

P2P 资源的拍卖激励机制

刘洪涛^{1,2,3} 黄智兴^{2,3} 邱玉辉²

(重庆邮电大学计算机学院 重庆 400065)¹ (西南大学计算机与信息科学学院 重庆 400715)²
(西南大学语义网络实验室 重庆 400715)³

摘要 激励机制是 P2P(对等网)中的一个重要的研究课题。P2P 这种新的成功模式需要建立一个应用已有成熟的技术的激励机制来实现。本文提出了一种在 P2P 环境中基于拍卖的激励机制。在 P2P 所有资源都标以虚拟价格, P2P 中节点通过拍卖来决定它获得需要的怎样所应该付出的代价,并用虚拟货币进行支付,而节点通过贡献资源得到虚拟货币。在这种激励机制下,节点可以最大化利用自己的资源,如果 P2P 每个节点都能够实现资源的最大化利用,我们就可以实现在 P2P 中自私的节点也愿意贡献自己的资源这一目的。

关键词 P2P, 随机拍卖, 激励机制, 价格, 期望收益

A Contingent Auction Incentive Mechanism in P2P Resources

LIU Hong-Tao^{1,2,3} HUANG Zhi-Xing^{2,3} QIU Yu-Hui²

(Computer College, Chongqing University of Posts and Telecommunications, Chongqing 400065)¹
(College of Computer and Information Science, Southwest University, Chongqing 400715)²
(Semantic Network Laboratory, Southwest University, Chongqing 400715)³

Abstract Incentive mechanism in P2P is a important problem. The models of new and successful computing requires the development of appropriate incentive mechanisms that are consistent with the enabling technologies. This paper presents a contingent auction incentive mechanism in P2P environment. All resources are marked price in virtual money, The peers bid for resources in an auction to determine who can get the resources by pay for it with virtual money. The peers can get virtual money through share their resources So the peers' maximize their revenue, if every peer maximize their revenue. We achieve the goal that rational and self-interest peers would like to share their resources.

Keywords P2P, Contingent auction, Incentive mechanism, Price, Expect revenue

1 引言

P2P(对等网)作为一个成功的网络模式,人人贡献出自己的资源,人人享受他人提供的资源,每一个加入 P2P 的节点,既是资源的提供者又是资源的使用者(这里的资源包括计算能力,存储空间等),可以匿名、动态、几乎无代价地加入,这样的众多特点,在现在实际投入应用的系统 Napster Gnutella Freenet BitTorrent Kazaa 中得到了充分的体现^[1~5],使得 P2P 已经成为应用最广泛的资源共享系统,并且 P2P 技术的分布性、自治性、可测量性^[6~9]是 P2P 技术在各种各样的应用中越来越受重视。

在现存的 P2P 中存在这经典的“公共悲剧问题”^[10~12],在 P2P 中大量存在的是理性的、自私的节点即只享受资源而不提供资源的节点。数据统计表明 70% 的节点存在搭便车现象,这一现象将导致 P2P 系统负荷不平衡,而通过资源贸易(付费后享受资源)可以在资源拥有者之间形成一个良好的合作环境。

基于市场机制的原理,本文给 P2P 的每一个资源都标记上虚拟价格。节点使用资源付出虚拟货币,贡献资源获得虚拟货币。在一个 P2P 网络或者社区中系统对资源进行拍卖,节点对需要资源节点进行广播,假定希望得到资源的节点都参加资源的竞价,贡献节点和使用节点都是自私节点,在拍卖的过程中都追求最大收益和最大的边际效益。

在第 2 节本文进一步介绍对等网中激励机制的相关工作,第 3 节本文建立了一个拍卖机制使对等网中的节点贡献资源的节点收益最大化。第 4 节我利用模拟试验来检验本文的拍卖激励机制是否能够使节点的收益最大化。最后得出结论,指出本机制的不足之处并给出将来的工作。

2 相关工作

文[13]提出了一个静态和一个动态的价格激励机制来鼓励每个节点采取理性行为,直到整个系统达到资源最优化。Hemant K 在文[14]提出,在市场机制下价格的确定可以通过拍卖的方式来得到。随着网络的发展和对私密性的要求,网络拍卖方式在最近几年有了飞速的发展^[15],Bhargaya^[16]提出了一种针对柔性计算资源的预搜索方法,促进了按需计算和 IT 资源外购的解决。他应用随机拍卖方式来形成资源的合理价格。Lange 和 Economides 在文[17]提出在随机拍卖中应用赌博中出现的派利分成法。Bergemann 和 Valim'aki 在文[18, 19]中用标记贡献来构建在动态第一价格拍卖中的有效平衡。

3 随机拍卖激励机制

本文提出在 P2P 资源共享模型以价格为基础参与资源分配的激励机制中。在随机拍卖中,节点提供资源就是卖者,相反节点获得资源就是买者。而且节点都设定为理性和

自私的节点,节点都是以资源效用最大化为目的。

卖者有 M 单位的资源,同时有 N 个买者,假设已经使用过该资源的节点对资源的评价是 $\beta, \beta \in [0, 1]$, 而资源贡献节点兑现的可能性是 θ , 卖者设置资源的价格为 P , 那么卖者的盈利为:

$$c_i = \begin{cases} p & \text{show-up} \\ \theta p & \text{cancel} \end{cases}$$

买者效用的期望值为:

$$\mu_i = \theta(\beta - p) - (1 - \theta)\theta p \quad (1)$$

在本文的随机价格机制中,资源使用者 i 提出预订资源的要求被接受并得到满足,它需要付出 p , 如果他的预订被它自己取消它需要支付 θp , 如果它的要求被拒绝它不需要为这个请求付出任何代价。

在基于卖者对资源的标价 p 的分配机制中,节点对的对资源拍卖报价兑现的可能性为 θ 。资源提供节点即卖者挑选 M 个最高报价的节点作为拍卖过程的获胜者, 获胜者的支付函数如公式(1)。我们需要对价格 p 的值进行计算, 以达到卖者的收益期望值最大。

对于卖者给出的资源价格 p , 买者只有在自己的效用 $\mu_i \geq 0$ 的情况下才会参与拍卖, 这就意味者 $\theta \geq 2 - \beta/p$ 。假设使用过该资源的节点对资源的评价是 β 在 $[0, 1]$ 上均匀分布而且 $\theta \in [0, 1]$, 这样的 θ 可能最小值为

$$\theta = \max(0, \min(1, 2 - \beta/p)) \quad (2)$$

我们设定

$$\Pr(p) = \begin{cases} \Pr_A(p), & p > 0.5 \\ \Pr_B(p), & p \leq 0.5 \end{cases}$$

A) 如果 $p > 0.5$, 那么就有 $\theta = 2 - \beta/p, \theta \in [2 - \beta/p, 1]$, 只有当节点对资源的评价 β 大于价格 p 即 $\beta \geq p, \beta \in [p, 1]$, 节点才有意愿参与拍卖过程。

$$\Pr_A(p) = \int_{p-\frac{\beta}{2}}^1 \int_{2-\frac{\beta}{p}}^1 d\theta d\beta = \frac{1}{2p} + \frac{p}{2} - 1 \quad (3)$$

B) 当 $p \leq 0.5$, 这里存在两个情况 1) $\theta = 0, 2) \theta = 2 - \frac{\beta}{p}$

1) 由 $\theta = 0$ 得到 $\theta \geq 2p$

$$\Pr_{B1}(p) = \int_{2p}^1 \int_0^1 d\theta d\beta = 1 - 2p$$

2) 由 $\theta = 2 - \beta/p$ 得到 $p \leq \beta \leq 2p$

$$\Pr_{B2}(p) = \int_{p-\frac{\beta}{2}}^{2p} \int_{2-\frac{\beta}{p}}^1 d\theta d\beta = \frac{p}{2}$$

由上面两式可以得到这样的结果如果 $p \leq 0.5$

$$\Pr_B(p) = \Pr_{B1}(p) + \Pr_{B2}(p) = 1 - \frac{3}{2}p \quad (4)$$

参与到拍卖中的节点的评价期望值是 $\psi(p, N) = \Pr(p)$ N , 有 k 个节点参与到拍卖的过程可能性是

$$\Pr(p, k, N) = \binom{N}{k} \Pr(p)^k (1 - \Pr(p))^{N-k} \quad (5)$$

$$\psi(p, N) = \sum_{k=1}^N \Pr(p, k, N) \quad (6)$$

节点怎样能够得到期望的收益? 我们设定有 M 单位的资源可以被预订, 希望从潜在的节点中挑选出 M 个对资源的节点请求, 这些请求挑选的原则是兑现可能性 θ 最高的 M 个请求。在开始应用拍卖机制前我们要说明: 如果这里有 N 个数值均匀独立分布在 $[0, 1]$ 上, 第 i 个最大的值为 $\frac{N-i+1}{N+1}$ 。我们用 $\pi(p, M, k)$ 来代表当资源价格为 p 时, 从 k 个潜在节

点中挑选出 M 个兑现可能性最高的节点的期望收益。

A) 当 $p > 0.5$, 和 $k \geq M$, 从 k 个数值挑选 M 个最高的数值, 这些值独立均匀的分布在 $[2 - \frac{1}{p}, 1]$ 上。第 M 个最大值为

$$\bar{\theta}_m = \frac{(\frac{1}{p} - 1)(k - M + 1)}{k + 1} + (2 - \frac{1}{p}) \quad (7)$$

$$\pi_A(p, M, k) = pM \frac{k+1}{(M+1)(1/p-1)\bar{\theta}_{m+1}} \left\} \theta + (1-\theta)\bar{\theta}_m d\theta \quad (8)$$

如果 $k < M$,

$$\pi_A(p, M, k) = pk \frac{1}{1/p-1} \left\} \theta + (1-\theta)\bar{\theta}_k d\theta \quad (9)$$

B) 当 $p \leq 0.5$, 如果 $k \geq M, \bar{\theta}_m = \frac{(k-m)}{(k+1)}$

$$\pi_B(p, M, k) = pM \frac{k+1}{(M+1)(1/p-1)\bar{\theta}_{m+1}} \left\} \theta + (1-\theta)\bar{\theta}_m d\theta \quad (10)$$

如果 $k < M$

$$\pi_B(p, M, k) = pk \left\} \theta + (1-\theta)\bar{\theta}_k d\theta \quad (11)$$

期望收益可以用下式来进行计算

$$ER(p, M, N) = \sum_{k=1}^N \Pr(p, k, N) \pi_{A,B}(p, M, k)$$

显然在这个激励机制中价格是关键因素, 对于 M 和 N 的最优价格 p^* 是

$$p^*(M, N) = \arg \max_p \{ER(p, M, N)\}$$

最大的期望收益是

$$MER(M, N) = \pi(p^*, M, N)$$

在本文的拍卖激励机制值, 希望得到资源他必须付出虚拟货币, 如果所有的节点(贡献资源的节点)都希望并且能够最大化他们的收益, 贡献资源的行为将通过付给虚拟货币的方式受到鼓励。这样这个激励机制就可以达到目的。

4 实验

设定有 $N=100$ 个节点节点贡献资源的评价是 β , 用户节点兑现可能性为 θ 贡献的资源 $M=3$ 。

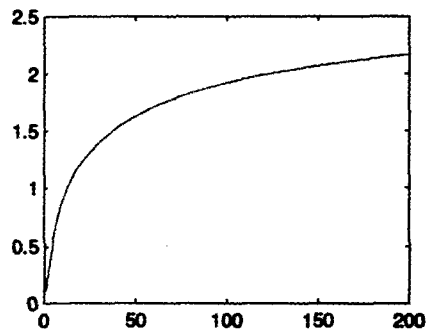


图 1

从图 1 可以得到期望收益和节点数之间的关系。

从图 2 可以看到实际模拟拍卖得到的结果和期望收益之间的比较。

从实验的结果我们可以得到这样的结果贡献资源的节点的期望收益要好于实际拍卖得到的收益, 因为我们不能保证

使用资源的节点说真话,并且贡献资源的节点不能确定最正确的资源价格。

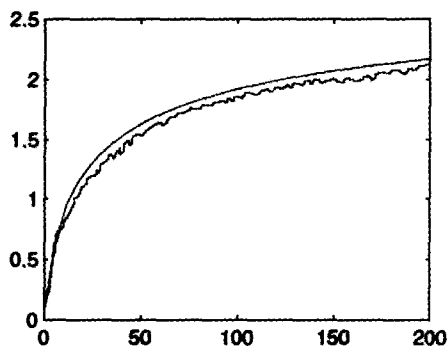


图 2

结论和将来的工作 本文提出了一种新的 P2P 激励机制,在这种激励机制中所有的资源都用虚拟货币进行标价。节点通过随机拍卖来确定那些节点是拍卖的获胜者,就可以使用资源并付出虚拟货币,而节点可以通过贡献自己的资源来得到虚拟货币。我们描述了拍卖的工作原理和资源贡献节点得到多少期望收益。通过分析实验结果,我们确定只有当 P2P 中的节点是诚实的,节点说的和行为一致时,激励机制才能发挥比较好的作用。所以在未来的工作中我们希望能够找到一种激励机制,鼓励节点说真话或者说真话要得到鼓励,并且说真话是节点收益最大化的重要保障。

参考文献

- 1 Feldman M. FreeRiding and Whitewashing in PeertoPeer Systems. SIGCOMM'04 Workshop, Aug. 30+Sept. 3, 2004
- 2 Kenyon C, Cheliotis G, Buyya R. 10 Lessons from Finance for Commercial Sharing of IT Resources. In: Peer-to-Peer Computing: The Evolution of a Disruptive Technology. IRM Press, 2004
- 3 Hardin G. The Tragedy of the Commons. Science, 1968, 162:

1243~1248

- 4 Feigenbaum J, Shenker S. Distributed algorithmic mechanism design: Recent results and future directions. In: Proc. 6th Int'l Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Atlanta, GA, Sept. 2002. 1~13
- 5 Golle P, Leyton-Brown K, Mironov I, et al. Incentives for sharing in peer-to-peer networks. In: Proc. 3rd ACM Conf. on Electronic Commerce, Tampa, FL, Oct. 2001
- 6 Milojevic D S, Kalogeraki V, Lukose R, et al. Peer-to-Peer Computing; [Technical Report HPL-2002-57]. HP Laboratories Palo Alto, 2002
- 7 Ratnasamy S, Francis P, Handley M, et al. A scalable content addressable network. In: Proc. of ACM SIGCOMM, 2001
- 8 Rowstron A, Druschel P. Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer systems. Lecture Notes in Computer Science, 2001, 2218: 329~350
- 9 Stoica I, Morris R, Karger D, et al. Chord: A scalable peer-to-peer lookup service for internet applications. ACM SIGCOMM, 2001
- 10 Kenyon C, Cheliotis G, Buyya R. 10 Lessons from Finance for Commercial Sharing of IT Resources. In: Peer-to-Peer Computing: The Evolution of a Disruptive Technology. IRM Press, 2004
- 11 Adar E, Huberman B. Free Riding on Gnutella. First Monday, 2000, 5(10)
- 12 Yu Bin, Singh M P. Incentive Mechanisms for Peer-to-Peer Systems. <http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/ap2pc-03-mechanism.pdf>
- 13 Ma R T B. A Game Theoretic Approach to Provide Incentive and Service Differentiation in P2P Networks. SIGMETRICS/Performance'04, 2004
- 14 Bapna R, Goes P, Gupta A. Insights and analysis of online auctions. Communications of the ACM, 2001, 44: 42~50
- 15 Bhargava H K, Sundaresan S. Contingent Bids in Auctions: Availability, Commitment and Pricing of Computing as Utility. In: Proc. of the 37th Hawaii International Conference on System Sciences, 2004
- 16 Lange J, Economides N. A parimutuel market microstructure for contingent claims. European Financial Management, 2005, 11(1): 25~49
- 17 Bapna A, Weber T. Efficient Dynamic Allocation with Uncertain Valuations. Stanford University
- 18 Bergemann D, V'alim'aki J. Dynamic Common Agency. Journal of Economic Theory, Forthcoming
- 19 Bergemann D, V'alim'aki J. Dynamic Price Competition. Journal of Economic Theory, 127: 232~263

(上接第 57 页)

户能够匿名地从 Web 服务器取回信息而不对服务器和第三方泄露用户自己的信息,其基本思想是把自己隐藏在群体中。

假设攻击者知道在 crowds 中有 n 台计算机($d_1 d_2 \dots d_n$) 参加访问了某个网页(该行动用 a_1 表示),也知道某台计算机 d_k 访问了另一个网页(该行动用 a_2 表示)。攻击者知道用户使用哪台计算机,则攻击者的函数决定集合为 $F = \{(d_1 d_2 \dots d_n) \rightarrow a_1, d_k \rightarrow a_2, u_1 \rightarrow d_1, u_2 \rightarrow d_2, \dots, u_n \rightarrow d_n, u_k \rightarrow d_k\}$ 。

下面分析用户行动是否具有匿名性。

行动 a_i 的闭包为 a_i , 用户 u_i ($i = 1, 2, \dots, n$) 的闭包为 $u_i d_i$, u_k 闭包为 $u_k d_k a_2$ 。

显然用户 u_i 的行动是匿名的,即不能从 u_i 推出某个行动。由于从 u_k 能够推出 a_2 , 因此用户 u_k 的行动不是匿名的。

小结 对于一个匿名系统而言,对象之间是否具有关联性不一定是明显的。如果攻击者根据获得的知识无法推断对象之间的关联性,则认为对象是匿名的。本文给出的完备的匿名推理系统能够推断对象之间的关系,从而能够发现隐藏的安全性问题。匿名分析算法给出了评估匿名机制的安全性方法,并对设计匿名机制具有很好的指导作用,与现有的隐私钻石模型相比具有分析能力强以及简单实用等优点。

参考文献

- 1 Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84~88
- 2 Reiter M, Rubin A D. Crowds; anonymity for Web transactions. ACM Transactions on Information and System Security, 1998, 1(1): 66~92
- 3 Ren K, Lou W, Kim K, et al. A novel privacy preserving authentication and access control scheme for pervasive computing environments. IEEE Transactions on Vehicular Technology, 2006, 55(4): 1373~1384
- 4 Konidala D M, Duc D N, Kim K. A capability-based privacy-preserving scheme for pervasive computing environments. In: Proc. IEEE International Workshop on Pervasive Computing and Communication Security, 2005. 8~12
- 5 Wu X. Applying pseudonymity for anonymous data delivery in location-aware mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 2006, 55(3): 1062~1073
- 6 Kobza A, Schreck J. Privacy through pseudonymity in user-adaptive systems. ACM Transactions on Internet Technology, 2003, 3(2): 149~183
- 7 Zugenmaier A, Kreutzer M, Muller G. The freiburg privacy diamond: an attacker model for a mobile computing environment. In: Kommunikation in Verteilten Systemen (KiVS) '03, 2003
- 8 Iachello G, Truong K N, Abowd G D, et al. Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. In: Proc. ACM Conference on Human Factors in Computing Systems, New York: ACM Press, 2006. 1009~1018