对等网络中的基本弱公平资源交换协议*)

周世杰 秦志光 张险峰 刘锦德

(电子科技大学计算机科学与工程学院 IBM 技术中心 成都 610054)

摘 要 对等计算(P2P)可在 Internet 或者自组网边界进行计算,从而可提供一种全新的应用模式。从对等计算与公平交换的基本概念入手,讨论了协议中的基本假设,设计了一个适合于对等网络的基本弱公平交换协议(BWFEP),并对协议的交互过程做了详尽分析。对 BWFRP 协议公平性的分析结果表明,该协议具有无需可信第三方(TTP)、简单、弱公平性的特点,从而适合于对等网络中用户之间直接资源交换的需要。

关键词 对等计算,分布式计算,公平交换,自组网络,网格计算,普及计算

A Basic Weak Fair Exchange Protocol for Resource in P2P Networks

ZHOU Shi-Jie QIN Zhi-Guang ZHANG Xian-Feng LIU Jin-De

(College of Computer Science and Engineering, UEST of China, Chengdu 610054)

Abstract Peer-to-Peer (P2P) computing, which occurs on the edge of Internet or ad hoc networks, is regarded as an alternative to distributed computing. With some prominent features, P2P can also act as the elementary infrastructure for pervasive computing and ad hoc computing. Being a novel application model, P2P can also be used to connect some small ad hoc networks together to from a uniform open network and thus make P2P can be adapted to many new application areas. Among these applications, resources' fair exchanging is the one which catches the eyes of many peoples. A basic weak fair exchange protocol (BWFEP) is presented in this paper to address this issue. BWFEP is designed to allow two peers in P2P community to exchange file-like resource directly. Unlike most other exchange protocols that rely on the trusted third party (TTP) to guarantee fairness, BWFRP employs the natural features of file to provide the fairness. Except for its simpleness, BWFRP can also achieve weak fair at the cost of minimum.

Keywords P2P computing, Distributed computing, Fair exchange, Ad hoc networks, Grid Computing, Pervasive computing

1 引言

对等计算(Peer-to-Peer Computing,简称 P2P)[1~4]是 20 世纪末兴起的不同于传统客户/服务器计算模型的一种全新的通信模型和应用模型,并随着 Napster[1]的流行而为人瞩目。从技术的角度来看,它是使用分布资源,并以分布计算技术来完成关键任务的系统和应用的总称。P2P 一般在互联网或者 Ad hoc 网络的边界进行计算,其通信基础设施属于全分布式模型,但在混合型 P2P 系统中,也允许保留某些集中的特性。由于具有全分布式的特点,P2P 技术适合个人之间的直接信息交流,因而在协作通信、资源共享和科学计算等领域有着广泛的应用。随着资源的数字化程度的提高和从用户经济利益的角度来看,用户之间不应仅仅满足于资源的共享,也应该注重资源的交换。与资源共享不同,用户之间资源交换则要求公平性,即如何保证参与资源交换协议用户的公平性,是该类应用所面临的至关重要的问题[9~12]。

传统的公平交换可采用两种方式实现[5~8]。第一种方式是在假设双方具有同等计算能力的条件下,逐步将数据传给对方。第二种方式则是在可信第三方(TTP)的保证下,来进行数据的公平交换。不论是采用在线式 TTP,还是离线式 TTP,第三方的存在均要求一定的通信开销和额外的管理费用开销。而作为无控制中心的对等网络,其基本特征包括自组织、无管理要求等特点,因而难以采用 TTP 方式来进行资源交换,只可能在没有可信方的参与下,依赖对等网络的自身特征来进行。本文从对等网络文件(如音乐文件,电影文件等)的公平交换具体需求出发,设计了一个无可信第三方的基本的弱公平交换协议(Basic Fair Exchange Protocol, BWFEP),希望以此推动对等网络中公平资源交换协议的研究工作。

2 基本弱公平交换协议中的基本假定

根据对等网络的基本特征,基本弱公平交换协议(BWFEP)协议在无可信第三方的环境中执行,参与交换的双方为用户 Alice(A)和 Bob(B),他们分别拥有密钥对 PK_x 和 SK_x,其中 PK_x 和 SK_x,分别为用户 x 的公钥和私钥(即 Alice 的密钥对为 PK_A 和 SK_A,Bob 的密钥对为 PK_B 和 SK_B)。$\{m\}_K$ 表示用密钥 K 对消息 m 加密,m_1, m_2 表示消息 m_1 和 m_2 的连接。通信双方的工作密钥用 K 表示。"用户执行本地操作"表示用户根据已经收到的协议数据进行本地计算,用"U:E"表

*)本课题得到国家高新技术研究发展引导计划(863 引导计划)网络化系统容灾技术(项目编号:2002AA001042),国家高新技术发展计划(863 计划)战略预警与监管体系结构研究(项目编号:2002AA142040)资助。**周世杰** 博士研究生,主要研究方向为对等计算、信息安全和中间件技术。**秦志光** 博士,教授,博士生导师,主要研究方向为信息安全、分布式计算和中间件技术。**刘锦德** 教授,博士生导师,主要研究方向为开放分布式系统与中间件技术,移动代理技术。

示(即表示用户 U 执行操作 E)。

协议假定用户 Alice 和 Bob 需要进行两个文件 F_A 和 F_B 的交换(其中文件 F_A 属于 Alice 所有,F_B 属于 Bob 所有)。假定如果对文件进行足够大的分块后,在不知道分块规则的情况下,重组该文件很困难。这也符合实际情况,比如对电影文件,如果进行 N 块(N 足够大)划分后,重组该文件的复杂度为 $N(N-1)/2$,因此在不知道分块规则的情况下重组文件很难。此外,我们还假定加密算法或者不可破,或者破译难度对双方来说都相同,即不会因为某个用户可以破译加密算法,从而造成交换协议的不公平性。

3 基本弱公平交换协议的设计

BWFEP 协议分为四个步骤,这个协议的基本执行步骤框架如图 1 所示。

初始化: A 和 B 生成各自的工作密钥 K_A,K_B

Step 1: 用户 A 和 B 互换公钥并协商对文件划分最大的数据块数 N。如果双方达成一致,则 A 和 B 各自产生 N 个工作密钥 K_{A_i} 和 K_{B_i}($i=1,2,\cdots,N$)并转 Step 2;否则转 Step 4。

Step 2: 用户 A 和 B 按照协商的 N 值,将文件分别划分为 $F_A(i)$ 和 $F_B(i)$($i=1,2,\cdots,N$),用对应的工作密钥对数据块进行加密,并以随机顺序发送给对方。

Step 3a: 用户 A 和 B 要求对方发送自己希望组合的两个数据块的相关信息;

Step 3b: 用户 A 和 B 接收相关信息,并执行组合操作,任意一方如出错或不满意,转 Step 4;如果双方均满意,且重组数据没有完成,转 Step 3a;否则如已经完成交换转 Step 4。

Step 4: 退出协议

图 1 BWFEP 基本流程图

步骤 1:交换密钥及协商文件分块

图 1 中步骤 1 是双方交换公钥,并就文件的划分情况进行协商。该步骤不影响资源的交换,因而可以按照双方的要求进行反复协商,直到满足彼此的要求为止。如果不能达成一致,则任何一方均可中止协议。图 2 是本步骤的消息交换示意图。

A→B: $PK_A, N1$

B→A: $PK_B, N2$

A→B: $\{Max(N1,N2), K_B\}_{SK_A}$

B→A: $\{Max(N1,N2), K_B\}_{SK_B}$

A: $\{\{Max(N1,N2), N2\}_{SK_B}\}_{PK_B}$

$ACK_{AB}=(Max(N1,N2)>=N1?\ Yes;No)$

B: $\{\{Max(N1,N2), N1\}_{SK_A}\}_{PK_A}$

$ACK_{BA}=(Max(N1,N2)>=N2?\ Yes;No)$

A→B: $\{ACK_{AB}\}_{K_A}$

B→A: $\{ACK_{BA}\}_{K_B}$

图 2 BWFEP 中步骤 1 的详细情况

步骤 1 的执行比较直观,首先 A 和 B 分别向对方发送自己的公钥和所希望的文件分块数,当收到对方的消息后,取 N 为自己的期望值和对方发送的期望值中最大者(用图 2 中用函数 Max()表示)。如果都收到对方的消息,则将 N 值和期望的工作密钥 K 用自己的私钥加密后发送给对方。双方用收到的对方的公钥解密消息,得到协商结果和工作密钥,并将自己的最终意见用工作密钥加密后发送给对方。如果双方协商一致,协议继续执行,否则取消协议。在协商文件分块时,协议采用取最大值的方法,不仅减少了通信开销,也保证了选择对双方的公正性。这是因为按照我们的假设,任何用户均不可能提供比自己期望小的文件分块方案,否则遭受损失的只可能是其自身。

步骤 2:随机发送加密数据块

步骤 2 按照协商的数据块数对文件进行划分、加密和随机传送。虽然用户是随机传送数据块,但发送方必须记录文件的划分顺序和发送顺序之间的对应规则,以便自己可重组文件。图 3 是步骤 2 的消息处理示意图。

A: 生成 N 个工作密钥 $K_{A_{1\cdots N}}$

B: 生成 N 个工作密钥 $K_{B_{1\cdots N}}$

A→B: $\{F_A(i)\}K_{A_i}$,$i=1\cdots N$,$F_A(i)$为随机的第 i 块数据

B→A: $\{F_B(i)\}K_{B_i}$,$i=1\cdots N$,$F_B(i)$为随机的第 i 块数据

图 3 BWFEP 中步骤 2 的详细示意图

步骤 3:步式进传送密钥

当收到加密的数据块后,双方进行密钥的交换。为了验证对方在第二个步骤中发送的正确、真实的数据块,用户随机要求解密指定的数据块,并要求和后续快进行组装。这个过程循环执行,直到组装完成,或者协议终止。图 4 是本步骤的消息处理示意图。

A→B: $\{Random()\}K_A$

B→A: $\{Random()\}K_B$

A: $i=\{\{Random()\}K_B\}K_B$

B: $j=\{\{Random()\}K_A\}K_A$

A→B: $\{K_{A_i}, K_{A_{j+1}}\}K_A$

B→A: $\{K_{B_i}, K_{B_{j+1}}\}K_B$

A: $\{\{F_B(i)\}K_{B_i}\}K_{B_i}+\{\{F_B(i+1)\}K_{B_{i+1}}\}K_{B_{i+1}}$

B: $\{\{F_A(i)\}K_{A_i}\}K_{A_i}+\{\{F_A(i+1)\}K_{A_{i+1}}\}K_{A_{i+1}}$

图 4 BWFEP 中步骤 3 的详细示意图

在步骤 3 中,用户随机指定期望进行解密和重组的数据块号(图中用 Random()表示),对方则返回相应的密钥。如果解密成功并且重组结构满意,则协议继续执行,否则任意一方均可要求终止协议。当然,为了减少不必要的通信开销,用户随机指定的块号,应是以前没有发送过的,这可以由用户自行判断。

4 BWFEP 协议公平性分析

所谓公平是指如果交易的双方都诚实,则协议的执行结果是各获所需,达到交易的目的;如果交易的一方不诚实(如过早终止协议或者有欺骗行为),另一方也不会遭受损失。公平交换协议也有强公平交换协议和弱交换协议之分,强公平性指协议能保证协议双方均不会因为对方的不诚实而遭受任何损失。而弱公平性则是指虽然一方可能遭受损失,但可以通过诸如法律等手段讨回损失。在对等网络中,由于没有可信的第三方,因而用户不可能提供法律证据,因此这里的弱公平性

是指用户遭受的损失可以最小。

在BWFEP协议的第一步中，如果对协商的结果不满意，任意一方均可以退出协议，因而不存在不公平现象。步骤2中，由于传输的是加密数据，因此按照我们关于"算法不可破"的假设，虽然上方均得到了数据，但是由于没有解密密钥，因而恢复数据是不可能的。此外，即便某一方的计算能力比另外一方强，可以破解加密算法，得到 N 个明文数据块，但是由于 N 足够大，因而重组数据块也需要更多的计算开销。因此，第二步中也可以满足公平性的要求。

在第二步中，虽然协议对双方都是公平的，但并不排除发送虚假的数据，即第二步中可能存在欺骗现象。这个问题可以在第三步中被检查出来，这是因为发送方可以随机要求对方重组其中的任意两块。如果在第二步发送的数据为虚假数据，则重组后的结果自然不成立，用户可以立即发现该问题，并终止协议。第三步中另外一个问题是，如果用户不诚实，也有可能存在欺骗问题，从而导致协议的弱公平性。比如用户A如果不诚实，他可以发送不正确的解密密钥 K_{A_i} 或者 $K_{A_{i+1}}$，使得用户B不能解密或者重组数据，因此协议对B是不公平的。但是我们认为这只是弱公平性。理由如下：(1)在步骤3中，用户只可能蒙受一个数据块的损失，这是显而易见的，因为如果用户一旦发现重组后的数据不满意，可立即退出协议。(2)由于 N 足够大，数据块又是随机的，因而一个数据块的价值很小，这样的损失用户可以接受，即因为协议的不公平性，用户的损失可以最小化，保证了我们对"弱公平性"的要求。在步骤3中，唯一可能导致不公平的情况是最后一个数据块的交换，即一方得到了最后一个数据块，但却拒绝发送自己的最后一个数据块。在BWFEP协议中，没有考虑这一问题，我们拟在今后的问题中采用零知识证明的方法解决这个问题。

总结 对等计算模型在移动计算，移动自组网等均有着广泛的应用前景。本文设计的基本弱公平交换协议(BWFEP)，可在无可信第三方的条件下保证协议双方资源交换的弱公平性，从符合对等网络的基本要求和特征。对该协议的分析结果表明，BWFEP协议无法保证用户在最后一个数据块发送时实施欺骗行为，因此还需要对协议加以改进，从而满足用户对资源交换的强公平性的要求。

参考文献

1 Napster Home Page. http://www.napster.com/.
2 Yang B, Garcia-Molina H. Comparing Hybrid Peer-to-Peer Systems. Technical report. Stanford University, Feb. 2001. Available at: http://dbpubs.stanford.edu/pub/2000-35
3 Buyya R. Economic models for Management of the Resources in Peer-to-Peer and Grid Computing. Proc. of the Commercial Applications for High-Performance Computing Conf. 2001
4 Milojicic D S, et al. Peer-to-Peer Computing, HP Laboratories Palo alto: [Technique Report: HPL-2002-57]. March, 2002
5 王彩芬，葛建华．带脱线半可信第三方的公平非否认交换协议．电子学报，2002，30(2)：286～288
6 姬东耀，王育民．基于Pay Word的小额电子支付协议．电子学报，2002，30(2)：301～303
7 李志江，李明柱，杨义先，等．一个实用的公平电子合同协议．北京邮电大学学报，2002，25(2)：28～32
8 邓所云，詹榜华，胡正义，等．一个优化的公平的电子支付方案．计算机学报，2002，25(2)：1094～1098
9 Ray I, Ray I. Fair Exchange in E-commerce. ACM SIGecom Exchange, 2002, 3(2): 9～17
10 Levente B, Jean-Pierre H. Ratinal Exchange - A Formal Model Based on Game Theory. In: Proc. for the 2nd Intl. Workshop on Electronic Commerce (WELCOM 2001), Springer-Verlag, 2001
11 Shmatikov V, Mitchell J C. Finite-state analysis of two contract signing protocols. Theoretical Computer Science, 2002, 283(2): 419～450
12 Pfitzmann B, Schunter M, Waidner M. Optimal efficiency of optimistic contract signing. In: Proc. of the seventeenth annual ACM symposium on Principles of distributed computing, 1998. 113～122
13 周世杰，秦志光，张峰，等．基于P2P的信息存储技术．见：第12届全国信息存储技术学术会议(NCIS2002)，上海，2002

(上接第34页)

个交换路径，而所需要的标签数目为 $(n/A)\times d$。如果结合标签的聚合策略，例如令具有相同出口LER的分组(即具有相同CIDR前缀的分组)都使用相同的标签，则仅需要 n/A 个标签，这极大地提高了网络的可扩展性。当然，这是以支配LER的处理开销为代价的。

(4)时延分析 时延包括节点的时延和链路的时延。这里节点时延主要考虑支配LER的时延，因为支配LER的处理速度对该聚合网络的性能产生较大影响；而连路的时延主要考虑被支配LER到支配LER的链路的时延。如果图 $G=(V, E)$ 每个节点 $v\in V$ 具有一个非负的权 w，用 w_v 表示，那么考虑LER时延的支配集 D 的选取可以描述为：选择 D，使得 $W_D=\sum_{i\in D} w_i$ 最小。这是一个NP完全问题[9]。链路时延的减小可以考虑在链路最大时延要求下，被支配LER选择满足时延约束条件的支配LER作为其支配点，同时支配LER的选取也可以综合考虑节点的时延和链路的时延。这都将在后续工作中进行研究。

结论 本文提出了一种通过构建LER支配集对MPLS网络进行拓扑聚合的算法，证明了算法生成的支配集的正确性，并对算法和聚合网络的性能进行了分析。由于该聚合策略采用分布式算法，实现简单，对网络拓扑的变化具有较好的适应性，并能有效地减少MPLS网络的LSP和标签的数量，从而减少控制信息的通信量。同时支配LER的冗余性可以作为LSP的保护备份，因此使MPLS网络具有较好的可护展性和健壮性。

参考文献

1 Rosen E, Viswanathan A, Callon R. Multiprotocol Label Switching Architecture. RFC 3031, Jan. 2001
2 Awduche D, et al. RSVP-TE: Extensions to RSVP for LSP Tunnels. RFC3209, Dec. 2001
3 Andersson L, et al. LDP Specification, RFC3036, Jan. 2001
4 Fredette A, White C. Loa Andersson and Paul Doolan, Internet Draft, draft-fredette-mpls-aggregation-00. txt, Nov. 1997
5 Saito H, Miyao Y, Yoshida M. Traffic Engineering using Multiple Multipoint-to-Point LSPs. IEEE INFOCOM'2000, Tel Aviv, Israel, 2000, 2: 894～901
6 Urvoy-Keller G, Hébuterne G, Dallery Y. Traffic Engineering in a multipoint-to-Point Network. IEEE Journal on Selected Areas in Communications, 2002, 20(4): 834～849
7 Bhatnagar S, Ganguly S, Nath B. Label Space Reduction in Multipoint-point LSPs for Traffic Engineering. In: 2nd European Conf. on Universal Multiservice Networks, ECUMN'2002, Colmar, France, 2002. 29～35
8 Oh Y K, et al. Scalable MPLS Multicast using Label Aggregation in Internet Broadcasting Systems. In: 10th Intl. Conf. on Telecommunications, ICT'2003, Tahiti Papeete, French Polyn-esia, 2003
9 Alber J, et al. Fixed Parameter Algorithms for dominating set and related problems on planar graphs. Algorithmica, 2002, 33: 461～493