·网络空间安全· 文章编号：1000-3428(2020)05-0181-06 文献标志码：A 中图分类号：TP393

群智感知中基于维诺单元的隐私保护方法

龙 浩[1,2]，张书奎[1,3]，张 力[1,3]

（1. 苏州大学 计算机科学与技术学院，江苏 苏州 215006；
2. 徐州工业职业技术学院 信息与电气工程学院，江苏 徐州 221002；
3. 江苏省现代企业信息化应用支撑软件工程技术研发中心，江苏 苏州 215104）

摘 要： 现有隐私保护方法多数仅利用匿名机制和加扰混沌方法隐藏用户的身份信息，恶意用户仍能从时空相关感知数据中推断出用户的活动轨迹。为建立混沌区域保障用户隐私并在混沌区域实现数据传输，面向移动群智感知网络提出一种基于维诺单元的隐私保护方法。参与者建立维诺单元，通过单跳或者多跳的方式广播需求，并联合其他参与者构建混沌区域，同时利用混沌区域的参与者代表与感知平台进行数据交互，从而将用户身份信息隐藏于不规则的维诺单元和混沌区域中。实验结果表明，该方法能有效建立不规则的混沌区域，提高了用户隐私保护成功率与效率。

关键词： 群智感知；维诺单元；混沌区域；隐私保护；数据融合

开放科学（资源服务）标志码（OSID）：

中文引用格式： 龙浩，张书奎，张力. 群智感知中基于维诺单元的隐私保护方法[J]. 计算机工程，2020，46(5)：181-186，192.

英文引用格式： LONG Hao，ZHANG Shukui，ZHANG Li. Privacy protection method based on Voronoi cell in crowd sensing[J]. Computer Engineering，2020，46(5)：181-186，192.

Privacy Protection Method Based on Voronoi Cell in Crowd Sensing

LONG Hao[1,2]，ZHANG Shukui[1,3]，ZHANG Li[1,3]

（1. School of Computer Science and Technology，Soochow University，Suzhou，Jiangsu 215006，China；
2. School of Information and Electrical Engineering，Xuzhou Vocational College of Industrial Technology，Xuzhou，Jiangsu 221002，China；3. Jiangsu Province Support Software Engineering R&D Center for Modern Information Technology Application in Enterprise，Suzhou，Jiangsu 215104，China）

【Abstract】 In existing privacy protection methods based on the anonymity mechanism and scrambled chaos，malicious users can still infer the activity trajectory of a user from obtained spatial-temporal sensing data. In order to establish an effective chaotic region to protect user privacy and achieve effective data transmission in the chaotic region，this paper proposes a privacy protection method based on Voronoi cells for mobile crowd sensing network. Users establish Voronoi cells and then a chaotic region with other users. The calculated participant representatives in the chaotic region submit sensing data by using data fusion，so as to hide user privacy in the irregular Voronoi cells and chaotic region. Experimental results show that the method can effectively establish irregular chaotic regions，and improve the success rate and efficiency of privacy protection for users.

【Key words】 crowd sensing；Voronoi cell；chaotic region；privacy protection；data fusion

DOI： 10.19678/j.issn.1000-3428.0053980

0 概述

在信息化时代，随着智能手机的普及，移动群智感知应用得到迅速发展。移动用户通过携带移动终端设备能够在不同的位置监测到复杂的数据信息，比如噪音、天气、大气、交通。目前，研究人员已开发了大量移动感知应用，如环境检测、交通监测、噪音监测等[1-2]。然而，在大多数情况下，感知任务需要

基金项目： 国家自然科学基金(61201212)；徐州市应用基础研究计划项目(KC17074)；苏州市融合通信重点实验室项目(SKLCC2013XX)；江苏省青蓝工程人才培养计划(102508999008)；江苏省“六大人才高峰”项目(2014-WLW-010)；江苏省高等学校自然科学研究面上项目(19KJB520061)。

作者简介： 龙 浩(1984—)，男，副教授、博士研究生，主研方向为群智感知计算、数据挖掘与隐私保护；张书奎(通信作者)，教授、博士；张 力，博士研究生。

收稿日期： 2019-02-22 **修回日期：** 2019-05-14 **E-mail：** longhhao@163.com

参与者在不同位置获得感知数据,参与者的位置信息很容易被暴露。由于隐私保护问题会影响用户参与感知任务的积极性,因此保护参与者的位置隐私信息是群智感知应用研究的重要内容。

现有隐私保护方法利用多匿名机制来隐藏用户的身份信息[3],然而恶意用户通过获得大量时空相关信息仍能够推测出用户的真实信息。文献[4]通过将随机噪音加入参与者位置信息中,使得恶意用户很难分辨出参与者的真实位置信息,然而加扰的位置信息在恢复过程中容易出现失真情况。文献[5]通过建立多匿名混沌区域来保护参与者的身份和位置信息,基于多个参与者组成混沌区域,然而该方法并没有考虑到混沌区域用户之间的协作问题,因此感知数据的传输效率受到较大影响。如何建立有效的混沌区域保障用户隐私,并在混沌区域实现数据的有效传输是本文研究的主要内容。因此,本文在移动群智感知网络中提出基于维诺单元的隐私保护方法(PP-Voronoi),参与者建立维诺单元,然后通过单跳或者多跳的方式广播需求,联合其他用户建立混沌区域,并利用混沌区域的参与者代表与感知平台进行数据交互,从而实现参与者的隐私保护。

1 相关工作

隐私保护是目前群智感知研究的重要内容,参与者在完成感知任务时会面临隐私泄露的风险,由于考虑到隐私成本影响其参与感知任务的积极性,因此现有提出的隐私保护方法主要分为加密、匿名、感知位置隐藏和建立混沌区域 4 类方法。文献[6-7]提出盲签名和部分盲签加密数据的隐私保护激励机制,但是算法计算量均较大。文献[8]采用 TLC 加密和匿名方法在参与者上传竞标与感知数据以及更新声誉值 3 个阶段进行隐私保护。文献[9]对参与者敏感属性进行隐私保护,根据敏感程度设计不同的敏感等级,实现个性化的隐私保护,然而恶意用户仍能根据参与者上传的感知数据推断出参与者的位置信息。文献[10]针对位置数据发布应用提出一种差异隐私保护算法,通过隐私位置聚类收缩来隐藏参与者的真实位置和访问某个位置的频率,该算法主要针对稀疏位置数据集,但由于其采用聚类方式,因此时间复杂度较高。文献[11-12]通过空间区域的时延特点为用户增加虚拟位置和用户信息。然而,这些方法在计算用户感知数据时容易出现信息误差,为加强参与者身份和位置信息的隐私保护,构建不同位置和大小的混合区域,引入多用户 k-匿名算法来保护参与者身份和位置信息。文献[13]针对感知参与者较少场景中暴露用户位置隐私的问题,提出多匿名多方服务器协作验证方法来保护用户的位置隐私。然而,该方法没有考虑混沌区域内用户之间位置信息的隐藏,另外其中混沌区域内用户数据采用 CP-ABE 加密的方式,增加了计算复杂度。

为建立有效的混沌区域并实现混沌区域用户有效的协作和数据传输,用户先根据感知任务建立维诺单元,再通过广播方式单跳或者多跳联合其他用户建立混沌区域,并为每一个混沌区域选择一个代表,实现其与感知平台的信息交互。

2 隐私保护方法的构建

在群智感知网络中,任务发布者通过感知平台发布感知任务,希望能找到距离感知任务节点尽可能近的移动用户来完成感知任务。在传统方法中,是参与者将位置发送给平台,平台根据参与者位置和感知节点位置的匹配度来分发任务给参与者,另外,参与者上传的感知数据也具有感知节点的位置信息。因此,该过程存在隐私泄露的问题,使得参与者不愿意将自己的隐私位置发送给平台,即使参与者隐藏自己的位置,由于参与者的移动或者在稀疏的网络环境中,平台也很容易推断出参与者的位置。为解决隐私泄露问题,本文提出一种基于维诺单元的隐私保护方法。

2.1 维诺单元的建立

为保护参与者的隐私,参与者通过建立维诺单元来隐藏自身的位置。维诺单元是计算几何中一种几何结构,也是一种空间分割方法。二维平面上的维诺图中的多边形通常被称为维诺单元。在几何空间中,维诺单元代表了各个节点相应的空间描述或作用范围。维诺单元的建立如图 1 所示。

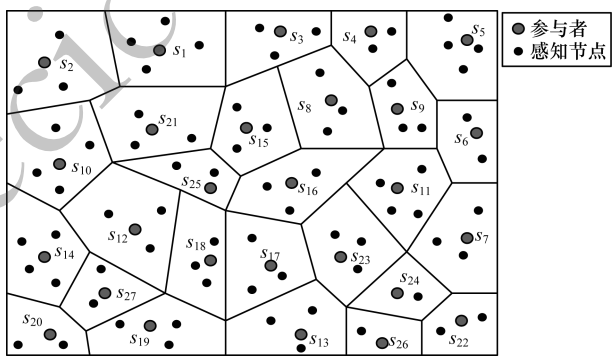

图 1 维诺单元的建立示意图

Fig. 1 Schematic diagram of establishment of Voronoi cells

定义 1 假设参与者集合 $S=\{s_1,s_2,\cdots,s_n\}$,$N>3$是欧几里德平面 R 上的一个点集,并且这些点不共线,任意 4 点不共圆,用 $d(v_i,v_j)$表示 v_i 和 v_j 之间的欧几里德距离,$E(P,S)$表示感知节点和参与者集合的环境,设 $\forall p\in E$,则区域 $V_i=\{p\in R^2 \mid d(p,s_i)\leqslant d(p,s_j),i,j=1,2,\cdots,n,i\neq j\}$ 称为 s_i 的维诺单元,各点的维诺单元共同组成维诺图。

平面上的维诺图可看作是将参与者集合 S 中的每个点作为生长核,以相同的速率向外扩张,直到彼此相遇为止而在平面上形成的图形。除了最外层的

点形成的开放区域外,其余每个点都形成一个凸多边形(维诺单元)。在维诺图中,任意一个维诺单元中的任意一个内点到该维诺单元控制点 s_i 的距离都小于该点到其他任何控制点 s_j 的距离。在维诺图中,维诺单元通常用于生成“领地”或控制区域,而且由于维诺图中的每个控制点唯一被一个维诺单元包含,因此可以用维诺图清晰地表达控制点之间的空间相邻关系。结合人类日常行为习惯与社会活动准则来看,人们通常会选择最短时间、最近距离、最低成本以及最优路线来解决生活中遇到的问题,这就反映出人类所遵循的空间行为准则。从这一层面来说,如果将维诺图中的种子点理解为人类日常行为或活动的出发点或目的地,那么维诺图内的各个维诺单元就反映了在一段时间内其对应行为活动的空间参考或影响的范围。

感知平台将维诺单元中所有感知节点的任务转发给对应的参与者 s_i,由于维诺单元中感知节点离 s_i 距离最近,因此参与者能更好地完成任务,获得高质量的感知数据。然而,参与者基于隐私的考虑,不愿意将自己的位置发送给感知平台。因此,本文需要解决的问题是如何保护每一位参与者的隐私,并且使感知平台能够将维诺单元中感知节点的任务分发给对应的参与者。

2.2　混沌区域的建立

由于通过感知平台来计算参与者的维诺单元存在很大程度的隐私泄露,因此参与者可以通过联系他的邻居来建立各自的维诺单元,然后每个参与者将建立好的维诺单元发送给感知平台获得对应的感知节点任务。该方法从表面上看参与者并没有将自己的隐私位置发送给平台,然而其感知平台还是能够通过足够的信息推断出参与者的位置,首先感知平台能获得参与者维诺单元的范围,然后感知平台获得参与者提交的感知点数据,通过两个数据的匹配,感知平台同样能确定参与者的位置信息。因此,参与者仅依靠建立维诺单元还不能完全实现隐私保护,为解决该问题,本文提出一种基于维诺单元的隐私保护算法,每个参与者可以通过联系其他参与者共同建立混沌区域来保护各自隐私,参与者的隐私保护水平由参与者请求隐私保护值(K,$A_{\min}$)决定,其中,K 代表参与者建立混沌区域中至少包含 K 个参与者,$A_{\min}$ 表示混沌区域的最小面积。算法具体步骤如下:1)每个参与者采用分布式方法建立自己的维诺单元 V_i;2)相邻参与者形成一个混沌区域 C;3)为混沌区域选取一个参与者代表 s_r。

本文参考文献[14]中的算法来建立参与者的维诺单元。算法主要分成两步:首先寻找参与者的邻居;其次通过参与者节点和邻居节点几何平分线的交点来计算维诺单元的边界。参与者通过相互通知的方式来发现各自的维诺邻居,当参与者确认了维诺邻居后,通过与邻居节点几何平分线的交点来建立维诺单元,并计算维诺单元的面积 A_i。

当各参与者建立维诺单元后,为进一步保护参与者隐私,相邻参与者建立一个混沌区域。本文采用 P2P SKA[15] 方法来建立混沌区域,参与者 s_i 先通过单跳路由向其维诺邻居广播一个请求,寻找邻居加入,如果没有找到足够的邻居,将继续通过多跳路由进行寻找,直到找到 $K-1$ 个邻居。参与者 s_i 与邻居采用匿名的方式进行通信,如果邻居收到请求后同意加入混沌区域,则将自己的匿名信息和维诺单元的面积 A_i 发送给 s_i。由于寻找邻居需要耗费比较长的搜索时间,多次广播请求也会耗费网络资源,因此为节省时间和网络开销,当邻居加入到混沌区域后,邻居节点也可以广播请求寻找自己的邻居加入,并为每一个参与者建立缓存联系清单,在广播请求时优先缓存清单的邻居,找到新的邻居后更新缓存清单。在群智感知网络中,参与者为动态移动,然而事实上,在很多情况下参与者的移动在一段时间内处于维诺单元范围内(比如家、公司),尤其是当参与者想要接收维诺单元的感知任务时,考虑到最坏情况下,即使混沌区域的参与者离开当前位置,新的邻居也可以动态加入混沌区域。图 2 中灰色区域为建立的混沌区域 $C=\{s_8, s_{15}, s_{16}, s_{21}, s_{25}\}$,其中 $K=5$。具体混沌区域的建立过程见算法 1。

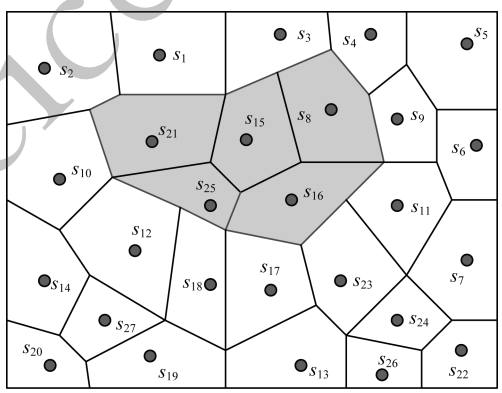

图 2　混沌区域的建立示意图

Fig. 2　Schematic diagram of establishment of the chaotic region

算法 1　建立混沌区域并计算混沌区域参与者代表的算法

输入　$S=\{s_1, s_2, \cdots, s_n\}$, K

输出　the set A of the chaotic region area, the representative s_r

1. C←{ϕ}; V←{ϕ}; h←1; A←{ϕ}
//V represents the Voronoi diagram and V_i represents the
//Voronoi cell
//Step 1: The establishment of the Voronoi diagram
2. for i from 1 to n do
3. V←V_i of s_i
4. end

//Step 2:The establishment of the cloaked region
5. A←A ∪ area(V_i)// Calculate the area of s_i
6. while |C|<K do //|C| represent the number of neighbors
7. Broadcast a request to the cached contact list of the neighbors within h hop(s) from s_i
8. C←C∪{s_j}
9. A←A ∪ area(V_j)
10. h←h + 1
11. end
12. return A
//Step 3:The calculation of the representative
13. for s_i in C do
14. Calculation the average distance d_i from s_i to other users
15. D←D∪{d_i} //D represent the set of the participants' //distances
16. end
17. Finding the user of the smallest average distance as the representative s_r
18. return s_r

在混沌区域构建完成后,其中隐含了 K 个匿名参与者及其维诺单元面积,为能够通过混沌区域来获取任务发布者的感知节点任务以及上传感知数据,需要在混沌区域中选取一个参与者代表 s_r。选择参与者代表的方法有很多,如文献[16]提出的 greedy algorithm,该算法选择覆盖感知节点最多的维诺单元的参与者作为代表,但其仅应用于集中式结构中,而在分布式结构中参与者并不知道各自维诺单元中覆盖的感知节点;文献[14]根据邻居打分投票的方式来决定参与者的代表,该方法在复杂网络环境中计算过于复杂,网络开销较大。为降低网络开销,本文选择一个与其他用户平均距离最近的用户作为混沌区域代表,代表的计算应避免感知平台的参与,由混沌区域内部用户通过算法完成计算。由于考虑到混沌区域内部用户的隐私,内部用户之间采用匿名的方式进行通信,参与者之间并不知道各自的真实身份信息,混沌区域用户间除了共享维诺单元的面积之外,还需要共享维诺单元的中心点坐标,节点间的距离通过 $d(s_i,s_j)=\sqrt{(x_i-x_j)^2+(y_i-y_j)^2}$ 计算,然后计算节点和其他节点的平均距离存入集合 D 中,并将集合 D 共享给混沌区域内所有的参与者,最后找出与其他节点平均距离最小的节点作为混沌区域的参与者代表 s_r。

2.3 混沌区域的数据收集及奖励与惩罚机制

混沌区域参与者完成感知任务后,需要将感知数据提交到平台。为保护参与者的位置信息,本文将混沌区域参与者的感知数据汇总后,由混沌区域的代表进行提交。参与者完成感知任务后,将感知数据封装成数据包,其格式包括维诺单元的编号 CID,获取感知数据的时间 Time、感知数据节点的编号 NID 和感知数据 DATA,具体格式如图 3 所示。参与者将数据包发送给混沌区域的代表 s_r,收到数据包后 s_r 为每一个参与者计算其数据质量(Quality of Data,QoD)评价值 $E(s_i)$,将 $E(s_i)$ 和数据包汇总后形成一个新的数据包,并将新的数据包发送给感知平台。新的数据包格式包括混沌区域编号 RID 和 K 个参与者的汇总数据,具体数据包格式如图 4 所示。

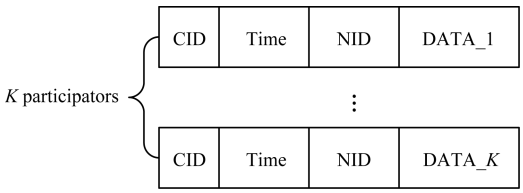

图 3 K 个参与者的数据包

Fig. 3 Data packets of K participants

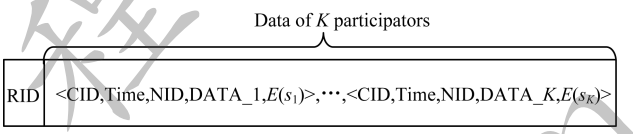

图 4 混沌区域感知数据包

Fig. 4 Sensing data packets of the chaotic region

感知平台收到混沌区域发送过来的汇总数据后,首先计算每一个维诺单元区域的 QoD 评价值,然后将平台计算的评价值和发送过来的评价值进行比较,如果这两个值不相等,则平台将发送一个验证信息给混沌区域的代表 s_r,验证数据包是否出错或者存在丢失。由 s_r 确认后重新计算评价值发送给平台,平台再次验证无误后进行最终的奖励和处罚。

在感知系统中,通过计算参与者提交感知 QoD 评价值来决定是否分发奖励给参与者。感知系统主要惩罚质量评价值过低的参与者,如果参与者提交伪造数据,当 QoD 评价值低于阈值 ε 时,参与者将不能获得奖励。为鼓励成员提高整体的感知 QoD,混沌区域的 K 个成员关系被看作是一种协作的裙带关系,系统为混沌区域设置一个整体感知 QoD 评价阈值 α,整体 QoD 评价值 $E(K)$ 决定了每个参与者声誉值的更新。混沌区域的 QoD 评价值计算公式如下:

$$E(K)=1-\sqrt{\frac{\sum_{i\in K}(n_i-d_i)}{\sum_{i\in K}n_i}} \tag{1}$$

其中,n_i 代表平台需求的样本数据,d_i 代表参与者提交的感知数据。式(1)中通过平台要求的样本数据和混沌区域参与者提交的有效数据容量的差值与样本数据比值的平方根来检测参与者采集感知数据的失真程度,然后将量化值转化为数据质量评价值 $E(K)$。

本文定义 r_i 为当前任务声誉值,r_i' 为这次任务之前的声誉值。为保证任务执行的质量,每个任务设置一个声誉阈值 r_m。以混沌区域中的一个参与者为例,具体声誉更新方法如下:

$$r_i=\begin{cases}r_i'+1, E(K)>\alpha \text{ 且 } r_i'>r_m\\ r_i'-1, E(K)<\alpha \text{ 且 } r_i'>r_m\\ r_i', r_i'\leqslant r_m\end{cases} \tag{2}$$

声誉值更新方法将混沌区域看作一个团队,如

果团队某个成员提交了质量低的感知数据,使得整个团队数据质量评价值小于阈值,则团队所有的成员声誉值都将降低,因此为保证团队成员的利益,要求团队的每个参与者都能提交真实可靠的数据。另外,当参与者声誉值$r_i' < r_m$且考虑一定的冗余度时,即使$r_i' = r_m$,平台都不会把任务分配给该参与者。参与者为获得更多参与任务的机会,需要提交高质量的数据来提高自身的声誉值。

3　仿真与性能评价

本文首先对仿真实验的参数和实验方法进行介绍说明,然后根据不同的用户数量与隐私保护水平,对隐私保护成功率、平均响应时间、平均通信量进行比较与评价。隐私保护成功率是指在恶意用户攻击下能够成功隐藏的用户数量,本文采用文献[17]中提出的恶意攻击方法。平均通信量指感知任务过程中参与者之间信息交互的平均流量。平均响应时间是指参与者建立混沌区域并与感知平台进行数据交互耗费的总时间。平均通信量和平均响应时间反映了隐私保护方法的效率。隐私保护水平在实验中主要是指混沌区域中包含的用户数量。为评价 PP-Voronoi 方法的性能,本文选择 Coprivacy 方法[18]和 Privacy_1 方法[19]进行对比实验。Coprivacy 方法通过用户之间的协作形成匿名区域,匿名区域内的用户使用该组的密度中心代替真实位置交互数据。Privacy_1 方法通过用户协作博弈建立匿名区域,然后使用安全求和协议计算区域的锚点与感知平台进行数据交互。两种方法在形式上与本文方法类似,因此具有较好的可比性。

3.1　仿真设置

为验证本文方法的性能,基于 Dev-cpp 5.4 C++ 开发隐私保护仿真系统。实验软硬件环境为:Windows 7, Intel(R) Core(TM) i5-3470 3.20 GHz 的 CPU,8 GB 内存。选用城市的真实数据集 Milano,平均每千米的用户数为 7 382[20],拥有智能手机的用户比例为 40% 。网络用户通信采用 NS2 进行仿真,用户之间的通信基于 4G 网络,带宽为 20 Mb/s,隐私保护水平(K)为 5 ~ 10,所有实验结果至少进行 100 轮后取平均值。

3.2　性能分析

仿真比较在不同参与者数量和隐私保护水平下 3 种方法的隐私保护成功率。如图 5 所示,由于本文 PP-Voronoi 方法采用不规则混沌区域,且考虑了混沌区域内部用户之间的位置保护,因此其随着参与者增多,隐私保护成功率随之增加直至最高。如图 6 所示,随着参与者数量增多,加入混沌区域内的用户数增多,隐私保护成功率随之提高,由此可以看出,Coprivacy 方法的隐私保护成功率基本保持不变,PP-Voronoi 方法呈缓慢增长,且隐私保护成功率最高。

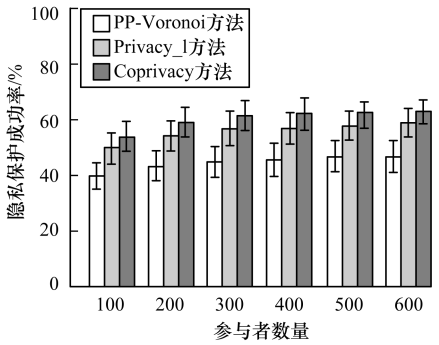

图 5　3 种方法在不同参与者数量下的隐私保护成功率

Fig. 5　Success rate of privacy protection of three methods under different numbers of participants

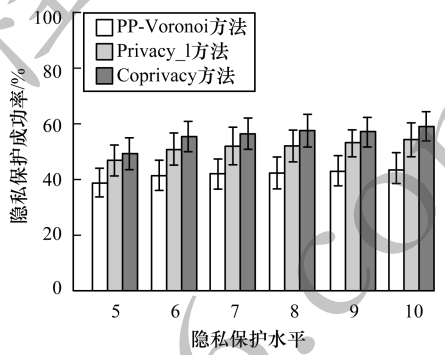

图 6　3 种方法在不同隐私保护水平下的隐私保护成功率

Fig. 6　Success rate of privacy protection of three methods at different levels of privacy protection

图 7 表示 3 种方法在不同参与者数量下的数据交互平均响应时间。Privacy_1 方法需要耗费时间构建一个可信区域,因此其平均响应时间最多。需要指出的是 Coprivacy 方法假设混沌区域内的参与者都是可信的,且混沌区域的锚点为直接指定,因此其平均响应时间最低。PP-Voronoi 方法由于需要通过计算参与者的平均间距确定混沌区域代表,需要耗费时间,因此平均响应时间要高于 Coprivacy 方法,但是比 Privcay_1 方法平均响应时间要低。如图 8 所示,随着隐私保护水平的提升,由于建立混沌区域及混沌区域内用户的交互时间增加,因此各方法的平均响应时间均增加。

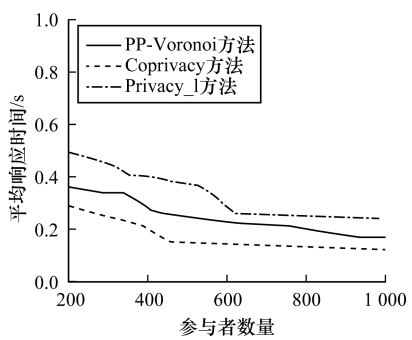

图 7　3 种方法在不同参与者数量下的平均响应时间

Fig. 7　Average response time of three methods under different numbers of participants

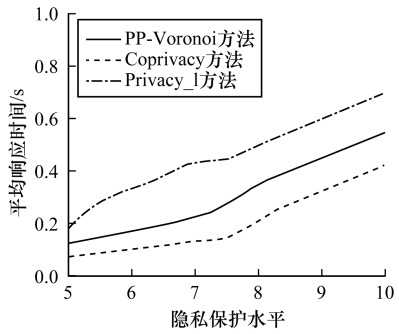

图 8 3 种方法在不同隐私保护水平下的平均响应时间

Fig. 8 Average response time of three methods at different levels of privacy protection

由图 9 可以看出,仿真初期由于参与者数量有限,因此建立混沌区域需要参与者与邻居进行更多的通信量。Privacy_1 方法需要更多的协作通信建立混沌区域和锚点,因此其需要的平均通信量最多,且随着参与者数量的增加通信量下降较慢。PP-Voronoi 方法通过参与者的邻居缓存清单建立通信,平均通信量低于 Privacy_1 方法,但是比假设完全可信环境的 Coprivacy 方法要高,且随着参与者数量增加,平均通信量已经接近 Coprivacy 方法。如图 10 所示,随着隐私保护水平的提高及混沌区域内参与者数量的增加,3 种方法的通信量随之增加。

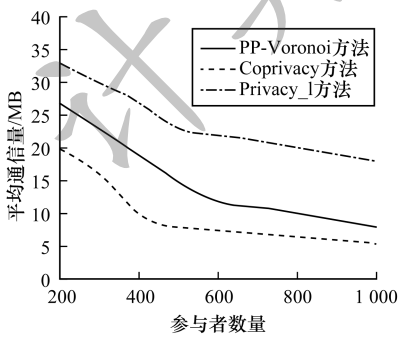

图 9 3 种方法在不同参与者数量下的平均通信量

Fig. 9 Average communication volume of three methods under different numbers of participants

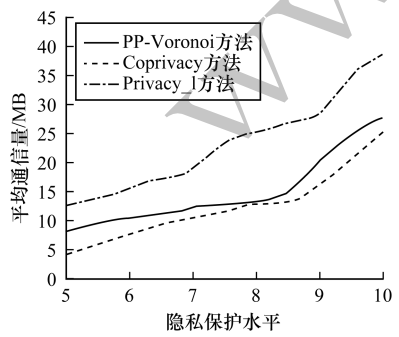

图 10 3 种方法在不同隐私保护水平下的平均通信量

Fig. 10 Average communication volume of three methods at different levels of privacy protection

4 结束语

本文提出一种基于维诺单元的隐私保护方法,在用户构建维诺单元的基础上形成不规则的混沌区域,使感知平台无法直接推断出参与者的隐私信息,同时混沌区域中内部用户构建的维诺单元也能保护内部用户的隐私。此外,本文通过选择混沌区域代表的方式并采用数据融合的方法与感知平台进行数据交互,进一步保护参与者的位置信息,且对混沌区域整体数据质量进行评价来更新参与者的声誉值,从而保证感知数据的质量。在真实数据集上的仿真结果验证了本文 PP-Voronoi 方法的可行性与有效性。下一步将优化混沌区域内部参与者动态更新方法,并在此基础上设计参与者进行数据传输的轻量级加密算法。

参考文献

[1] WANG Yufeng, JIA Xueyu, JIN Qun, et al. Mobile crowdsourcing: framework, challenges, and solutions [J]. Concurrency and Computation Practice and Experience, 2017, 29(3): 1191-1200.

[2] WU Yao, ZENG Juru, PENG Hui, et al. Survey on incentive mechanisms for crowd sensing[J]. 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[J]. 软件学报, 2016, 27(8): 2025-2047.

[3] POURNAJAF L, GARCIA-ULLOA D A, XIONG L, 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] TO H, GHINITA G, SHAHABI C. A framework for protecting worker location privacy in spatial crowdsourcing [J]. Proceedings of the VLDB Endowment, 2014, 7(10): 919-930.

[5] DARGAHI T, AMBROSIN M, CONTI M, et al. ABAKA: a novel attribute-based k-anonymous collaborative solution for LBSs[J]. Computer Communications, 2016, 85: 1-13.

[6] LI Qinghua, CAO Guohong. Providing privacy-aware incentives for mobile sensing [C]//Proceedings of IEEE International Conference on Pervasive Computing and Communications. Washington D.C., USA: IEEE Press, 2013: 76-84.

[7] LONG Hao, ZHANG Li, WANG Jin, et al. An incentive mechanism with privacy protection and quality evaluation in mobile crowd computing[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2011, 30(3): 187-198.

[8] WANG Yingjie, CAI Zhipeng, YIN Guisheng, et al. An incentive mechanism with privacy protection in mobile crowdsourcing systems [J]. Computer Networks, 2016, 102: 157-171.

[9] JIA Junjie, YAN Guolei. A personalized (p, k)-anonymity privacy protection algorithm [J]. Computer Engineering, 2018, 44(1): 176-181. (in Chinese)
贾俊杰, 闫国蕾. 一种个性化(p, k)匿名隐私保护算法[J]. 计算机工程, 2018, 44(1): 176-181.

(下转第 192 页)

(上接第 186 页)

[10] XIONG Ping, ZHU Tianqing, NIU Weijia, et al. A differentially private algorithm for location data release[J]. Knowledge and Information Systems, 2016, 47(3): 647-669.

[11] WU Xu, LUO Min. Privacy-preserving method of location based service in sparse environment[J]. Computer Engineering, 2017, 43(5): 108-114. (in Chinese)
伍旭,罗敏. 稀疏环境下基于位置服务的隐私保护方法[J]. 计算机工程,2017,43(5):108-114.

[12] PEI Yuanyuan, SHI Runhua, ZHONG Hong, et al. User privacy protection for location-based service [J]. Computer Engineering, 2015, 41(10): 20-25. (in Chinese)
裴媛媛,石润华,仲红,等. 面向位置服务的用户隐私保护[J]. 计算机工程,2015,41(10):20-25.

[13] CHEN Jianwei, MA Huadong, ZHAO Dong, et al. Participant density-independent location privacy protection for data aggregation in mobile crowd-sensing[J]. Wireless Personal Communications, 2018, 98(1): 699-723.

[14] KAZEMI L, SHAHABI C. A privacy-aware framework for participatory sensing[J]. ACM SIGKDD Explorations Newsletter, 2011, 13(1): 43-51.

[15] CHO H J, KWON S J, JIN R, et al. A privacy-aware monitoring algorithm for moving k-nearest neighbor queries in road networks[J]. Distributed and Parallel Databases, 2015, 33(3): 319-352.

[16] KLEINBERG B J, TARDOS E. Algorithm design[M]. Boston, USA: Addison-Wesley Longman Publishing Co., Ltd., 2010.

[17] JIANG Hongbo, ZHAO Ping, WANG Chen. RobLoP: towards robust privacy preserving against location dependent attacks in continuous LBS queries[J]. IEEE/ACM Transactions on Networking, 2018, 26(2): 1-15.

[18] HUANG Yi, HUO Yan, MENG Xiaofeng. CoPrivacy: a collaborative location privacy-preserving method without cloaking region[J]. Chinese Journal of Computers, 2011, 34(10): 1976-1985. (in Chinese)
黄毅,霍峥,孟小峰. CoPrivacy:一种用户协作无匿名区域的位置隐私保护方法[J]. 计算机学报,2011,34(10):1976-1985.

[19] CHEN Yufeng, LIU Xuejun, LI Bin. Collaborative position privacy protection method based on game theory[J]. Computer Science, 2013, 40(10): 92-97. (in Chinese)
陈玉凤,刘学军,李斌. 基于博弈论的用户相互协作的位置隐私保护方法[J]. 计算机科学,2013,40(10):92-97.

[20] Focus on Milan [EB/OL]. [2019-01-12]. http://allegati.comune.milano.it/Statistica/AnnuariStatistici/MilanoIn Breve2012/FocusOnMilano2012.pdf.

编辑 陆燕菲