对等网络中基于信任的访问控制研究

张书钦[1] 芦东昕[2] 杨永田[1]

(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1] (中兴通讯技术中心 深圳 518057)[2]

摘 要 在对等网络中,通常模拟人际网络的信任来指导用户协作决策。本文给出了一个对等协作基于信任的访问控制框架,并讨论了其中各功能组件的关系。最后在RBAC中设计了一个基于信任的角色分配方案。

关键词 访问控制,信任,对等网络

Trust-Based Access Control in P2P Networks

ZHANG Shu-Qin[1] LU Dong-Xin[2] YANG Yong-Tian[1]

(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001)[1]

(Technology Center, ZTE corporation, Shenzhen 518057)[2]

Abstract In P2P networks, trust mechanism in social networks can be used to build trust in peers for collaboration decisions. In this paper, as an initial step towards a definition of trust based access control framework, we focus on the relationship among components of the framework. We also exemplify how the trust based role assignment scheme can be designed in RBAC.

Keywords Access control, Trust, P2P networks

1 引言

当前,随着以对等(Peer-to-Peer, P2P)计算、网络服务(Web Services)等为代表的新的计算形态的兴起,分布式计算也进入了一个新的阶段。相对于传统的客户机/服务器(C/S)计算体系结构,此类系统中的实体是平等的、自主的,其典型的特点是开放性和动态性。在P2P网络中,参与的实体(Peer)可以动态地加入和退出,并且可以自主地决定在网络中的行为,一个实体既可提供服务也可以消费服务,实体间并可以自由地进行服务交换,且不依赖于第三方。而在C/S计算体系结构中,严格地区分了服务提供者和消费者。在P2P网络中,由于实体的平等性和自主性也决定了此类计算环境具有以下几个显著的特点:1) 实体间的协作是自由的;2) 实体间的协作关系是临时的;3) 实体间的协作并无权威中心管理。以上的这些特点决定了网络中的实体之间没有确定的信任关系,协作的实体可能也是以前未知的,因此对于一个实体来说无法保证协作方的行为的可靠性。但是开放环境中实体间的交互与协作关系非常类似于人际网络中个体间的关系,因此已有研究开始借鉴人际网络的信任机制来建立实体间的信任关系,并用以指导实体间的协作决策[1]。

本文给出了一个P2P网络中的基于信任的访问控制框架,通过将信任组件集成到访问控制机制中,从而实现基于协作实体可信性的访问控制决策。

2 对等协作

协作是多个实体为完成一项计算任务而进行的交互过程。在对等网络中,各个实体可以扮演不同的协作角色,在协作过程中其扮演的角色也可以动态变化,其并不依赖于实体所处的位置,实体间通过端到端的服务交换完成灵活的、自组织的协作。

一般来说,实体间的协作可以分为两个阶段:服务查找和服务交换。实体首先需要在网络中定位所需的服务,从而形成一个协作群组,之后群组中的各个实体依据其协作角色交换服务。如,在一个P2P文件共享网络中,如Gnutella、Freenet和Kazaa等,各个实体都可以贡献自己拥有的文件,并可以在网络中发出文件查询,持有所查询文件的目标实体反馈一个响应消息,从而从一个目标实体处下载所选择的文件,即两个实体通过协作完成了一次文件下载。

由于P2P网络是开放的、动态的,其中的实体行为的动态性,以及未知实体的加入,都导致了协作的不可靠性,也增加了更多的安全威胁,如不真实的服务、服务的滥用等。在封闭的环境中,一般可以通过可信第三方的认证和授权服务,以及惩罚措施来保证协作实体的可靠性。

3 P2P网络中的访问控制

访问控制是提供系统安全的主要保障手段,是为了限制访问用户对系统资源的访问权限,以阻止未经允许的访问。现有的针对分布式应用的访问控制模型一般针对的是C/S体系结构,其假设了系统中有一个权威中心来集中的实施预先制定的访问控制策略,并根据请求的实体的身份来赋予访问权限。此类模型实际上是一个集中式管理模型,只适用于封闭的系统,其访问策略针对都是熟知的用户,不能处理系统所未知的新用户。

在P2P网络中,访问控制涉及到协作的两个阶段,分别为协作群组的加入控制和访问服务的许可约束。前者主要是在群组的形成过程,组中的实体都相互同意所充当的协作角

张书钦 博士生,研究方向:分布式系统、网络安全。芦东昕 博士后,研究方向:嵌入式系统、信息安全。杨永田 教授,博士生导师,研究方向:计算机网络、信息安全。

色，从而可以开始服务交换。在协作群组形成之后，实体间即可开始服务交换，并需要对所接收的请求和欲提供的服务给予相应的许可约束。这两个阶段的访问控制过程都是是否许可(或授权)的决策，本文下面的内容并不进行区分。

显然，在P2P网络中传统的访问控制机制是不适用的。首先，P2P网络是无中心的网络，实体间的协作并没有中心进行协调，实体只需对自己所拥有的资源和数据进行管理。另外，在P2P网络中实体都是自治的，并可以随意移动、自组织，协作实体容易发生变化，都使得系统更容易产生快速的、不可预料的变化。而且，由于可能的协作实体数目巨大，经常有未知实体加入进来，为每一个协作实体定义访问控制策略显然是不可能的，尤其是在实施细粒度访问控制时需要定义更为详细的策略。因此，在本文的访问控制方案中即不直接针对实体的身份，而是依据其可信性来实施访问控制为对等协作提供安全保证。

4 信任和声望

信任是人际网络中一个复杂的概念，难于严格的定义和理解。基于P2P环境，本文给出这样的一个定义：信任是一个实体根据相关信息而对其他实体的未来可靠的、安全的、期望的行为的主观可能性判断，也可以说信任是对实体行为可靠性的判断。信任有如下的一些属性：1) 主观性；2) 上下文相关性；3) 动态性。

对信任的度量不是在信息充分的条件下做出的，因此信任有很强的主观性，对客体的信任判断会依评价主体不同而得出不同的结论，信任判断也会受多种因素影响。信任是内容相关的，对目标的一个方面的信任可能不会影响到在另一个方面的不信任，信任只有在一定的上下文中才有意义。目标的信任会随着信任信息的更新、实体行为等的变化而动态变化。

P2P网络中的信任模型需要对信任传递、扩散、形成机制展开研究，并避免使用集中式的可信权威。声望则是网络中实体对特定目标实体的综合信任评价。P2P网络中的实体可以目标实体的交互经验对其进行信任评估，实体间可以通过交换和传播信任评估信息以获取目标实体的声望。目标实体的声望一般需要综合其他实体给出的信任推荐而得，形式地表示为：

$$R=\Sigma w_i \cdot r_i \qquad (1)$$

其中 w_i 为针对推荐实体 i 的采纳权值，r_i 为实体 i 给出的推荐信任值。R 是目标实体的声望。

一般来说，对目标实体的信任除了考察直接交互经验外，还需要考察目标实体在网络中声望，尤其在缺乏同目标实体的交互经验时，因此，对实体的信任由两部分组成：本地的交互经验(或称直接经验)和来自其他实体的信任推荐(或称声望)，形式地表示为：

$$T_{total}=\alpha \cdot T+(1-\alpha) \cdot R \quad 0<\alpha<1 \qquad (2)$$

其中 T_{total} 是对目标实体总的信任，而 T 是由直接交互经验而得直接信任。α 代表了二者的不同影响力。

信任关系的量化使实体能够表达对其他不同实体在信任程度上的差别。这种差别可以使实体做出不同的安全决策，如其对某个实体的信任度较高，则在该实体请求某类协作活动时，其安全审查的措施相对较少，而当其对某个实体的信任程度较低时，则对该实体的协作请求，将增加安全审查措施，甚至拒绝该请求。

5 基于信任的访问控制框架

在开放的系统中，信任机制的应用促进了实体间的复杂交互。信任提供了一种保障机制：在没有第三方权威的情况下就可以建立同实体间的信任，并用于决定在一定的情景中给予对方多大程度的访问权限。针对对等协作，基于信任的实体访问控制决策框架应包括如下几个主要部分：

1) 一组负责提交、搜集、处理协作请求、响应，并依据本地策略交互决策的组件；

2) 一个指导实体间信任关系评估的信任模型；

3) 一种用于描述实体安全策略和信任策略的语言。

图1为一个基于信任的访问控制框架示意，其中阐明了各组件之间的关系。

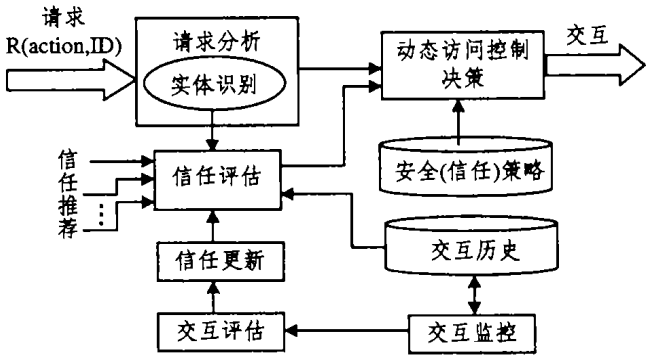

图1 基于信任的访问控制框架示意

5.1 实体识别

在对等协作中，实体的身份标识通常需要用于关联于其相关的协作记录，以及相关的信任判断[4]。在P2P网络中，由于缺乏权威中心，传统的认证方案是不可行的，如X.500等，需要依赖于一个可信的第三方，或要求协作的实体是已知的。由于无法利用权威中心认证实体的身份，通常需要实体以自举(Self-Certification)的方式来证实自己的身份，防止其他恶意实体的冒充，整个识别过程无需第三方即可在交互的两个实体间完成，如在SPKI/SDSI方案中，实体独立地生成一个非对称密钥对，其中公钥用作在网络中的身份标识，在交互时协作实体通过私钥来认证自身的身份。通过认证的实体标识可以将相关的协作记录关联到相应的实体，以积累同该实体的经验用于信任计算。在P2P环境中，实体的身份标识只是假名，通常并不破坏匿名的要求。

5.2 协作监控

协作监控是监视协作过程中协作实体的交互动作。为交互定义策略并不能保证交互的安全进行，因此监控扮演了关键的角色。最根本的是要保证交互要朝所期望的方向发展(可以为交互定义一个风险评估模型)。而且，我们可以度量协作过程中实体的状态和行为，可以及时停止对方不安全的行为，并削减其信任值。这种保护可以立即而不是等待到交互完全结束。协作监控为动态地控制协作过程提供了支持。

在一次交互完成后，交互的结果将被记录，并对其进行评估。交互结果至少可以区分不同的信任等级，如正面的和负面的，从而可以影响对该交互实体的信任评估。

5.3 信任计算

根据之前同协作实体的交互记录可以分析其可信性，若交互历史不足，还可以向网络中的其他实体查询其信任状况，通过其他实体给出的信任推荐来计算目标实体在网络中的声

望，从而综合得到一个信任值用于访问控制决策。不同的信任模型可能有更详细的信任计算方案，这里不做进一步的讨论。

若协作实体是新加入网络，网络中并没有的信任信息，可以为其赋予一个初始的信任值以为其分配访问权限。

5.4 访问控制决策

在交互的过程中，需要对对方提出的请求以及自身相应协作动作进行决策。这里决策需要权衡多方面的因素，如对该协作实体的信任、其所请求的动作，以及决策可能带来的开销、效用、风险等，但只有协作实体具有一定的信任度，才可能赋予其相应较高的访问权限，以执行风险和效用都较高的访问。因此，安全(访问控制)策略需要定义不同的访问权限对协作实体的信任度的要求。

本文提出的基于信任的访问控制框架是依据协作实体的可信性实施访问控制决策，其可以构建于不同的信任模型之上，并不依赖于特定的信任模型，但一个可行的信任模型需要允许实体动态地更新信任关系，并能够确切地反映实体在网络中的行为。

6 基于信任的 RBAC 的设计

基于角色的访问控制(RBAC)[7]是近年来研究和使用较多访问控制方案，其为角色赋予一定的访问权限，使用户通过充当一定的角色而拥有相应的访问权限。在 RBAC 中，用户可以通过角色非常容易地管理对所拥有的资源的访问权限，管理员则通过角色的分配实现灵活的授权。针对 P2P 应用的特点，这里通过在 RBAC 中引入信任因素实现信任强化的角色分配。

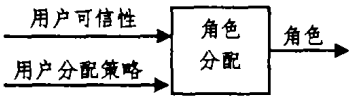

图 2 角色分配过程

在对等协作中，一个协作实体至少充当了一个协作角色，如，服务提供者或消费者。在一个协作角色中，由于协作实体得到的访问权限的不同，这里区分了不同的操作角色，如，在 P2P 文件共享网络中，不同的操作角色可能意味着文件下载中所能享受的带宽。实体可以通过为具有不同信任度的协作实体分配不同的角色来实施访问控制。表 1 给出了一个信任强化的角色分配策略的简单示例。

表 1 基于信任的角色分配策略示例

协作角色 CR	操作角色 OR	信任度 T
FileRequester	VIP	0.5～1.0
	Ordinary	0.2～0.5
FileProvider	Reliable	0.5～1.0
	Uncertain	0.1～0.5

这里假定了实体的信任值是一个单一的、相对的数值。在示例的角色分配方式中，若由于信任度的限制，某些请求实体可能是无法获得一定的协作角色，因此也无法形成协作群组，如示例中信任度小于 0.2 的实体不能享受所提供的文件下载服务。而且，不同的操作角色体现了在下载中所能得到的服务质量，如，在信任度为 0.2～0.5 时享受普通的下载服务质量。

基于信任的角色分配的实质是一种强化了信任因素的安全策略描述与授权决策机制，用于描述实体依据与其他实体的信任程度的不同进行不同的安全决策活动。角色可看作是实体定义的与自身资源访问相关的权限集合，依据授权实体对其他潜在协作请求实体不同的信任度为其他实体分配相应的角色，亦即根据信任程度的不同为其他实体授予不同的访问权限，体现了实体基于信任的访问控制决策。

讨论和总结 近年来，随着分布式计算环境的发展，模拟人际网络的信任机制也得到了广泛的研究，现有的文献中多数都只是讨论了信任的形成、计算机制，即信任模型，如文[2,3]，只有较少工作给出了基于信任的应用方案。文[5]给出了一个基于信任的协作方案，其中主要讨论了信任和风险在协作决策中的关系和作用。文[9]提出了一个软件服务中的信任管理框架，并给出了一个基于直接经验的信任度评估模型。而本文则给出了一个基于信任的访问控制框架，并结合 RBAC 给出了一个信任强化的角色分配方案，以实现对对等实体的访问控制决策。

本文给出的访问控制框架并不依赖于具体的信任模型，即，特定的信任传递、扩散、形成机制。实际上，该框架同样适合于其他开放的、动态的计算环境，如 Ad Hoc，普适计算(Pervasive Computing)等。

参 考 文 献

1 Marsh S. Formalising Trust as a Computational Concept: [Ph. D. Thesis]. University of Stirling, 1994

2 Aberer K, Despotovic Z. Managing Trust in a Peer-2-Peer Information System. In: Proc. of the Tenth Intl. Conf. on Information and Knowledge Management (ACM CIKM'01), 2001. 310～317

3 Xiong L, Liu L. A Reputation-Based Trust Model for Peer-to-Peer Ecommerce communities. In: IEEE Conference on E-Commerce (CEC'03) 2003

4 Seigneur J-M, Jensen C. The Role of Identity in Computational Trust. In: Proc. of The First Workshop on Security and Privacy at the Conf. on Pervasive Computing, Vienna, Austria, April 2004

5 English C, Terzis S, Wagealla W. Engineering Trust Based Collaborations in a Global Computing Environment. In: Proc. of the Second Intl. Conf. on Trust Management (iTrust 2004), LNCS, Springer-Verlag, 2004

6 Gray E, O'Connell P, Jensen C, et al. Towards a Framework for Assessing Trust-Based Admission Control in Collaborative Ad Hoc Applications: [Technical Report TCD-CS-2002-66]. Department of Computer Science, Trinity College Dublin, December 2002

7 Park J S, Hwang J. Role-Based Access Control for Collaborative Enterprise in Peer-to-Peer Computing Environment. In: 8th ACM Symposium on Access Control Models and Technologies (SACMAT), Como, Italy, June 2-3, 2003

8 Fenkam P, Dustdar S, Kirda E, et al. Towards an access control system for mobile peer-to-peer collaborative environments. In: IEEE 11th Intl. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002), Carnegie Mellon University, Pittsburgh, Pennsylvania, USA. IEEE Computer Society Press, June 2002

9 徐锋，曹春，郑玮，等. 一个软件服务协同中的信任管理框架设计. 计算机科学，2003,30(9)