# 基于信任域的P2P访问控制模型研究

张国治[1],党小超[2],魏伟一[1]
(1.西北师范大学 数学与信息科学学院,甘肃 兰州 730070;
2.西北师范大学 网络学院,甘肃 兰州 730070)

**摘 要**:P2P作为一项愈来愈流行的技术,在资源共享和协同协作方面有崭新的应用。但是这种新的技术面临传统的网络所未曾遇到的网络安全方面的严重考验。文中从实际应用出发,分析了现有的访问控制技术并在此基础上提出一种新的基于信任域的P2P访问控制模型。该模型不同于传统的基于PKI的访问控制模型,它能够在信任管理的基础上对P2P用户进行域划分,并针信任对域制定访问控制策略,从而使得访问控制在实际应用中更加简洁和可行。

**关键词**:P2P;访问控制;角色;信任管理
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0228-03

# Trust Domain-Based Management Model in P2P Access Control

ZHANG Guo-zhi[1], DANG Xiao-chao[2], WEI Wei-yi[1]
(1. College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China;
2. College of Network, Northwest Normal University, Lanzhou 730070, China)

**Abstract**: Peer-to-peer (P2P) has become popular as a new technology for the resources sharing and coordination. However, the P2P environments make the task of controlling access to network security more difficult, which cannot be done by traditional access control methods. In this paper, analyses the technique of access-control requirements in such environments and proposes a trust domain-based access control framework for P2P environment. The framework is different from traditional access-control framework, which can define P2P user's trust domain-based in reputation management and define the access-control strategy for trust domain. The proposed scheme is realistic and feasible in P2P application.

**Key words**: P2P; access control; role; reputation management

## 0 引 言

P2P在资源共享等方面的应用已经非常成熟,不断有新的应用出现,已经有类似Bit torrent的第三代技术在广泛使用。在协同工作和分布式计算等方面的应用也正在进行广泛的研究。然而,在目前的网路环境下P2P技术的应用存在安全方面的诸多问题。相对于传统的C/S模式和分布式环境,P2P是一种完全分散式的体系结构,作为每一个P2P网络的节点,其中的任何一个实体虽然处于同等的地位,但是形式复杂,这就导致了P2P网络控制的复杂性。

访问控制技术从20世纪70年代诞生到现在已经经过了将近30年的发展,在这个过程中先后出现了很多重要的访问控制技术,它们的基本目标都是防止非法用户进入系统和合法用户对系统资源的非法使用。为了达到这个目标,访问控制常以用户身份认证为前提,在此基础上实施各种访问控制策略来控制和规范合法用户在系统中的行为。

**收稿日期**:2005-11-05

**作者简介**:张国治(1977-),男,甘肃凉州人,讲师,硕士,研究方向为计算机网络应用;党小超,教授,硕士生导师,研究方向为计算机网络工程及应用。

## 1 访问控制的安全策略

目前主流的访问控制策略主要有自主访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制(RBAC)策略。DAC基于对主体的识别来限制对客体的访问,这种控制是自主的。MAC通过比较主体与客体的安全属性来决定是否允许主体访问客体,安全属性是由系统自动或由安全管理员分配给每个实体(主体和客体)的,它不能被任意更改。如果系统认为具有某一安全属性的主体不能访问具有一定安全属性的客体,那么任何人(包括该客体的主人)都无法使该主体访问该客体。在基于角色的访问控制中,在用户(User)和访问许可权(Permission)之间引入角色(Role)的概念,用户与特定的一个或多个角色相联系。角色与一个或多个访问许可权相联系,角色可以根据实际的工作需要生成或取消,而且登录到系统中的用户可以根据自己的需要动态激活自己拥有的角色,避免了用户无意中危害系统安全。除此之外,角色之间、许可权之间、角色和许可权之间定义了一些关系,比如角

色间的层次性关系,而且也可以按需要定义各种约束(Constraints),如定义出纳和会计两个角色为互斥角色(即这两个角色不能分配给同一个用户)。RBAC 是一种策略无关的访问控制技术。

由于强制访问策略中的强制的安全策略越来越复杂,给安全管理增加了很大的负担,在这种情况下,要求把策略的表达和策略的强制分开,希望用同样的程序来强制可能随时间变化的安全策略,这就是所谓的基于策略的访问控制技术。基于策略的访问控制技术的根基就是一个表达力强的策略预言,用这个预言来表达安全策略,再用一个解释引擎来执行这些策略。

## 2　P2P 环境下的访问控制技术

P2P 下的访问控制有其自己的特殊性[1,2]。由于 P2P 是一种无中心的分布式环境,在这种环境下,所有的用户彼此陌生,无法确认彼此身份,严格来说是一种"陌生人访问陌生人"的方式,在这种环境下无法确定每个用户的具体身份,因此无法使用 RBAC 模型;其次,由于用户出于自身考虑,一般不愿意把自己的相关信息提供给对方,可以采用匿名等方法来实现这种目的,这种方式增加了访问控制的难度;另外,在这类应用中,由于大量的用户频繁地进出网络,使得网络的结构频繁地变化,这给访问控制带来复杂性,加大了系统的开销。

建立 P2P 的访问控制策略,首先要建立 P2P 的信任管理模型,在信任模型的基础上给每个节点给出信任值和可靠度,然后在这个基础上应用相应的访问控制策略[3,4]。如何建立信任模型,这与 P2P 的环境密切相关,主要是 P2P 的节点可用性、数据源的真实性、节点的匿名性和访问控制等方面的问题,而这些问题又密切联系,难以分割。以下分别描述。

(1)可用性主要指在 P2P 网络中存在 DDOS 和 fail - stop 攻击,比如在 Gnutella 中,可用性问题主要指 P2P 网中存在的 DDOS 和 fail - stop 攻击。因为在 Gnutella 中,各个节点都可以对查询请求进行应答,导致某些恶意节点充当起中心的角色,对所有的请求都应答某一个牺牲品(victim)可以提供服务。导致大量请求聚集耗尽了该节点的资源,实现了 DDOS 攻击,可以通过检测 - 预防 - 管理的手段防止这类攻击。

(2)文档的真实性可以采用时间戳法、专家体系、投票方法和信任体系来实现。这里的讲到的信任体系只是概念性的,即具有高的信任值(Reputation)就更可靠、更权威。而真正实现的信任系统是综合上述方法的综合体系。如专家系统用到的专家签名机制可以用于信任体系中。具体设想的实现如下:可以将 P2P 网络中通过投票系统选出一组最可靠的用户团队,作为这个网络社区的可信机构(CA),通过这个中心来签发社区中各节点在可靠性和可信赖性方面需要的数字证书(Digit certification),在 PKI/CA 体系用于 P2P 系统的实现中充当了第三方的角色。这些可信的专家团队是可变的,并且可采用多方安全计算方式实现。

(3)匿名性问题是 P2P 系统的一个难点问题,在信任体系中主要表现为匿名性与签名机制之间的矛盾。节点要实现签名就要有惟一可识别的 ID,但是要实现匿名性,可以通过多个伪标识的方式,节点任意使用多个标识实现匿名性,这样签名就没有意义了。同时匿名性造成了节点查询的不方便,没有确切的查询目标了。在基于反馈的可信体系统中,单节点的多标识会造成"liar farm"现象,现在某些系统如 FreeHeavn,Crowds 是通过多级代理的方式实现匿名性的。这会造成网络的负担,不是真正意义上的点对点了。

(4)访问控制是以上综合因素的实施。对于 P2P 网络而言,访问控制是个复杂的概念。尽管现有的访问控制技术都可以应用到 P2P 网络中,但是 P2P 的完全分散结构却导致了访问控制的复杂性。不论是 DAC,MAC 还是 RBAC,都无法解决 P2P 环境中的复杂性,基于信任体制的访问控制是解决这一问题的有效途径。

## 3　基于信任的访问控制技术

基于信任的访问控制从本质上来说是一种基于策略的访问控制技术。由于在完全分散的 P2P 网络中,访问控制策略不再集中管理,很有可能由别人替资源的拥有者制定部分的访问控制策略,在这种情况下,访问控制决策所需的信息都要在运行时收集和评估。然后得出最终的结果。对于信任模型,最核心的问题是如何计算每个节点的信任度和可靠性。对于信任值的计算目前有很多的模型。以下是其中的两种模型。

### 3.1　基于反馈的信任体系

在基于反馈的信任体系中,可以通过提供的满意的反馈的同级、所有参与的交易统计、提供的反馈的节点的可信度、交易的具体情形和社区的背景情形等方面来构成具体模型,并共同参与信任系统的计算[5]。具体的信任模型可以表示为:

$$T(u)=\alpha\cdot\frac{\sum_{i=1}^{I(u)}S(u,i)\cdot Cr(P(u,i))\cdot TF(u,i)}{I(u)}+\beta\cdot CF(u)$$

其中的 $S(u,i)$ 表示节点 $u$ 在第 $i$ 次的交易中的平均满意度,$P(u,i)$ 表示在节点 $u$ 的第 $i$ 次交易中的某一结点,$Cr(P(u,i))$ 则表示被 $P(u,i)$ 提交的反馈可信度,$TF(u,i)$ 表示 $u$ 的第 $i$ 次交易的交易内容,$I(u)$ 表示在某段时间内的交易次数,$CF(u)$ 表示在 $u$ 交易的这段时间内的社区背景,通过 $\alpha$ 和 $\beta$,可以强化和弱化社区背景的作用。这个模型综合考虑了一个 P2P 社区综合交易的各个方面,是一个比较全面的模型。

### 3.2　基于名声的信任体系

在基于名声的信任体系中,利用了 Trust Vector 和 Credibility Vector 来实现可靠性和可行性的统计[3,6]。针对上面的模型,这个模型将可靠性和可信性分开考虑,在

计算节点可靠性的同时还计算了节点的不可靠性,而且不可靠性要重要于可靠性,这也是现实模型中经常采用的方法。这种机制可以使得欺骗者受到严重的惩罚。同时由于可靠的节点不一定可信,因此采用这种体制可以避免某些恶意的节点积累很高的可靠性以后,转而对其他的可靠节点进行诽谤攻击的行为。目前的 BT 社区广泛地采用了这种模型。

关于 P2P 的信任管理还有其他的一些模型,比如 Abererand 和 Despotovic 等提出的 Complaint - based system,Kamvar 提出的 Eigen Trust Scheme 等模型。不管哪种信任模型,最终的目的是给出一个量化的节点信任值,P2P 的访问控制则依赖于节点的信任值。

## 4 基于信任域的访问控制

通过上述信任管理模型计算出每个节点的信任值,然后针对每个节点的信任值,采用相应访问控制策略,就可以实施对相应节点的访问控制了[7]。由于 RBAC 采用了策略和表达分开的思想,因此在 P2P 的网络中可以对所有节点根据信任值划分为若干个域,对于信任值和可靠性高的节点可以划分到比较高的信任域中,从而可以获得比较高的访问控制权限。针对可靠性和信任域,笔者定义一个信任域为 D。其模型可以简单表示为图 1。

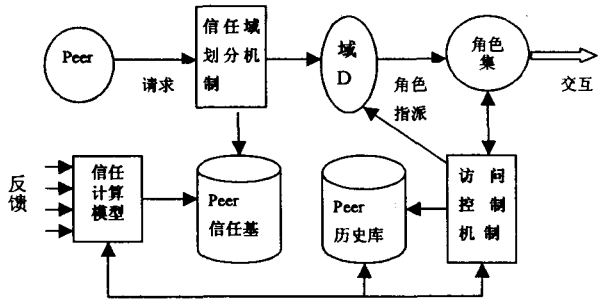


图 1 基于信任域划分的访问控制模型

信任模型可以是现有的成熟的信任管理模型,其对信任基的计算依赖于节点的历史记录系统反馈、名声和社区背景等因素,将计算的结果表示为信任基,供信任划分机制查询。信任域划分机制则通过信任基的查询,根据节点的查询结果,将节点划分到相应的信任域 D,而访问控制中的角色指派则可以将某一个信任域指派到角色集的一个角色上,从而实现从节点到角色的指派。

该模型的关键在于如何根据节点信任值和可靠性划分信任域,以及不同的信任域可以指派何种角色,计算模型的实施要通过相应的统计模型实现。

## 5 总 结

通过信任模型将复杂的 P2P 访问控制转换为对每个节点信任值的计算,简化了访问控制的实施,同时也可以利用现有的成熟访问控制模型来进行 P2P 的访问控制。目前关于 P2P 的信任管理正在进行深入研究,也有一些模型在类似在线交易的系统中使用。通过信任管理模型建立 P2P 的访问控制策略,是一种切实可行的方法。促进 P2P 环境下的应用健康正常的发展要有完善的技术,更重要的是如何通过信任管理建立良好的道德和信任体系。没有好的信任管理模型,必将使 P2P 成为谎言和欺骗的温床。

**参考文献:**

[1] Tran H, Hitchens M, Varadharaj V, et al. A Trust based Access Control Framework for P2P File - Sharing Systems[A]. Proceedings of the 38th Hawaii International Conference on System Sciences, 2005 [C]. Washington, DC, USA: IEEE Computer Society, 2005.

[2] Gupta R, Somani A K. Reputation Management Framework and Its Use as Currency in Large - Scale Peer - to - Peer Networks, p2p[A]. Fourth International Conference on Peer - to - Peer Computing (P2P'04)[C]. Washington, DC, USA: IEEE Computer Society, 2004. 124 - 132.

[3] Dewan P, Dasgupta P. Securing P2P Networks Using Peer Reputations: Is there a silver bullet? [A]. consumer communications & networking conferece[C]. Nevada, USA: CEA, 2005.

[4] Neil D, Garcia - Molina H, Beverly Y. Open problems in data - sharing peer - to - peer systems[A]. The 9th Int'l Conf on Database Theory (ICDT)[C]. Siena, Italy: [s. n.], 2003. 1 - 15.

[5] Li Xiong, Ling Liu. A Reputation - Based Trust Model for Peer - to - Peer eCommerce Communities[A]. 2003 IEEE International Conference on E - Commerce Technology (CEC'03)[C]. New York: IEEE Comput Soc, 2003. 275 - 286.

[6] Selcuk A A, Uzun E, Pariente M R. A Reputation - based Trust Management System for P2P Networks[A]. In: 4th IEEE/ACM International Symposium on Cluster Computing and the Grid[C]. Chicago, Illinois: [s. n.], 2004.

[7] 张书钦,芦东昕,杨永田. 对等网络中基于信任的访问控制研究[J]. 计算机科学,2005(5):31 - 33.

(上接第 207 页)

[3] Thomson S, Huitema C, IETF. RFC 1886, DNS Extensions to support IP version 6[S]. www. ietf. org/rfc/rfc1886. txt, 1995 - 12.

[4] Crawford M, Huitema C, IETF. RFC 2874, DNS Extensions to Support IPV6 Address Aggregation and Renumbering[S]. www. ietf. org/rfc/rfc2874. txt, 2000 - 07.

[5] WANG Ling - fang, ZHANG Yu, LI Ying - hua. Implementing Cisco IPV6 Networks[M]. Beijing: Posts & Telecom Press, 2003.