P2P 模式下协同工作安全群组通信模型的探索

马 勇[1,2]，田玉敏[1]

(1. 西安电子科技大学 计算机科学与技术学院，陕西 西安 710071；
2. 武汉大学 计算机科学与技术学院，湖北 武汉 430072)

摘要：提出了点到点(P2P)模式下协同工作安全群组通信模型，实现了 P2P 模式下协同工作节点动态加入和退出，以及群组安全可靠有序的通信机制. 算法设计的节点管理和节点通信为 P2P 模式下协同工作应用开发提供了必要的支持. 通过理论分析，证明了点组内节点操作的一致性，协同绘图作为实例说明了该方法的有效性.

关键词：点到点；计算机支持的协调工作；群组通信

中图分类号：TP391 **文献标识码**：A **文章编号**：1001-2400(2006)06-0965-05

Exploring the group secure communication model of CSCW in the P2P network

MA Yong[1,2]，*TIAN Yu-min*[1]

(1. School of Computer Science & Technology, Xidian Univ., Xi'an 710071, China;
2. School of Computer Science & Technology, Wuhan Univ., Wuhan 430072, China)

Abstract: A group secure communication model of CSCW in the P2P network is proposed, which permits users to join and quit the system dynamically and freely, and provides secure, warranted and ordered communication between peers. User management and peer communication supply the necessary support for CSCW applications in the P2P network. Theoretical analysis can prove the persistence between the different peers in the group, and collaborative draw is used as an example to express the factual effect.

Key Words: P2P; CSCW; group communication

传统客户/服务器或者浏览器/服务器分布式系统中，由中央服务器统一管理各个节点，为他们提供服务. 虽然这种结构易于实现有序的群组通信，但是所有节点访问服务器必然会造成服务器的繁忙和系统对服务器的单点依赖；如果服务器出现故障，会导致整个系统的瘫痪. 基于集中式的计算机支持的协调工作(CSCW)实现技术主要包括采用 TCP/UDP 协议，以及基于分布式中间件技术(DCOM 和 CORBA)实现节点管理和有序群组通信技术. 这些特点都限制了客户/服务器结构不可能适用于动态、节点平等的点到点(P2P)网络.

Napster 音乐下载软件的成功推动了 P2P 技术的发展，基于 P2P 的应用也越来越多. P2P 网络是组建在现有网络基础上的一个虚拟功能网，强调节点自治和直接通信. SUN 公司推出的 JXTA 为 P2P 的开发提供了一个基础平台. JXTA 将有相同爱好或兴趣的节点组成一个点组，在组的范围内管理节点和资源，这些都符合协同工作本质要求. SUN 公司提供了 JXTA 不同操作系统、不同编程语言的实现版本，从而屏蔽了不同操作系统、编程语言、网络传输协议之间的差异. 同时 JXTA 还是一个开源项目便于定制和集成新的应用. 笔者在 JXTA 的平台基础上提出了一个 P2P 模式下 CSCW 节点管理和群组通信的算法(JLSR). JLSR 主要满足如下要求：

(1)提供一套统一 P2P 模式下 CSCW 节点管理和有序群组通信的操作原语；

收稿日期：2005-12-20

作者简介：马 勇(1977-)，男，武汉大学博士研究生.

(2)为消息的传递提供一个统一的接口;

(3)通过对消息实行认证和加密实现安全通信和节点评估;

(4)实现版本号和内容的绑定,对消息的传递实现增量传输.

1 相关工作

Sun 和 ELLise 提出了协同工作的 3 个一致性:因果一致、结果一致和对象一致[1].这 3 个一致性是衡量协同操作算法正确性的标准.何发智提出了一个 CoCADToolAgent 系统,该系统采用 TCP 作为通信协议,可以实现 AutoCAD 软件的在线迅即协作[2].利用中间件技术(DCOM 和 CORBA)也是 CSCW 典型的研究方向.利用 DCOM 技术,Jeffrey D. Campbell 对微软的 Office 组件 Visio 进行了研究,提出了一个基于 C/S 结构的共享 Visio 系统 CoDiagram[3]. NetFeature[4]是利用 CORBA 技术来实现 CSCW 技术的典型代表,但是他们都需要由中央服务器来转发消息.以上这些协同都属于典型的集中式协同建模系统,这样的系统结构简单、并发控制容易,但存在网络负载重、通信延迟明显、中心服务器易成瓶颈和单点依赖等问题.

复制式 CSCW 典型应用是复制式同步建模系统,德国 Stork 等研发的 CSCW-FeatureM[5] 和 TOBACO[6]是复制式同步建模系统的典型代表.但这两个系统仍然采用 CORBA 的通信转发服务实现通信支持,因此不可能摆脱通信转发的痕迹.

P2P 模式 CSCW 是复制式 CSCW 的新的发展方向,Ozalp 等开发 Anthill [7]和 XEXÉO [8]提出的基于 Ontologies 的协同编辑是 CSCW 采用 P2P 模式的典型应用. Anthill 主要是用来开发文件共享和网格计算系统;XEXÉO 虽然给出了一个协同编辑的应用,但是更多的是强调通过 JXTA 提供的查询服务、成员资格服务和管道通信核心服务实现基于 Ontologies 的协同编辑,并没有给出如何建立和维护 P2P 连接以及安全有效的群组通信.

2 JLSR

2.1 定 义

这里给出了与群组通信和 CSCW 一致性相关的概念.群组通信主要涉及节点和 P2P 的连接,CSCW 一致性主要包括顺序、因果、操作、对象和结果一致性,在此基础上给出了这些定义的数学表达形式.

定义 1 设 T 代表协同任务,N 是加入 T 的节点的个数,$p(i)$ 是第 i 个加入 T 的节点,则加入 T 的节点集合 P_N^T 可以定义为:$P_N^T=\{p(i)\mid 0<i\leqslant N\}$,显然,$p(1)$ 创建 T.

定义 2 设 $i\neq j$,$p(i)$ 是第 i 个加入 T 的节点,则有 $p(i)\rightarrow p(j)$,表示建立了节点 $p(i)$ 到节点 $p(j)$ 的连接. $p(i)\leftrightarrow p(j)$ 表示 $p(i)\rightarrow p(j)$ 和 $p(j)\rightarrow p(i)$ 同时成立,$p(i)\leftrightarrow p(i)$ 表示建立了自连接.

定义 3 点到点对等模式:

$$\text{任意}((p(i),\ p(j))\rightarrow p(i)\leftrightarrow p(j)\qquad 1\leqslant i,\ j\leqslant N\quad , \tag{1}$$

$$\text{不存在}((p(i)\leftrightarrow p(j))\quad ,\quad 1\leqslant i\leqslant N,\ j>N\quad . \tag{2}$$

定义 4 $O_{p(s)}(m)=<D_m,B_m,R_m>$ 表示节点 $p(s)$ 上执行的第 m 个操作 D_m,操作对象 B_m,执行结果 R_m. $O_{p(s)}(m)>O_{p(t)}(n)$ 表示节点 $p(s)$ 上的第 m 个操作先于节点 $p(t)$ 上的第 n 个操作发生.

定义 5 顺序一致性:节点 $p(s)$ 上操作 m 先于操作 n 发生 $O_{p(s)}(m)>O_{p(s)}(n)$,那么节点 $p(t)$ 上按同样的顺序执行操作($O_{p(t)}(m)>O_{p(t)}(n)$).

$$\forall(p(s),p(t),m,n)\{m>n\ \wedge\ O_{p(s)}(m)>O_{p(s)}(n)\rightarrow O_{p(t)}(m)>O_{p(t)}(n)\}\quad .$$

定义 6 因果一致性:节点 $p(s)$ 上操作 m 先于节点 $p(t)$ 上操作 n 发生 $O_{p(s)}(m)>O_{p(t)}(n)$,那么节点 $p(s)$ 和节点 $p(t)$ 上先执行 m 操作,后执行 n 操作 $O_{p(s)}(m)>O_{p(s)}(n)$ 和 $O_{p(t)}(m)>O_{p(t)}(n)$.

$$\forall\ (p(s),p(t),m,n)\{O_{p(s)}(m)>O_{p(t)}(n)\rightarrow O_{p(s)}(m)>O_{p(s)}(n)\ \wedge\ O_{p(t)}(m)>O_{p(t)}(n)\}\quad .$$

定义 7 操作一致性:节点 $p(s)$ 执行 m 操作和节点 $p(t)$ 执行 m 操作的命令是一样的.

$$O_{p(s)}(m)\ D_m=O_{p(t)}(m)\ D_m\quad .$$

定义 8　对象一致性:节点 $p(s)$ 执行 m 操作和节点 $p(t)$ 执行 m 操作的对象是一样的.

$$O_{p(s)}(m)\ B_m = O_{p(t)}(m)\ B_m \quad .$$

定义 9　结果一致性:节点 $p(s)$ 执行 m 操作和节点 $p(t)$ 执行 m 操作的结果是一样的.

$$O_{p(s)}(m)\ R_m = O_{p(t)}(m)\ R_m \quad .$$

2.2　标　　记

实现安全可靠有序的群组通信技术,系统采用公钥和对称密钥相结合的加密算法.所用标记如下:

$E_{KU}(p(i))$:用节点 $p(i)$ 的公钥进行加密.$D_{KP}(p(i))$:用节点 $p(i)$ 的私钥进行解密.$\mathrm{Sig}_{KP}(p(i))$:用节点 $p(i)$ 的私钥进行签名,$\mathrm{Ver}_{KU}(p(i))$:用 $p(i)$ 的公钥验证签名.E_K:用公共密钥 K 进行加密,D_K:用公共密钥 K 进行解密.SetDone($p(i)$):节点 $p(i)$ 保留已经执行任务序列集合,SetWait(($p(i)$):节点 $p(i)$ 等待执行任务集合,MaxSerDone ($p(i)$):节点 $p(i)$ 完成任务的最大序列号.NewSerAlloted($p(i)$):节点 $p(i)$ 向全局序列服务器(GSS)申请全局序列号,MaxSerAllot:GSS 已经分配任务的最大序号.

2.3　JLSR 原语

JLSR 采用点组作为资源管理的单位,其点组结构如图 1 所示.JLSR 点组内的节点可以分为参与者(Actor)和 GSS.参与者主要完成具体的操作.全局序列服务器主要向参与者提供全局序列号,同时缓存参与者所执行的操作序列,向参与者提供操作序列的副本.JLSR 实现 P2P 模式下 CSCW 主要完成的两个方面的工作:P2P 系统建立和维护,安全有效的群组通信.P2P 系统建立和维护主要通过加入和退出两个原语实现,安全有效的群组通信通过发送和接收两个原语保证在点组节点之间进行安全有序的通信.

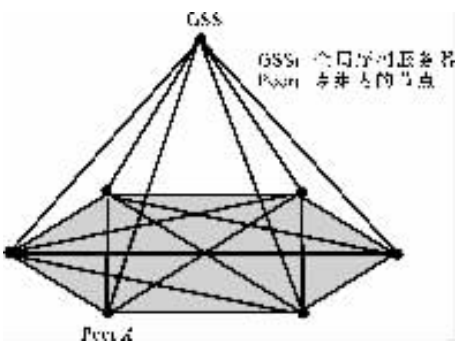

图 1　JLSR 系统结构图

(1) 节点加入　假设新加入的节点是 $p(i)$,根据定义知道已经有 $i-1$ 个节点加入点组,那么原有的节点为任意 $p(j)(0<j<i)$.

建立 $p(i)$ 到 $p(i)$ 的连接:　$p(i)\leftrightarrow p(i)$　.　(3)

建立 $p(i)$ 到 $p(j)$ 的连接:　任意 $j\{\ p(i)\rightarrow p(j)\mid 0<j<i\}$　.　(4)

建立 $p(j)$ 到 $p(i)$ 的连接:　任意 $j\{\ p(j)\rightarrow p(i)\mid 0<j<i\}$　.　(5)

节点加入算法满足定义 3 的两个条件(1)和(2),证明如下:

当节点 $p(1)$ 加入时,执行式(3),很明显满足定义 3.假如 P_K^T,节点加入算法满足定义 3.那么节点 $p(K+1)$ 加入时,要执行式(3),建立$p(K+1)\leftrightarrow p(K+1)$,产生了一个新的连接.执行式(4),建立任意 $j\{\ p(K+1)\rightarrow p(j)\mid 0<j<K+1\}$,生成 K 个新的不同连接.执行式(5),建立任意$j\{\ p(j)\rightarrow p(K+1)\mid 0<j<K+1\}$,生成了 K 个新的不同连接.如果 P_{K+1}^T 不满足定义 3 的要求,只可能是存在 $p(j)\ (0<j\leqslant K+1)$ 和$p(K+1)$ 不满足$p(j)\leftrightarrow p(K+1)$,否则和假设 P_K^T 相矛盾.如果不满足$p(j)\rightarrow p(K+1)$,与式(4)相矛盾;如果不满足$p(K+1)\rightarrow p(j)$,与式(5) 相矛盾;如果不满足$p(K+1)\rightarrow p(K+1)$,与式(3) 相矛盾.所以$p(K+1)$ 加入到 P_K^T,P_{K+1}^T 满足定义 3 的要求.

(2) 节点退出　假设节点 $p(i)$ 离开点组,那么其他节点为 $\forall j\{\ p(j)\mid 1\leqslant j\leqslant N$ 且 $j\neq i\}$,该算法描述如下:

断开其他节点 $p(j)$ 到节点 $p(i)$ 的连接,取消 $p(j)\rightarrow p(i)$　.　(6)

断开节点 $p(i)$ 到其他节点 $p(j)$ 的连接,取消 $p(i)\rightarrow p(j)$, $p(j)$ 成为 $p(j-1)-1, N=N-1$　.(7)

取消 $p(i)\leftrightarrow p(i)$　.　(8)

利用同样的方法,可以证明节点退出算法也是正确的.

(3) 发送消息　节点向 GSS 申请全局序列号,然后对所要发送的消息进行加密(如图 2 所示),发送协议具体执行步骤如下:

如果节点 $p(j)$(假设节点 $p(j)$ 发消息) 要执行新的操作并且 MaxSerDone($p(j)$) 等于 MaxSerAllot,可以向 GSS 申请新的任务序列号 NewSerAlloted(($p(j)$)　.　(9)

节点 ($p(j)$) 执行操作 object,将 E_K(NewSerAlloted($p(j)$), object, ID(($p(j)$)), $\mathrm{Sig}_{KP(p(j))}$(ID($p(j)$)))

和 $E_{KU(p(i))}(K)$ 打包成消息发送给点组内的其他节点 $p(i)$(包括节点($p(j)$) . (10)

(4) 接收消息 节点首先对接收到的消息进行解密(如图 3 所示),然后根据相应的算法执行所接收到的命令,接收协议具体执行步骤如下:

对于接收的消息(假设节点 $p(i)$ 接收节点 $p(j)$ 发送的消息),执行 $D_{KP(p(i))}(E_{KU(p(i))}(K))$,$D_K$(NewSerAlloted($p(j)$), object, ID($p(j)$), $Sig_{KP(p(j))}$(ID($p(j)$)), $Ver_{KU(p(j))}(Sig_{KP(p(j))}ID(p(j)))$. (11)

将<NewSerAlloted($p(j)$)RecMessSer, object>插入到 SetWait($p(j)$),如果 SetWait($p(j)$)最小的 NewSerAlloted($p(j)$等于 MaxSerDone($p(j)$)加 1,执行 SetWait($p(j)$)中合适任务(SetWait($p(j)$)中任务序列号和 MaxSerDone($p(j)$)相连的任务),将这些任务序列插入到 SetDone($p(j)$). (12)

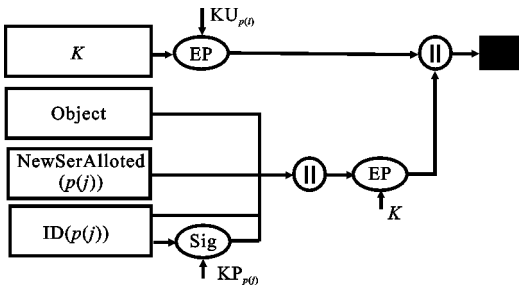

图 2 发送消息加密过程

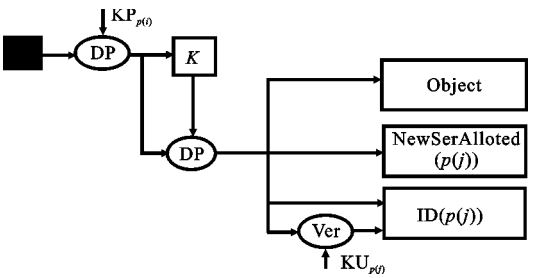

图 3 接收消息解密过程

在发送原语中,式(10)用对方公钥对会话密钥进行加密,然后用会话密钥对传送的对象、身份标识以及身份标识的签名进行加密. 在接收原语中,式(11)用自己的私钥解出会话密钥,然后用会话密钥解密收到的消息,通过身份标识和身份标识的签名来验证消息发送者的身份. 从而可以避免第三方攻击,实现对节点的操作实现身份追踪. 发送和接收原语可以满足 CSCW 的要求,并且提供了安全可靠的群组通信.

2.4 一致性分析

衡量点到点网络下各个节点之间的一致性,对于协同参与者,最主要的是结果一致性. 如果协同参与者执行的操作同时满足操作一致性和对象一致性,那么各个协同参与者肯定会得到结果一致性. 采用远程对象序列化方法将操作和对象一起传递,从而保证操作和对象的绑定,存在如下定理.

定理 1 如果多个操作同时满足顺序一致性与操作一致性和这些操作同时满足因果一致性与顺序一致性是等价的.

证明 如果多个操作中的任何两个操作满足顺序一致性和操作一致性,存在 $O_{p(t)}(m) = O_{p(s)}(m)$,$O_{p(t)}(n) = O_{p(s)}(n)$ 和 $O_{p(s)}(m) > O_{p(s)}(n)$,$O_{p(t)}(m) > O_{p(t)}(n)$,那么肯定有 $O_{p(s)}(m) > O_{p(t)}(n)$ 和 $O_{p(t)}(m) > O_{p(s)}(n)$. 所以当多个操作同时满足顺序一致性与操作一致性时,这些操作肯定同时满足因果一致性和顺序一致性.

如果多个操作中的任何两个操作满足顺序一致性和因果一致性,存在 $O_{p(t)}(m) = O_{p(s)}(m)$,$O_{p(t)}(n) = O_{p(s)}(n)$ 和 $O_{p(s)}(m) > O_{p(t)}(n)$ 可以推出 $O_{p(s)}(m) > O_{p(s)}(n)$ 和 $O_{p(t)}(m) > O_{p(t)}(n)$. 所以当多个操作同时满足因果一致性与操作一致性时,这些操作肯定同时满足因果一致性和顺序一致性. 证毕.

式(9)确保节点发送的操作序列号大于其他节点已经发送的命令,式(12)确保各个节点按序执行接收的操作. 从而,确保所有节点操作满足因果一致性和操作一致性. 根据定理 1,所有节点操作满足操作一致性和对象一致性,各个节点可以得到结果一致性.

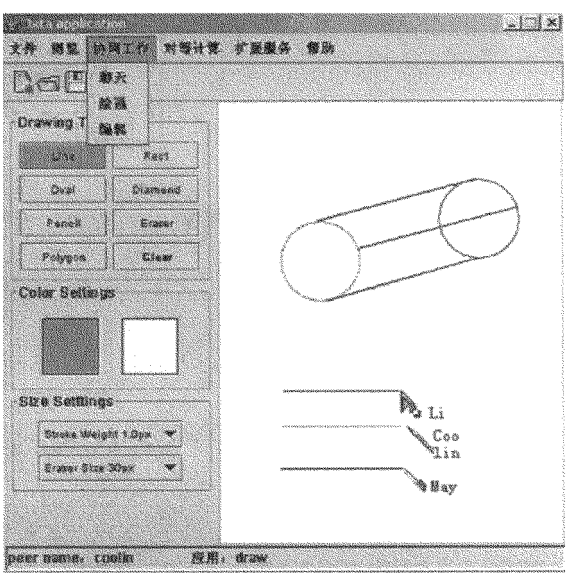

图 4 JLSR 协同绘图实例

3 实　　现

在上面操作原语的基础上实现了 P2P 模式下协同编辑和协同绘图,以协同绘图作为该算法的一个实例来说明该算法在实际中的应用. 图 4 是各个节点进行协同绘图的一个瞬间快照. may,Coolin 和 li 分别绘制了圆柱体的后面、前面和侧面. 图 4 以不同的颜色代表不同节点,不同的鼠标表明了节点当前鼠标所在的位置,实现多鼠标感知,方便节点交流.

4 结 束 语

客户/服务器结构的 CSCW 软件存在一个中央服务器来管理各个节点的运行和消息转发. 这必然会引起服务器的繁忙和系统对服务器的过度依赖. P2P 网络具有动态和平等的特点,更符合 CSCW 的本质. 文中定义了 P2P 模式下 CSCW 加入、离开、发送和接收原子操作,实现异构网络下节点管理和群组通信,为不同应用提供统一的接口,从具体应用中抽象出中立的接口. 对现有单机版的软件改造,使其支持节点之间协同工作是今后努力方向.

参考文献:

[1] Sun C Z, Ellis C. Operational Transformation in Real-time Group Editors: Issues, Algorithms, and Achievements [A]. ACM CSCW[C]. Seattle: ACM Press, 1998. 59-68.

[2] He Fazhi, Wang Shaomei, Sun Guozheng, et al. Computer-aided Tool for Collaborative Integrated Design Environments [J]. Journal of Mechanical Engineering, 2002,38(6):16-20.

[3] Campbell J D. Interaction in Collaborative Computer Supported Diagram Development[J]. Computers in Human Behavior, 2004, 20(2): 289-310.

[4] Zhou Xun, Li Jie, He Fazhi. Collaborative Solid Modeling System Over Internet [A]. China National Conference on CAD&CG' 02[C]. Guiyang: Tsinghua University Press, 2002. 751-754.

[5] Stork A, Lukas U V. Schultz R. Enhancing a Commercial 3D CAD System by CSCW Functionality for Enabling Co-operative Modeling Via WAN [A]. ASME Design Engineering Technical Conference [C]. Atlanta Georgia: DETC1998/CIE-5711, 1998. 306-315.

[6] Lukas U V. Collaborative Geometric Modeling Using CORBA Services [A]. ECSCW'97 Workshop on Object Oriented Group Ware Platforms OOGP'97[C]. Lancaster UK;ACM Press, 1997. 91-92.

[7] Babaoglu O, Meling H, Montresor A. Anthill: a Framework for the Development of Agent-based Peer-to-Peer Systems [A]. The 22th International Conference on Distributed Computing Systems (ICDCS '02) [C]. Vienna, Austria: IEEE Computer Society, 2002. 15-22.

[8] Xexéo G, de Souza J M. Peer-to-Peer Collaborative Editing of Ontologies[A]. The Eighth International Conference on CSCW in Design[C]. Xiamen: IEEE Computer Society Press, 2004. 186-190.

(编辑:齐淑娟)