

移动群智感知中基于雾节点协作的感知用户身份隐私保护

刘慧¹, 毕仁万¹, 熊金波^{1,2}, 赵明烽¹, 金彪¹, 林劼¹

(1. 福建师范大学数学与信息学院, 福建 福州 350117;
2. 福建省网络安全与密码技术重点实验室, 福建 福州 350007)

摘要: 在移动群智感知中, 攻击者可利用感知用户间的社交关联信息以及感知用户身份信息与感知数据的关联性重构感知用户间的社交圈, 进一步攻击用户社交团体。针对这一问题, 提出一种基于雾节点协作的感知用户身份隐私保护方案。首先, 创建任务分配中心(TC)和数据中心(DC), 并由位于终端边缘的2个雾节点承载, 分别处理感知任务的合理分配问题和感知数据的聚合计算问题; 然后, 通过差分隐私加噪干扰防御攻击者获取感知用户间具体的社交关联权重; 最后, 感知用户使用不同的盲身份分别与TC和DC通信, 防止攻击者同时获取感知用户的身份信息和感知数据。安全分析表明, 所提方案可以确保感知用户在完成感知任务过程中的身份隐私信息安全。实验结果显示, 所提方案可以有效保护感知用户间的社交关联信息, 且具有较低的时延。

关键词: 差分隐私; 移动群智感知; 身份隐私保护; 雾节点; 社交关联关系; 盲身份

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019056

Fog-aided identity privacy protection scheme for sensing users in mobile crowd sensing

LIU Hui¹, BI Renwan¹, XIONG Jinbo^{1,2}, ZHAO Mingfeng¹, JIN Biao¹, LIN Jie¹

1. College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China

Abstract: In mobile crowd sensing(MCS), attackers can reconstruct the social circle among sensing users, who use the social association information among sensing users and the correlation between the sensing user's identity and sensing data to further attack a social alliance. In order to tackle this issue, a fog-aided identity privacy protection scheme is proposed. Firstly, two fog nodes are introduced which located at the edge of the sensing terminal. The one

收稿日期: 2019-05-20; 修回日期: 2019-08-09

通信作者: 熊金波, jinbo810@163.com

基金项目: 国家自然科学基金资助项目(No.61872088, 61872090); 福建省自然科学基金资助项目(No.2019J01276); 信息网络安全公安部重点实验室开放课题资助项目(No.C18602)

Foundation Items: The National Natural Science Foundation of China(No.61872088, No.61872090), The Natural Science Foundation of Fujian Province(No.2019J01276), Key Lab of Information Network Security, Ministry of Public Security(No.C18602)

论文引用格式: 刘慧, 毕仁万, 熊金波, 等. 移动群智感知中基于雾节点协作的感知用户身份隐私保护[J]. 网络与信息安全学报, 2019, 5(6): 75-84.

LIU H, BI R W, XIONG J B, et al. Fog-aided identity privacy protection scheme for sensing users in mobile crowd sensing[J]. Chinese Journal of Network and Information Security, 2019, 5(6): 75-84.

is task allocation center (TC) for handling the reasonable allocation of sensing tasks, and the other is data center (DC) for calculating sensing data. Furthermore, differential privacy is employed for preventing attackers from acquiring the specific social association weight of sensing users. Finally, in order to prevent attackers from obtaining the sensing users' identity information and sensing data at the same time, sensing users use different blind identities to communicate with TC and DC. Security analysis indicates that the proposed scheme can ensure the security of identity privacy information of sensing users in the process of completing sensing tasks. Experimental results show that the proposed scheme can protect the social association information between sensing users, and has a low delay.

Key words: differential privacy, mobile crowd sensing, identity privacy protection, fog node, social association information, blind identity

1 引言

移动群智感知作为新兴的数据采集手段, 结合移动感知和众包思想, 以普通感知用户作为数据采集的基本单元, 通过深度分析感知用户提交的海量异构感知数据, 有效完成庞大复杂的感知任务最终服务于人类社会。智能设备的不断丰富以及内置传感器感知能力的不断提升, 为移动群智感知网络提供了更加异构、多样化的数据, 满足更高的感知任务需求^[1-2]。近年来, 群智感知技术不仅在公共设施环境^[3-4]、智慧医疗^[5-6]、智慧交通^[7-8]等行业得到了深度应用, 而且在新兴的绿色制造、智能服务等领域实现了有价值的创新应用^[9-10]。移动群智感知的快速发展, 极大地丰富了智慧城市的应用与服务, 进一步推动当代万物互联的发展。

在移动群智感知中, 感知用户在参与执行任务的过程中, 攻击者可通过任务关联或感知数据获取感知用户的身份信息、地理位置、社交圈等敏感信息, 进一步攻击感知用户造成隐私信息泄露。针对这一问题, Wang 等^[11-12]提出一种基于分组映射的感知用户身份隐私保护方案, 通过分类算法将可信程度相同的感知用户映射到同一隐私水平的分组中, 从而隐藏感知用户的真实 ID, 实现感知用户的身份隐私保护。Hu 等^[13]提出一种基于数据分割的隐私保护方案, 感知用户将感知数据分割成 K 份, 秘密共享于 K 个节点, 并由各

个节点直接上传给感知平台, 从而有效防止攻击者将具体的感知用户和感知数据相结合。进一步地, Wu 等^[14]在文献[13]的基础上增加了对转发节点的可信度评估, 从社会贡献和个性属性两方面评估转发节点的可靠性, 且分割数据的数量由感知用户所遇到的可信转发节点的个数决定, 但该方案中节点的可信度评估需要较长的时延, 且计算开销和通信开销比较大。Jin 等^[15-16]提出在感知平台可信的情况下, 感知用户可用自己的真实身份直接上传投标信息和感知数据, 并使用差分隐私加噪于用户的投标信息, 防止攻击者获取其他用户的投标信息后更改自己的投标信息造成投标结果的不公平; 同时, 感知平台也将聚合数据结果进行加噪干扰后发布从而防御攻击者从感知数据中推测用户的敏感信息。然而, 方案中对于感知平台的可靠性定义过强, 不适合现阶段移动群智感知环境。

综上所述, 现有方案一般采用数据分割和 K 匿名的方法确保感知用户身份隐私信息的安全, 虽具有较强的身份隐私保护, 但对于具体感知用户的有效认证比较复杂, 且计算开销和能耗较大; 此外, 由于感知用户与云服务器之间距离较远, 感知数据往往需要通过中间网络传输, 造成传输时延较大。雾计算^[17]作为边缘计算的典型范例, 不仅具有一定的计算和存储能力, 同时支持很强的移动性, 且位于感知终端的边缘, 数据传输具有极低的时延。因此, 利用雾节点的计算和存储

能力为感知用户提供更加便捷的服务,成为当前新型移动群智感知的研究热点。Fiandrino 等^[18]首次将雾计算应用于群智感知系统,并提出一种基于社交驱动智慧城市的移动群智感知数据采集框架,并提出通过用户与任务的距离、社交能力以及设备能耗三要素来筛选用户,且实验表明,与仅以空间距离作为选择标准的策略相比,该方案成功招募用户的平均数量提高了近 20%。Sun 等^[19]提出基于两层雾框架的异构数据收集方案和一种基于信任管理的数据安全查询方案,并通过获取用户的外包加密地图列表(MPL)实现对恶意参与者的在线跟踪和身份检索。基于雾计算的群智感知边缘扩展,不仅大幅度提高了实时收集用户数据的效率,而且大幅度提高了实时分析数据的能力,为用户提供更加精确便捷的服务。但因为雾节点更加靠近终端用户的边缘,感知用户的动态属性信息更容易泄露,所以对于感知用户的报酬反馈和信任管理更加严格。但现有方案对于移动群智感知边缘扩展模型下的隐私保护研究还处于初始阶段,需进一步深度研究。

本文提出一种基于雾节点协作的感知用户身份隐私保护方案,该方案的主要贡献如下。

1) 该方案引入位于感知终端边缘的 2 个半可信雾节点,其中一个雾节点(任务分配中心 TC)负责基于身份验证的任务分配和报酬奖励更新,另一个雾节点(数据计算中心 DC)负责数据聚合计算工作,从而将感知用户的身份 ID 信息与感知数据分开处理,同时提高感知数据的计算效率、减轻云端的计算负担。

2) 设计一种社交关联询问模型,并对任意的询问结果进行随机加噪干扰从而保护感知用户间的社交关联信息,防止攻击者在获取该关联信息后重构感知用户间的社交关系网。

3) 感知用户使用不同的盲身份完成与 TC 和 DC 的通信过程,确保感知用户(同一身份 ID)

在执行任务过程中与任务关联的地理位置、时间、身份等敏感信息的安全性。

4) 安全分析表明,该方案可以保护感知用户在参与任务过程中的身份隐私,实验结果显示该方案可以有效保护感知用户间的社交关联信息,进一步防御攻击者重构感知用户间的社交圈。

2 问题描述

本节依次介绍本文方案的系统模型、威胁模型以及方案概述。

2.1 系统模型

本文方案的移动群智感知系统是基于雾计算构建的系统模型,该系统主要由任务发起者、雾节点以及感知用户组成,如图 1 所示。

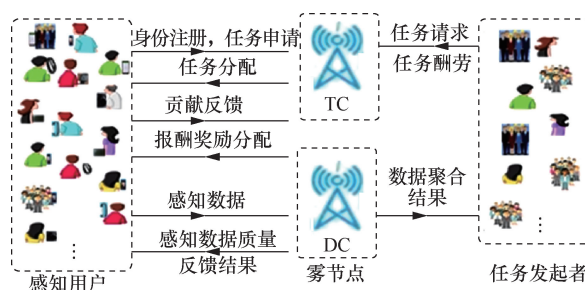


图 1 系统模型

任务发起者: 作为感知任务的请求者,主要负责将任务具体要求以及可支付报酬上传给雾节点(TC),并与另一个雾节点(DC)完成感知数据的安全交易。任务发起者根据所得的感知数据进一步进行训练和挖掘,最终服务于人类社会。

雾节点: 是位于云服务器边缘具有计算和存储能力的智能服务器,在本文方案模型中,2 个雾节点是半可信的,即它们是诚实而好奇的^[20]。2 个雾节点会好奇所收集数据的内容,但不会篡改数据更不会相互勾结。作为任务发起者和感知用户的中介,主要负责任务分配和数据的计算与交易,并由 2 个半可信雾节点承载。其中,一个雾节点称为基于身份验证的任务分配中心(TC),

主要负责用户身份注册、收集任务、分配任务、收集竞标、筛选用户以及声誉报酬奖励的更新与分配。另一个雾节点称为数据处理中心 (DC)，主要负责收集用户的感知数据以及数据的分析计算，并返回相应的反馈结果。基于安全保密协议的约束，两雾节点之间不能相互通信勾结，确保 TC 与 DC 其中有一方受到攻击时，敌手不能从获取的片段信息中进一步推测用户的敏感信息。相比于在云端专门设置两个服务器分别处理 TC 和 DC，雾节点之间的分离状态更适合此系统模型。

感知用户：作为感知数据的来源，主要负责感知数据的收集与上传。感知用户通过各种智能设备收集与感知任务相关的数据，感知数据经过合适的隐私保护机制（确保数据实用性与隐私保护之间的平衡）处理后上传给 DC，最终通过 DC 反馈的数据质量贡献获得相应的报酬补偿或者进行相应的惩罚。

2.2 威胁模型

本文系统模型是基于雾计算的移动群智感知边缘扩展模型。在该系统中，攻击者可能是系统外的某个功能实体，也可能是参与感知任务的用户、任务发起者。由于雾计算是云计算的边缘拓展，更加靠近感知用户，所以感知用户在参与执行任务过程中，用户的位置、时间、情境等动态属性信息更加容易泄露。首先，一个恶意的任务发起者，可以向 TC 申请在特定范围且只有少数感知用户参与的感知任务，从而发起任务关联攻击^[21]，一旦 TC 发布此类感知任务，感知用户只要参与执行任务，任务发起者就会获取用户的动态敏感属性信息，进一步分析挖掘用户的感知设备类型、爱好习惯等敏感信息；其次，感知用户之间频繁的通信交互以及长时间相似的行为特征，形成一个比较稳定的社交关联关系圈，一旦被攻击者获取，就会造成一个社交团体的隐私泄露，此外，攻击者可利用感知数据与感知用户身

份信息的关联性进行信道监听感知用户，进一步挖掘感知用户更加深层次的隐私信息，造成严重的隐私泄露；最后，恶意感知用户通过女巫标识的多个 ID 参与感知任务，通过提交相似数据获取较多的报酬奖励，从而发起女巫攻击^[22]。

2.3 方案概述

本文方案概述如下。1) 感知用户和任务发起者都需要在 TC 进行实名注册。2) TC 收集任务发起者提交的任务以及要求报酬，返回相应的反馈信息以便任务发起者可以合法向 DC 获取最终的感知数据聚合结果。3) 感知用户利用不同的盲身份分别与 DC 和 TC 进行通信，完成任务的申请参与和感知数据的上传。4) 设计随机询问模型 (SQM)，SQM 用以获取任意 2 个感知用户间的社交关联权重，询问结果为一个三元组 $\{N_A, N_B, \omega_{AB}\}$ ，其中 N_A 、 N_B 代表该系统中的 2 个感知用户， ω_{AB} 代表这 2 个感知用户间的社交关联权重。对于任一询问结果添加噪声，用以保护感知用户间的社交关联信息，防止攻击者重构感知用户间的社交关系网。5) DC 对感知数据进行分析计算并将数据质量反馈结果返回给感知用户。6) 感知用户将 DC 的反馈结果发送给 TC，TC 对反馈信息进行验证后对感知用户进行相应的声誉更新和报酬分配。

3 方案构造

本节首先定义了感知用户间的社交关联关系，并通过差分隐私加噪干扰防御攻击者获取感知用户间的社交关联信息；然后介绍了从任务分配到聚合数据的发布过程中，感知用户和任务发起者与雾节点 TC 和 DC 的有效通信过程。图 2 表示 3 个实体之间的通信过程，其中，重要符号描述如表 1 所示。

3.1 社交关联分类及保护机制

由于感知用户间频繁的通信交流以及长期的行为特征信息会形成相对稳定的社交关系圈。攻

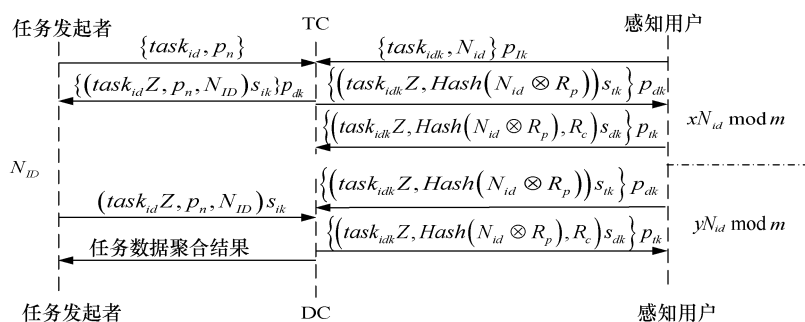


图2 感知用户参与执行任务流程

表1 重要符号描述

变量	描述
R_p	感知用户当前的声誉积分
R_c	数据的反馈结果
Z	随机数
$task_{id}, task_{id1}$	感知任务标签
N_{ID}, N_{id}	任务发起者 ID, 感知用户 id
S_{ik}, P_{ik}	TC 的公钥, 私钥
S_{dk}, P_{dk}	DC 的公钥, 私钥
xN_{id}, yN_{id}	盲身份
P_n, P_i	任务发起者竞标报酬, 用户报酬
ω, ω_{AB}	用户间的社交关联权重, 用户 A 和用户 B 之间的社交关联权重
ε	隐私预算
D, D'	相邻数据集
$Hash$	单散列函数
ω_r, ω_i	差分隐私加噪过后用户的社交关联权重, 用户原始社交关联权重

攻击者可利用感知用户的行为特征信息或身份属性信息获取以该感知用户为中心的社交圈, 攻击其他感知用户甚至是整个社交圈的所有感知用户。感知用户间的社交关系网如图3所示。

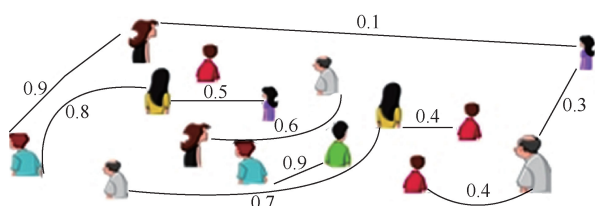


图3 感知用户间的社交关系网

3.1.1 感知用户间的社交关联关系分类

本文用 ω 代表感知用户之间社交关联权重,

且 ω 的取值范围为 $[0,1]$ 。当感知用户间的社交关联权重 $\omega = 0$ 时,说明这2个感知用户之间不存在社交关联关系; 当感知用户间的社交关联权重 $\omega \neq 0$ 时,说明这2个感知用户存在一定的社交关联关系, 一旦被攻击者获取, 就会造成用户隐私信息的泄露。本文根据感知用户的身份属性信息以及历史行为特征信息将用户间的社交关联关系分为熟悉用户和相似用户。

熟悉用户: 每个感知用户都有相对稳定的社交圈, 如朋友、亲人、同事等, 这些感知用户往往会进行频繁的通信交互, 称这些用户为熟悉用户。熟悉感知用户之间的社交关联权重可以通过历史行为特征信息获取。

相似用户: 以人为中心的社交关系网络的复杂性, 使一些没有或者较少通信互动的感知用户存在一定的关联关系, 这些感知用户在长期的任务执行过程中, 产生较多相似的行为特征信息, 称这些感知用户为相似感知用户。相似感知用户间的社交关联权重是通过 JS 散度计算获得的, 并用 $\omega_{AB} = 1 - JS_{AB}$ 表示。若两感知用户之间的相似关联 $JS_{AB} = 1$, 则两感知用户间的社交关联权重 $\omega_{AB} = 1 - 1 = 0$, 即两感知用户不存在社交关联关系; 反之, 存在。

定义1 (KL-散度^[23])。设 $F = \{f_1, f_2, \dots, f_n\}$ 和 $Q = \{q_1, q_2, \dots, q_n\}$ 是两随机变量 $A = \{x_1, x_2, \dots, x_n\}$ 和 $B = \{y_1, y_2, \dots, y_n\}$ 的概率分布, 则 F 和 Q 的 KL-散度定义为

$$KL(F \parallel Q) = \sum_{i=1}^n f_i \ln \left(\frac{f_i}{q_i} \right) \quad (1)$$

由于 KL-散度不具有对称性, 本文采用基于 KL-散度变形的 JS-散度计算。

定义 2 (JS-散度^[23])。设 $F = \{f_1, f_2, \dots, f_n\}$ 和 $Q = \{q_1, q_2, \dots, q_n\}$ 是两随机变量 $A = \{x_1, x_2, \dots, x_n\}$ 和 $B = \{y_1, y_2, \dots, y_n\}$ 的概率分布, $M = \frac{1}{2}(F + Q)$, 则 P 和 Q 的 JS 散度定义为

$$JS(F \parallel Q) = \frac{1}{2} (KL(F \parallel M) + KL(Q \parallel M)) = \sum_{i=1}^n \left(f_i \ln \left(\frac{2f_i}{f_i + q_i} \right) + q_i \ln \left(\frac{2q_i}{f_i + q_i} \right) \right) \quad (2)$$

设 $A = \{a_0, a_1, a_2, a_3, \dots\}$ 和 $B = \{b_0, b_1, b_2, b_3, \dots\}$ 表示感知用户 N_A 和感知用户 N_B 的系列属性, 通过上述公式定义计算 JS_{AB} 。由于 JS 散度的值域范围为 $[0, 1]$, 且相同为 0, 不同为 1; 本文用 $\omega_{AB} = 1 - JS_{AB}$ 表示两感知用户间的社交关联权重。

3.1.2 社交关联信息的加噪保护

社交关联询问模型 (SQM) 用以获取任意 2 个感知用户的社交关联权重, 并进一步重构感知用户间的社交关联关系网, 且询问结果为一个三元组 $\{N_A, N_B, \omega_{AB}\}$ 。在移动群智感知系统中, 假设有 N 个感知用户参与某一任务, 则这些感知用户两两之间存在的社交关联关系构成 $c = \frac{N(N-1)}{2}$ 个三元组, 形成感知用户间的社交关联权重数据集, 即 $SQM_c = \{N_A, N_B, \omega_{AB}; N_A, N_C, \omega_{AC}; \dots\}$ 。攻击者可利用感知用户间的社交关联关系重构感知用户间的社交圈, 进一步挖掘整个社交圈中感知用户的敏感信息。因此, 本文提出使用差分隐私加噪干扰用户间的社交关联信息, 防止攻击者获取感知用户间的社交关联权重。

定义 3 (ε -差分隐私^[24]) 设 D 和 D' 为 2 个仅相差一个元组的相邻数据集, ζ 是数据集上的随机算法, ω 为 ζ 任意一组可能的输出, 则 ζ 满足 ε -差分隐私需满足

足 ε -差分隐私需满足

$$\frac{P_r(\zeta(D) = \omega)}{P_r(\zeta(D') = \omega)} \leq \exp(\varepsilon) \quad (3)$$

其中, ε 称为差分隐私预算, 且 ε 值越小, 隐私保护度越高。本文方案通过对 SQM 的任意询问结果进行加噪干扰防御攻击者重构移动感知用户的社交关系网。

3.2 任务分配

在本文方案中, 首先, 任务发起者和所有的感知用户都需要在 TC 进行实名注册。TC 在收集任务发起者提交的任务及相应要求和报酬后, 向系统内所有注册的用户进行广播 $\{task_{id1}, task_{id2}, \dots, task_{idn}\}$, 同时给任务发起者返回 $\{(task_{id} Z, p_n, N_{ID}) s_{tk}\} p_{dk}$ 以便任务发起者可以从 DC 获取相应的任务数据聚合结果; 其次, 感知用户用盲身份 $xN_{id} \bmod m$ 向 TC 申请参与任务, 并向 TC 发送 $\{task_{idk}, N_{id}\} p_{tk}$ 。TC 验证感知用户的合法性后, 合理分配任务并返回相应的信息, 即

$$\begin{aligned} N_{ID} &\rightarrow TC: \{task_{id}, p_n\}, \\ xN_{id} &\rightarrow TC: \{task_{idk}, N_{id}\} p_{tk}, \\ TC &\rightarrow xN_{id}: \{(task_{idk} Z, Hash(N_{id} \otimes R_p)) s_{tk}\} p_{dk}, \\ TC &\rightarrow N_{ID}: \{(task_{id} Z, p_n, N_{ID}) s_{tk}\} p_{dk}. \end{aligned}$$

3.3 感知数据处理

感知用户使用另一盲身份 $yN_{id} \bmod m$ 将感知数据和 $\{(task_{idk} Z, Hash(N_{id} \otimes R_p)) s_{tk}\} p_{dk}$ 上传给数据处理中心, 数据处理中心通过解密 $\{(task_{idk} Z, Hash(N_{id} \otimes R_p)) s_{tk}\} p_{dk}$ 验证感知用户的合法性, 同时对提交的感知数据进行质量贡献计算处理, 并将计算反馈结果 R_c 返回给感知用户, 即

$$\begin{aligned} yN_{id} &\rightarrow DC: \{(task_{idk} Z, Hash(N_{id} \otimes R_p)) s_{tk}\} p_{dk}, \\ DC &\rightarrow yN_{id}: \{(task_{idk} Z, Hash(N_{id} \otimes R_p), R_c) s_{dk}\} p_{tk}. \end{aligned}$$

3.4 声誉更新与报酬奖励分配

感知用户在收到 TC 的数据质量反馈结果后, 通过盲身份 $xN_{id} \bmod m$ 向 TC 发送 DC 的反馈结果 R_c 。TC 通过解密所接收信息 $\{(task_{idk}Z, Hash(N_{id} \otimes R_p), R_c)s_{dk}\}_{p_{tk}}$ 来验证感知用户的合法性, 并根据反馈结果 R_c 更新感知用户的声誉值, 给予用户相应的报酬奖励, 即

$$\begin{aligned} xN_{id} \bmod m &\rightarrow TC: \\ &\{(task_{idk}Z, Hash(N_{id} \otimes R_p), R_c)s_{dk}\}_{p_{tk}} \\ TC &\rightarrow N_{id}: p_i. \end{aligned}$$

3.5 数据聚合结果的发布

任务发起者通过 N_{ID} 向 TC 发送 $\{(task_{idk}Z, p_n, N_{ID})s_{tk}\}_{p_{dk}}$, TC 通过该信息和任务发起者的 ID 验证其合法性。若任务发起者是合法的, 则 TC 将数据聚合结果返回给任务发起者, 否则不回复。通过该机制有效避免攻击者在截取 $\{(task_{idk}Z, p_n, N_{ID})s_{tk}\}_{p_{dk}}$ 后向平台索要数据聚合的结果, 即

$$\begin{aligned} N_{ID} &\rightarrow DC: (task_{idk}Z, p_n, N_{ID})s_{tk}, \\ DC &\rightarrow N_{ID}: \text{数据聚合结果}. \end{aligned}$$

由上述可得, 从任务分配阶段一直到数据聚合结果的发布, 感知用户都没有使用真实的 ID 而是使用盲身份 $xN_{id} \bmod m$ 和 $yN_{id} \bmod m$, 从而防御感知用户在参与执行任务过程中身份隐私信息的泄露。同时为防止恶意用户使用盲身份参与任务, TC 和 DC 必须对感知用户提交的信息进行合法性验证, 确保与感知用户进行有效的通信。

4 方案安全性分析

该方案可以确保感知用户在任务执行过程中身份隐私信息的安全。首先, 感知用户使用盲身份申请参与任务, TC 虽然知道感知用户注册的真实 ID, 但并不能知道感知用户在申请执行任务时的状态, 从而防御任务发起者或其他攻击者通过

任务关联进一步获取感知用户的时间、位置、情境等动态敏感信息。其次, TC 处理与身份相关联的任务分配和奖惩分配, 而 DC 处理感知数据的计算和质量评估, 且 TC 和 DC 基于安全保密协议不能互相通信, 确保感知用户的身份验证和感知数据的聚合计算分开处理; 此外, 感知用户使用不同的盲身份 $xN_{id} \bmod m$ 和 $yN_{id} \bmod m$ 分别与 TC 和 DC 进行通信, 所以, 对于诚实而好奇的 TC, 尽管有感知用户的真实 ID 和声誉信息, 但不能获取感知用户与 DC 通信时的盲身份, 更不能获取用户提交的感知数据, 从而防御 TC 或攻击者同时得到感知用户的身份信息 and 感知数据; 同理, DC 只知道感知用户匿名提交的感知数据, 并不能获取感知用户申请任务时的盲身份, 更不能知晓感知用户的真实 ID, 从而防御 DC 或攻击者同时得到感知数据和用户身份信息。

该方案可以抵御女巫攻击, 即由贪婪感知用户通过女巫标识的多个 ID 提交相似数据从而获得更多的奖励报酬。感知用户在整个任务的完成过程中虽然使用不同的盲身份, 但 TC 是根据 $(task_{idk}Z, Hash(N_{id} \otimes R_p), R_c)s_{dk}$ 进行相应验证和声誉更新的, 从反馈结果中可以得知, 每个感知用户 N_{id} 都唯一对应一个 R_c , 且反馈内容有 DC 的签名, 使反馈结果不可更改, 因此即使恶意感知用户提交多份相似数据, 最终一个 N_{id} 也只能得到相应的唯一一个 R_c , 从而有效抵御女巫攻击。

5 实验分析

本节对本文所提方案进行仿真实验, 通过仿真结果来评估方案性能, 并与 CAPP 方案^[14]进行对比分析。两种方案中感知用户均使用盲身份参与任务, 使用数据质量评估感知用户贡献; 不同的是, 在 CAPP 中, 数据进行分割上传, 同时对转发节点进行可信度评估, 而本文方案中使用不

同的盲身份分别与 DC 和 TC 进行通信, 实验采用 C++ 实现, 在 INTEL I7-6500U、3.1 GHz 处理器、4 GB 内存的 Windows 10 平台上运行, 具体仿真参数如表 2 所示。

表 2 实验仿真参数

参数	值
感知用户数/个	80
传送范围/m	10
缓冲大小/MB	30
信息大小/kB	0~200
感知用户的移动速度/ $\text{m}\cdot\text{s}^{-1}$	0.5~1.5
传输率/ $\text{kbit}\cdot\text{s}^{-1}$	250

假设本系统中有 80 个感知用户参与执行感知任务, 其中 ω 为该系统感知用户之间的社交关联权重值。本文采用加权互信息熵来表示用户的隐私泄露程度^[25], 当 2 个用户的相似度越高或通信交互越频繁, 他们之间的加权互信息熵就越大, 隐私泄露程度就越高。当 2 个用户间的社交关联权重为 1 时, 2 个用户完全关联, 即 2 个事件等概率发生, 两用户的互信息熵为 1, 当用户间的关联权重为 0 时, 用户间完全不相关, 即两用户的互信息熵为 0。

$$I_{\alpha}(N_A, N_B) = \sum_{\alpha=i}^n \alpha_i \sum_{N_A} \sum_{N_B} p(N_A, N_B) \lg \frac{p(N_A, N_B)}{p(N_A)p(N_B)} \quad (4)$$

由图 4 可以看出, 感知用户间的社交关联权重越大, 用户间相似程度越高, 互信息熵也越大, 造成的隐私泄露程度越大。这是因为感知用户间的社交关联权重越大, 说明感知用户间进行频繁的通信或者行为特征信息的相似度极高。一旦攻击者获取感知用户间的社交关联权重, 攻击者就会根据某一感知用户的行为轨迹信息推测与其相关的其他感知用户的敏感信息, 造成其隐私信息的泄露。

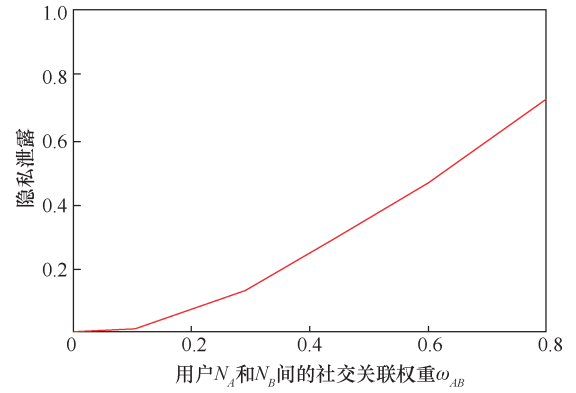


图 4 感知用户间的关联权重对隐私泄露的影响

通过差分隐私随机加噪干扰数据达到保护用户隐私的目的, 其本质在于对于任意随机询问结果都具有失真性。本文采用用户社交关联关系的误差 $E = \sum_N |\omega_r - \omega_i|$ 衡量不同差分隐私预算对数据质量的影响, 从图 5 可以看出, 经过差分隐私加噪处理后的数据, 隐私预算越小, 用户间的社交关联关系误差越大, 攻击者获取确切的社交关联关系的可能性越小, 造成的隐私泄露越小, 且当感知用户数量增加时, 用户间的误差以平稳缓慢的趋势增加。说明隐私预算的值越小, 对数据的保护强度越高, 但数据的失真也越大。因此, 在保护用户隐私信息的同时, 也需考虑数据的实用性, 本文模型通过设置误差门限来选取合适的隐私预算。

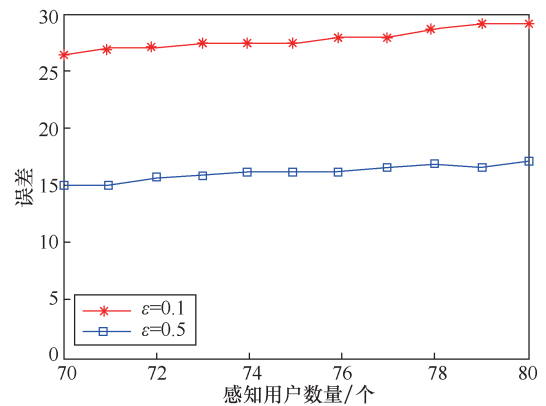


图 5 差分隐私预算对数据质量的影响

由图 6 可以看出, 虽然 CAPP 和本文方案都将用户身份验证和数据聚合分开处理, 感知用户

都是使用盲身份参与执行任务，但本文方案的时延不会随着该系统中不诚实用户的比例增加而大幅度增加。因为本文方案不存在对其他感知用户的可信度评估，每个感知用户独立上传自己的感知数据与反馈信息，且本文方案的 TC 和 DC 采用位于终端边缘的雾节点来承载，不仅减轻云端的能耗负担，而且支持很强的移动性。

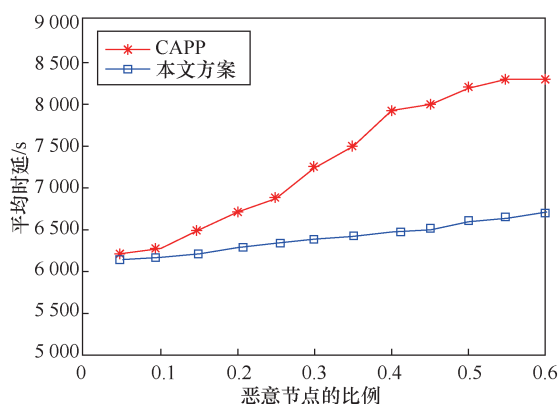


图6 两种方案的平均时延对比

6 结束语

移动群智感知作为新兴发展的物联感知模式，通过收集和分析海量多维异构数据，解决大规模复杂社会任务的需求问题。然而，感知用户间的社交关联以及感知数据和感知用户身份关联造成用户隐私的泄露，使感知用户的参与积极性不高，影响感知平台最终的数据聚合结果。因此，本文提出一种基于雾节点协作的感知用户身份隐私保护方案，创建 TC 和 DC 分别处理基于身份验证的任务分配问题和数据计算问题，并采用位于终端边缘的 2 个半可信雾节点承载；此外，感知用户使用不同的盲身份分别与 TC 和 DC 进行通信，从而有效防御感知用户在执行任务过程中，其身份、地理位置、时间等动态属性信息的泄露。仿真实验结果表明，所提方案的可行性和有效性。但是，感知用户在参与执行感知任务的过程中，其隐私信息会有或多或少的泄露，因此，合

适的隐私度量和隐私泄露补偿是未来的重点研究方向。

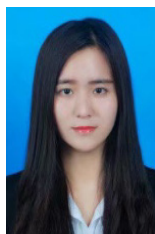
参考文献：

- [1] CHRISTIN D. Privacy in mobile participatory sensing: current trends and future challenges[J]. Journal of Systems and Software, 2016, 116: 57-68.
- [2] RESTUCCIA F, GHOSH N, BHATTACHARJEE S, et al. Quality of information in mobile crowd sensing: survey and research challenges[J]. ACM Transactions on Sensor Networks, 2017, 13(4): 34-43.
- [3] XIONG J, MA R, CHEN L, et al. Achieving incentive, security, and scalable privacy protection in mobile crowd sensing services[J]. Wireless Communications and Mobile Computing, 2018: 1-12.
- [4] NIE J, LUO J, XIONG Z, et al. A stackelberg game approach toward socially-aware incentive mechanisms for mobile crowd sensing[J]. IEEE Transactions on Wireless Communications, 2019, 18(2): 724-738.
- [5] LIU J, CAO H, LI Q, et al. A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing[J]. IEEE Internet of Things Journal, 2019, 6(2): 1321-1330.
- [6] LUO E, BHUIYAN M, WANG G, et al. Privacy protector: privacy-protected patient data collection in IoT-based healthcare systems[J]. IEEE Communications Magazine, 2018, 56(2): 163-168.
- [7] NI J, ZHANG K, XIA Q, et al. Enabling strong privacy preservation and accurate task allocation for mobile crowd sensing[J]. IEEE Transactions on Mobile Computing, 2019, 99: 1.
- [8] MA R, XIONG J, LIN M, et al. Privacy protection-oriented mobile crowd sensing analysis based on game theory[C]//2017 IEEE Trustcom/BigDataSE/ICSS. 2017: 990-995.
- [9] 马蓉, 陈秀华, 刘慧, 等. 移动群智感知中用户隐私度量与隐私保护研究[J]. 信息安全学报, 2018(8): 64-72.
MA R, CHEN X, LIU H, et al. Research about user privacy measurement and privacy protection in mobile crowd sensing[J]. Information Network Security, 2018(8): 64-72.
- [10] 房卫东, 张武雄, 单联海, 等. 无线传感器网络用户认证协议研究进展[J]. 网络与信息安全学报, 2017, 3(1): 1-12.
FANG W D, ZHANG W X, SHAN L H, et al. Research progress on user authentication protocol for wireless sensor networks [J]. Journal of Network and Information Security, 2017, 3(1): 1-12.
- [11] WANG X O, CHENG W, MOHAPATRA P, et al. Enabling reputation and trust in privacy preserving mobile sensing[J]. IEEE Trans. Mobile Comput, 2014, 13(12): 2777-2790.
- [12] WANG X O, CHENG W, MOHAPATRA P, et al. ART sense: anonymous reputation and trust in participatory sensing[C]//2013 the INFOCPM. 2013: 2517-2525.
- [13] HU L, SHAHABI C. Privacy assurance in mobile sensing network: go beyond trusted servers[C]//The Per Com Workshops. 2010: 613-619.
- [14] WU D, FAN L, ZHANG C, et al. Dynamical credibility assessment of privacy-preserving strategy for opportunistic mobile crowd sensing[J]. IEEE Access, 2018, 6: 37430-37443.
- [15] JIN H, SU L, XIAO H, et al. INCEPTION: incentivizing priva-

cy-preserving data aggregation for mobile crowd sensing systems[C]//2016 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing. 2016: 341-350

- [16] JIN H, SU L, DING B, et al. Enabling privacy-preserving incentives for mobile crowd sensing systems[C]//2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). 2016: 344-353.
- [17] DASTJERDI A V, BUYYYA R. Fog computing: helping the internet of things realize its potential[J]. Computer, 2016, 49(8): 112-116.
- [18] FIANDRINO C, ANJOMSHOA F, KANTARCI B, et al. Sociability-driven framework for data acquisition in mobile crowd sensing over fog computing platforms for smart cities[J]. IEEE Transactions on Sustainable Computing, 2017, 2(4): 345-358.
- [19] SUN G, SUN S, SUN J, et al. Security and privacy preservation in fog-based crowd sensing on the internet of vehicles[J]. Journal of Network and Computer Applications, 2019, 134: 89-99.
- [20] YANG M, ZHU T, LIU B, et al. Machine learning differential privacy with multifunctional aggregation in a fog computing architecture[J]. IEEE Access, 2018, 6: 17119-17129.
- [21] LU J, CAI Z, WANG X, et al. An edge correlation based differentially private network data release method[J]. Security and Communication Networks, 2017, (2): 1-14.
- [22] 曾菊儒, 陈红, 彭辉, 等. 参与式感知隐私保护技术[J]. 计算机学报, 2016, 39 (3): 595-614.
ZENG J R, CHEN H, PENG H, et al. Participatory awareness privacy protection technology[J]. Chinese Journal of Computers, 2016, 39(3): 595-614.
- [23] ZHOU T, CAI Z, WU K, et al. FIDC: a framework for improving data credibility in mobile crowd sensing[J]. Computer Networks, 2017, 120: 157-169.
- [24] DWORK C. Differential privacy[C]//The 33rd International Colloquium on Automata, Language and Programming. 2006: 1-12.
- [25] KE H, FU A, YU S, et al. AQ-DP: anew differential privacy scheme based on quasi-Identifier classifying in big data[C]//2018 IEEE Global Communications Conference (GLOBECOM). 2018: 1-6.

[作者简介]



刘慧 (1994-), 女, 山西吕梁人, 福建师范大学硕士生, 主要研究方向为隐私保护技术。



毕仁万 (1996-), 男, 湖南常德人, 福建师范大学硕士生, 主要研究方向为隐私度量、隐私保护。



熊金波 (1981-), 男, 湖南益阳人, 博士, 福建师范大学副教授, 主要研究方向为物联网数据安全、隐私保护技术。



赵明烽 (1996-), 男, 江苏张家港人, 福建师范大学硕士生, 主要研究方向为云数据安全与隐私保护。



金彪 (1985-), 男, 安徽六安人, 福建师范大学讲师, 主要研究方向为信息地理。



林劫 (1972-), 男, 福建三明人, 博士, 福建师范大学副教授, 主要研究方向为生物信息学、序列分析与算法。