第 56 卷　第 1 期
2020 年 1 月

南京大学学报(自然科学)
JOURNAL OF NANJING UNIVERSITY
(NATURAL SCIENCE)

Vol. 56, No. 1
Jan., 2020

DOI:10. 13232/j. cnki. jnju. 2020. 01. 012

基于社交网络的分布式机制设计

何　昕,徐珺平,赵登吉*

(上海科技大学信息科学与技术学院,上海,201210)

摘　要:人们通过社交关系构成一个庞大的社交网络,网络中的每个节点只能与其周围的节点进行通信,因此当网络中的某个节点进行物品拍卖销售时,在不借助第三方推广的情况下只能邀请其邻居节点参与. 中心化机制能使网络中的其他非邻居节点都能参与拍卖,以此可以提高卖家节点的最终收益,然而在该机制中卖家可以轻易地与买家串通,并且买家需要将社交网络结构(买家的私人社交信息)完全透露给卖家,因此网络中的节点没有很强的动机来参与该机制. 提出一种分布式的解决方案,可以防止卖家与买家勾结,同时保持网络结构不被泄露. 实验证明,该分布式机制保留了传统机制的优点,而且不需要一个可以完全获得网络结构的中心机构来执行该机制. 通过模拟实验还发现,在大多数情况下,社交网络越复杂,泄露的隐私信息就越少.

关键词:分布式机制设计,拍　卖,信息传播,算法博弈论

中图分类号:TP301　　**文献标识码:**A

Distributed mechanism design on social networks

He Xin, Xu Junping, Zhao Dengji*

(School of Information Science and Technology, ShanghaiTech University, Shanghai, 201210, China)

Abstract: This paper studies a market where a seller sells one item on a social network, but she can only directly communicate with her neighbours in the network. The seller′s goal is to promote the sale to all potential buyers in the network to increase her revenue. This problem has been first attempted with a centralised mechanism. However, buyers are not well incentivised to participate in the mechanism due to (i) the seller can easily collude with a buyer, and (ii) the network structure is fully revealed to the seller. Hence, we propose another novel distributed solution that prevents the seller′s collusion with buyers and also keeps the network structure unrevealed. We also prove that our mechanism preserve the advantages of the centralized mechanisms and show that we don′t need a central part to run this mechanism. Our simulations show that the more complicated social networks are, the less privacy information are revealed.

Key words: distributed mechanism design, auction, information diffusion, algorithmic game theory

本文研究一个区别于传统设定的物品拍卖场景. 传统的拍卖场景假设所有的参与者都是相互独立的,但在现实中,参与者之间存在一定的社会关系(特别是在社交网络发达的互联网时代),社交关系把他们联系在一起构成了一个社交网络,社交网络中的每个节点只能与其邻居节点直接通信. 因此如果某个节点需要拍卖一件商品,在不借助任何第三方推广的情况下,他只能邀请其邻居参与. 为了让拍卖的价格更高,卖家需要进行推广使得更多非邻居节点也能参与. 本文主要研

收稿日期:2019－08－31

* 通讯联系人,E-mail:zhaodj@shanghaitech.edu.cn

究如何通过节点的社交关系来邀请更多节点参与卖家的拍卖,从而提高卖家的收益. 此问题的难点在于潜在买家节点没有动机去邀请其邻居节点参与拍卖,因为他们在竞争同一件商品. Li et al[1]首先研究了这个问题,在2017年提出一个中心化的解决方案. Zhao et al[2]又对这个问题在多物品拍卖的维度上进行了扩展.

Li et al[1]的机制着眼于激励那些已经知道并参与了拍卖的买家去邀请他们的邻居参与(传播拍卖信息给他们的邻居). 如果他们的传播行为使得卖家最终获利,那么卖家将会给那些对此次拍卖结果产生贡献的买家节点进行奖励. 但Li et al[1]的机制存在一些潜在的应用问题:当卖家使用该机制进行拍卖时,他可以获得整个网络的拓扑结构信息,即卖家可以获得所有买家的私人信息(包括他们的估价和社交关系),这将导致买家隐私遭到泄露;同时,卖家知道整个网络结构后可以忽略节点的传播贡献直接与最高报价买家交易. 为解决以上不足,本文提出一种分布式解决方案,它要求网络中的所有买家一起执行该分布式机制以完成最终的物品交易和收益分配. 与此同时,该机制还将邀请一些网络中完全不会参与最终收益分配的节点共同参与计算,这些节点称为中立节点,而只有中立节点会收集小部分参与者的私人信息. 在该网络中,包括卖家在内的所有节点都不会拥有完整的网络结构信息.

关于分布式算法机制设计,Nisan et al[3]已对相关文献进行了整理与探讨,例如,如何以分布式方式实施中心化机制的研究[4-5],尤其是Vickrey-Clarke-Groves机制[6]. 此外,Archer et al[7]探讨了组播成本分摊机制的分布式实现. Shneidman and Parkes[8]提出一个基于智能体的策略空间来设计和度量一个分布式机制的框架,Peng et al[9]和Yang et al[10]在此框架下研究了分布式无线频谱拍卖的相关机制. 本文的主要工作是提出一个新的分布式机制设计框架,并且在新框架下将Li et al[1]提出的中心化机制进行分布式化. 关于分布式算法机制设计的早期调查综述参见文献[11]. 关于在线广告最新相关研究可在2019年Liu[12]的综述中找到.

1 模型描述

考虑由 n 个网络节点组成的社交网络,记为 $N=\{1,2,3,\cdots,n\}$. 每个节点 $i\in N$ 都有一个唯一的id和一组邻居,记为 $r_i\subseteq N\backslash\{i\}$. 网络中的每个节点仅可与其邻居通信. 此外,网络中的每个节点都是自私的,即他们都以最大化自己的收益为最终目标. 同时,网络中有一个卖家(seller)希望将一个不可分割的商品出售给社交网络中的其他人. 每个买家节点 i 对此商品都有私有估价 v_i,但是只有少数买家(通常是卖家的邻居)知道这次拍卖. 令 $\theta_i=(v_i,r_i)$ 表示买家 i 的私有信息类(type),同时,Θ_i 表示买家 i 的所有可能的私有信息类的空间. 一个买家的私有信息类包括对待拍卖物品的心理估值以及他的社交信息(即,到他的邻居的网络链接). 将集合 $\theta=\{\theta_1,\theta_2,\cdots,\theta_n\}$ 表示为所有买家的私有信息类的一个描述(profile),那么 $\Theta=\Theta_1\times\Theta_2\times\cdots\times\Theta_n$ 则为所有可能私有信息类描述的空间. 接下来定义分布式机制的一些重要的概念和性质.

定义 1 买家 $i\in N$ 的内部状态定义为 $c_i=(\gamma_1,\gamma_2,\cdots,\gamma_m)$,其中 $\gamma_j,j\in[1,\cdots,m]$ 是状态变量,可以为任何类型的信息,令 C_i 成为 i 的内部状态空间.

通常,买家 i 的内部状态可能包含仅与 i 私有信息类相关的信息,这些变量称为私有信息类汇报状态变量. 因此,状态可以被分解为两个部分 $c_i=(t_i,a_i)$,其中 t_i 是私有信息类汇报状态变量的集合,a_i 是计算状态变量的集合.

设 $s_i:\Theta_i\to C_i$ 为买家 i 的策略. 令 Σ_i 为 i 的策略空间,特别的,当 i 没有收到拍卖信息或 i 不想参与拍卖时,令 $s_i(\theta_i)=\text{null}$ 表示买家的一个虚拟策略. Σ_i 包括 i 可以执行的所有策略. 设 $\Sigma=\Sigma_1\times\Sigma_2\times\cdots\times\Sigma_n$ 表示所有买家的联合策略空间. 设 $s=\left(s_i\in\Sigma_i\right)_{i\in N}$ 是所有买家的一个策略描述. 特别的,将一个诚实的私有信息汇报策略记为 $s_i^{tr}(\theta_i)=(t_i^*,a_i)$,一个诚实计算策略为 $s_i^{tp}(\theta_i)=(t_I,a_i^*)$,一个机制的建议策略为 $s_i^*(\theta_i)=(t_i^*,a_i^*)$. 这个建议的策略表示买家既诚实地汇报

私有信息又诚实地按照机制进行计算.

定义 2　社交网络中的分布式机制 d^M 是一个二元组 (π,p),其中 $\pi=(\pi_i)_{i\in N}$ 是分配函数,$p=(p_i)_{i\in N}$ 是所有买家的支付函数. 特别的,$\pi_i:\Sigma\to\{0,1\}$ 和 $p_i:\Sigma\to R$ 分别是某个买家 i 的分配和支付函数.

具体来说,$\pi_i(s)=1$ 表示买家 i 得到物品,$\pi_i(\theta)=0$ 表示 i 没有得到物品. 类似的,$p_i(\theta)\geqslant 0$ 表示买家 i 支付 $p_i(s)$,而 $p_i(s)<0$ 表示买家 i 得到 $|p_i(s)|$ 奖励. 为方便起见,令 $\theta_{-i}=(\theta_j)_{j\neq i,j\in N}$ 且 $s_{-i}=(s_j)_{j\neq i,j\in N}$. 给定一个私有信息类描述 Θ,策略描述 s 和机制 (π,p),买家 i 的收益定义为:

$$u_i\big(\theta_i,s(\theta),(\pi,p)\big)=\pi_i(s)\times v_i-p_i(s)$$

定义 3　中心化机制 $M=(f,q)$ 是激励相容(Incentive Compatible,IC)的,当且仅当对所有的 θ_i,所有的 $\theta'_i\neq\theta_i$ 以及所有的 θ'_{-i},都有:

$$u_i\big(\theta_i,(\theta_i,\theta'_{-i}),(f,q)\big)\geqslant u_i\big(\theta_i,(\theta_{i'},\theta_{-i}),(f,q)\big)$$

其中,$f:\Theta\to\{0,1\}$ 是分配函数,$q:\Theta\to R$ 是支付函数,Θ 是所有可能私有信息类描述的空间.

定义 4　一个分布式机制 d^M 的建议策略描述 s^* 是一个后验纳什均衡,当且仅当:

$$u_i\big(\theta_i,(s_i^*,s_{-i}^*),(\pi,p)\big)\geqslant u_i\big(\theta_i,(s_i,s_{-i}^*),(\pi,p)\big)$$

对于所有的 $i\in N$,所有的 $s_i\neq s_i^*$ 以及所有的 $\theta_i\in\Theta_i$ 和 $\theta_{-i}\in\Theta_{-i}$ 均成立.

接下来定义算法相容(Algorithm Compatible,AC)的概念. 算法相容性质表示对于任何买家 i,如果所有其他买家执行建议策略 s_{-i}^*,则无论 i 报告什么私有信息,i 都不能通过违背计算协议来获得更高的收益.

定义 5　对于任意的买家 $i\in N$,分布式机制 d^M 是算法相容(AC)的,当且仅当:

$$u_i\Big(\theta_i,\big((t_i,a_i^*),s_{-i}^*\big),(\pi,p)\Big)\geqslant u_i\Big(\theta_i,\big((t_i,a_i),s_{-i}^*\big),(\pi,p)\Big)$$

对所有的 $\theta_i,t_i\neq t_i^*$ 以及所有的 a_i 都成立.

直观地说,算法相容性鼓励那些理性买家诚实地执行预期的算法. 回想一下,买家的行为可以分为两类,即这些行为是否与私人信息有关. 形式化地说,对于任何买家 i,如果定他的策略总是 $s_i^{ip}(\theta_i)=(t_i,a_i^*)$,那么总可以找到中心化的机制 M,使得 $\pi(s^{ip})=f(\theta')$ 和 $p(s^{ip})=q(\theta')$ 对所有的私有信息类描述 $\theta'\in\Theta$ 都成立,其中 π,f 分别是 d^M 和 M 的分配函数,p 和 q 是这两种机制的支付函数. 称这个中心化机制 M 为 d^M 的中心化规约机制(Centralized Reduction Mechanism,CRM).

定理 1　给定一个算法相容(AC)分布式机制 d^M,如果 d^M 的 CRM(记作 M)是激励相容(IC)的,那么 d^M 一个建议的策略描述 s^* 是一个后验纳什均衡.

证明　由 M 是 d^M 的 CRM 可得:

$$u_i^M\big(\theta_i,\theta',(f,q)\big)=u_i^{d^M}\big(\theta_i,s(\theta),(\pi,p)\big)$$

又由于 M 是 IC 的,则有:

$$u_i^{d^M}\Big(\theta_i,\big((t_i^*,a_i^*),s_{-i}^*\big),(\pi,p)\Big)\geqslant u_i^{d^M}\Big(\theta_i,\big((t_i,a_i^*),s_{-i}^*\big),(\pi,p)\Big)$$

因此,根据 d^M 的 AC 性质,得到:

$$u_i^{d^M}\Big(\theta_i,\big((t_i^*,a_i^*),s_{-i}^*\big),(\pi,p)\Big)\geqslant u_i^{d^M}\Big(\theta_i,\big((t_i,a_i),s_{-i}^*\big),(\pi,p)\Big)$$

由定义 5 易得,s^* 是一个后验纳什均衡.

证毕.

由定理 1 可知,如果能找到一种方法来监督分布式网络中的计算过程,就可以在该网络上分布式地运行任何激励相容的中心化机制,同时确保该分布式机制将获得与中心化机制相同的结果. 本文就使用这些属性在后验纳什均衡中构建分布式机制.

2　中心化的信息传播机制

Li et al[1] 提出一种通过社交网络销售商品的中心化机制,称为信息扩散机制(Information Diffusion Mechanism,IDM),并证明该机制是激励相容(IC)的. 此外,该机制保证卖家的收入与无需任何信息传播相比所能获得的收入总数不减少,因此卖家可以在任何社交网络下使用该机制而不会比使用不传播的机制更差. 该机制要求所有买家向卖家或其他第三方平台报告其估值,并且卖家或者第三方平台必须知道网络的整体结构以计算分配和支付. 以下是对该机制的简要描述.

机制 1 Information Diffusion Mechanism, IDM

步骤 1:给定一个可行的私有信息类描述报告 θ',找到具有最高估值报告(如果有相同的就随机挑选)的买家,用 w 表示.

步骤 2:找到 w 的关键节点序列,用 CR_w 表示. 定义 $j \in CR_w$ 当且仅当如果没有 j 的私有信息汇报 θ'_j,w 无法加入拍卖. 即如果买家 j 没有汇报他的私有信息类,那么就无法找到从卖家到 w 的一条邀请链. j 还表示为 w 的关键节点. 特别的,有 $w \in CR_w$.

步骤 3:令

$d_i = \{j \mid j \in N \wedge j \in CR_w\}$ 以及 $-d_{-i} = N \backslash \{d_i\}$.

步骤 4:对于任意两个买家 $i, j \in CR_w$,定义一个排序关系 $\succ_w$,有 $i \succ_w j$ 当且仅当从卖家到 j 的所有邀请链包含 i,即 $i \in CR_j$.

步骤 5:对于每个 $i \in CR_w$,如果 i 最终得到了物品,则 i 支付的是没有 i 参与时的最高估值(注意,当 i 不参加拍卖时,那些只能通过 i 的邀请才能加入拍卖的买家也不存在了). 用 p_i 表示 i 的支付. 如果令 $v^*_S = \max_{\{t \in S\}} v'_t$, $S \subseteq N$,就有 $p_i = v^*_{d_{-i}}$.

步骤 6:卖家将物品交给根据 $\succ_w$ 关系排在 CR_w 第一位的买家 i,令 $l = 1$ 并重复以下过程直到该项目被分配:

(1)如果 i 是 CR_w 中的最后一位买家或 $v'_i = p_j$,其中 j 是 CR_w 中排名 $l+1$ 的买家,那么 i 赢得该物品,支付 $x_i(\theta') = p_i = v^*_{-d_{-i}}$;

(2)否则,i 将物品传递给买家 j,同时,i 支付

$x_i(\theta') = p_i - p_j = v^*_{-d_i} - v^*_{-d_j}$

其中,j 是 CR_w 中排名 $l+1$ 买家. 置 $i = j$ 和 $l = l+1$.

步骤 7:所有其他买家都没有收到该物品,他们的支付为零.

直观地说,IDM 找到具有最高估值的买家,并确定到达该买家的关键节点买家,然后分配只发生在这些买家之间. 卖家首先将物品交给距离卖家最近的关键买家,而买家必须支付在没有他参与的情况下的全网汇报的最高估价(之后无论谁最终得到物品,这就是卖家的最终收入). 然后买家有两种选择:持有物品或将其传递给下一个关键买家. 如果下一个关键买家支付的款项大于其估价,则他将该物品传递给下一个关键买家(接收下一个关键买家支付的款项). 否则,他保留该物品.

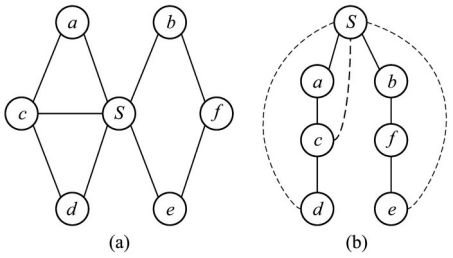
为防止卖家欺骗买家,并防止在执行 IDM 之后卖家发现整个社交网络(这是一个关键的隐私问题并且可能使得部分买家不愿加入拍卖),本文提出一种分布式机制,该机制将一起解决这两个问题.

3 分布式的信息传播机制

本文提出分布式信息扩散机制(Distributed Information Diffusion Mechanism, DIDM)以克服 IDM 的两个缺点. 注意,假设网络中还存在一个名为 Bank 的中立的受信任节点,同样,Bank 将无法获得有关此网络的所有信息,他的职责是检查买家报告的信息的正确性并监督交易过程. 特别的,所有买家都通过私有的稳定的信道与 Bank 连接,但是 Bank 对社交网络的拓扑结构没有任何了解. 如果在拍卖阶段 Bank 发现有买家没有诚实计算,Bank 可以对所有买家施加一个巨大的惩罚并停止拍卖.

IDM 中的关键目标是找出网络的关键节点序列并计算关键节点的支付. 首先介绍分布式算法来找出关键节点序列. 如果使用深度优先搜索(Depth First Search, DFS)算法遍历一个无向图,当同时令所有买家记录首次邀请他们参与拍卖的邻居作为其父节点时,就可以得到一棵生成树,此生成树经常被称为 DFS 树.

基于这个生成树,原始图的边可以分为两类:树边,即属于 DFS 树的边;回边,即连接某个买家和他的某个祖先买家的边. 在 DFS 树中,分别定义 $P(i)$ 为买家 i 的父买家和 $C(i)$ 为子买家的集合. 例如,在图 1 中,$P(c) = \{a\}$, $C(c) = \{d\}$ 和 $C(s) = \{a, b\}$. 还可以定义 $T(i)$ 为生成树中以 i 为根的一棵子树.



(a)原始图;(b)在任意深度优先访问顺序下构建的生成树(直边是树边,曲线边是回边)

图 1 DFS 树

Fig. 1 An example of DFS tree

此外,对于任何买家i,定义dt_i是买家i首次被邀请的时间,并令$et_i = \min_{j \in r_i \setminus \{p(i)\}} \{dt_i, et_j\}$. 直观地说,$et_j$是$i$经过非父邻居的所有路径中可以到达最早被邀请的祖先的加入时间. 图1中,$et_c = dt_s$.

定理2　给定社交网络N的任意一棵DFS树,对于其中的任意一棵子树$T(i)$和任意一个买家$j \in N$,j是$T(i)$中的一个节点当且仅当$dt_i \leqslant dt_j \leqslant dt_{T(i)}$,其中$dt_{T(i)} = \max_{k \in T(i)} dt_k$.

定理2可以直接从图论推导. 由于dt由买家的被邀请时间决定,则可验证对任何子树$T(i)$有$T(i) \supset T(j)$且$dt_i < dt_j$,其中$j \in T(i), j \neq i$. 例如,在图2中$T(b) \supset T(e) \supset T_4$. 回想一下,$et_i$表示$i$经过非父邻居的所有路径中可以到达的其他祖先的最早加入时间. 如果存在这样的路径,无论其父母是否加入都有其他人邀请其加入拍卖.

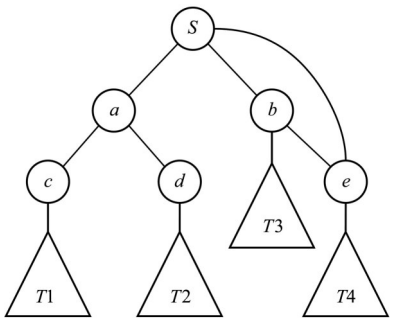


图2　DFS树的一个例子:三角形是其父母的一棵子树

Fig. 2　An example of DFS-tree: the triangles are subtrees of their parents

定理3　对于任何买家$j \in C(i), i \in N$,当i不参与拍卖时,在$T(j)$中的买家也不能被邀请加入拍卖,当且仅当$dt_i \leqslant et_j$. 同时,这样的j是i的一个关键孩子.

此处省略定理3的证明,因为它可从Tarjan算法[13]的结论中得出. 有关图论中的相关定理和讨论可参考Erciyes[14]的著作. 根据定理2,给出如下的例子:在图2中,由于$dt_a < et_c = dt_c$,如果a未加入拍卖,则c和$T1$的买家不会被任何人邀请. 设D_i是i的所有关键孩子的集合. 令$T(D_i) = \{i\} \bigcup_{j \in D_i} T(j)$,因此可以得出如下结论:对于任何买家$i, j \in N$,$j$只有在$i$参与了拍卖时才会被邀请当且仅当$j \in T(D_i)$. 联想上一节中对关键节点的定义,假设$w$是网络中报价最高的买家,对于$N$中的任何买家$i$,$i$是一个关键节点当且仅当$w \in T(D_i)$.

定义在查找关键节点的过程中买家需要存储的计算状态,通常买家i的计算状态包含:

$$a_i = \{P(i), dt_i, dt_{T(i)}, et_i, w_i, v'_{w_i}\}$$

其中$w_i = argmax_{j \in T(i)} v_j$,$v'_{w_i}$是$w_i$上报的估价. 在根节点的状态中记录$dt_i$和$dt_{T(i)}$,这是因为如果要检查是否$j \in T(i)$,只需得到$i$的状态并检查$dt_i \leqslant dt_j \leqslant dt_{T(i)}$是否满足.

可以使用分布式DFS算法构造DFS树并计算买家的计算状态. 使用DFS树构造协议[15]并递归计算计算状态,因为i的所有状态变量都与r_i或$T(i)$相关. 此处省略详细的算法. 之后的讨论都是基于DFS树已经被构建,并且每个买家都已经构建了相应状态这一假设进行的.

构造DFS树,有$w'_{\text{seller}} = w = argmax_{i \in N} v'_i$. 之后,卖家可以向Bank报告$w$,Bank将向所有买家广播$w$的状态. 接下来,卖家$i$可以通过检查$w \in T(D_i)$来判断他是否是一个关键节点. 如果买家$i$是关键节点,他将向Bank报告他的计算状态及他的私有信息类. 注意,Bank可以通过询问得到i的子节点的状态来验算i是否诚实地计算了他的状态. 一旦发生错误或异常,Bank可以停止拍卖并执行处罚.

在接下来的交易过程中,物品将沿着关键序列进行转移,并且后一个关键节点将向前一个关键节点支付一些资金以获得该物品. Bank监督此流程并确定物品应该在何时停止传递. 由IDM可知,对于任何关键节点i及其下一个关键节点$i+1$,Bank将首先找出在没有$i+1$参与的情况下该网络的最高报价. 由于已经知道没有i参与的最高报价(这是i的支付),为了计算$i+1$的付款,可以先在集合$T(D_i) - T(D_{i+1})$中搜索最高报价v',然后选择v'和i的支付中较大的一个作为$i+1$的支付.

为保护隐私,Bank应尽可能少地获取信息. 但Bank只有部分信息,所以需保证向Bank报告的所有信息都经诚实的计算得出. 此外,由于已经知道一个节点的状态可以由其孩子节点计算得

出,因此可以检查某个节点的孩子节点们的状态来判断他们的父节点是否在撒谎.

以下是一个对该机制的简要描述.

机制 2 Distributed Information Diffusion Mechanism, DIDM

步骤 1:给定卖家及其邻居 r_{seller},从卖家开始运行分布式 DFS 算法,邀请更多买家参与拍卖,并构建 DFS 生成树,同时每个买家在该过程中计算自己的状态 $\left\{P(i),\ dt_i, dt_{T(i)}, et_i, w_i, v'_{w_i}\right\}$.

步骤 2:卖家向 Bank 报告他的计算状态,同时 Bank 向买家 $w=w_{\text{seller}}$ 询问并获得他的状态. 然后,Bank 向所有买家公开 dt_w, v'_w. 接下来,每个买家都可以检查他们是否处于关键节点序列中,如果是则将他们的状态报告给 Bank. 最后,Bank 会向所有买家询问,如果他们的父辈买家在关键序列中,那么他们就将向 Bank 汇报自己的状态. 这样就可以记录下每个关键点 i 的当前孩子节点 $C(i)$. 最后,Bank 根据 i 和 $C(i)$ 的状态来判断 i 是否诚实地计算了自己的状态. 如果发生错误,Bank 将停止拍卖并对所有买家执行处罚.

步骤 3:根据 dt_i 对关键节点进行升序排序,卖家用 0 表示,将关键点序列记为 $\{0,1,2,\cdots,w\}$.

步骤 4:对于每个 $i\in\{0,1,2,\cdots,w\}$,Bank 要求所有买家 $j\in N\backslash\{i,i+1\}$ 运行以下协议:

(1) 如果 $dt_i<dt_j<dt_{i+1}\wedge w_j=w$,则计算 $x_j=\max_{k\in C(j),\ w_k\neq w} v'_{w_k}$ 并返回 $y_j=\max\left\{x_j, v'_j\right\}$;

(2)否则,什么都不做.

收到所有回复后,Bank 将选择回复中的最大值,表示为 z_1. 然后,Bank 计算:

$$z_2=\max_{j\in D_i\cup\left(C(i+1)-D_{i+1}\right)\wedge w_j\neq j} v'_{w_j}$$

最后,令 $v'=\max\left\{z_1,z_2\right\}$.

步骤 5:定义 v^i 是 i 付给前一个关键节点 $i-1$ 的支付. 则 $v^{i+1}=\max\left\{v', v^i\right\}$:

如果 $v^{i+1}>v'_i$,则让 $i+1$ 支付 v^{i+1} 并继续将物品传给下一个买家;否则,让 i 保留该项目并终止拍卖.

直观地说,DIDM 的步骤 1 到步骤 3 构造了一个 DFS 树并找出网络中的关键节点序列. 同时,Bank 收集这些关键节点的孩子的状态以检查其计算的正确性. 请注意,Bank 不会直接向关键节点询问其孩子的状态. 在步骤 4 中,Bank 收集小部分买家的状态,以计算 $T(D_i)-T(D_{i+1})$ 中的最大估值 v'. 最后,Bank 在步骤 5 中执行类似 IDM 的分配策略.

4 分布式的信息传播机制的性质及证明

分析 DIDM 的一些重要性质并简单证明.

定理 4 IDM 是 DIDM 的一个中心化规约机制 (Centralized Reduction Mechanism, CRM).

证明 要证明这个定理,需要证明当所有节点都诚实计算时,DIDM 总会得到与 IDM 一致的结果,即 $\pi(s^{tp})=f(\theta')$, $p(s^{tp})=q(\theta')$.

给定一个可行的策略描述 $s=\left\{(\theta'_1,c^*_1),(\theta'_2,c^*_2),\cdots,(\theta'_n,c^*_n)\right\}$,在 IDM 中,已经知道物品最终会被分配给第一个在关键传播链上且满足条件 $v'_i=v^*_{-d_{i+1}}$ 的买家 i. 而在 DIDM 中,物品会被沿着关键链 $\{0,1,2,\cdots,i,\cdots,m\}$ 传递直到遇到第一个刚好满足 i 是集合 $\bigcup_{k=0}^{k=i}\mathrm{T}(D_k)-T(D_{k+1})$ 中拥有最大估值的买家. 容易验证,这个条件与 $v'_i=v^*_{-d_{i+1}}$ 等价.

因此,有 $\pi(s^{tp})=f(\theta')$.

在 IDM 中,关键链上的排在赢家之前的买家将支付 $v^*_{-d_i}-v^*_{-d_{i+1}}$,而赢家将支付 $v^*_{-d_i}$. 在 DIDM 中,由之前的论证可知买家支付也与 IDM 一致(对关键链上的排在赢家之前的买家,他们先支付 $v^*_{-d_i}$ 以得到物品再收到 $v^*_{-d_{i+1}}$ 以将物品转卖出去;对赢家,直接支付 $v^*_{-d_i}$ 拿走物品),即 $p(s^{tp})=q(\theta')$. 这样就可以证明 IDM 是 DIDM 的一个 CRM.

证毕.

直观地看,如果每个买家都诚实地进行计算,那么在同一个社交网络中,IDM 与 DIDM 就会得到相同的分配结果和相同的支付. 此外,由于 IDM 是一个激励相容(IC)的中心化机制,因此,只需说明 DIDM 是一个算法相容(AC)的机制,就可以说 DIDM 的建议策略是一个后验纳什均衡.

定理 5 建议策略 s^* 是 DIDM 的一个后验纳什均衡.

证明 由 Li et al[1] 可知,IDM 是一个中心化的激励相容(IC)的机制. 接下来需要证明 DIDM 是 AC 的,那么由定理 1 就可以说 DIDM 的建议策

略是一个后验纳什均衡.

已知AC的定义等价于对于任意给定的私有信息类描述$\theta'=\{\theta'_1,\theta'_2,\cdots,\theta'_n\}$,当其他买家都执行建议策略时,任何企图通过操控计算过程来提高收益的策略都无效.首先证明对任意买家i而言,他们都没有动机通过操控计算来改变最高估值买家的关键链.为了便于表达,将这条关键链记作$\{1,2,\cdots,i,i+1,\cdots,m\}$.

如果i原本不在最高估值的关键链中,但是他通过违背算法协议将自己加入到了关键链中.根据机制,Bank在最终结算时会要求i支付整个网络的最高报价v^*.这是因为i的支付为集合$T(D_{i-1})\backslash\{i-1\}-T(D_i)$中的最高报价,由于$i$实际上不是关键点,因此Bank在计算支付时会将$v^*$计算进去.此时,$i$的收益将小于零.同理,$i$也没有动机通过操控计算来使自己成为赢家.又由于$i$本身不在关键链中,因此操控计算来使其他人加入或者离开关键链也不能让i受益.

如果i原本就在最高估值的关键链中但不是最终赢家,首先i没有动机退出关键链;其次,如果i企图通过改变他在关键链中的排序来获益,那么i有两种选择:第一种,i可以将他在关键链中的位置后移(通过虚报增大自己的dt_i来做到),当i成功将自己的排序升高之后,Bank在执行检查时会发现$et_j>dt_i^{'},j\in D_i$对所有的j都成立.此时Bank发现i不再是关键点因此i会受到巨大惩罚.同理,如果i降低自己的排序或者改变他人的排序,那么由于其他人都执行了诚实计算,Bank在进行状态检查的时候也会发现i的异常行为,从而使i遭到巨大损失.

如果i原本就在最高估值的关键链中且他是最终赢家.在此种情况下,由于其他人的诚实计算,且i的最终支付与其私有信息类无关,因此i无法进一步提高自己的收益.

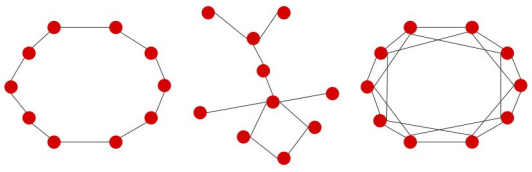
这样证明不论是关键链上的买家还是非关键链上的买家都没有动机来操控计算以使自己获得更高的收益.因此,DIDM是一个算法相容的机制.综上所述,建议策略s^*是一个后验纳什均衡.

证毕.

5　实验验证

本节通过在随机生成的社交网络中模拟DIDM拍卖的过程,并通过在不同实验条件下的对比来分析DIDM在隐私保护、拍卖交易链长度以及卖家收益等几个方面表现.其中,用隐私泄露率这一指标来衡量隐私保护,隐私泄露率指的是在一次拍卖过程中,第三方或者拍卖执行者需要询问的买家计算状态的总数量占网络中节点总数的比例.形式化定义:$PRR=\frac{\sum_{i\in N}o_i}{|N|}$,其中,$o_i\in\{0,1\}$,$o_i=1$表示买家$i$向Bank汇报状态,$o_i=0$表示买家$i$没有向Bank汇报状态.一般来说,在中心化IDM机制中$PRR^{\mathrm{IDM}}=1$.拍卖交易链长度是指拍卖时最高估值关键链的长度.

此次实验中使用小世界网络模型来生成虚拟社交网络,关于小世界网络的详细描述参见文献[16].小世界网络主要由两个参数控制,即参数k与参数p,其中k表示每个节点在网络中的最大度数,$p\in[0,1]$表示一个概率值.一个小世界网络$N(k,p)$的生成过程如下:先在n个节点上创建一个环,然后环中的每个节点与其k个最近邻居连接,再通过如下操作创建一些点之间的捷径:对于上述环中的每条边(u,v),以p的概率将其替换成一条新的边(u,w),其中w从剩余节点中均匀地随机选出.图3为小世界网络的一些例子.

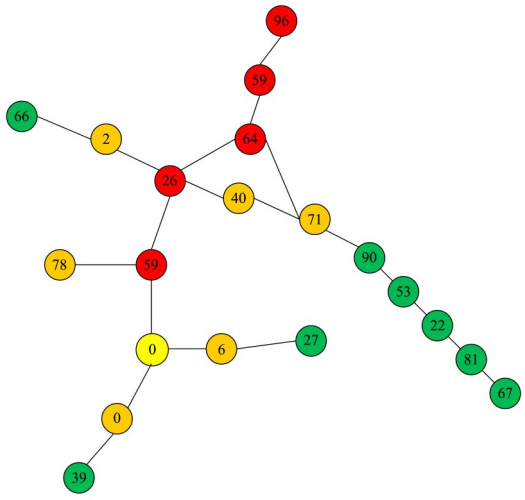


Networks were generated with the parameter of ($k=2,p=0$)($k=2,p=0.5$) and ($k=4,p=0$).

图3　小世界网络的一些例子

Fig. 3　Some examples of small world networks

在实验过程中,为了方便统计以及呈现可视化结果,在运行DIDM时将卖家节点标记为黄色,将关键链上的节点标记为红色,将非关键但是向Bank汇报了状态的节点标记为橙色,其他无关节点标记为绿色.如图4所示.



Colors of circles represent the privacy status of agents and numbers in circles represent valuations of agents.

图 4　一个随机生成的小世界网络

Fig. 4　An example of small world networks

实验中,网络规模设置为 100 个节点,每个节点的估值为 $v_i = U\{0,100\}$,即服从 0 到 100 的均匀随机分布. 固定 $p=0.5$,观察 DIDM 在不同 k 值下的表现. 对于每个不同的 k 值,运行 1000 次拍卖并取所有结果的均值作为最后结果. 得到结果如表 1 所示. 其中,RedR,OrangeR,GreenR 分别表示拍卖过程中分别被标记为红色、橙色以及绿色的节点的比例. ChainL 表示支付链长度,Revenue 表示卖家收入.

表 1　不同 k 下的小世界网络 PRR 对比图

Table 1　PRR values of small world networks generated with different k

k	RedR	OrangeR	GreenR	PRR	ChainL	Revenue
2	10.29%	14.51%	73.2%	0.268	3.99	48.44
4	5.73%	13.64%	79.63%	0.201	2.3	90.43
6	1%	11.48%	86.52%	0.135	1.0	98.48
8	1%	5.27%	92.73%	0.073	1.0	98.73

表 1 显示,网络中链接数量的升高使整个网络的隐私泄露程度大幅下降,交易链长度也随之下降,卖家收入也逐步上升. 这是符合直觉的. 随着网络中链接数量增多,买家间可以相互交换的信息量也随之增多,信息"垄断"的关键点也随之变少,网络可以完成更多的计算任务,从而使 Bank 需要的信息减少,使隐私得到更好的保护.

由于 k 值表示网络的复杂程度,不难得出,网络越复杂,DIDM 的隐私保护的表现越好.

6　总　结

本文为卖家提供了一种新的分布式和免费拍卖机制,以便在社交网络中销售产品. 该机制保证卖家永远不会亏本,并且所有买家都被激励参与而无需担心泄露他们的社会关系. 这是第一个处理卖家拍卖的分布式解决方案并改进了 Li et al[1] 提出的中心化的解决方案. 该机制本身也是分布式算法机制设计中的一个新的例子. 值得注意的是,本文并没有对分布式机制运行在网络中的复杂度进行严格的分析与证明,并且也没有讨论对相应的算法优化. 这部分相关问题将留到以后的工作去解决.

参考文献

[1] Li B, Hao D, Zhao D J, et al. Mechanism design in social networks//The 31st AAAI Conference on Artificial Intelligence. San Francisco, CA, USA: AAAI Press, 2017: 586－592.

[2] Zhao D J, Li B, Xu J P, et al. Selling multiple items via social networks//Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems. Stockholm, Sweden: International Foundation for Autonomous Agents and Multiagent Systems, 2018: 68－76.

[3] Nisan N, Roughgarden T, Tardos E, et al. Algorithmic game theory. Cambridge: Cambridge University Press, 2007, 776.

[4] Parkes D C, Shneidman J. Distributed implementations of vickrey - clarke - groves mechanisms//Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems, New York, NY, USA: IEEE, 2004: 261－268.

[5] Petcu A, Faltings B, Parkes D C. Mdpop: faithful distributed implementation of efficient social choice problems//Proceedings of the 5th International Conference on Autonomous Agents and Multiagent Systems. Hakodate, Japan: IEEE Computer Society, 2006: 1397－1404.

[6] Groves T. Incentives in teams. Econometrica, 1973, 41(4): 617－631.

[7] Archer A, Feigenbaum J, Krishnamurthy A, et al. Approximation and collusion in multicast cost sharing. Games and Economic Behavior, 2004, 47(1): 36－71.

[8] Shneidman J, Parkes D C. Specification faithfulness in networks with rational nodes//Proceedings of the 23rd Annual ACM Symposium on Principles of Distributed Computing. St. John′s, Canada: ACM, 2004: 88－97.

[9] Peng D, Yang S, Wu F, et al. Resisting three-dimensional manipulations in distributed wireless spectrum auctions//2015 IEEE Conference on Computer Communications. Hong Kong, China: IEEE, 2015: 2056－2064.

[10] Yang S, Peng D, Meng T. On designing distributed auction mechanisms for wireless spectrum allocation. IEEE Transactions on Mobile Computing, 2019, 18(9): 2129－2146.

[11] Feigenbaum J, Shenker S. Distributed algorithmic mechanism design: recent results and future directions//Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications. Atlanta, GE, USA: ACM, 2002: 1－13.

[12] Liu T Y. A decade of online advertising research: what we learned and what we need to know. Journal of Advertising, 2019, 48(1): 1－13.

[13] Tarjan R. Depth-first search and linear graph algorithms//2nd Annual Symposium on Switching and Automata Theory. East Lansing, MI, USA: IEEE, 1971: 114－121.

[14] Erciyes K. Guide to graph algorithms. Cham: Springer, 2018, 471.

[15] Makki S A M, Havas G. Distributed algorithms for constructing a depth-first-search tree//1994 International Conference on Parallel Processing. North Carolina, CA, USA: IEEE, 1994: 270－273.

[16] Watts D J, Strogatz S H. Collective dynamics of ′small-world′ networks. Nature, 1998, 393(6684): 440－442.

（责任编辑　杨可盛）