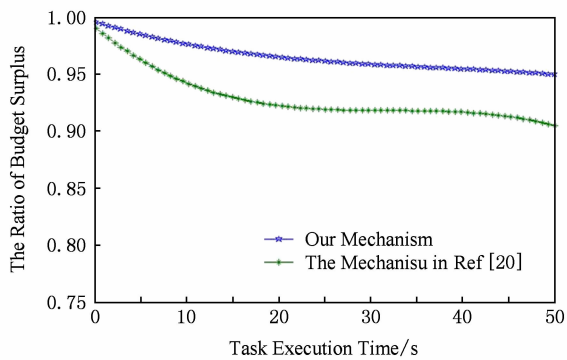
由表 3 中可看出,与 Abadi 等人[25]方案相比,本文所提协议采用对称加密操作,计算复杂度具有显著的优势,适合在移动群智感知环境下大规模数据集计算,而 Abadi 等人[25]所提方案虽然计算复杂度较高但是利用同态加密方式可以实现较高的安全性保障,适用于数量级别不大但安全需求较高的场景中.

对信誉感知激励机制有效性的评价,本文通过在 MATLAB R2014a 环境下的仿真实验进行验证说明,并与文献[20]所提机制进行对比,设置感知用户(联盟)总数 $N=100$、感知任务数量 $K=1\,000$、初始预算 $B=1\,000$. 并按照感知用户(联盟)的阈值将感知用户(联盟)分为 3 组,分别为高阈值、低阈值和中间阈值感知用户(联盟),为每个感知用户(联盟)设置信誉值 Q_i,实验结果如图 5 所示.

本文目标之一就是能使任务尽快地被处理完成,也就是说能在更短的时间内获得更高的任务完成比例. 在图 5(a)中很明显地看出在一段时间内本文机制能够更快地处理完任务集,并在处理任务速度方面具有更好的稳定性. 通过设置用户的信誉值,区别划分用户,每次选择信誉度高的用户来依次处理子任务,这样通过影响平台支付报酬函数 P_x 和用户的代价函数 c_i,使这两者的比例大于用户阈值 $Thres_i$,从而使得用户参与比例不断增大,并最终趋于平稳. 此外,在保证任务在顺利处理完的基础上减少用户的花费代价和平台支付给用户的报酬,从而使得预算剩余比例增大也是本文的另一主要目标. 在图 5(b)中的曲线可以很明显地看出在一段时间内本文机制能在保证任务顺利处理的基础上,减少了用户花费代价和平台支付给用户的报酬,从而使剩余的预算比例更高,即花费的预算更少. 综上本文中选择了信誉高的用户处理子任务,使得用户参与比例不断增大(即 $n(t)$值增大),从而降低了平台支付给用户的报酬(即 P_x 值不断减小). 同时平台通过因子调节用户在处理子任务时的代价 c_i. 这样使得该机制有效的在提高任务处理效率的同时也减少了预算的花费.



(a) Comparison of task completion proportion



(b) Comparison of budget surplus proportion

Fig. 5 Experimental comparison of incentive mechanism

图 5 激励机制实验对比图

6 总 结

本文针对移动群智感知网络中在激励更多感知用户参与感知任务并提供真实数据的同时如何更好地保护大量蕴含用户敏感、隐私信息的感知数据和感知平台安全性的问题. 提出了一种基于布隆过滤器的用户联盟匹配方案,使得用户在上传感知数据之前进行隐私信息匹配形成感知联盟,有效保护个人隐私信息;同时提出了一种轻量级感知数据交集计算协议,在不泄露任一方真实数据的情况下,实现

隐私数据交集运算;最后提出了一种基于隐私信息匹配的信誉感知激励机制,在提高感知任务处理效率的基础上有效地控制了预算开支.但在移动群智感知网络中的大量感知用户和感知数据对隐私保护方案和激励机制在确保安全性的同时对算法效率有着更高的要求,在今后的研究工作中,将继续对移动群智感知网络中的隐私保护方案的安全性和高效性进行更加深入的探讨研究.

参 考 文 献

[1] Guo Bin, Yu Zhiwen, Zhou Xingshe, et al. From participatory sensing to mobile crowd sensing [C] //Proc of the 12th IEEE Int Conf on Pervasive Computing and Communications Workshops. Piscataway, NJ: IEEE, 2014: 593-598

[2] Yu Ruiyun, Wang Pengfei, Bai Zhihong, et al. Participatory sensing: People-centric smart sensing and computing [J]. Journal of Computer Research and Development, 2017, 54(3): 457-473 (in Chinese)
(于瑞云, 王鹏飞, 白志宏, 等. 参与式感知: 以人为中心的智能感知与计算[J]. 计算机研究与发展, 2017, 54(3): 457-473)

[3] Pournajaf L, Garcia-Ulloa D A, Li Xiong, et al. Participant privacy in mobile crowd sensing task management: A survey of methods and challenges [J]. ACM SIGMOD Record, 2016, 44(4): 23-34

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

[5] Huang Kuanlun, Kanhere S S, Hu Wen. Preserving privacy in participatory sensing systems [J]. Computer Communications, 2010, 33(11): 1266-1280

[6] Bao Guohua, Wang Shengyu, Li Yunfa. Research on data security protection method based on privacy awareness in cloud computing [J]. Netinfo Security, 2017 (1): 84-89 (in Chinese)
(包国华, 王生玉, 李运发. 云计算中基于隐私感知的数据安全保护方法研究[J]. 信息网络安全, 2017 (1): 84-89)

[7] Ganti R K, Pham N, Tsai Y E, et al. PoolView: Stream privacy for grassroots participatory sensing [C] //Proc of the 6th ACM Conf on Embedded Network Sensor Systems. New York: ACM, 2008: 281-294

[8] Ma Rong, Xiong Jinbo, Lin Mingwei, et al. Privacy protection-oriented mobile crowdsensing analysis based on game theory [C] //Proc of the 16th IEEE Int Conf on Trust, Security and Privacy in Computing and Communications. Piscataway, NJ: IEEE, 2017: 990-995

[9] Zhang Fan, He Li, He Wenbo, et al. Data perturbation with state-dependent noise for participatory sensing [C] //Proc of the 31st Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2012: 2246-2254

[10] Christin D, Roßkopf 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

[11] Androulaki E, Choi S G, Bellovin S M, et al. Reputation systems for anonymous networks [C] //Proc of the 8th Int Symp on Privacy Enhancing Technologies. Berlin: Springer, 2008: 202-218

[12] Shi Jing, Zhang Rui, Liu Yunzhong, et al. Prisense: Privacy-preserving data aggregation in people-centric urban sensing systems [C] //Proc of the 29th Conf on Information Communications. Piscataway, NJ: IEEE, 2010: 758-766

[13] Castelluccia C, Mykletun E, Tsudik G. Efficient aggregation of encrypted data in wireless sensor networks [C] //Proc of the 2nd Annual Int Conf on Mobile and Ubiquitous Systems: Networking and Services. Los Alamitos, CA: IEEE Computer Society, 2005, 5(3): 109-117

[14] Shen Liyan, Chen Xiaojun, Shi Jinqiao, et al. Survey on private preserving set intersection technology [J]. Journal of Computer Research and Development, 2017, 54(10): 2153-2169 (in Chinese)
(申立艳, 陈小军, 时金桥, 等. 隐私保护集合交集计算技术研究综述[J]. 计算机研究与发展, 2017, 54(10): 2153-2169)

[15] Zhao Dong, Li Xiangyang, Ma Huadong. Budget-feasible online incentive mechanisms for crowdsourcing tasks truthfully [J]. IEEE/ACM Trans on Networking, 2016, 24(2): 647-661

[16] Li Qinghua, Cao Guohong. Providing privacy-aware incentives for mobile sensing [C] //Proc of the 11th IEEE Int Conf on Pervasive Computing and Communications. Piscataway, NJ: IEEE, 2013: 76-84

[17] Duan Lingjie, Kubo T, Sugiyama K, et al. Incentive mechanisms for smartphone collaboration in data acquisition and distributed computing [C] //Proc of the 2012 IEEE Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2012: 1701-1709

[18] Han Kai, Zhang Chi, Luo Jun, et al. Truthful scheduling mechanisms for powering mobile crowdsensing [J]. IEEE Trans on Computers, 2016, 65(1): 294-307

[19] Jaimes L G, Vergara-Laurens I, Labrador M A. A locationbased incentive mechanism for participatory sensing systems with budget constraints [C] //Proc of the 2012 IEEE Int Conf on Pervasive Computing and Communications. Piscataway, NJ: IEEE, 2012: 103-108

[20] Angelopoulos C M, Nikoletseas S, Raptis T P, et al. Design and evaluation of characteristic incentive mechanisms in mobile crowdsensing systems [J]. Simulation Modelling Practice & Theory, 2015, 55(6): 95-106

[21] Xiong Jinbo, Zhang Yuanyuan, Li Xuan, et al. RSE-PoW: A role symmetric encryption PoW scheme with authorized deduplication for multimedia data [J]. Mobile Networks & Applications, 2017 (7): 1-14

[22] Wan Sheng, He Yuanyuan, Li Fenghua, et al. Bloom filter-based lightweight private matching scheme [J]. Journal of Communications, 2015, 36(12): 151-162 (in Chinese)
(万盛, 何媛媛, 李凤华, 等. 基于布隆过滤器的轻量级隐私信息匹配方案[J]. 通信学报, 2017, 36(12): 151-162)

[23] Lu Rongxing, Lin Xiaodong, Shen Xuemin. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency [J]. IEEE Trans on Parallel and Distributed Systems, 2013, 24(3): 614-624

[24] Sun Jingchao, Zhang Rui, Zhang Yanchao. Privacy-preserving spatiotemporal matching [C] //Proc of the 2013 Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2013: 800-808

[25] Abadi A, Terzis S, Dong Changyu. O-PSI: Delegated private set intersection on outsourced datasets [C] //Proc of the 30th IFIP Int Information Security Conf. Berlin: Springer, 2015: 3-17

Xiong Jinbo, born in 1981. Received his MSc degree in communication and information systems from Chongqing University of Posts and Telecommunications, China, in 2006, and PhD degree in computer system architecture from Xidian University, China, in 2013. Associate professor in the College of Mathematics and Informatics at Fujian Normal University. Member of IEEE, ACM and CCF. His main research interests include cloud data security, privacy protection, and mobile Internet security.

Ma Rong, born in 1992. Master candidate and student member of CCF. Her main research interests include reputation incentive and privacy protection in mobile crowd sensing (miaronger@163.com).

Niu Ben, born in 1985. Received his BSc degree in information security, MSc and PhD degrees in cryptography from Xidian University in 2006, 2010 and 2014 respectively. Associate professor in State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. He was a visiting scholar in Pennsylvania State University from 2011 to 2013. His main research interests include wireless network security, privacy computing (niuben@iie.ac.cn).

Guo Yunchuan, born in 1977. Received his PhD degree in information security from the University of Chinese Academy of Sciences in 2011. Associate professor of the Institute of Information Engineering, Chinese Academy of Sciences. His main research interests include access control and formal verification (guoyunchuan@iie.ac.cn).

Lin Li, born in 1982. PhD candidate in computer science and engineering at Huazhong University of Science and Technology. He received his BE, MS degrees in computer science and technology from Sichuan University in 2005 and 2008. Lecturer in Fujian Normal University. His main research interests include mobile cloud computing and edge computing (llfjfz@163.com).