基于 RBAC 的 P2P 网络环境信任模型研究*)

文珠穆　卢正鼎　唐　卓　辜希武
(华中科技大学计算机科学与技术学院　武汉 430074)

摘　要　P2P 网络的匿名性和动态性带来了许多安全问题,传统的分布式访问控制模型以及信任管理模型并不能很好地适应对等网络环境。本文提出了一种信任管理加权限控制的双重验证方法来实现 P2P 网络环境中的节点协作和资源访问等安全互操作。节点用户通过本文中的轻量级身份证书,不仅可以验证其合法身份,同时也可以通过该证书中用户的相关角色信息来获取对资源的访问控制权限。而且通过证书中的信任度字段,系统可以吊销低信任度的节点的证书,能有效地遏制恶意节点的非法行为。本文重点介绍了用户信任度的计算,以及用户节点身份证书的获取以及权限验证。最后,通过相关的实验,验证了本方法在效率上要优于传统的信任管理模型。

关键词　角色,P2P,信任,访问控制

Trust Model Research in the P2P Environment Based on RBAC

WEN Zhu-mu　LU Zheng-ding　TANG Zhuo　GU Xi-wu
(School of Computer Science and Technology, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract　The anonymity and dynamics of the P2P network bring many security problems. The traditional access control models and trust management models can not satisfy the P2P environment commendably. This paper proposes a double validation method employing trust management and privilege control to implement the security inter-operations which includes the nodes' cooperation and accessing resources. Through the lightweight peer certificates, the peers can be validated their legal identities and also can acquire their privileges for the resources according to the role information in the lightweight certificates. Further more, the system can revoke the peers' certificates whose trust degrees are too low by the trust degree field in the certificates. The illegality of the vicious peers can be kept down availably. This paper focuses on the calculations of the trust of the peers, the acquirement and the validation of the lightweight certificates. Finally, to prove the feasibility of the proposed ideas, the examination system is implemented and their scalability and performance are evaluated.

Keywords　Role, P2P, Trust, Access control

1　引言

P2P 网络是近年来兴起的技术,随着其规模的迅速增大,P2P 网络提供服务的安全性和可靠性成为了重要的问题。在对等网络中,所有的实体是平等的、自主的,其环境有分布性、匿名性和动态性这三个特点,正是由于这些特点给 P2P 系统带来了许多安全问题[1,2]。各节点是不同种类的未知的,有些节点能诚实地提供正确服务,而有些恶意节点则提供劣质服务,如传播病毒和木马,提供虚假文件下载等[3]。网络中不可避免地存在着大量的欺诈行为,P2P 网络难以提供可靠的服务质量保证,信息共享面临很大的安全问题。而在分散式的 P2P 网络中,没有中央节点发挥管理者的作用来对恶意节点的行为进行制止和惩罚,不能很好地集中控制存在的安全问题[4]。此外,一些传统的安全技术[5,6],如服务节点需要访问授权,或者消费节点需要服务认证,虽然能一定程度地防患与恶意节点进行信息交换,但是不能够制止恶意节点提供不可靠的服务质量。

在解决 P2P 网络安全方面的问题时,信任机制是抵抗不良行为的一种重要而有效的方法[7],它通过对系统中的用户或资源进行评价来预测用户或资源的未来行为,从而起到鼓励用户善意行为,惩罚用户恶意行为,辅助用户决策的作用。通过信任机制的激励作用,有助于维护系统的良性运行。但是当前的 P2P 网络环境普遍缺乏一种成熟的信任管理和访问控制机制,这已成为 P2P 应用推广的瓶颈。P2P 网络是一种典型的开放式环境,基于 RBAC 的分布式跨域安全互操作模型并不能完全应用于这种环境下。基于 RBAC 的安全互操作模型主要依靠 RBAC 安全策略的映射完成,然而 P2P 网络环境的一个显著特点即是用户集合不可预知性,以及用户的高度动态性,因而这种方式的可扩展性存在着很大的不足。尽管信任管理提供了很好的可扩展性,并适合开放式环境,但现有的信任管理模型仍存在着种种不足。首先,现有的信任管理系统在进行权限委托时没有考虑两个互操作实体之间的信任程度,这与实际情况不相符合。其次,现有的信任管理系统并不能对节点的行为提出更加细粒度的控制,并不能方便地实现根据节点的身份判别节点的角色,以及该节点具有访问哪些资源和服务的权限。

*)国家自然科学基金项目(项目编号:60403027),湖北省自然科学基金项目(项目编号:2005ABA258),软件工程国家重点实验室开放基金项目(项目编号:SKLSE05-07)。**文珠穆**　博士研究生,研究方向为分布式异构系统中的安全;**卢正鼎**　教授,博士生导师,主要研究领域为分布式系统、智能信息系统、信息安全。

因此，本文提出一种信任管理加权限控制的双重验证方法来实现 P2P 网络环境中的节点协作和资源访问等安全互操作。本文提出了一种轻量级的节点证书，该证书中的身份信息用来确定节点的身份，防止恶意节点的加入来对网络环境构成威胁。角色信息用来指明节点的具体的访问控制权限，节点的信任度进一步指明了节点在该网络中的信誉程度，该信息会根据节点的历史访问记录动态地进行调整。该节点正常的无威胁的访问次数越多，其信任度也越高，反之，就会越来越低，直到低于某个阈值而被收回证书。这也是识别该节点是否是恶意节点的重要标志。

通过该节点证书，就可以在 P2P 环境中实现基于角色的访问控制，从而解决 P2P 环境中的节点的身份确认以及节点权限控制等问题。本文第 2 节介绍相关工作和进展，第 3 节介绍轻量级节点证书以及节点信任度的调整，第 4 节介绍基于轻量级证书的访问控制框架，第 5 节是仿真实验及性能评测，最后总结了全文。

2 相关工作及进展

目前 P2P 网络中的信任系统都是基于反馈信息的，大致可分为全局信任模型和局部信任模型。全局信任模型可分为两类：一类是根据节点获得的正面反馈和负面反馈的数目，进行简单的算术运算，得出节点的全局可信度。该方法计算简单易理解，但无法处理节点给出的不公正反馈，容易受到恶意节点的联合欺诈攻击；另一类是通过对信任传递链上的信任值重复迭代来计算网络中节点的信任值。这种方法需要节点之间合作处理信任计算，计算和通信开销都较大。全局信任模型忽略了信任的私人化特征，对于某个特定的节点，其他节点对他的信任值都是相同的。此外，在大规模的 P2P 网络中为每个节点计算全局信任值的必要性和可行性仍有待进一步研究。现在关于 P2P 网络的信任模型大多是基于共享信息的局部信任模型。在基于共享信息的局部信任模型中，共享信息的获取有两种途径：一种是通过向其他节点洪泛信任请求获得的，该方法可扩展性差；另一种是通过采用 DHT 机制的 P2P 存储系统如 Chord、P-Grid 等获得，这种方法不适合当存在节点频繁加入和离开 P2P 系统的情况。

在 P2P 环境下，目前有 4 个有代表性的信任机制：(1)使用信任传递行和矩阵迭代的 EigenTrust[8]，EigenTrust 定义了有向图，使用类似于 PageRank[9]，通过迭代计算来获得每个节点的全局信任度，同时提出了基于 DHT 的安全分布式计算方式；(2)已经部署并使用的基于对文件投票的 Credence[10]，它是建立在 Gnutella[11]之上的主观、独立、局部、阈值的信任机制；(3)在 P2P 文件共享系统中使用文件的平均保留时间来计算信任值的 LIP[12]，LIP 发现并证明“用户倾向于更长时间地保留真实文件，而较快地删除污染文件”；(4)安全的信任机制架构 TrustGuard[13]，它是建立在 PeerTrust[14]之上的安全信任机制框架。

信任机制中的信任度量和评估，其实质是采用一种相对的方法对安全信息进行度量和评估，能够较好地反映出分布式环境下的多变性和不确定性，并且该方法较适合信任信息收集评估的自动化实现。但当前的一些代表性的信任度评估模型还存在一些问题：(1)信任的表述和度量的合理性有待于进一步解释，现有的模型倾向于采用事件概率的方式来表述和度量信任关系，都是基于一定的概率分布假设；(2)不能很好地解决恶意推荐对信任度评估的影响，现有的模型大多采用求简单算术平均的方法综合多个不同推荐路径的信任度；(3)当前的信任度评估模型缺少灵活的机制，如参数设置，以反映不同主体进行信任评估时所具有的个性特点；(4)有些模型虽有信任的推导和综合公式，但没有解决初始信任值如何获得的问题。(5)现有的 P2P 环境中的信任管理机制往往只是考虑了节点的身份认证，并没有涉及到如何管理节点对资源的访问控制权限。

3 轻量级节点证书(LC)

本节介绍对等网络中节点所拥有的轻量级节点证书，重点将介绍节点证书中有关节点信任度信息的计算和更新。

3.1 节点证书概述

对等网络有其实时性、动态性等特点，需要寻求一种简单，快速的方法来完成对节点身份的确认，并且传递节点的角色信息，以及快速地完成角色到节点的指派。一种值得考虑的办法是采用 x.509 证书来证明节点的身份，但是要维持各个不同节点的不同的访问控制权限，必须在节点的属性信息中含有节点的角色信息，这可以通过属性证书来实现。但是，在一个高度动态的 P2P 网络环境中，同时维持身份证书和属性证书的系统开销是很大的，而且这种方法不得不将节点的身份确认和节点的授权完全分开。典型的 x.509 证书一般来说都有一个比较长的生命周期，且它的撤销需要维持一个证书回收列表(CRLs)，这都会带来较大的系统开销，显然不适合动态的对等网络环境。

为了解决在 P2P 网络中使用身份证书来维持节点的角色等信息的问题，本文提出建立一种轻量级节点证书(LC)。这种证书可以在动态的和敏感的对等网络环境中同时完成节点的身份认定和授权的功能，其比 x.509 证书更加轻便，而且更加灵活，能更好地适应 P2P 环境。

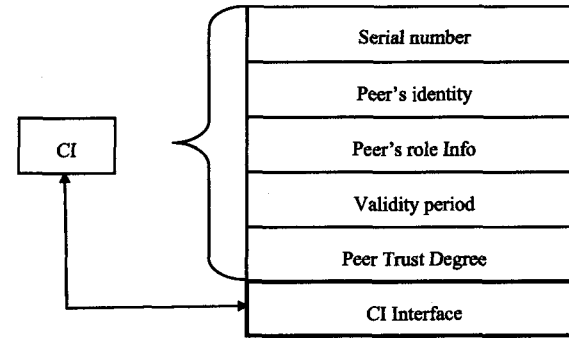

图 1 轻量级节点证书(LC)

LC 中主要由节点的身份信息和授权信息来组成，如图 1 所示，在一个典型的 P2P 环境中，主要包括：序列号(Serial number)，节点 ID(Peer's identity)，节点角色信息(Peer's role Info)以及证书有效期(Validity period)，以及节点的信任度(Peer Trust Degree)。同时，P2P 网络中有一个证书的发行者，在本文中称之为 CI(Certificates Issuer)。当证书颁发给某个节点时，需要初始化这些信息，其中节点 ID 是节点的唯一标识，节点身份信息用于对节点身份的第一级验证。节点角色信息指为该节点所指派的角色，其间接地指明了该角色对资源和服务的访问权限。证书有效期指的是证书的有效期限，只有在这个时间段内，该证书才能被 CI 所承认。这样，在一定程度上可以适应节点频繁地动态加入和离开。

3.2 节点信任度的计算

为了给节点的好坏提供一个度量，让每个节点拥有一个信任度(Trust)。系统可以根据节点的信任度的高低来决定是否给该节点颁发或者收回给节点的证书。该信任度存在于节点的证书中，在请求资源的时候提交证书以便被审核。该模型中给出了这样一个激励机制，提供高品质的服务则可提高自身的 Trust，反之提供虚假或劣质的服务则降低其 Trust 作为惩罚。

信任值的计算采用基于评价的全局信任模型，根据节点的交易历史评价记录和节点的信任值来综合计算节点新的信任值。历史记录表中只存放一定时间范围内的服务评价值。因为 P2P 是一个高度动态不确定的网络环境，而 peer 自身也处于动态变化中。因此过于久远的历史记录对当前 Trust 的计算参考意义较小。历史评价记录会不断更新，只存放一定时间范围内的服务评价值。历史记录的不断更新有利于计算更为精确有用的信任值。

交易历史记录是用来记录节点一次信息交换的过程，它包含了节点对信息交换的服务质量的评价值和信息交换的时间等信息。peer 的交易历史记录是计算 Trust 的重要依据。

在一次交易完成以后，消费节点根据本次服务质量公平地给出对服务节点所提供服务的质量的评价值。peer 的历史交易记录是计算 Trust 的重要依据。每个节点带有一个文档结点，用来存放其他节点的历史记录表，表中记录了节点 id、评价值、被评价节点 id 和时间序号这四项信息。文档节点对应存放哪个节点的历史记录通过分布哈希表(DHT)机制决定，使用 CAN 来实现 DHT 机制。

如果只是单纯地用 0 表示对服务不满意或 1 表示对服务满意，就不能准确细化地评价服务质量。根据服务节点所提供的服务质量，把服务分成四种类别，如表 1。把服务质量形式化定义为一个集合：$SQ=\{G,L,N,W\}$，则表 1 对应的 $SQ=\{1,0.5,0,-1\}$。集合 SQ 各元素的数值可以根据不同资源共享系统的需求具体设置。

考虑到实际上大多数 peer 一般都能提供正确的服务，为了加大对恶意节点的惩罚力度可将 SQ 中的 N 和 W 都设为非正值。N 和 W 表示的服务均为不满意的服务，将导致节点信任值的降低。值得注意的是把 No Response 视为不满意的服务行为，因为倘若 peer 频繁地连接又马上离开系统，这一高度动态的行为将降低系统对服务的响应能力。

表 1　四种不同的服务质量

服务质量	评价值	服务描述
Good	1	服务节点提供了高质量服务，交易非常顺利。
Low Grade	0.5	服务节点提供的正确服务，但是服务有些延迟或降低。
No Response	0	服务节点拒绝合理的服务请求响应。
Worst Behavior	−1	服务节点提供错误信息，甚至提供恶意的文件下载。

信任度是对节点信任程度的定量表示。在本文中，把信任度表示为一个实数区间，如[−1,1]，其中−1 代表完全不信任，1 代表完全信任。

信任值的计算采用基于评价的全局信任模型[X]。在对节点进行信任评估时，综合考虑其他与之进行过信息交换的节点对其的评价信息。对节点 ps 的信任值计算来源于两部分：一部分称为信任评价 T_{Eu}，它是所有请求过节点 ps 的资源和服务的请求节点的信任值与它们曾对 ps 的评价值乘积之和的平均值；另一部分是资源节点 ps 自身的信任值 T_{dd}。

考虑到 P2P 是一个高度动态不确定的网络环境，而 peer 自身也处于动态变化中。曾经能够提供诚实优质服务的“好节点”，可能随着网络环境的改变或主观原因，已经退化成“坏节点”。过于久远的历史记录对当前 Trust 的计算参考意义较小，因此有必要考虑评价记录的时间效应。为了解决时间给信任评价值的计算带来的影响，在一次新的信息交易中对服务节点信任值的计算时增加考虑时间衰减因子 δ。时间最近的交易评价更为重要，对应的权重较高；时间较远的交易评价较不重要，对应的权重也较低。

因此，当请求节点 Pr 广播服务请求时，为了便于在历史数据库中进行查询，应给出历史交易事件发生的时间段$\{t_1, t_2, \cdots, t_L\}$，$t_k<t_{k+1}$，且 $1\leqslant k\leqslant L$，t_L 表示最近的时间。在获得了它所感兴趣的服务节点的历史交易数据后，Pr 还应在计算新的信任值前对交易评价的权重进行赋值 $\delta=\{\delta_k,\ 1\leqslant k\leqslant L\}$，$\delta_k<\delta_{k+1}$。

在考虑时间衰减因子 δ 的情况下，相应得到的信任计算公式如下：

公式(1)在一次新的信息交互中资源请求节点为 Pr，服务节点 Ps，且假定 $E_{j\to s}^{(k)}$ 表示在时间段 k 节点 Pj 对服务节点 Ps 的评价值，n 是 Pr 所获得的历史交易数据的总个数，则节点 Ps 的信任度计算公式如下：

$$Trust=A\times\frac{\sum(T_j\times\delta_k\times\sum E_{j\to s}^{(k)})}{n}+(1-A)T_{dd} \quad (1)$$

其中

$$T_{Eu}=\frac{\sum(T_j\times\delta_k\times\sum \dot{E}_{j\to s}^{(k)})}{n},A\in[0,1],\text{且 } Trust,T_{Eu},T_{dd}\in[-1,1] \quad (2)$$

信任评价 T_{Eu} 其实是综合考虑了推荐信任和直接信任两方面，推荐信任是来自其他节点的推荐评价，直接信任是来自请求节点与资源提供节点的直接交互历史经验。推荐信任要综合评价节点的信任值和评价值的时间衰减效应，而直接信任是完全采纳评价值，因为请求节点 Pr 有理由相信它的直接交易经验具有更高的参考价值。

时间段 t_k 对应的权重计算公式如下：

$$\delta_k=e^{\frac{-u}{k}},u\in\{1,2,3,\cdots,n\},1\leqslant k\leqslant L \quad (3)$$

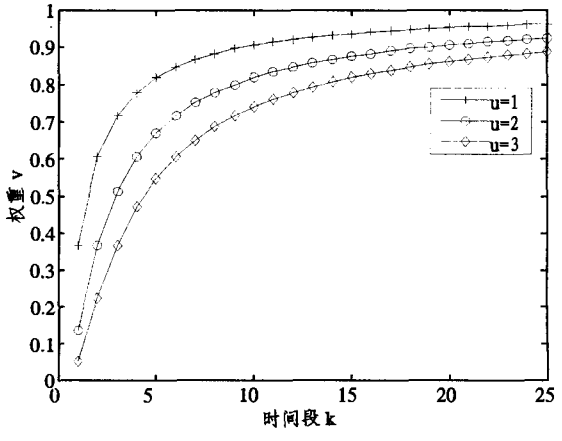

图 2　δ_k 的函数曲线

根据公式(2)，只要给出参数 u，则对应的权重 δ_k 便可计算出来。因为 δ_k 是单调递增的函数，所以 $\delta_k<\delta_{k+1}$，这就满足

了最近时间的交易评价对应的权重更高。假设 $L=25$，相应的 δ_k 的函数曲线如图 2 所示。图 2 表明，参数 u 越大，函数计算得到的 δ_k 值就越小。从图 2 中可以看到：$u=1$ 时函数曲线位于最上方，则在 k 值相等的情况下，对应的 δ_k 比 u 的任何其他取值都要大；u 的取值越大，在同一 k 值时计算得到的 δ_k 就越小。

本文中对于节点的信任度定义了一个阈值 ζ，当某个节点证书中的信任度大于这个阈值的时候，该证书有效，节点可以对资源提出访问请求。一旦证书中的信任度小于阈值 ζ，则该证书自动失效，节点对资源的访问请求将被驳回，且在一个规定的时间 Γ 内，该节点将无法申请新的证书。下面将介绍 P2P 网络中节点如何申请证书，并根据证书中的信息来请求所要访问的资源。

4 P2P 网络环境中基于证书的 RBAC 访问控制框架

本节讨论的是在一个大规模的 P2P 网络环境中，节点在请求资源的时候如何传递证书以证明自己具备对资源的访问权限。在这里所讨论的是一个混合型 P2P 网络，资源和资源的请求者都受相应的超级节点(Ultrapeer)的控制。主要过程如图 3 所示：一个受超级节点 1(Ultrapeer1)控制的资源的请求节点(Alice)，请求访问一个受超级节点 4(Ultrapeer4)控制的资源节点(Bob)。在初始条件下假设 Alice 并不清楚谁是资源的提供者，需要在超级节点间遍历以寻找资源的提供者，资源的提供者对请求者的验证也分成两部分，首先是由 CI 验证节点的身份，称为第一级验证，也叫身份验证。通过第一级验证的节点可以获得包含其角色信息的 LC。当请求节点 Alice 向资源的提供节点 Bob 发出请求的时候，资源节点的超级节点(超级节点 4)需要对请求节点的 LC 证书进行验证，将 Alice 的身份证书 LC 转发给 CI，根据 LC 中的角色信息来询问 Alice 的角色是否具有访问 Bob 的资源的权限，如果验证成功，则将资源提供给请求者 Alice，如果验证失败，则拒绝 Alice 的此次访问，这称为第二级验证，也叫权限验证。

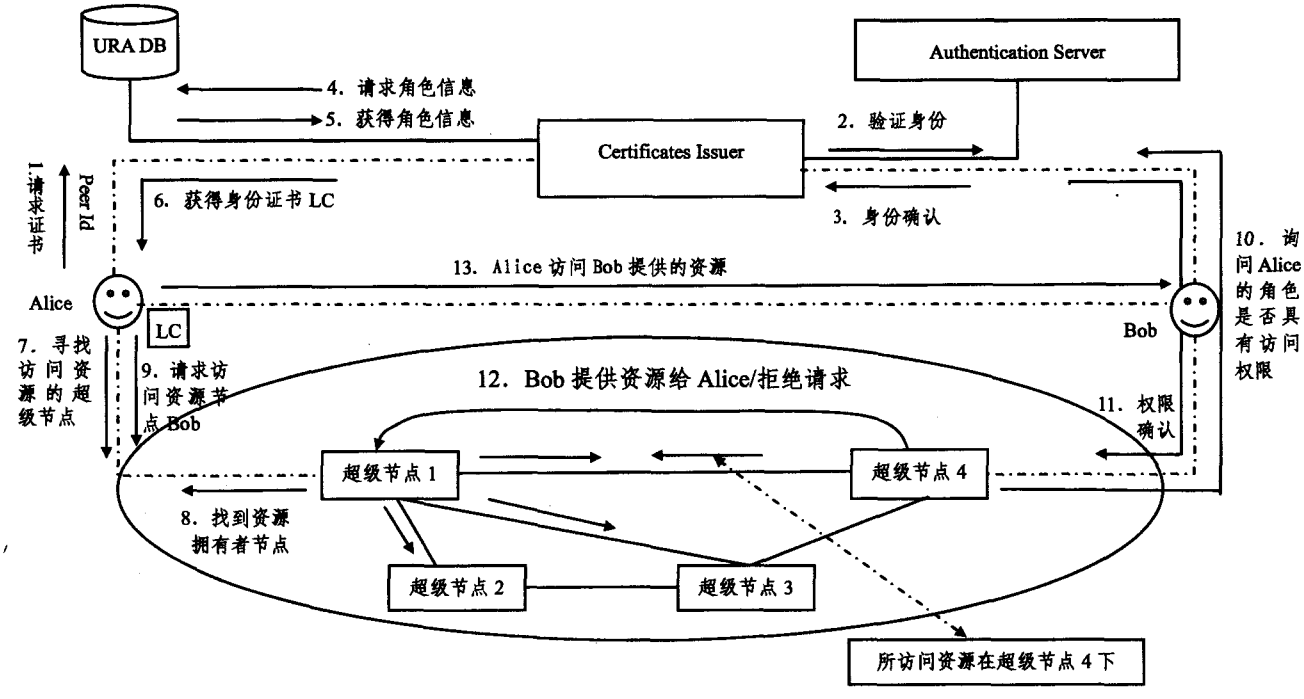

图 3 P2P 网络环境中基于 LC 的身份确认流程

从以上的过程可以看出，资源的请求节点 Alice 和资源的提供节点 Bob 之间的通讯都是经过其相应的超级节点来进行的。在上面的例子中，Alice 并不需要和任何非超级节点(普通节点)进行通讯，一个普通节点在资源请求的过程中总是只和其当前的超级节点或者资源提供节点的超级节点进行通讯。对于一个被请求节点(资源提供者)也同样只和其当前的超级节点或请求节点的超级节点进行通讯。这样，每个节点的超级节点在这里充当了其管辖的普通节点的代理角色。这样就能显著地减少数量占绝大多数的普通节点的负担，能够提供更加灵活的身份认证和访问控制功能。由此可见，这种方式非常地适应动态的、普通节点加入和注销变化频繁的 P2P 网络。

URA DB 是维护用户和角色指派关系的数据库。在本文中，这是一个集中式的数据库，处于混合式的 P2P 网络中的中央节点上。这种网络结构有如下几个好处：

1. 在大规模动态 P2P 网络中，节点的加入和离开变化频繁，使用集中的 URA 数据库来管理节点与角色之间的指派关系，能更方便地维护和管理各个节点的权限。通过访问 URA 数据库，能比其他分散的管理方式更方便快速地从节点 LC 证书中的角色信息获得节点的权限。

2. 在多安全域的 P2P 环境中能方便地协调各个自治组织之间的权限管理。通过各个分布的 URA DB 之间的互操作，能够方便地实现不同域间的节点的职责分离(SoD)等安全约束。

Authentication Server 是身份认证服务器，主要完成节点的第一级身份验证，也即确认节点的基本身份，通过此验证的节点可以获得节点身份信息(Peer's authentication Info)。这同样也是一个集中式的服务，可以由 Kerberos 等方式来实现。

5 仿真实验及性能分析

为了对本文的框架和模型进行验证和分析，对基于

RBAC 的 P2P 网络环境进行了仿真模拟。在实验中，采用 Windows xp 作为操作系统平台，采用 JXTA 来实现一个带有 RBAC 服务的 P2P 系统。其中采用 JXTA 的 security 包来实现加密等功能，使得 CI 颁发的 LC 证书被有效地签名。在本实验中，没有采用 JXTA 的标准通讯机制，而是自己开发了节点间利用 java 的 networking 包通过 socket 进行通讯的方案。其目的是开发基于 XML 的通信协议，实现节点间互操作。通过实现这样一个基于 XML 的通讯子系统，所有的互操作的节点间的消息都通过 XML 格式进行传输和交换，相对于 JXTA 的通讯机制，这样一种子系统应该更容易被理解和操纵。

图 4 表示的是对网络性能评估的实验结果。在本实验中，比较了基于传统的 x.509 证书的 P2P 间的信任管理机制和基于轻量级证书 LC 的性能。实验网络包括 5 个路由器，1000 个对等节点和 3 个超级节点。每两个节点间的通讯延迟设定为 7ms，实验中总共设定 10 个角色，每个角色设定 10 个权限，该图中 x 轴指的是网络中的节点个数，y 轴为节点从发出资源访问请求到获得资源访问许可的时间。

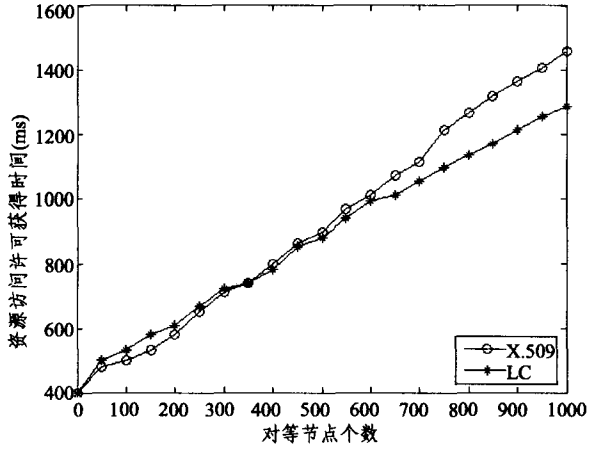

图 4　网络性能评估的实验结果

从图 4 的结果来看，随着节点数的增多，使用轻量级证书 LC 的对等网络中的用户从请求资源到获取访问资源许可的时间要远远低于传统的使用 X.509 的方式。本文所提出的基于 RBAC 的 P2P 网络信任模型，不仅仅验证了用户的身份，防止了恶意节点的破坏，而且进一步提供了细粒度的访问控制机制，在保证系统运行效率的情况下，使得资源只能被合法的、已授权的用户所访问。

结束语　对等网络中的安全问题已成为影响对等网应用的主要问题。本文提出一种信任管理加权限控制的双重验证方法来实现 P2P 网络环境中的节点协作和资源访问等安全互操作。在该信任模型中，用户节点通过使用一种轻量级的身份证书来证明自己的身份和获得对资源的相关访问控制权限。当用户请求资源的时候，首先要通过身份验证来获得角色信息。然后通过证书中的角色信息来获得对资源的访问权限。

用户的身份证书中含有节点用户的信任度参数，其随用户的访问行为动态变化。当用户进行非法操作的时候，该信任度会不断减少。当用户的信任度减少到某个设定的阈值时，其证书会被吊销，并且在规定的时间内不能再申请身份证书。本文给出了用户信任度的计算模型，这种方式能有效地识别、遏制和打击恶意节点的非法操作，加强对等网络的安全性。

参 考 文 献

[1] Aberer K, Despotovic Z. Managing Trust in a Peer-To-Peer Information System // Proc. of ACM International Conference on Information and Knowledge Management (CIKM). 2001

[2] Kamvar S, Schlosser M, Garcia-Molina H. The Eigentrust Algorithm for Reputation Management in P2P Networks // Proc. of the Twelfth International World Wide Web Conference. Budapest, 2003

[3] McKnight D H, Chervany N L. The Meanings of Trust. Technical Report WP9604. University of Minnesota Management Information Systems Research Center, 1996

[4] Selcuk A, Uzun E, Pariente M. A Reputation-Based Trust Management System for P2P Networks // 4th IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID). 2004

[5] Ratnasamy S. Routing algorithms for DHTs: Some open questions // Kaashoek F, ed. Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. Cambridge: Springer-Verlag, 2002: 45-52

[6] Wang Yan, Lin Fu-ren. Trust and Risk Evaluation of Transactions with Different Amounts in Peer-to-Peer E-commerce Environments // IEEE International Conference on e-Business Engineering (ICEBE'06). IEEE, 2006: 102-109

[7] Kamvar S. EigenRep: Reputation Management in P2P Networks. Technical Report, SCCM-02-16. Stanford University, 2002

[8] Kamvar S D, Schlosser M T. EigenRep: Reputation management in P2P networks // Lawrence S, ed. Proc. of the 12th Int'l World Wide Web Conf. Budapest: ACM Press: 123-134

[9] Bianchini M, Gori M, Scarselli F. PageRank and Web communities; Web Intelligence, 2003. WI 2003 // Proceedings. IEEE/WIC International Conference on. Oct. 2003: 365-371

[10] Liu Jun, Li Zhe, Lin Dan, et al. A security enhanced AODV routing protocol based on the credence mechanism. Wireless Communications, Networking and Mobile Computing, 2005 // Proceedings. 2005 International Conference on. Volume 2, Sept. 2005: 719-722

[11] Nagaraja K, Rollins S, Khambatti M. peer-to-peer community: looking beyond the legacy of Napster and Gnutella. Distributed Systems Online, IEEE, 2006, 7(3)

[12] Damiani E, Vimercati S, Paraboschi S, et al. A reputation-based approach for choosing reliable resources in peer-to-peer networks. In CCS, 2002

[13] Srivatsa M, Xiong Li, Liu Ling. TrustGuard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks. WWW 2005, Chiba, Japan, May 2005

[14] Xiong Li, Liu Ling. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7)