文章编号:1671-6833(2006)03-0093-05

一种实用的P2P文件共享系统访问控制框架

何 伟[1], 薛素静[2], 孔梦荣[3]

(1.郑州大学成人教育学院,河南 郑州 450052;2.华北水利水电学院信息工程系,河南 郑州 450008;
3.中原工学院计算机科学系,河南 郑州 450007)

摘 要:由于P2P环境自身的分布性与匿名性等,传统的访问控制机制无法为P2P共享文件系统提供高效、安全的访问控制服务.为此,基于信任推荐机制与公平参与机制,提出了一种新的访问控制框架.这一框架能够在不改变P2P环境本身特性的条件下,实现高效文件访问控制服务.

关键词:对等网络;文件共享系统;访问控制

中图分类号:TP 391.1 **文献标识码**:A

0 引言

近年来,P2P文件共享系统做为一种新的信息交换途径得到了广泛应用.随着技术日趋成熟,P2P文件共享技术已经能够支持多种数字媒体类型以及满足用户不同需求[1].然而,已有的P2P文件共享系统普遍缺乏安全高效的访问控制机制,这些系统完全依赖用户自觉控制本身的下载行为,却没有采用任何技术措施对恶意用户或有害内容进行监测,导致任意用户可以随意下载系统文件.这种严重的安全缺陷大大制约了P2P文件共享系统被企业和商家广泛使用.

针对该问题,笔者提出一种基于信任评估的访问控制机制.利用该机制,P2P文件共享系统可在不改变P2P系统分布式特性的条件下,实现高效、安全的文件访问控制.

1 访问控制的需求

P2P文件共享系统对访问控制机制的需求可归纳如下:

无集中式控制:P2P环境中不存在传统控制模型通常使用的集中式权威中心.P2P用户具有高度自治性,能够存储和管理自身的访问控制策略.因此,访问控制机制必须符合P2P环境的分布式特性.

区分用户类别:用户匿名性是P2P系统的另一特性.P2P用户通常不愿泄露自己的真实身份.一般用户不知道通信伙伴是谁,充当服务器的用户(以下简称为"服务器用户")很可能接收到来自陌生用户(以下简称为"客户端用户")的文件访问请求.从服务器用户的角度来看,客户端用户存在差异.因此,访问控制机制必须使服务器用户能够区分客户端用户类别并分配相应访问权限.特别是处理来自陌生客户端用户的访问请求时.

鼓励文件共享:用户加入P2P文件共享系统的动机是获得系统中丰富的共享文件.然而,访问控制机制势必减少用户得到文件的机会,从而导致用户不愿加入共享系统.因此,访问控制机制必须避免自身的负面影响,应提供鼓励用户共享自身文件的功能.

控制恶意文件扩散:最后,访问控制机制必须能够有效控制恶意文件(如病毒、木马)的扩散,同时能够追踪和惩处恶意用户.

2 P2P文件共享系统

P2P文件共享系统使任意两个用户能够直接访问对方硬盘并且下载文件.为此,用户必须能够支持两个基本接口:

* 资源发现接口:该接口使用户能够发现其它用户当前提供的共享文件;同时,该接口也使其它用户能够了解该用户当前提供的共享文件.P2P资源发现算法[2,3]不是本文的重点,不再赘

收稿日期:2006-04-30;**修订日期**:2006-06-06

基金项目:国家自然科学基金资助项目(60472022);河南省软科学资助课题(0313025300,0313033100).

作者简介:何 伟(1969-),女,河南信阳人,郑州大学讲师,硕士,主要从事分布式计算和神经网络方面的研究.

述.

* 文件传输接口:该接口负责将本地文件传输给其它用户.现有的P2P文件共享系统一般在应用层之上实现该接口.

已有的P2P文件共享系统允许这两个接口直接访问本地文件系统,任由客户端用户自由下载所有本地共享文件,因此存在很大的安全隐患.

3 访问控制框架

笔者提出一种基于自主访问控制模型(discretionary access control, DAC)[4]的访问控制框架.服务器用户根据每个共享文件的大小和内容对其分级,并为共享文件指定两个对应门限PT(Parameter Threshold).当客户端用户希望从服务器用户处下载某个共享文件时,他必须具有不小于该文件对应门限的访问值AV(Access Values).计算AV有4个参数:直接信任DT(Direct Trust)、间接信任IDT(Indirect Trust)、直接贡献DC(Direct contribution)、间接贡献IC(indirect Contribution).客户端用户收集计算AV所需的推荐意见.每次下载结束后,客户端用户和服务器用户都将根据本次下载的满意度SL(Satisfaction Level)更新DT与DC,从而决定这两个用户AV值的变化.

该框架也能够实现P2P用户间协作式访问控制服务.客户端用户计算自身的IDT和IDC时,必须以其它用户对其评价为依据.因此,P2P用户间存在着显式的协作关系.通过协作式访问控制服务,P2P用户可以追踪和隔离恶意用户.

3.1 整体结构

如图1所示,本文提出的访问控制框架在传统P2P接口和本地文件系统之间插入了"认证与访问控制层",该层功能包括:认证P2P用户、计算AV、管理文件访问权限以及更新访问控制策略.同时,该层授权本地用户控制客户端用户访问本地共享文件.利用框架的访问控制接口,P2P用户间可以交换各自的访问控制信息.我们将在下一节详细说明这些功能.

3.2 认证

在授予主体某种访问权限之前,必须首先认证该主体.

设每位P2P用户拥有128位长的全局唯一标识GUID(global unique identifier)[5]和一对密钥(*PK*/*SK*).

P2P共享文件系统要求实现双向认证.认证由客户端用户发起,过程如下:

(1)客户端用户首先向服务器用户发送认证请求消息,该消息含有客户端用户的*GUID*,*PK*和经过服务器公钥加密的秘密值.

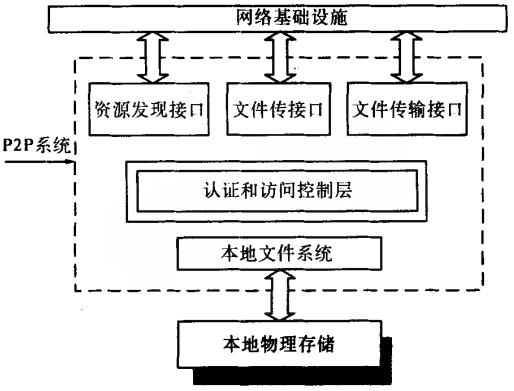

图1 带访问控制功能的P2P用户

Fig.1 Users with access control function

(2)服务器用户检旦本地数据库,如果存在与该客户端用户交互的记录项,那么调出相应的信任信息.否则,就为客户端用户创建新记录项.接着,服务器用户将执行认证协议(如基于SSL的认证协议).

考虑到存储资源限制,服务器用户可能会限制本地数据库容量.如果某个P2P用户在一段时间内没有与服务器用户交互,那么服务器用户删除该用户对应的记录项.

3.3 AV计算

为授予P2P用户适当的访问权限,访问控制框架采用基于用户的计分系统.认证成功后,客户端用户向服务器用户提交等级证书RC(Rating certificate, RC),后者据此计算前者的整体信任值和整体贡献分.这两个AV分别反映服务器用户对客户端用户的可信度和贡献度的评价.

计算AV值有两种参数来源:一是服务器用户对客户端用户的直接经验;二是其它用户针对客户端用户提供的推荐意见.因此,有4个具体参数如下:

DT:服务器用户基于自身直接经验对客户端用户的信心.

IDT:服务器用户根据其它用户的推荐意见对客户端用户的信心.

DC:客户端用户在上传/下载文件方面对服务器用户的贡献度.

IDC:客户端用户在信息交换方面对整个P2P系统的贡献程度.

设置DT和IDT是考虑了P2P环境的不可预

知性.服务器用户一般不知道客户端用户的真实身份,无法判定是否相信并允许该用户访问本地共享文件.服务器用户评价客户端用户可信度的唯一方法是考查自身和其它用户和该用户之间的已完成交互.显然,服务器用户只能以一定概率相信其它用户的推荐意见.

设置 DC 和 IDC 是考虑实现某种"补偿"机制.基本思想是:用户上传 P2P 系统的文件越多,则该用户从系统下载期望文件的机率越大.

3.3.1　直接信任

访问控制框架采用 Beth 等人提出的直接信任值计算公式[5]:

$$T_{ij} = 1 - \alpha^n \tag{1}$$

式中:T_{ij}表示用户 i 对用户 j 的直接信任值;n 是用户 i 和用户 j 之间的满意交互次数.n 的初始值为 0.当用户 i 对用户 j 的正向经验增加时(即增加时),T_{ij}将趋近 1.α 是处于[0,1]上的特殊经验值.选择 α 很关键,α 越小,则 T_{ji}增长速度越快.

3.3.2　间接信任

针对陌生客户端用户,服务器用户可以向他相信的其它用户请求推荐意见,然后根据反馈的推荐意见评估客户端用户的可信度.基于推荐意见的间接信任计算公式为

$$R_{ij} = (\sum_{i=1}^{k} T_{it} * T_{tj})/k \tag{2}$$

式中:R_{ij}表示用 i 户对用户 j 的间接信任值;k 是服务器用户选择的常数.如果反馈的推荐值多于 k 个,那么服务器用户只使用其中值最大的个.如果反馈推荐值不足 k 个,那么 R_{ij}仍被除以 k.显然,这样得到的间接信任值较低.这里强调推荐值必须来自那些同时和用 i 户和用 j 户都有过交互的用户.T_{it}和 T_{tj}均在[0,1]之间,R_{ij}总小于 T_{it}和 T_{tj}.

3.3.3　直接贡献

直接贡献表示以往交互中客户端用户到服务器用户的相对共享信息传输量(单位为 Mbytes),定义如下:

$$Q_{ij} = D_{ij} - D_{ji} \tag{3}$$

式中:D_{ij}表示用户 i 从用 j 户下载的文件大小;D_{ji}表示 j 从 i 下载的文件大小.如果 j 从 i 下载的文件大小高于 i 从 j 下载的文件大小,那么 Q_{ij}是负值.长时间相互下载使 Q_{ij}趋于 0,此时,交互过程对信任值的影响可由直接信任值反映.

3.3.4　间接贡献

间接贡献表示以往交互中客户端用户到其它 P2P 用户的相对共享信息传输量(单位为 MBytes).服务器用户计算间接贡献的依据是客户端用户访问文件之前提交的推荐值.但是,不同用户反馈的推荐值的权重应有所不同.服务器用户根据对用户信任度加权计算客户端用户的间接贡献:

$$P_{ij} = \sum_{i=1}^{k} T_{it} * Q_{tj} \tag{4}$$

式中:Q_{ij}是 i 对 t 的直接信任;k 是反馈推荐值的用户数量.基本思想是:服务器用户只关心客户端用户和被服务器用户信任的那些用户间的以往交互.

直接贡献和间接贡献都鼓励 P2P 用户共享自身文件.这就隐含实现了一种"补偿"机制.

3.3.5　授权访问

访问控制框架为每个文件规定两个门限:对应信任值的门限 $A_{th}(0 \leqslant A_{th} \leqslant 1)$和对应贡献分的门限 B_{th}(单位是 MBytes).只有整体信任值和整体贡献分都不小于门限的客户端用户才能访问该文件.整体信任值用 A 标记,是直接信任和间接信任的加权和.整体贡献分用 B 标记,用直接贡献和间接贡献的加权和.直接信任的加权因子用 W_T 标记;间接信任的加权因子用 W_R 标记;直接贡献的加权因子用 W_Q 标记;间接贡献的加权因子用 W_P 标记.加权因子的设置方式和设置粒度都由 P2P 用户自己决定,以满足 P2P 用户需要的灵活性.这些加权因子满足两个条件:

$$W_T + W_R = 1 \tag{5}$$

$$W_Q + W_P = 1 \tag{6}$$

当客户端用户 j 想访问服务器用户 i 的文件时,i 计算 j 的整体信任值和整体贡献分:

$$A_{ji} = W_T * T_{ij} + W_R * R_{ij} \tag{7}$$

$$B_{ji} = W_Q * Q_{ij} + W_P * R_{ij} \tag{8}$$

只有 $A_{ij} \geqslant A_{th}$和 $B_{ij} \geqslant B_{th}$均成立时,j 才能得到访问权限.i 还可以设置 T_{ij},R_{ij},Q_{ij}和 P_{ij}的最低值,以便对文件实施更严格的访问控制.i 也可以根据自身访问控制策略,删去公式(7)和公式(8)中的某个分量.例如,如果根本不考虑其它 P2P 用户的意见,则式(7)和(8)中的 W_R 和 W_P 被删去.

3.4　信任值和贡献分的管理

3.4.1　等级证书

访问控制框架使用等级证书传递推荐值.推荐用户使用自身私钥签名证书,确保证书内容不被篡改.被推荐用户存储等级证书,等级证书含有推荐用户对被推荐用户的直接信任值和直接贡献

分.证书还包含一个有效期选项以防止等级证书被重复使用.当证书即将超期时,被推荐用户向推荐用户申请更新等级证书.图2给出了一张等级证书的实例.

```
<RatingCertificate Signature=' 24fy79hut879hiyb7h9' />签名
<Expiration Date Data=04.07.2005 Time=' 17.59' />有效期
<Recommending GUID={ARD7665V-7GXC-4E92-5BB349D63320}
PublicKey=' xxxxxxxxxxxxxxxxxxxxxxxxx' />推荐用户身份标识
<RecommendedGUID={BCD2332D-10XH-6E32-8DT439D58310}
PublicKey=' xxxxxxxxxxxxxxxxxxxxxxxxx' />被推荐用户身份标识
<Value DirectTrust=0.8 DirectContribution=520/>直接信任值和直接贡献分
<IssueDate Date=01.01.2005 Time=' 17.59' />颁发时间
</AuthenticationCertificate>
```

图2 等级证书实例

Fig.2 Hierarchy certificate instance

3.4.2 本地存储

考虑到可扩展性,P2P用户不保留与其它用户的交互细节,只在本地数据库存储两组等级证书.一组是作为被推荐用户接收的等级证书,以方便未来下载.另一组是作为推荐用户签发给其它用户的等级证书,以方便验证.此外,P2P用户维护一张黑名单记录存在恶意行为的用户,不再为黑名单中用户签发等级证书,也不和这些用户交互.为抵御恶意用户,P2P用户之间周期性的和自己信任的用户交换黑名单.

3.4.3 交互计分

一次下载操作结束后,客户端用户必须根据自己对此次交互的满意级别向服务器用户签发新等级证书,以更新他对服务器用户的直接信任值和直接贡献分.如果客户端用户没有这样做,那么服务器用户就将他列入黑名单.一次满意交互将增加服务器用户的直接信任值,从而增加服务器用户从其它P2P用户那里下载文件的成功率.

客户端用户对交互的满意程度取决于两个因素:下载速度和文件质量.如果下载速度高于下载速度门限,那么认为该速度是可接受的.下载速度对直接信任值的影响如下:如果可接受,那么 $T = 1 - \alpha^{(n+1)}$,否则 $T = 1 - \alpha^{(n-1)}$.同时,框架将文件质量分为5个等级:好、尚可、差、损坏、有害.客户端用户根据自身感受对文件进行评价.文件质量对直接信任值的影响如下:①好:$T = 1 - \alpha^{(n+1)}$;②尚可:T 不变;③差:$T = 1 - \alpha^{(n-1)}$;④损坏:$T = 1 - \alpha^{n/2}$;⑤有害:列入黑名单.

在计分系统中,如果P2P用户提供了损坏或者有害文件,那么他的直接信任值将严重降低,甚至被放入黑名单.这种机制将有效阻止P2P用户扩散恶意文件.

3.4.4 验证签名

访问控制框架对P2P系统性能将带来一些影响.最主要的负担是服务器用户对等级证书的签名验证操作.实际上,服务器用户不必对客户端用户反馈的所有等级证书都进行验证.他既可以选择只验证那些加权值较高的等级证书,也可随机验证部分等级证书.如果验证失败,服务器用户就将客户端用户放入黑名单.因此,任何想要伪造等级证书或者使用旧证书的P2P用户都会被排除.

3.5 典型的交互过程

图3说明了服务器用户与客户端用户之间的典型的交互过程.交互过程由三个阶段组成:预备阶段、交互阶段和反馈阶段.首先,预备阶段包括认证、信任值和贡献分计算.客户端用户自行选择能够得到最佳间接信任值和间接贡献分的等级证书提交给服务器用户.其次,交互阶段允许客户端用户从服务器用户那里下载一个或者多个文件.最后,反馈阶段包括评价交易满意级别、颁发新的等级证书.

从整个交互过程可以看出:客户端用户在每个阶段都扮演了主动角色,而服务器用户所做工作很少.服务器用户从客户端用户和本地数据库得到所需的所有信息并且做出决定.因此,访问控制框架更多的采用了"推"(push)的设计思想.我们认为这是较为适当的设计原则.这是因为得益的主要是客户端用户,服务器用户不能耗费很多资源(如CPU计算能力、网络通信带宽等).

4 性能讨论

笔者提出的基于信任的访问控制框架能够满足第2节提出的P2P文件共享系统对访问控制的特殊需求.通过扩展传统的自主访问控制模型,P2P系统的分布性和用户匿名性等特性得以保留,同时实现了个人用户和多个用户之间的访问控制服务.信任模型和计分系统使服务器用户能够根据整体信任值和整个贡献分来区分不同用户,从而为不同用户分配适当的访问权限.框架的贡献分计算系统是一种隐含的"补偿"机制,有效调动了P2P用户共享自身文件的积极性.框架的交互计分机制不仅能够区分P2P用户之间的性能优劣,也可以追踪和惩处那些扩散有害文件的恶意用户.

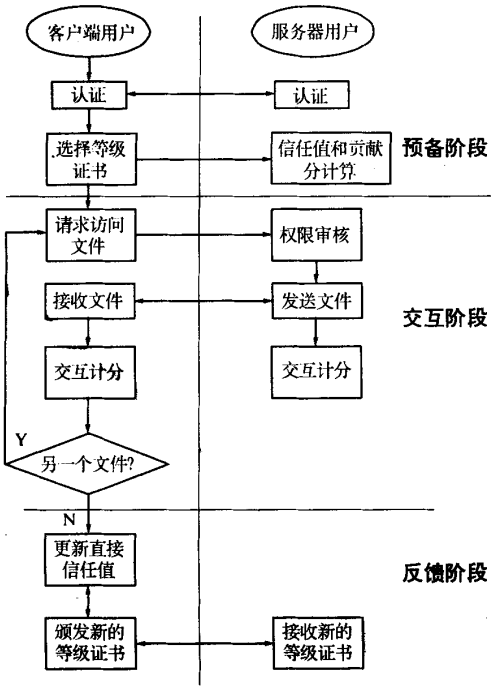

图 3　交互过程

Fig.3　Intercommuncation process

综上所述，访问控制框架的优点归纳如下：

(1) 在实现访问控制服务的同时，没有破坏 P2P 系统的原有特性.

(2) 即使 P2P 用户以等级证书形式在本地存储其它用户对自己的等级评价，他也无法篡改自身的信任值和贡献分.

(3) 提供损坏文件或是有害文件的 P2P 用户将被惩处，甚至被隔离于共享文件系统之外.

(4) 为了增加下载所期望文件的机会，P2P 用户必须更加主动的共享自身文件.

(5) P2P 形式的评价方式使得共谋用户无法从 P2P 系统得到比普通用户更多的利益.

5　结论

作者提出了一种基于信任的访问控制框架. 该框架将信任推荐模型和公平参与体制综合应用于 P2P 文件共享系统，能够在保持 P2P 环境原有特性不变的前提下，实现高效的访问控制服务.

参考文献：

[1] PARK S J, HWANG J. Role - based access control for collaborative enterprise in P2P computing environment [C], Italy: 8th ACM Symposium on Access Control Models and Technologies (SACMAT), 2003, 62 ~ 75.

[2] YANG B, MOLINA H G. Efficient search in Peer - to - peer systems [J]. IEEE Computer Society, 2002, 26(4): 5 ~ 14.

[3] GRESPO A, MOLINA H G. Routing indices for peer - to - peer systems [J]. IEEE Computer Society, 2002, 26 (4) : 23 ~ 34.

[4] MCLEAN J. The specification and modeling of computer security [J]. IEEE Computer, 1990, 23(1): 9 ~ 16.

[5] AYDIN S A, ERSIN U, MARK R P. A reputation - based trust management system for P2P networks [C]. New - York, USA: IEEE/ACM CCGRID'04, 2004, 154 ~ 176.

Study and Design of Access Control Mechanism for P2P File Sharing System

HE Wei[1], XUE Su-jing[2], KONG Meng-rong[3]

(1. School of Adult Education, ZhengZhou University, Zhengzhou 450052, China; 2. Information Engineering Department, North China Institute of Water Conservancy and Hydroelectric Power, Zhengzhou 450008, China; 3. Computer Science Department, Zhong Yuan Institute of Technology, Zhengzhou 450007, China)

Abstract: Because the decentralized and anonymous characteristics of P2P (Peer - to - Peer) environments, the traditional access control mechanisms can't be used to provide a efficient and secure access controlling services for P2P sharing file system. Thus, based on the trust and recommendation mechanism and fair participation idea, this paper proposes a new access control framework. While preserving the special characteristics of the P2P sharing file system, this framework can implement the realistic and effective access control service.

Key words: peer-to-peer network; file sharing system; access control