一种对等社区网络多层次可靠访问控制机制

徐小龙,窦孝晨
(南京邮电大学 计算机学院,江苏 南京 210003)

摘 要:在P2P计算环境中进行资源的可靠共享需要解决分散于各个节点上的资源的访问控制问题。当前的各种访问控制模型及策略不能很好地适用于P2P计算环境。提出了一种适用于对等社区网络的多层次可靠访问控制机制,可根据节点间关系、资源类别和自身当前策略等因素来灵活设置符合当前需要的访问权限,从而更可靠地实现P2P计算环境中各种资源的充分共享。详细描述了对等社区网络多层次可靠访问控制机制的体系结构、功能模块、工作流程以及相应的实验系统。文中的研究成果为设计更加可靠的P2P软件平台和应用提供了有益的参考。

关键词:对等计算;安全;访问控制
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2011)04-0044-04

A Multi-Level Secure Access Control Mechanism for P2P Community Networks

XU Xiao-long, DOU Xiao-chen
(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Sharing of distributed resources in P2P computing environment reliably, the issue of access control needs to be solved firstly, because the current access control models and strategies are not well applied to P2P computing environment. A new multi-level secure access control mechanism is proposed for P2P community networks, which can set required access rights, according to the relationship between nodes, resource types and peer's own strategy, etc., the multi-level secure access control mechanism helps to share resources fully. Describe the architecture, function modules, workflow and the corresponding experimental system of this mechanism. The study result of this paper provides a useful reference for designing more reliable P2P software platforms and applications.

Key words: peer-to-peer computing; security; access control

0 引 言

P2P计算(Peer-to-Peer Computing)技术[1-3]为网络节点之间的各种资源(CPU、存储空间、数据信息等)的直接共享提供了一种高效的途径。每个对等节点(Peer)都可同时成为资源的使用主体和提供主体。然而在包含各种资源的P2P计算环境中进行资源的充分共享重点要解决的问题之一就是分散于各个节点上的资源的访问控制问题。

现有的各种的访问控制模型及策略,如自主访问控制(Discretionary Access Control,简称DAC)、强制访问控制(Mandatory Access Control,简称MAC)和基于角色的访问控制(Role-based Access Control,简称RBAC),以及应用于分布式系统中的基于任务的授权控制模型(Task-based Authentication Control,简称TBAC)、基于任务和角色的访问控制模型(Task-Role-based Access Control,简称T-RBAC)以及被称作下一代访问控制模型的使用控制模型(Usage Control,简称UCON,也称为ABC模型)等等[4-6],都是应用于传统的基于C/S(Client/Server,客户/服务器)结构的集中式计算环境或是传统的、相对稳定的分布式计算环境,不能很好地适用于P2P计算环境。Gummadi等[4,7]提出基于可信和信誉模型以及安全组模型来实现P2P系统的组信任访问控制模型,并用RBAC实现了P2P系统的安全策略;Tran等[4,8]提出一种可信访问控制框架,该框架包括节点公平参与机制和可信访问控制机制,将DAC扩展到P2P文件共享系统中。这些研究成果都具有一定的参考价值,但机制常常过于复杂或是考虑不够全面。

收稿日期:2010-08-20;**修回日期**:2010-11-29
基金项目:教育部博士点基金(20093223120001);教育部科技发展中心网络时代的科技论文快速共享专项研究资助项目(2009117);国家重点基础研究发展计划(973计划)项目(2011CB302903);江苏省科技支撑计划项目(BE2009158);江苏省高校自然科学研究项目(09KJB520010)
作者简介:徐小龙(1977-),男,副教授,博士,硕士生导师,计算机学会会员,研究方向为网络计算、计算机软件技术等。

针对这种情况,文中的贡献在于:提出了一种适用于对等社区网络的多层次可靠访问控制机制,使对等节点可根据节点间关系、资源类别、自身当前策略来灵活设置符合当前情况的合理的访问权限,从而可以更可靠地实现P2P计算环境中各种资源的充分共享。

1 对等社区网络

P2P计算技术的核心思想是强调节点的地位对等性,这就和互联网(Internet)中传统的、不对称的C/S计算(Client/Server Computing,客户/服务器计算)模式或是B/S计算(Brower/Server Computing,浏览器/服务器计算)模式有明显的区别。P2P网络中的每个节点(Peer)可以不经过服务器直接进行消息通信、文件交互和协同工作,这就可以避免系统中因为节点规模的扩大造成服务器负载过重从而成为系统性能瓶颈的问题。[3,9]

P2P网络系统所采用的拓扑结构可以分为三种类型[10,11]:

(1)集中式P2P网络,采用中心化拓扑(Centralized Topology)(如Napster[12]),在服务器端集中存储全局的资源目录,而资源都存放于Peer节点上。

(2)纯分布式P2P网络,采用全分布式非结构化拓扑(Decentralized Unstructured Topology)(如Gnutella[13])或全分布式结构化拓扑(Decentralized Structured Topology)(如Tapestry[14]),即不需要存储全局资源目录的服务器,资源均存放于Peer节点上。

(3)混合式P2P网络,常采用半分布式拓扑(Partially Decentralized Topology)(如BitTorrent[15]),网络中存在多个服务器作为Super Peer,构成服务器集群。服务器既可存储资源,也存储资源目录,甚至可以作为覆盖网路由转发节点,功能灵活,性能、可扩展性较好。

"物以类聚,人以群分",群体与集群成为人类社会生活中最常见、最普遍的社会现象[16]。一些P2P网络系统中提出的社区概念与人类社会中的群体理论极为契合。因此,类比人类社会的群体结构,可构建一种基于P2P计算技术的对等社区网络。对等社区网络可将整个P2P网络共享空间按节点及其所有者的属性、行为或兴趣划分为若干对等组(Peer Group)。Peer可以互相合作来建立自我组织、自我管理的对等组。通过对信息资源的重组,以期建立开放的及专业化的对等组使兴趣相同的节点可更高效地相互合作,简化信息资源的存储、查找和使用,从而提高资源利用率。Peer也可以同时属于不同服务类别的对等组;某一对等组中的成员也会因为资源、兴趣或需求等情况的变化而加入其它对等组,或是退出原本加入的对等组。对等组内的Peer可基于DHT技术直接与组内的其它Peer进行通信和定位资源;Peer将服务器作为P2P覆盖网的组间路由节点来与其它对等组的Peer进行通信。

2 对等社区网络多层次可靠访问控制机制

2.1 体系架构

在对等社区网络系统中实现数据共享、分布式计算或分布式存储等应用时,首先要解决的就是如何认证Peer的身份和控制其访问权限。访问控制机制目的是为检测和防止系统中的未经授权的操作,对资源予以保护所采取的软硬件措施和一系列管理措施等。访问控制一般是在操作系统的控制下,按照事先确定的规则决定是否允许主体访问客体,它贯穿于系统工作的全过程,文中提出的对等社区网络多层次可靠访问控制机制正是在本地操作系统和共享资源之间加入了身份认证和访问控制机制,在为用户提供更好的访问控制服务的同时,维护P2P平台的分布式结构,满足其安全需求。

对等社区网络多层次可靠访问控制机制中的"多层次"和"可靠性"主要体现在以下三个层面:

层1:分布式成员资格审核——新成员资格审核权被分散到整个对等网络中,网络中的每一个成员都拥有部分审批权。当新成员获得一定阈值下的成员批准,则该新成员就获得了加入对等网络的合法资格。

层2:多级权限控制——各节点和对等组均被资源提供节点自主地赋予相应权限,主要包含特别好友、好友、陌生人、黑名单四种访问权限,节点可以指定其它节点可以访问的本地目录、子目录、文件的资源范围和操作权限。

层3:节点行为评估——根据基于交互情况的分布式评估机制来确定节点的可信值,依此来决定该成员是否能继续留在网络中和具有什么样的资源访问权限。当发现某些成员发布恶意信息或可信值低于系统规定的阈值时,通过发布黑名单来驱逐这些节点,从而维持系统的稳定性、可靠性和可持续性。

2.2 功能模块与工作流程

文中的研究主要是基于集中式P2P网络或是混合式P2P网络来展开的。应用多层次可靠访问控制机制的对等社区网络中的服务器仅存放全局节点目录与资源列表信息,Peer之间的实际交互则通过服务器,避免服务器成为系统瓶颈。

下面分别描述服务器端对等节点端模块内容。

1)服务器端模块。

服务器端存放了各对等节点的注册信息和所有用户共享资源的目录列表,而具体资源文件仍存储于各对等节点上。

具体功能包括：

(1)节点目录管理。

每个对等节点首先要在服务器上进行注册，通过服务器认证后，节点会获得一个唯一的PID(Peer ID，节点标识符)，然后才能与服务器和其它节点进行交互。注册后服务器给每个用户设定初始积分等级及评价值。

(2)资源列表管理。

每个对等节点将自己可共享的资源服务器端发布到全网上，以供其它节点检索。服务器系统显示各对等节点每日更新的共享和推荐资料，删除被用户取消共享的资料。

(3)节点状态监控。

当对等节点加入网络系统时，系统将节点状态会由0修改为1，标明节点当前处于在线(Online)状态。

(4)节点评价管理。

系统管理并负责更新各对等节点的可信值，以及向评价不良的用户提出警告，或将恶意节点驱逐出网络系统。

模块的运行流程如图1所示。

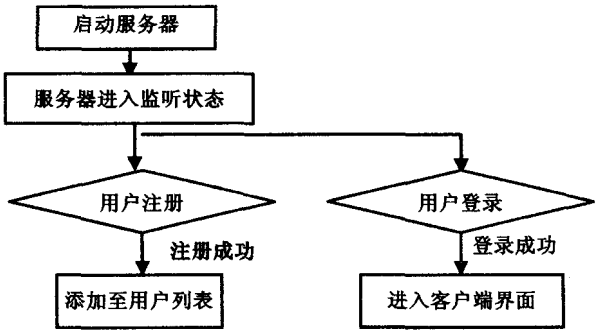

图1 服务器端工作流程

2)对等节点端模块。

基于P2P技术，每个对等节点既是服务器又是客户端，对等节点端模块是整个对等社区网络系统的重要部分。

具体功能包括：

(1)资源管理。

负责对可共享内容进行管理，可按照资源共享的权限将资源放置不同的本地文件夹中，并以共享列表的形式提供给节点参考。

(2)资源搜索与获取。

负责按用户输入的资源名称来搜索合适的文件资源，显示所有搜索到的资源列表，用户可选择需要下载的资源，然后直接从资源所在的Peer中下载该文件(如果该Peer允许下载)。

(3)资源首页。

负责显示服务器上存在的所有共享资源列表，用户可从中挑选需要的资源，然后直接从资源所在的Peer中下载该文件。

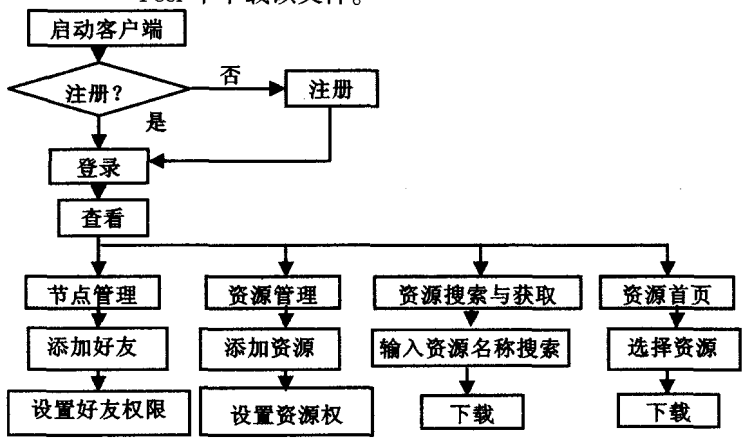

图2 对等节点端工作流程

(4)节点管理。

负责管理其它节点列表，并将节点与自己的关系分为4个级别：A级别，特别好友(查看自己所有共享资源)；B级别，一般好友(可查看普通的共享资源)；C级别，陌生人(经过允许可以查看指定的共享资源)；D级别，黑名单(不允许查看任何资源)。模块的运行流程如图2所示。

3 实验系统构建

为了验证文中提出的多层次可靠访问控制机制的功能与性能的可行性与实用价值，构建对等社区网络资源共享系统。系统采用Visual C++ 6.0开发出来，并将系统部署于基于Intranet的实验室局域网环境中。服务器端系统的共享的资源列表界面如图3所示。

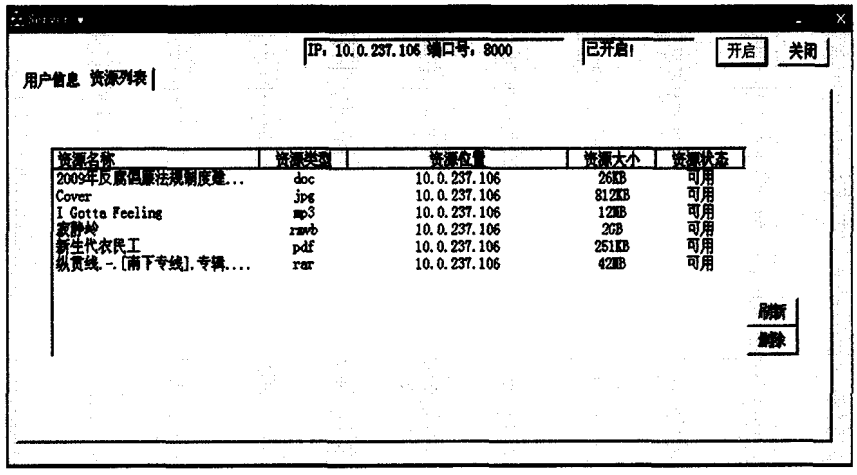

图3 用户信息以及共享的资源列表

对等节点端系统的部分界面如图4~6所示。用户可通过图4所示界面的搜索功能查看要下载的资源,或利用资源首页浏览全部的资源,也可以选择本地资源进行共享设置。

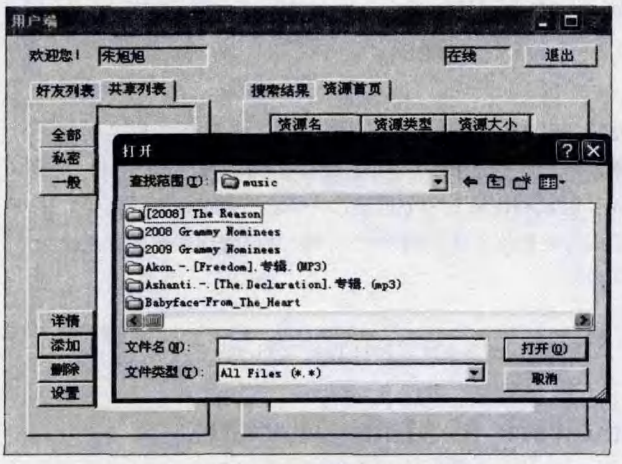

图4　对等节点端系统的部分界面

用户选中要共享的文件后,可以设置共享的级别,如图5所示。

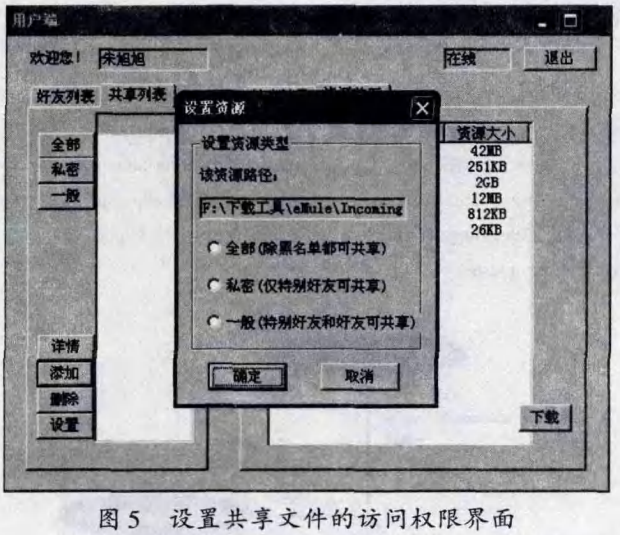

图5　设置共享文件的访问权限界面

对等节点端系统的用户管理模块,如图6所示,用户可根据与自己的关系为将其它节点用户设置相应的级别。

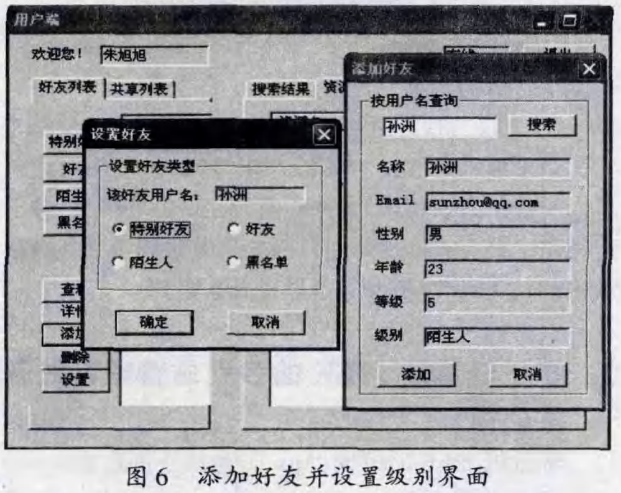

图6　添加好友并设置级别界面

4　结束语

文中研究成果将弥补目前在P2P网络系统中访问控制机制的不足,其价值在于不但可以进一步保障P2P网络应用系统的安全,而且为在P2P应用如此普及的今天设计更加可靠的P2P软件平台和应用提供了参考,由此而设计和实现的高效的各类P2P软件将有广泛的应用前景。

参考文献:

[1] 徐小龙, 王汝传. 一种基于多移动Agent的对等计算动态协作模型[J]. 计算机学报, 2008,31(7):1261-1266.

[2] 徐小龙, 王汝传. 对等计算中的基于多移动Agent的协作联盟机制[J]. 电子与信息学报, 2007, 29(2): 345-349.

[3] 陈贵海. 对等网络: 结构、应用与设计[M]. 北京:清华大学出版社,2007.

[4] 林　闯, 封富君, 李俊山. 新型网络环境下的访问控制技术[J]. 软件学报,2007,18(4):955-966.

[5] 杨秋伟, 洪　帆,杨木祥,等. 基于角色访问控制管理模型的安全性分析[J]. 软件学报, 2006,17(8):1804-1810.

[6] 桂劲松, 陈志刚, 郭　迎. 基于改进UCONA的服务网格授权策略规范[J]. 华中科技大学学报(自然科学版), 2008,36(8):75-78.

[7] Gummadi A, Yoon J P. Modeling group trust for peer-to-peer access control[C]//In:Proc. of the 15th Int'l Workshop on Database and Expert Systems Applications. [s. l.]: IEEE Computer Society, 2004:971-978.

[8] Tran H, Hitchens M, Varadharajan V,et al. A trust based access control framework for P2P file-sharing systems[C]//In: Proc. of the 38th Hawaii Int'l Conf. on System Sciences (HICSS). Hawaii: IEEE Computer Society, 2005.

[9] 吴国庆. 对等网络技术研究[J]. 计算机技术与发展, 2008, 18(7):100-103.

[10] 罗杰文. Peer to Peer (P2P) 综述[EB/OL]. 2005-11-03. http://www.intsci.ac.cn/users/luojw/papers/p2p.htm.

[11] Lua E K,Crowcroft J, Pias M, et al. A survey and comparison of peer-to-peer overlay network schemes[J]. Communications Surveys & Tutorials,2005,7(2):72-93.

[12] Napster[EB/OL]. 2010-04-29. http://www.napster.com.

[13] Gnutella[EB/OL]. 2010-04-29. http://www.gnutella.com/news/4210.

[14] Tapestry[EB/OL]. 2010-04-29. http://en.wikipedia.org/wiki/Tapestry_(DHT).

[15] BitTorrent[EB/OL]. 2010-04-29. http://www.bittorrent.com/introduction.html.

[16] Newcomb T M. Readings in social psychology[M]. New York: Holt, Rinehart & Winaton,1969.