基于双向拍卖的 k-匿名激励机制

童 海[1,2] 白光伟[1] 沈 航[1,3]
(南京工业大学计算机科学与技术学院 南京 211816)[1]
(南京大学计算机软件新技术国家重点实验室 南京 210093)[2]
(南京邮电大学通信与网络技术国家工程研究中心 南京 210003)[3]

摘 要 在基于位置的服务(LBS)中,k-匿名是重要的位置隐私保护技术之一。k-匿名要求至少k名用户参与匿名集的构建,使得集合中任何用户都不能从其他$k-1$名用户中区分开来。然而,很多参与者希望得到回报或顾忌个人隐私泄漏,导致匿名集人数不足。为了提高用户参与匿名集构建的积极性,提出了一种基于双向拍卖的k-匿名激励机制(Double-Acution-based Incentive,DAI),以保证交易公平的同时最大化买卖双方的效用。首先,利用多阶段采样来筛选候选用户集;然后,根据预算平衡性选择获胜用户集和合理的报酬;最后,从个体理性、计算效率、预算平衡和真诚可信等方面,通过理论证明了机制的合理性。仿真结果表明,DAI能够抑制用户恶意竞价情况的发生,同时提高买方的满意度和效用。

关键词 位置隐私,k-匿名,激励机制,双向拍卖
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.03.030

Double-auction-based Incentive Mechanism for k-anonymity

TONG Hai[1,2] BAI Guang-wei[1] SHEN Hang[1,3]
(College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China)[1]
(State Key Laboratory for Novel Software Technology (Nanjing University), Nanjing 210093, China)[2]
(National Engineering Research Center for Communication and Network Technology (Nanjing University of Posts and Telecommunications), Nanjing 210003, China)[3]

Abstract k-anonymity has become one of the most important location privacy technologies in LBS (Location Based Service). At least k users should be required to build an anonymous set, in which any user cannot be distinguished from other $k-1$ users. However, many users are not interested in their location privacy, so they have little interest in participating in the construction of anonymous sets. In order to improve the enthusiasm of users to participate in building anonymous sets, this paper proposed a double-auction-based incentive(DAI) mechanism for k-anonymity, which maximizes both the utility of buyers and sellers while guaranteeing fair transaction. To this end, multi-stage sample is used to filter the candidate user sets, then a reasonable remuneration and the winning set of users are determined according to budget balance. Finally, the rationality of the mechanism is provided in consideration of individual rationality, computation efficiency, budget balance and truthfulness, and so on. Simulation results demonstrate that DAI can solve the problem of malicious competition in the existing methods, and improve satisfaction and utility of buyers effectively.

Keywords Location privacy, k-anonymity, Incentive mechanism, Double auction

1 引言

k-匿名是保护移动用户位置隐私的方法之一[1]。为了实现k-匿名,需要构建一个至少包含k名移动用户的匿名集。然而,一些用户希望从提供匿名服务中得到回报,而不是志愿参与;另外,提供隐私保护服务也会带来额外的通信和存储开

到稿日期:2018-02-11 返修日期:2018-05-14 本文受国家自然科学基金项目(61502230,61073197),江苏省自然科学基金项目(BK20150960),江苏省普通高校自然科学研究项目(15KJB520015),南京市科技计划项目(201608009),南京大学计算机软件新技术国家重点实验室资助项目(KFKT2017B21),南京邮电大学通信与网络技术国家工程研究中心资助项目,江苏省六大高峰人才基金资助项目(第八批)资助。
童 海(1993-),男,硕士生,主要研究方向为移动群智感知、激励机制、隐私保护,E-mail:tonghaiwork@163.com;**白光伟**(1961-),男,博士,教授,博士生导师,CCF杰出会员,主要研究方向为无线传感器网络、移动互联网、网络体系结构和协议、网络系统性能分析和评价、多媒体网络服务质量等;**沈 航**(1984-),男,博士,讲师,硕士生导师,CCF会员,主要研究方向为无线网络编码、移动互联网、无线多媒体通信协议等,E-mail:hsen@njtech.edu.cn(通信作者)。

销,例如手机电池消耗和计算开销。因此,大部分用户可能不会参与匿名集的构建。激励机制在提升用户参与积极性、保证交易公平性和提高数据质量等方面有着重要作用[2]。因此,许多研究者提出用激励机制来解决 k-匿名环境下的参与者选择和报酬支付问题,使得参与者能够积极、快速地加入到匿名集的构建中。

在 k-匿名中,大多采用集中式云服务器架构。云服务器掌握所有用户的真实位置信息,需要选择距离请求者地理位置较近且有意愿参与的用户进行匿名。然而,这种模式带来了参与者对自身位置隐私暴露的担忧,并且由于激励过程具有交互性强、时延敏感等特点,过大的访问量可能会导致系统延迟较高。与此同时,已有的激励机制[3-6]大多只能解决离线状态下的用户选择问题,没有考虑实际环境中的因素,例如参与者人数不确定,可用性也会随时间而改变。边缘计算[7]恰好能弥补这些不足:分布式边缘计算节点既能对用户进行时空匿名,保护参与者的位置隐私,又可以提供较强的计算能力,减轻云服务器的计算压力,降低延迟,提高实时性。

本文提出了一种基于双向拍卖的 k-匿名激励机制,以寻找满足预算和效用要求的用户。与现有方案不同,该机制将候选用户的选择任务迁移到边缘计算节点完成。首先,边缘计算节点利用多阶段采样法筛选出报价合适的候选用户,并对用户位置信息进行时空匿名,发送给云服务器;然后,根据预算平衡性的限制条件,计算获胜用户集,并为其分配合理的费用和报酬;最后,通过理论证明和仿真分析,观察此方案的特点。

本文第 2 节介绍了相关工作;第 3 节阐述了系统模型和拍卖模型以及模型具备的经济特性;第 4 节描述了激励机制的实现细节;第 5 节进行了理论分析与证明;第 6 节进行了仿真实验和性能分析;最后总结全文。

2　相关工作

在激励机制中,如何设计合理的激励方式(模型)来提高参与者的积极性并保证提供数据的可靠性,一直是人们关注的焦点。近年来,逐渐涌现出了许多有价值的研究工作。

激励方式从回报方式上可以分为金钱式激励和非金钱式激励。非金钱式激励主要通过虚拟积分、信用和娱乐游戏等方式来激励用户参与任务。Kawajiri 等[8]根据不同位置的任务制定不同的游戏积分,以此来激励用户到不同的地点收集数据,从而完成位置相关的感知任务。Li 等[9]提出基于信用的激励机制,通过为他人提供隐私保护服务来积累自身信用,信用值越高,用户的优先级就越高。文献[10]指出,含有金钱激励方式的机制的效果相对更好,其中,基于拍卖的激励模型通过支付报酬来鼓励用户参与,它是目前最直接和最主要的金钱激励方式。文献[11-14]采用逆向拍卖来激励参与者根据自己所在位置和感知范围竞价感知任务,服务器平台根据汇总的参与者竞价情况来选择获胜者。

然而,上述模型都属于一对一、一对多的激励方式,并不适用于 k-匿名这种多对多的应用场景。Yang 等[3]首次将激励机制引入 k-匿名,基于 Macfee 双向拍卖来激励参与者加入匿名集。其虽然严格证明了即使买卖双方存在欺骗行为也不会改变拍卖结果,但是拍卖成功的比例会随之变低。文献[4]在文献[3]的基础上弱化了买方真实性,提高了拍卖成功的比例。然而,这两种方案都没有考虑到在 LBS 中节点并不是相对固定的,它们会频繁移动,从而导致参与者人数发生变化,最终影响拍卖结果。文献[5]在激励报酬中引入协商议价理论和惩罚机制,提出了 k-least 集群来实现 k-匿名位置隐私保护,提高了用户的参与率。文献[6]针对位置隐私保护和信息服务质量相冲突的问题,提出了位置聚合方法,同时设计了一种激励机制来选择有效用户并计算合理的补偿,减轻了由于位置隐私保护所引起的信息损失。

上述文献所提出的激励机制都属于离线机制,即在拍卖过程中,参与者人数、报价和位置信息都是已知的。而在实际情况中,参与者人数和报价是不确定的,可用性也会随时间而改变,这样容易导致离线机制无法完成用户激励。文献[15]设计了基于多市场动态双向拍卖的在线激励机制,将拍卖的计算任务迁移到智能手机上,买卖双方通过广播来进行交易,但是带来了额外开销,且用户容易遭受攻击。文献[16-17]在众包系统中设计了在线激励机制,众包商在参与者到达时决定是否接受参与者。其中,文献[17]在指定截止日期之前选择一个参与者子集,在预算约束的情况下,最大化获胜参与者的服务价值。

为了兼顾 k-匿名环境下参与者的隐私保护,并缓解在线状态对激励结果造成的不利影响,本文提出一种基于双向拍卖的激励机制,分布式边缘计算节点对参与者进行时空匿名,利用多阶段采样解决参与者在线选择的问题。

3　双向拍卖激励模型

3.1　系统模型

本文的系统模型如图 1 所示,主要包括 3 个交互主体:移动用户、边缘节点和云服务器。

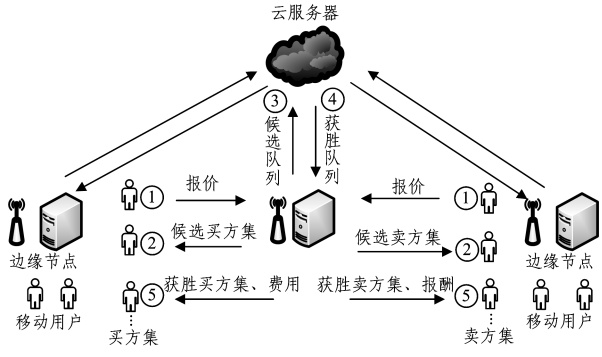


图 1　双向拍卖激励模型

Fig. 1　Double-auction-based incentive model

1)移动用户:移动用户包括匿名任务请求者和参与者,分别被形式化为买方和卖方。默认买方为离线状态,而卖方是在线状态,即在整个拍卖过程中,卖方人数、报价和位置信息都是不确定的。

2)边缘节点:具有存储、分发功能和较强的计算能力,可以将一些原本需要放在云服务器或者手机端的计算任务迁移到边缘节点上来完成,以减少能耗,特别是对于与云服务器有较强交互性的应用,可以降低延迟,提高实时性;可以对服务

范围内的用户进行时空匿名，以在提高参与者积极性的同时，有效保护用户隐私。

3)云服务器：集中式云服务器掌握全局的边缘节点信息，处理每个边缘节点所提交的请求。在整个拍卖过程中，边缘节点封装了用户位置信息，因此即使云服务器遭受攻击，用户的隐私依然不会泄漏。

本文的系统架构涉及边缘节点与用户、边缘节点与云服务器的交互情况。图 1 给出了这 3 个主体之间的交互顺序。

1)在每轮拍卖截止时间之前，买方将匿名服务的预算发送给边缘节点，卖方在到达边缘节点的服务范围时主动将报价发送给边缘节点。

2)边缘节点根据买方的总预算约束和卖方报价等条件筛选出候选买方集和卖方集。

3)在拍卖的截止时刻，边缘节点在本地存储一份映射表，其中，*key* 表示用户到达时间，*value* 表示位置信息与报价。然后，封装用户的位置信息，按报价进行排序形成候选列表，并将它发送给云服务器。

4)云服务器根据候选价格列表来计算主元买方(Pivot Buyer)的索引，从而得到获胜买方人数、每位买方所需支付的成交价格、获胜卖方人数和每位卖方所得报酬，最终形成获胜列表，将它返回给边缘节点。

5)边缘节点根据获胜价格列表，参照本地映射表匹配出真实用户，向获胜买方收取相应的费用，并统一向获胜卖方支付相应的报酬。

在整个激励过程中，边缘节点承担了其服务范围内候选用户选择的计算任务，减轻了云服务器的计算负担，降低了系统决策延迟。而且，边缘节点上传给云服务器的候选列表不包含参与者的位置信息，不会暴露买卖双方的真实位置信息，从而能够间接地降低隐私泄漏所带来的风险。

3.2 双向拍卖模型

本文将 k-匿名激励机制建模为双向拍卖。这是因为在激励过程中，匿名请求者和参与者的人数都不止一个，且双方是一种平等的供给和需求关系。假设在边缘节点覆盖区域内有 n 位买方 $U^b=\{U_1^b,U_2^b,\cdots,U_n^b\}$需要 k-匿名服务，每位买方 $U_i^b\in U^b$ 都期望一个 k_i-匿名，表示它所需要的隐私保护要求，即匿名集的大小，本文假设每位买方都期望相同的 k 值。买方 U_i^b 对请求所需的费用有一个估值 $v_i(v_i\geqslant 0)$，在拍卖中的报价是 b_i。在拍卖机制中，b_i 不一定等于 v_i。边缘节点作为拍卖中心，决定了买方 U_i^b 最终需要支付的费用 p_i^b。

每位卖方 U_j^s 均有一个到达时刻 $a_j\in\{1,\cdots,T\}$以及构建匿名集的成本 $c_j(c_j\geqslant 0)$，其中 T 表示每轮拍卖的截止时间。卖方 $U_j^s\in U^s$ 以随机顺序到达，并向边缘节点发送报价 λ_j。如果买方或卖方的报价相同，本文则依据他们的到达时间来打破平衡关系。在拍卖机制中，λ_j 与 c_j 不一定相等。卖方 U_j^s 最终的报酬 p_j^s 取决于边缘节点。

当卖方 U_j^s 到达时，边缘节点根据预算约束条件选择合适的卖方作为候选者，并将所选出的候选用户列表上传给云服务器。云服务器通过计算确定获胜用户列表，然后将其返回给边缘节点，最后边缘节点根据以上信息匹配出真实的获胜买方集 W^b 和卖方集 W^s。对于每一位买方 $U_i^b\in W^b$ 而言，拍卖成功的条件是：

$$|W^b|+|W^s|\geqslant k \tag{1}$$

另外，p_i^b 为边缘节点向买方 $U_i^b\in U^b$ 收取的费用，p_j^s 为边缘节点支付给卖方 $U_j^s\in U^s$ 的报酬。当然，对于拍卖失败的买方 $U_i^b\in U^b\backslash W^b$，费用 $p_i^b=0$；对于拍卖失败的卖方 $U_j^s\in U^s\backslash W^s$，报酬 $p_j^s=0$。因此，买方 U_i^b 的效用为：

$$u_i^b=\begin{cases}v_i-p_i^b, & \text{if } U_i^b\in W^b\\ 0, & \text{otherwise}\end{cases} \tag{2}$$

同理，卖方 u_j^s 的效用为：

$$u_j^s=\begin{cases}p_j^s-c_j, & \text{if } U_j^s\in W^s\\ 0, & \text{otherwise}\end{cases} \tag{3}$$

本文假设买卖双方都是理性的，其目标都是最大化自己的效用。

3.3 模型的经济特性

理想的激励机制应该具备一些经济特性，因此本文设计的激励机制需要满足以下 4 个期望特性。

1)计算效率(Computation Efficiency)。竞价结果，即获胜者的选择过程，需要在多项式时间内计算出来。

2)个体理性(Individual Rationality)。如果用户诚实地报价，那么机制一定要保证他们的效用为非负，即 $u_i^b\geqslant 0$ 且 $u_j^s\geqslant 0$。

3)预算平衡(Budget Balance)。所有获胜买家支付的总费用不小于所有获胜卖家得到的总报酬。

4)真诚可信(Truthfulness)。用户恶意报价所得效用不能高于用户诚实报价所得效用。

在 4 个期望特性中，前 3 个为基础特性，用于确保激励机制可行。真诚可信包含真实性和诚实性。拍卖真实性必须满足两个条件：1)选择规则必须单调。如果卖方以报价 λ_j 赢得了拍卖，那么报价小于 λ_i 的其他卖方一定能赢得拍卖(单调性)。2)获胜者的报酬是关键值。如果报价 λ_i 高于报酬，那么将不会赢得拍卖(关键值)。诚实性可以减轻买卖双方在竞拍失败等方面的担忧，抑制竞价过程中的恶意报价行为。

4 DAI 的实现细节

参与者在构建 k-匿名过程中会因为电量、流量、计算资源等原因产生一些开销，在不提供激励的情况下这些因素会降低参与者响应请求的积极性。本文设计的激励机制不仅能够在拍卖过程中保护用户隐私，而且能够解决用户恶意竞价问题。实现过程包括两个步骤：选择候选用户集和选择获胜用户集。

4.1 候选用户选择

反向拍卖是一种逐级向下竞价且以最低价成交的拍卖方式；Vickrey 拍卖是一种密封且以次高价成交的拍卖方式。如果候选买方的人数大于 k，则不需要卖方来参与匿名集构建。为了满足诚实性要求，本文采用反向拍卖与 Virckrey 拍卖相结合的方式，除了出价最低的买方，其他买方都选为获胜者。然而，如果买方人数少于 k，那么就需要考虑如何激励卖方参与、选择用户和支付报酬。

当买方人数少于 k 时，边缘节点将所有买方的报价降序排序，从而形成一个列表 $List[b_i](1\leqslant i\leqslant n)$，$b_1\geqslant b_2\geqslant\cdots\geqslant b_n$。因此，在每轮拍卖截止时间之前，边缘节点的总预算如式(4)所示：

$$B=\sum_{i=1}^{n-1}b_i \tag{4}$$

考虑到卖方到达边缘节点服务范围内的时间、人数和报价都不确定，本文基于多阶段采样法将每轮拍卖截止时间 T 分为 i 个子阶段。每个子阶段的结束时刻 T_i 可以表示为：

$$i=\lfloor \log_2 T \rfloor+1 \tag{5}$$

$$T_i=\lfloor 2^{i-1}T/2^{\lfloor \log_2 T \rfloor} \rfloor \tag{6}$$

则第 i 个子阶段的预算也相应地随时间进行分配。

$$B_i=2^{i-1}B/2^{\lfloor \log_2 T \rfloor} \tag{7}$$

在第 i 个子阶段，边缘节点通过式(8)判断卖方 U_j^s 的报价 λ_j 是否符合拍卖的预算要求。其中，S 是整个时间内的候选卖方集，也是一个映射表，存储候选卖方的真实位置、报价和到达时间信息。边缘节点将符合预算要求的卖方更新到样本集 S 中，λ_q 是样本集 S 中的第 q 位卖方。

$$\lambda_j \leqslant B_i-\sum_{q\in S}\lambda_q \tag{8}$$

候选用户的实现如算法 1 所示。

算法 1　DAI 候选用户选择算法

```
1. Input: B_i, λ_j, k, T
2. Output: S
3. for i=1 to ⌊log2 T⌋+1 do
4.    while TRUE do
5.       if a_j ≤ T_i then //筛选符合预算约束的卖方
6.          if λ_j ≤ B_i − Σ_{q∈S} λ_q then
7.             S ← S ∪ {j};
8.          end if
9.          j=j+1;
10.      else then
11.         break;
12.      end if
13.   end while
14. end for
15. if a_j = T then //参与拍卖的截止时间
16.   if S.size < k−(n−1)
17.      return FLASE;
18.   else then return S;
19.         sort S;//按报价升序排序
20.   end if
21. end if
```

图 2 给出了 $T=8$ 时，多阶段采样的示例。多阶段采样能够极大地提高卖方参与拍卖的积极性，其原因有以下 3 点：1)在每个子阶段中，符合拍卖预算要求的卖方都有机会拍卖成功；2)因为每个子阶段的预算固定不变，随着样本集的不断更新，预算余额会逐渐递减，那么对于卖方而言，报价提交得越早，成为候选卖方的可能性就越大；3)如果卖方成本过高或者卖方恶意抬高报价，那么其无法被选为候选用户，只能等待下一个阶段或者下一轮拍卖。

对于每位服务请求者而言，在 T 时刻会出现两种情况：1)样本集 S 中候选卖方人数仍然不足 $k-(n-1)$，表示构建匿名集的参与者人数不足，拍卖失败；2)候选卖方人数大于 $k-(n-1)$，虽然构建匿名集的人数达到要求，但是此时买方的效用并没有达到最大化。

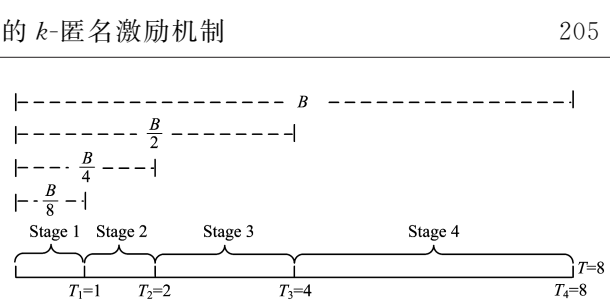


图 2　$T=8$ 时的多阶段采样

Fig. 2　Multiple-stage sampling-accepting process when $T=8$

4.2　获胜用户的选择

候选买方集为 $List[b_i](b_1\geqslant b_2\geqslant\cdots\geqslant b_{n-1})$。边缘节点将候选卖方集按报价升序排序，形成列表 $List[\lambda_j](\lambda_1\leqslant\lambda_2\leqslant\cdots\leqslant\lambda_m$，其中 m 表示候选卖方集的人数)，并将 $List[b_i]$ 和 $List[\lambda_j]$ 一起发送给云服务器。列表 $List[\lambda_j]$ 只含有报价和到达时间信息 a_j，并没有样本集中的卖方真实位置信息，其只存储在边缘节点中，即使云服务器遭受恶意攻击，卖方的位置信息也不会被泄漏，间接地保护了用户位置隐私。为了满足机制真诚可信的特性，本文令 $List[b_i]$ 中的前 x 位是最终获胜的买方，第 x 位买方的报价 b_x 作为每位获胜买方所需支付的费用；而由于所需要的匿名集大小是 k，因此显然 $List[\lambda_j]$ 中前 $k-x-1$ 位卖方都是最终获胜的用户，第 $k-x$ 位卖方的报价 λ_{k-x} 是每一位获胜卖方所得的报酬。为了满足预算平衡属性，卖方所得总报酬必须不能超过系统总预算。

$$(k-x-1)\lambda_{k-x}\leqslant xb_x \tag{9}$$

从而，云服务器需要找到报价最小的主元买方 $U_{x^*}^{b}$。因为 $List[b_j]$ 是降序排序，所以 x^* 一定是满足式(9)中索引最大的买方。

$$x^*=f(List[b_i],List[\lambda_j])=\max_{\substack{x\geqslant\frac{(k-x-1)\lambda_{k-x}}{b_x}\\ 1\leqslant x\leqslant n}} x \tag{10}$$

我们可以通过反向遍历 $List[b_i]$ 来找到 x^*，当 x^* 确定后就可以计算出获胜用户的人数和费用，然后云服务器将获胜用户集返回给边缘节点。$List[b_i]$ 中前 x^* 位买方的集合就是获胜买方集 W^b，$List[\lambda_j]$ 中前 $k-x^*-1$ 位卖方的集合就是获胜卖方集 W^s。

$$\begin{cases} W^b=\{U_1^b,U_2^b,\cdots,U_{x^*}^b\} \\ W^s=\{U_1^s,U_2^s,\cdots,U_{k-x^*-1}^s\} \end{cases} \tag{11}$$

边缘节点根据返回的获胜买方集 W^b，将主元买方 $U_{x^*}^b$ 的报价 b_{x^*} 作为每位获胜买方收取的费用 p_i^b。边缘节点通过式(9)计算每位获胜卖方所得的报酬 p_j^s，然后根据获胜卖方集 W^s 中的卖方到达时间信息 a_j，从本地映射表中查找出卖方的真实位置，并向他们分别支付相应的报酬。

$$\begin{cases} p_i^b=b_{x^*} \\ p_j^s=\lambda_{k-x^*} \end{cases} \tag{12}$$

5　有效性分析与证明

为了说明激励机制满足第 3 节中模型的期望经济特性，本文分别从计算效率、个体理性、预算平衡和真诚可信 4 个方面进行证明。

引理 1　DAI 是计算有效的。

证明：在拍卖之前，对所有买方进行排序的时间复杂度为

$O(n\log n)$；在每轮拍卖截止时间之前，计算卖方报价 λ_j 是否满足拍卖要求的时间复杂度为 $O(m)$；在截止时刻，将候选卖方进行排序的时间复杂度为 $O(m\log m)$。因此，候选用户选择过程的时间复杂度为 $O(n\log n+m\log m)$。而在获胜用户选择过程中，主元买方的索引通过反向遍历求得，时间复杂度为 $O(m)$。综上，整个激励机制的时间复杂度可表示为 $O(n\log n+m\log m)$。证毕。

引理 2 如果用户诚实报价，DAI 保证用户效用是非负的。

证明：当获胜买方 $U_i^b\in W^b$ 诚实报价，也就是说报价与估价相等，即 $b_i=v_i$ 时，根据式(12)可知他应付出的费用是 $p_i^b=b_{x^*}\leqslant b_i$。那么，由式(2)可计算出买方效用为：

$$U_i^b=v_i-p_i^b\geqslant v_i-b_i=0 \tag{13}$$

当获胜卖方 $U_j^s\in W^s$ 诚实报价，也就是说报价与成本相等，即 $\lambda_j=c_j$ 时，根据式(12)可知该卖方所得报酬为 $p_j^s=\lambda_{k-x^*}\geqslant\lambda_j$。那么，由式(3)可计算出卖方效用为：

$$U_j^s=p_j^s-c_j\geqslant\lambda_j-c_j=0 \tag{14}$$

因此，DAI 对于买方和卖方而言是个体理性的。证毕。

引理 3 DAI 是预算平衡的。

证明：分别从两个过程进行证明。在选择候选用户的过程中，如果 $n\geqslant k+1$，即不需要卖方来参与拍卖，那么边缘节点不需要给任何卖方支付报酬。那么，从获胜买方收取的全部费用是：

$$p^b=\sum_{i=1}^{n-1}p_i^b=(n-1)*b_n\geqslant 0 \tag{15}$$

由于没有获胜卖方，因此边缘节点的利润为非负。如果 $n<k+1$，由式(4)和式(7)可知，每轮拍卖都有一个总预算，每个阶段 $i\in\{1,2,\cdots,\lfloor\log_2 T\rfloor,\lfloor\log_2 T\rfloor+1\}$ 都有固定预算，算法 1 的第 4－9 行保证了在每个阶段中候选卖方的报价不会超过固定预算，因此在拍卖截止时刻，所有候选卖方的总报酬不会超过总预算 B。

在选择获胜用户的过程中，边缘节点从获胜买方收取的全部费用为 $p^b=\sum_{i=1}^{x^*}p_i^b=x^*\,b_{x^*}\geqslant 0$，而支付给获胜卖方的全部报酬为 $p^s=(k-x^*-1)\,\lambda_{k-x^*}$。边缘计算的利润是 p^b-p^s，由于 $List[b_i]$ 降序排序，因此 $x^*\leqslant n-1$，由式(9)和式(10)可计算出边缘节点的利润为：

$$\begin{aligned}p^b-p^s&=(n-1)b_n-(k-x^*-1)\,\lambda_{k-x^*}\\&\geqslant(n-1)b_n-(k-x^*-1)\frac{x^*\,b_{x^*}}{k-x^*-1}\geqslant 0\end{aligned} \tag{16}$$

综上可得，DAI 是预算平衡的。证毕。

引理 4 DAI 是真实的。

证明：因为我们对候选用户和获胜用户的报价都进行了对应的排序，且令报价相同的用户在序列中的位置取决于他们的到达时间，所以 DAI 满足单调性；而对于候选用户而言，拍卖成功的关键是报价。证毕。

引理 5 即使买方恶意报价，也不能增加买方的效用。

证明：当 $b_i=v_i$，即买方 U_i^b 诚实报价时，他支付的费用和效用分别是 p_i^b 和 u_i^b；当 $b_i\neq v_i$，即买方欺骗性地报价时，则令他所支付的费用和效用分别是 $\widetilde{p}_i^b$ 和 $\widetilde{u}_i^b$。也就是说，对于任何 $b_i\neq v_i$ 的情况，我们要证明的是 $u_i^b\geqslant\widetilde{u}_i^b$，下面分两种情况进行讨论。

1)当 $n\geqslant k+1$ 时，买方又有两种可能：拍卖获胜或者失败。如果拍卖获胜，他所支付的费用为 $p_i^b=b_{n-1}$，且 $b_i\geqslant b_{n-1}$，因此 $u_i^b=v_i-p_i^b\geqslant 0$。注意到，当买方的报价 $b_i>v_i$(高估竞价值)时，他的效用为 $\widetilde{u}_i^b=v_i-\widetilde{p}_i^b=v_i-p_i^b=u_i^b$，效用并没有因此增大，不影响拍卖结果；当 $b_i<v_i$(低估竞价值)时，具体来说，当 $b_{n-1}<b_i<v_i$ 时，因为 p_i^b 仍然等于 b_{n-1}，所以效用仍然没有变化；当买方报价比候选买方中的最低报价更小，即 $b_i<b_{n-1}<v_i$ 时，他就是唯一的竞拍失败者，$\widetilde{u}_i^b=0\leqslant u_i^b$。如果他因为诚实竞价而竞拍失败，那么 $u_i^b=0$，也符合 $b_i<b_{n-1}$ 的情况。综上所述，与 $b_i=v_i$ 相比，$b_i\neq v_i$ 时，买方效用不会变大。

2)当 $n<k+1$ 时，如果买方 U_i^b 通过诚实地报价而竞拍获胜，他所需支付的费用为 b_{x^*}，结果与第一种情况基本一样，效用不会增加。如果竞拍失败，那么一定有 $b_i<b_{x^*}$，效用 $u_i^b=0$。

基于上述分析可知，与诚实竞价相比，买方 U_i^b 欺骗性地竞价不会增加自身的效用。因此，对于所有买方而言，DAI 是满足诚实性的。证毕。

引理 6 即使卖方恶意报价，也不能增加卖方的效用。

证明：当 $\lambda_j=c_j$，即卖方 U_j^s 诚实地报价时，他所得报酬和效用分别是 p_j^s 和 u_j^s；当 $\lambda_j\neq c_j$，即卖方欺骗性地报价时，令他所得到的报酬和效用分别是 $\widetilde{p}_j^s$ 和 $\widetilde{u}_j^s$。也就是说，对于任何 $\lambda_j\neq c_j$ 的情况，我们要证明的是 $u_j^s\geqslant\widetilde{u}_j^s$。只有在引理 5 的第二种情况下，卖方才会参与拍卖。

如果卖方 U_j^s 通过诚实报价竞拍获胜，根据引理 2，有 $p_j^s=\lambda_{k-x^*}$ 和 $u_j^s=p_j^s-c_j\geqslant\lambda_j-c_j=0$；如果卖方欺骗性地报价 $\lambda_j<c_j$ 或者 $c_j\leqslant\lambda_j\leqslant\lambda_{k-x^*}$，不会影响拍卖结果(证明过程和引理 5 的第一种情况类似)；如果卖方欺骗性的报价比获胜卖方中最高的报价更高，即 $\lambda_j>\lambda_{k-x^*}$，那么 U_j^s 竞拍失败，效用是 $\widetilde{u}_j^s=0\leqslant u_j^s$；如果卖方 U_j^s 诚实报价但失败了，则效用 $u_j^s=0$，那么他的报价一定是 $\lambda_j>\lambda_{k-x^*}$。由上述分析可知，与诚实竞价相比，卖方 U_j^s 欺骗性地竞价不会增加自身效用，也就是说对于所有卖方而言，DAI 是满足诚实性的。

结合引理 4－引理 6 可以证明 DAI 是真诚可信的。证毕。

6 仿真实验与结果分析

本节通过仿真对 k-匿名激励机制进行性能分析。下面首先介绍实验环境和参数设置，然后分析实验结果。

我们在 Matlab 平台上实现 k-匿名激励机制，并设计了一系列仿真实验。基本参数设置如表 1 所列。其中，买方估值是服从标准正态分布的随机值；卖方的到达时间是服从泊松分布的随机值，取值范围取决于拍卖截止时间。

表 1 实验参数设置

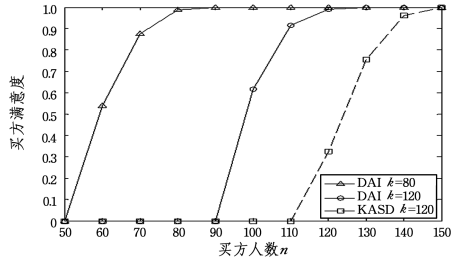
Table 1 Experimental parameters

参数名称	参数值
买方人数 n	[50,150]
卖方人数 m	[50,150]
买方 U_i^b 的估值 v_i	(0,2]
卖方 U_j^s 的成本 c_j	(0,1]
隐私保护要求 k	[20,120]
拍卖截止时间 T	64
卖方到达时间 a_j	(0,64)

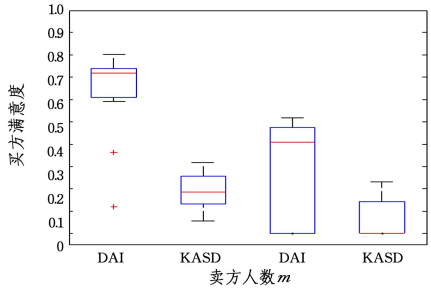
本文主要从买方满意度、真诚可信和拍卖利润 3 个方面考查机制的性能。

6.1　买方满意度

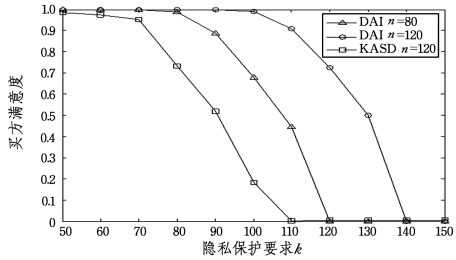
将匿名集中获胜买方人数所占的比例称为买方满意度,其反映了机制的有效性。图 3 给出了 DAI 与文献[3]所提出的 KASD 算法的满意度对比。



(a)买方人数 n 对买方满意度的影响



(b)卖方人数 m 对买方满意度的影响



(c)隐私保护要求 k 对买方满意度的影响

图 3　买方满意度

Fig. 3　Satisfaction of buyers

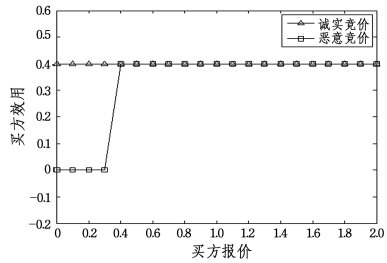
图 3(a)反映了 $m=70$ 时,不同隐私保护要求下买方满意度随买方人数的变化情况。可以看到,随着买方人数的增加,买方满意度呈上升趋势。当 $k=120$ 时,DAI 和 KASD 都存在满意度为 0 的情况,这是因为所有买方的总预算不能支付卖方的总报酬,从而导致拍卖失败。然而,在其他情况下,本文方案整体优于 KASD,原因在于 KASD 总是将买方集中第二低的报价作为每一位买方支付的费用,虽然这种方法可以增加买方效用,但是买方总预算很难大于卖方总报酬,这就导致拍卖成功的概率很低,买方满意度不高。而本文方案是根据式(9)、式(10)来确定每位买方支付的费用,拍卖成功的概率很大,因此买方满意度很高。

在图 3(b)中,m 从 50 增加到 150,两组对比数据分别反映的是 $n=100$,$k=120$ 和 $n=70$,$k=100$ 时,DAI 和 KASD 的买方满意度。因为 $n<k$,需要卖方参与拍卖,所以可以看到图中买方的满意度不会到达 1。然而,在数据分布上,本文方案的满意度总是高于 KASD 的。因为随着卖方人数的增加,KASD 的卖方总报酬会逐渐增大,而买方总预算却固定不变,从而容易导致拍卖失败,买方满意度总体很低。而在 DAI 中,由式(8)、式(9)可知,拍卖成功的概率随着卖方人数的增加而变大,买方满意度能够达到较高水平。

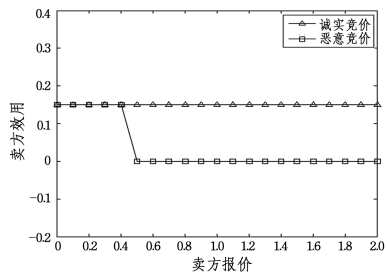
图 3(c)给出了 $m=100$ 时,不同买方人数下买方满意度随着隐私保护要求的变化情况。可以看到,在 DAI 中满意度整体呈下降趋势,这是因为当 k 逐渐逼近 n 时,满足式(8)、式(9)条件的概率会越低。而当 $k\geqslant n$ 时,符合条件的比例会急剧降低,导致拍卖失败,买方的满意度几乎为 0。但是在 k 相同时,DAI 的买方满意度仍然高于 KASD,这是因为 DAI 比 KASD 多了一个参与者候选阶段,参与者的人数得到了控制,获胜买方人数比 KASD 多。

6.2　真诚可信

图 4 给出了任意一位用户改变报价对自身效用的影响。其中,图 4(a)表示任意一位买方诚实竞价和恶意竞价对自身效用的影响。因为式(2)中买方效用并不是报价与支付的费用之差,另外,每位买方所支付的费用取决于主元买方,所以单个用户的报价并不能影响整个拍卖结果。如果将买方诚实报价所得到的效用当作基准线,则可以从图中看出,不管买方如何虚假或恶意报价,效用都不会超过基准线。同理,图4(b)表明卖方也不能通过欺骗或者恶意竞价来提高自身效用。



(a)买方恶意报价对效用的影响



(b)卖方恶意报价对效用的影响

图 4　真诚可信

Fig. 4　Truthfulness

6.3　拍卖利润

将获胜买方集支付的总费用与获胜卖方集得到的总报酬之差作为机制的拍卖利润,其反映了机制的预算平衡性。图 5 给出了 $m=70$ 时,不同隐私保护要求下拍卖利润随买方人数的变化情况。在候选阶段,预算约束是我们对卖方的筛选条件之一,而且在获胜用户选择阶段,我们也将支付报酬不能超过买方预算这一要求作为计算前提,因此在整个拍卖过程中,机制的利润不会为负数。当 $k=80$ 和 $k=120$ 时,因为买方总预算不能支付卖方总报酬,容易导致拍卖失败,所以 DAI 的利润为 0。而当 $n>k$ 时,不需要卖方来参与拍卖,总报酬为 0,所以拍卖利润会随着 n 的增加而线性增加。

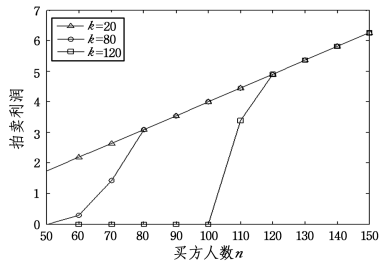


图 5 拍卖利润

Fig. 5 Profit of auction

结束语 本文提出了一种基于双向拍卖的 k-匿名激励机制，其在保证交易公平性的同时最大化买卖双方的效用，解决了匿名集人数不足的问题。本文主要有以下两个创新点：1)引入边缘计算架构，在减轻云服务器计算负担的同时对参与者进行时空匿名，不仅降低了系统决策延迟，而且能够保护参与者的位置隐私；2)利用多阶段采样法来筛选候选用户，不仅解决了参与者的在线选择问题，而且有效提高了参与者的积极性，同时抑制了用户恶意竞价情况的发生。最后，通过理论证明和仿真实验表明，DAI 在有效性和真诚性上有较好的表现，同时提高了买方满意度和效用。

参 考 文 献

[1] SWEENEY L. k-anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5): 557-570.

[2] YANG D, XUE G, FANG X, et al. Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing[C]// International Conference on Mobile Computing and Networking. ACM, 2012: 173-184.

[3] YANG D, FANG X, XUE G. Truthful incentive mechanisms for k-anonymity location privacy[C]// IEEE INFOCOM. IEEE, 2013: 2994-3002.

[4] YUAN Z, WEI T, SHENG Z. On Designing Satisfaction-Ratio-Aware Truthful Incentive Mechanisms for k-Anonymity Location Privacy[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(11): 2528-2541.

[5] WU Y, PENG H, PENG H, et al. MagiCrowd: A crowd based incentive for location-aware crowd sensing[C]// Wireless Communications and NETWORKING Conference. IEEE, 2016.

[6] WANG X, LIU Z, TIAN X, et al. Incentivizing Crowdsensing with Location-Privacy Preserving[J]. IEEE Transactions on Wireless Communications, 2017, PP(99): 1.

[7] SHI W S, SUN H, CAO J, et al. Edge Computing: An Emerging Computing Model for Internet of Everything Era[J]. Journal of Computing Research and Development, 2017, 54(5): 907-924. (in Chinese)
施巍松，孙辉，曹杰，等. 边缘计算：万物互联时代新型计算模型[J]. 计算机研究与发展，2017，54(5)：907-924.

[8] KAWAJIRI R, SHIMOSAKA M, KASHIMA H. Steered crowdsensing: incentive design towards quality-oriented place-centric crowdsensing[C]// ACM International Joint Conference on Pervasive and Ubiquitous Computing. ACM, 2014: 691-701.

[9] LI X, MIAO M, LIU H, et al. An incentive mechanism for K-anonymity in LBS privacy protection based on credit mechanism[J]. Soft Computing, 2017, 21(14): 3907-3917.

[10] REDDY S, ESTRIN D, HANSEN M, et al. Examining micropayments for participatory sensing data collections[C]// Proceedings of the 12th ACM International Conference on Ubiquitous Computing. ACM, 2010: 33-36.

[11] DANEZIS G, LEWIS S, ANDERSON R. How much is location privacy worth[C]// Proceedings of the Workshop on the Economics of Information Security Series (WEIS). ACM, 2005.

[12] LEE J S, HOH B. Sell your experiences: a market mechanism based incentive for participatory sensing[C]// IEEE International Conference on Pervasive Computing and Communications. IEEE, 2010: 60-68.

[13] LUO T, TAN H P, XIA L. Profit-maximizing incentive for participatory sensing[C]// Proceedings—IEEE INFOCOM. IEEE, 2014: 127-135.

[14] FENG Z, ZHU Y, ZHANG Q, et al. TRAC: Truthful auction for location-aware collaborative sensing in mobile crowdsourcing[C]// Proceedings—IEEE INFOCOM. IEEE〈2014: 1231-1239.

[15] ZHANG H, LIU B, SUSANTO H, et al. Incentive mechanism for proximity-based Mobile Crowd Service systems[C]// IEEE INFOCOM 2016—IEEE International Conference on Computer Communications. IEEE, 2016: 1-9.

[16] ZHANG X, YANG Z, ZHOU Z, et al. Free Market of Crowdsourcing: Incentive Mechanism Design for Mobile Sensing[J]. IEEE Transactions on Parallel & Distributed Systems, 2014, 25(12): 3190-3200.

[17] ZHAO D, LI X Y, MA H. Budget-Feasible Online Incentive Mechanisms for Crowdsourcing Tasks Truthfully[J]. IEEE/ACM Transactions on Networking, 2016, 24(2): 647-661.