ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.18, No.4, April 2007, pp.955−966
DOI: 10.1360/jos180955

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

新型网络环境下的访问控制技术*

林 闯[1+], 封富君[1,2], 李俊山[2]

[1](清华大学 计算机科学与技术系,北京 100084)

[2](第二炮兵工程学院 计算机系,陕西 西安 710025)

Access Control in New Network Environment

LIN Chuang[1+], FENG Fu-Jun[1,2], LI Jun-Shan[2]

[1](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

[2](Department of Computer Science, The Second Artillery Engineering College, Xi'an 710025, China)

+ Corresponding author: Phn: +86-10-62783596, E-mail: chlin@tsinghua.edu.cn, http://www.tsinghua.edu.cn

Lin C, Feng FJ, Li JS. Access control in new network environment. *Journal of Software*, 2007,18(4):955−966.
http://www.jos.org.cn/1000-9825/18/955.htm

Abstract: Access control is an important technology for system security, and its mechanism is different for different networks. This paper first introduces the characteristics and applications of three traditional access control policies which are DAC (discretionary access control), MAC (mandatory access control) and RBAC (role-based access control), introduces the UCON (usage control) model, and then analyzes access control technology and current researches in Grid, P2P and wireless environment respectively. In addition, this paper proposes that trustworthy networks as the developing goal of the next generation Internet require using trust-based the access control model to assure security. This paper investigates on the trust and reputation model in detail, and finally gives the prospects of access control.

Key words: DAC (discretionary access control); MAC (mandatory access control); RBAC (role-based access control); trust model

摘 要: 访问控制是系统安全的关键技术,不同网络环境下的访问控制机制也是不同的.首先对 3 种传统的访问控制策略加以介绍,给出 DAC(discretionary access control),MAC(mandatory access control)和 RBAC(role-based access control)各自的特点及应用,并简要介绍下一代访问控制 UCON(usage control)模型,然后分别针对网格、P2P、无线网络环境下的访问控制技术及目前的研究现状进行总结,详细阐述可信网络作为下一代互联网发展的必然目标,要求基于可信的访问控制模型保证其安全性,对可信和信誉模型进行了研究,最后给出访问控制技术的发展趋势.

关键词: 自主访问控制;强制访问控制;基于角色的访问控制;可信模型

中图法分类号: TP393 文献标识码: A

访问控制技术起源于 20 世纪 70 年代,当时是为了满足管理大型主机系统上共享数据授权访问的需要.但随着计算机技术和应用的发展,特别是网络应用的发展,这一技术的思想和方法迅速应用于信息系统的各个领

* Supported by the National Natural Science Foundation of China under Grant Nos.90412012, 60273009 (国家自然科学基金); the National Science Foundation for Distinguished Youth Scholar of China under Grant No.60429202 (国家杰出青年科学基金)

Received 2006-04-12; Accepted 2006-07-26

域.在 30 多年的发展过程中,先后出现了多种重要的访问控制技术,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),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.访问控制技术作为实现安全操作系统的核心技术,是系统安全的一个解决方案,是保证信息机密性和完整性的关键技术,对访问控制的研究已成为计算机科学的研究热点之一.

最早由 Lampson[1]提出了访问控制的形式化和机制描述,引入了主体、客体和访问矩阵的概念,它们是访问控制的基本概念.对访问控制模型的研究,从早期的 20 世纪六、七十年代至今,大致经历了以下 4 个阶段:

(1) 20 世纪六、七十年代应用于大型主机系统中的访问控制模型,较典型的是 Bell-Lapadula 模型[2]和 HRU 模型[3].Bell-Lapadula 模型着重系统的机密性,遵循两个基本的规则:“不上读”和“不下写”,以此实现强制存取控制,防止具有高安全级别的信息流入低安全级别的客体,主要应用于军事系统中.

(2) 美国国防部(Department of Defense,简称 DoD)在 1985 年公布的“可信计算机安全评价标准(trusted computer system evaluation criteria,简称 TCSEC)”[4]中明确提出了访问控制在计算机安全系统中的重要作用,并指出一般的访问控制机制有两种:自主访问控制 DAC 和强制访问控制 MAC.目前,DAC 和 MAC 被应用在很多领域.

(3) 从 1992 年最早的 RBAC 模型,即 Ferraiolo-Kuhn 模型[5]的提出,到 Sandhu 等人对 RBAC 模型的研究,先后提出了 RBAC96[6],ARBAC97[7],ARBAC99[8]模型,再到 2001 年 NIST RBAC 标准的提出[9].Ferraiolo-Kuhn 模型将现有的面向应用的方法应用到 RBAC 模型中,是 RBAC 最初的形式化描述.NIST RBAC 参考模型对角色进行了详细的研究,在用户和访问权限之间引入了角色的概念,为 RBAC 模型提供了参考.

(4) 此后,对访问控制模型的研究扩展到更多的领域,比较有代表性的有:应用于工作流系统或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)[10]、基于任务和角色的访问控制模型(task-role-based access control,简称 T-RBAC)[11]以及被称作下一代访问控制模型的使用控制(usage control,简称 UCON)模型[12,13],也称其为 ABC 模型[14].

访问控制作为系统安全的关键技术,既是一个古老的内容又面临着挑战.随着网络技术的发展,对网络安全的研究成为当前的研究热点,而访问控制技术也日益受到更多人的关注.本文针对不同网络环境下的访问控制技术进行研究,介绍了目前的研究现状与发展,并提出了一些未来访问控制的研究思路.

本文第 1 节介绍传统访问控制的 3 种安全策略,即主动访问控制、强制访问控制和基于角色的访问控制各自的特点及应用,并简要介绍 UCON 模型.第 2 节阐述在网格、P2P 和无线网络环境下的访问控制技术及其研究现状.第 3 节对可信网络中基于可信的访问控制模型进行研究.最后在第 4 节中对全文进行总结,指出访问控制的发展趋势.

1 访问控制策略

访问控制策略是面向应用的,可以跨越多个计算平台,可以基于最小特权、权能、认证、责任或利益冲突.访问控制策略往往是动态变化的,是随着商业因素、政府规则和环境条件而变化的,然而策略需求在系统设计时是无法完全确定的,因此,系统必须按照不断变化的策略进行设计.图 1 是访问控制的一般策略.访问控制策略最常用的是主动访问控制、强制访问控制和基于角色的访问控制.DAC 根据主体的身份和授权来决定访问模式,但信息在移动过程中主体可能会将访问权限传递给其他人,使访问权限关系发生改变;MAC 根据主体和客体的安全级别标记来决定访问模式,实现信息的单向流动,但它过于强调保密性,对系统的授权管理不便,不够灵活.总之,DAC 限制太弱,MAC 限制太强,且二者的工作量较大,不便管理.RBAC 则可以折衷以上问题,角色

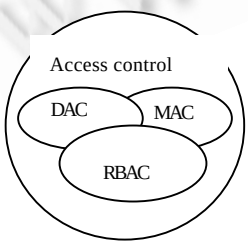

Fig.1 General access control policies

图 1 访问控制的一般模式

控制相对独立,根据具体的系统需求可以使某些角色接近 DAC,某些角色接近 MAC,于是出现了图 1 中 3 种访问控制策略的交集.

1.1 自主访问控制

自主访问控制是目前计算机系统中实现最多的访问控制机制,其核心思想是:主体的拥有者通常是它的建立者,可以主动授权给其他人访问该主体.因此,DAC 又称为基于主体的访问控制.DAC 的实现方法一般是建立系统访问控制矩阵,矩阵的行对应系统的主体,列对应系统的客体,元素表示主体对客体的访问权限.为了提高系统性能,在实际应用中常常是建立基于行(主体)或列(客体)的访问控制方法.访问控制表(access control list,简称 ACL)是实现自主访问控制最好的方法,访问控制系统通过检测 ACL 来决定访问是否被授权或拒绝.

DAC 根据用户的身份及允许访问权限决定其访问操作,这种访问控制机制的灵活性较高,被广泛地用在商业领域,尤其是在操作系统和关系数据库系统上.然而,也正是由于这种灵活性使信息安全性能有所降低,DAC 也存在一些缺点:授权读是可传递的,一旦访问权被传递出去将难以控制,使访问权的管理相当困难,会带来严重的安全问题;DAC 机制易遭到特洛伊木马攻击;在大型系统中,主、客体的数量巨大,使用 DAC 将使系统开销大到难以支付的程度.

1.2 强制访问控制

由于自主访问控制不能抵御特洛伊木马的攻击,强制访问控制作为一种基于格(lattice-based)的访问控制应运而生.强制访问控制最早被应用在军方系统中,在军事和安全部门中应用较多,访问者拥有包含等级列表的许可,其中定义了可以访问哪个级别的客体,其访问策略是由授权中心决定的强制性的规则.MAC 的本质是基于格的非循环单向信息流政策,通过无法回避的存取限制来阻止直接或间接的非法入侵,它的两个关键规则是:不向上读和不向下写,即信息流只能从低安全级向高安全级流动,任何违反非循环信息流的行为都是被禁止的.

MAC 同样具有一些弱点:对用户恶意泄漏信息无能为力;虽然 MAC 增强了信息的机密性,但不能实施完整性控制,而网络应用对信息完整性具有较高的要求,因此,MAC 可能无法胜任某些网络应用;在 MAC 系统中,实现单向信息流的前提是系统中不存在逆向潜信道,否则会导致信息违反规则的流动,这就给系统增加了安全性漏洞;此外,MAC 过于强调保密性,对系统的授权管理不便,不够灵活.

1.3 基于角色的访问控制

随着网络的发展和 Internet 的广泛应用,信息的完整性需求超过了机密性,传统的 DAC/MAC 策略已无法满足信息完整性的要求,于是提出了基于角色的访问控制.RBAC 现在已较为成熟,并且在许多大型系统中得以实现.2001 年 8 月,NIST 发表了 RBAC 建议标准[9],此建议标准综合了该领域众多研究者的研究成果,描述了 RBAC 系统最基本的特征,旨在提供一个权威的、可用的 RBAC 参考规范,为 RBAC 的进一步研究指明了方向.

NIST 包括两个部分:RBAC 参考模型和 RBAC 功能规范.RBAC 参考模型给出了 RBAC 集合和关系的严格定义,包括 4 个部分:核心 RBAC(core RBAC)、等级 RBAC(hierarchical RBAC)、静态职责分离(static separation of duties,简称 SSD)和动态职责分离(dynamic separation of duties,简称 DSD).RBAC 功能规范为每个组件定义了关于创建和维护 RBAC 集合和关系的管理功能、系统支持功能和审查功能,这里不再详述.

目前,RBAC 被应用在各个企业领域,包括操作系统、数据库管理系统、PKI(public key infrastructure)、工作流管理系统和 Web 服务等领域.驱动 RBAC 发展的动力是在简化安全策略管理的同时,允许灵活地定义安全策略,这一点使得在过去的几年中,无论是对 RBAC 理论研究还是实现 RBAC 的现实产品都有了很大的发展.随着 RBAC 的 4 层模型和各种 RBAC 规范的逐步建立,RBAC 技术必将在各领域迅速发展并得到充分的应用.

1.4 使用控制模型

UCON 模型包含 3 个基本元素:主体(subject)、客体(object)、权限(right)和另外 3 个与授权有关的元素:授权规则(authorization rule)、条件(condition)、义务(obligation),如图 2 所示.UCON 模型将义务、条件和授权作为使用决策进程的一部分,提供了一种更好的决策能力.授权是基于主体、客体的属性以及所请求的权利进行

的,每一个访问都有有限的期限,在访问之前往往需要授权,而且在访问的过程中也可能需要授权.

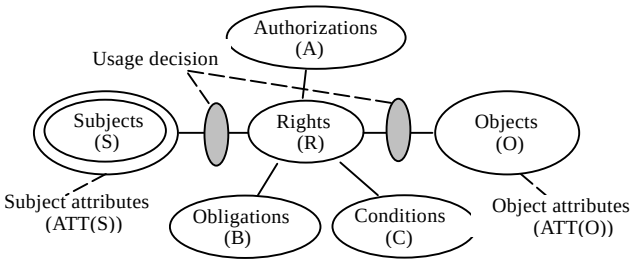

Fig.2 UCON model
图 2 UCON 模型

可变属性(mutable attribute)的引入是 UCON 模型与其他访问控制模型的最大差别,可变属性会随着访问对象的结果而改变,而不可变属性仅能通过管理行为改变.UCON 模型不仅包含了 DAC,MAC 和 RBAC,而且还包含了数字版权管理(digital rights management,简称 DRM)、信任管理等,涵盖了现代商务和信息系统需求中的安全和隐私这两个重要的问题.因此,UCON 模型为研究下一代访问控制提供了一种新方法,被称作下一代访问控制模型.

2 新型网络环境下的访问控制技术

2.1 网格中的访问控制

网格(grid)是近年来逐渐兴起的一个研究领域,当前的 Internet 技术实现了计算机硬件的连通,Web 技术实现了网页的连通,而网格技术是要把整个因特网上的各种资源整合成一台巨大的计算机,从而实现资源共享与协同工作.网格为每个人提供的是完全屏蔽了底层实现的、易于使用的、充分共享的资源操作平台.网格要达到资源共享的目的,必须解决资源的访问控制问题.网格的访问控制必须建立在现有的访问控制系统之上,但是,由于网格跨越多个不同的地点和不同的自治域,每个域的访问控制策略和需求可能不同,这使得资源的访问控制更加复杂,所以,传统的访问控制方法必须进行扩展才能移植到网格系统中.网格环境下需要动态和异构的访问控制策略,由于不同的异构系统有不同的需求,我们不可能期望为异构系统建立一个通用的认证标准.

目前常用的有 3 种网格计算环境:Condor[15],Legion[16]和 Globus[17],这 3 种网格计算中的访问控制一般是通过身份证书和本地审计来实现的,用户通常在请求服务之前要求注册到服务提供者,当用户和资源数量增加且用户动态变化的时候,这种方法的可扩展性不好.由于用户和资源可能在不同的域中,而且彼此可能没有了解,因此,基于身份的访问控制不能满足网格计算的需求,而传统的网格访问控制机制忽略了实体之间的区分和交互,并不能很好地应用于网格环境下.文献[18]为网格应用提出了一种基于动态角色和上下文的访问控制(role and context-based access control,简称 RCBAC)模型,在 RBAC 模型中加入了上下文约束,保持了 RBAC 的原有优点,根据收集到的上下文相关信息来动态地为用户授予权限,较好地考虑到了网格环境下资源的动态性,能够动态实现上下文相关的访问控制管理.

目前,网格计算和语义 Web 技术成为 Internet 研究领域的分支,并发展得很快,将会促进网格服务的进一步发展.文献[19]使用语义 Web 技术为面向服务的开放异构网格环境提出了一种语义访问控制(semantic access control)机制,使用语义策略语言(semantic policy language,简称 SPL)对系统中的实体和策略进行语义描述和分析,并给出了冲突语义的解决办法.该模型能够根据需求、主体、环境、服务和策略的语义属性来动态地保护资源,可以很容易地制定访问决策,适用于异构和复杂访问控制环境中,能够满足网格计算的需求.

可信协商(trust negotiation)是动态环境下建立可信的一种有效的方法,很适用于网格计算环境,因为它能够基于属性而不是身份,使不同安全域中的用户通过相互交换证书来动态建立相互的信任,这样避免了通过注册来获得访问权限.文献[20]提出了一种可适应的可信协商访问控制(adaptive trust negotiation and access control, 简称 ATNAC)框架,该框架建立在两个系统上:GAA-API 和 TrustBuilder,前者根据动态变化的系统安全需求制定访问控制策略,后者检测敏感信息是何时或怎样泄露的.图 3 为 ATNAC 框架,分为 3 级:可信协商级、访问控制级和服务级.该框架为不同安全域中的服务请求和服务提供者之间建立了可信关系,防止敏感信息的泄漏,并且可检测 DDOS 攻击,适用于电子商务系统、虚拟组织和 P2P 系统的可信协商中.

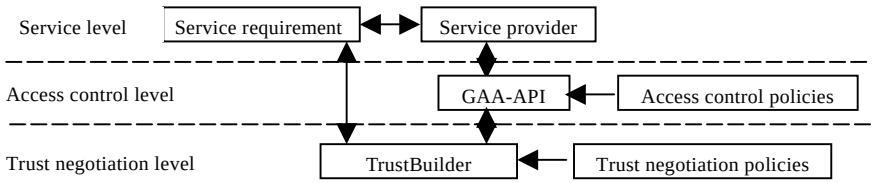

Fig.3 ATNAC framework

图 3 ATNAC 框架

2.2 P2P网络访问控制

随着 P2P 系统的应用,如文件共享系统、即时消息和分布式计算等,P2P 将成为网络技术的一项重要技术,并将决定 Internet 的未来,其安全问题势必会成为研究的热点,认证和访问控制是 P2P 系统安全的两个主要方面.然而当前,大多数对 P2P 系统的研究仅仅关注在提供服务上,而不是对资源的控制上.目前已经提出了一些适用于 P2P 系统的访问控制模型,如移动 P2P 协作环境下的访问控制[21]、基于 PKI 的多层访问控制平台[22]等.对 P2P 系统安全的研究主要集中在两个方面:

一是 peer 的选择问题,即如何有效地选择一个 peer 进行文件共享.这里涉及到 peer 的身份认证问题,研究较多的是基于可信和信誉的模型(trust and reputation based models)[23−26];

二是关于 peer 的安全组问题[27],即网络中的节点如何分组才能保证相互间能够安全地共享资源,且不会响应恶意的请求而消耗自身的服务能力.这里,认证和动态安全组管理是两种有效的方法.

在 P2P 系统中,peer 的加入和离开是动态的,为了建立一个安全的通信环境,提出了安全组的概念,这些组可以在本地实行特殊的安全策略,以保证组内的安全通信.当一个新 peer 要加入安全组时,必须通过当前活动安全组的认证,并选择所要归属的安全组,才能成为组中的成员.基于可信和信誉的模型可以解决 P2P 系统中的一些安全问题,但是当系统中的节点数目非常大时,每个 peer 都需要维护一个很大的可信列表,同时,计算复杂度也会随之增加,而将 peer 进行分组则可以很好地解决这个问题.此外,对请求的响应会消耗 peer 的能量,不可能对所有的请求都进行响应,必须有一个响应策略以丢弃一些恶意的请求,对组的访问控制策略则能够解决这个问题.此外,对于不同类型网络组成的异构可信网络,在不同的应用环境下,基于可信和信誉的模型可以提高网络的安全性和通信效率,适用于对可信要求程度较高的网络环境,如 Ad Hoc 网络.在第 3.2 节,我们会简要介绍可信和信誉模型能够满足所有访问控制的目标,并在网络环境下具有广泛的应用.

文献[28]扩展了基于可信和信誉模型以及安全组模型,提出了一个 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.同组中的 peer 遵循可信和信誉的模型,用来判断组中其他 peer 的行为,解决了 peer 的选择问题;用 RBAC 描述组访问的安全策略,解决了 P2P 系统中的请求响应问题.图 4 为一个简单的基于可信和信誉的分组 P2P 网络.

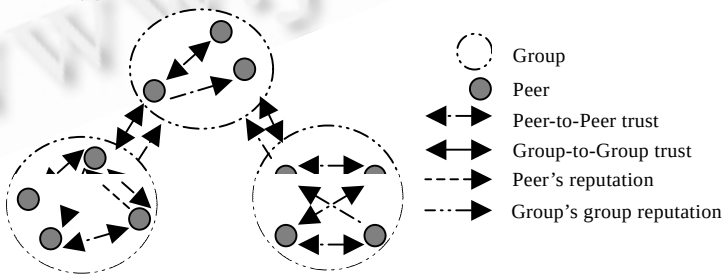

Fig.4 Trust and reputation based group P2P network

图 4 基于可信和信誉的分组 P2P 网络

虽然安全组概念的提出提高了通信的安全性,为 P2P 系统安全的研究提供了一种新的解决思路,但它仅通过身份和密码认证是不全面的,应该加入其他安全技术或安全机制,以保证机密性和安全性.文献[29]为 P2P 文

件共享系统提出了一个可信访问控制框架,该框架包括可信和信誉模型、公平参与机制和访问控制机制,将DAC扩展到P2P文件共享系统中,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.图5为P2P文件共享系统的访问控制实现结构,在本地文件系统和网络接口之间加入了认证和访问控制层.这种框架可以应用于其他P2P系统或分布式系统中,为可信访问控制模型的实现提供了有效的方法.

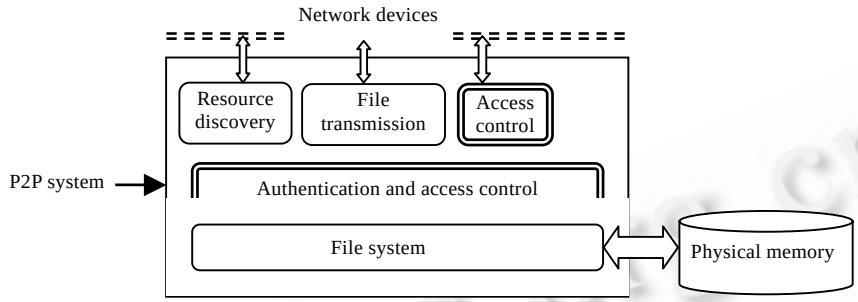

Fig.5 Access control implement structure in P2P file sharing system

图5 P2P文件共享系统中访问控制实现结构

认证服务是保障系统安全极其重要的手段之一,经常被用来区分系统中的合法用户与非法用户,其中,CA(certificate authority)认证是比较流行且有效的一种方法.但是,P2P系统的分散性决定了不能把CA认证直接应用于P2P系统.可见,在P2P系统中,访问控制与密钥、数字签名、证书、认证等技术的结合是解决系统安全访问控制的有效途径,P2P系统中的访问控制已不仅仅是对用户身份的认证和权限的限制.而如何体现交易的公平性、如何制定信誉机制和惩罚机制、如何提高用户之间交易的可信性和效率也引起了很大的关注.此外,对P2P系统基于可信和信誉访问控制模型的研究也将成为P2P网络安全的研究热点.

2.3 无线网络访问控制

随着计算机网络的发展,无线网络因其灵活和易于扩展等方面的优势,在众多领域得到了广泛的应用.无线网络的最大弱点是其安全性,它不像传统网络那样可以通过物理上的隔离来保证整个网络的信息安全,无线网络的信息可以被入侵者轻易截获,没有授权的访问将导致无线网络更加脆弱.因此,无线网络的安全控制主要是用户认证和授权.此外,对无线网络访问控制的研究也是无线网络安全的一个重要方面.

很多无线网络访问控制的研究是基于Stanford两层结构[30]:高层(应用层)的用户认证和密钥管理、低层(网络层或数据链路层)的细粒度访问控制.根据控制对象的粗细程度,访问控制可分为粗粒度和细粒度两种:通常把只控制到主机一级的称为粗粒度的访问控制,而把控制细到目录、文件、Web页面一级的称为细粒度访问控制.Stanford协议是一种基于两层结构和PKC(public key cryptosystems)、适用于有线和无线网络下的访问控制协议,能够满足安全需求,并克服了802.1X的一些缺陷,但是无法阻止DOS攻击或其他类型的攻击.图6所示为Stanford访问控制结构.

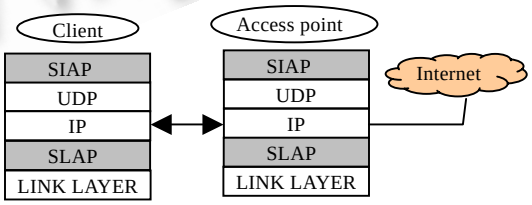

Fig.6 Stanford access control structure

图6 Stanford访问控制结构

Stanford协议结构由SIAP(secure internet access protocol)和SLAP(secure link access protocol)组成,SIAP运行在应用层,为SIAP客户端和服务器端提供相互认证,并更新会话密钥;SLAP运行在数据链路层之上,用与SIAP协商得到的会话密钥负责数据链路的访问控制.SIAP/SLAP协议在客户端设备和802.11接入点上运行,

因此没有认证服务中心,而是由接入点完成认证服务的功能.这种基于两层结构和 PKC 加密的方法是无线网络访问控制的理想解决方案.文献[31]在 Stanford 协议基础上加以改进,提出了新的访问控制模型,不仅能够阻止 DOS 攻击,保证用户身份的机密性,而且满足了前向安全性.

随着因特网技术、无线通信技术与电子技术的高速发展,无线传感器网络(wireless sensor network,简称 WSN)在世界范围内引起了广泛的关注,且被认为是 21 世纪最重要的技术之一,它将会对人类未来的生活方式产生深远影响.由于 WSN 自身的特点和各种应用的要求,导致了传统的无线协议很难在 WSN 中适用,这对 MAC 层协议的研究提出了挑战,近年来出现了很多以节能为主要目标的 MAC 层协议研究,成为 WSN 中一个新的研究热点.

WSN 的安全包括内部安全和外部安全:内部安全是指内部节点之间的通信或节点和基站之间的通信是安全的;外部安全是指外部用户和 WSN 之间的通信是安全的.目前对外部安全的完整性和可用性的研究较多,但对内部安全的机密性研究,即对 WSN 的访问控制研究相对较少.由于传感器设备在能量、计算和通信上的能力是有限的,传统的安全机制无法直接应用于 WSN 网络,此外,传感器节点通常放置在可触及的地方,容易受到物理攻击或被攻击者轻易捕获,这样,攻击者可以通过修改相应的程序将恶意节点置入网络中,从而控制整个网络.为了解决这个问题,需要为 WSN 提出新的安全机制.

在无线网络或 WSN 中,位置(location)信息对访问控制是很重要的,每个用户都与位置相关,而一个位置可以与多个用户相关,位置信息能够提高系统的安全性,如可以限制某位置范围内的用户可以访问资源、拥有某种权限,防止外来攻击者的入侵.传统的访问控制不能提供这种基于位置(location-based)的访问控制,必须对其进行扩展.文献[32]对 RBAC 进行扩展,引入位置的概念,提出了一个感知位置的 RBAC(location-aware RBAC)模型,将位置与 RBAC 中的所有组件相关联,并用位置信息决定一个用户是否有权访问某客体.该模型为无线移动环境下的访问控制提出了一个新的研究方向,可以应用于计算环境下.此外,对角色层次、静态 SoD、动态 SoD 及时态约束的研究,也是基于位置的访问控制模型需要考虑的因素.

无线网络的发展,使得 WSN 的应用也越来越广泛,其安全问题已引起关注.访问控制是计算机安全中的一个重要问题,但是在 WSN 中没有引起足够的重视.WSN 由于资源受限,节点的计算、通信和能量有限,拓扑结构动态性强等特点,使其安全问题较难实现.因此,WSN 的访问控制将是 WSN 安全的一个研究重点.可见,对无线网络访问控制的研究更多地涉及到密钥加密、密钥管理、认证协议、安全协议(如 IPSec/VPN),并考虑如何防止 DOS 攻击等.此外,目前对算法的研究较少,也将成为无线网络访问控制的一个研究热点.

2.4 访问控制模型的比较

访问控制的目标有以下 4 个方面:

(1) 机密性:防止信息泄露给未授权的用户;

(2) 完整性:防止未授权用户对信息的修改;

(3) 可用性:保障授权用户对系统信息的可访问性;

(4) 可审计性:防止用户对访问过某信息或执行过某一操作进行否认.

访问控制的目标主要是指机密性和完整性,访问控制模型的可扩展性也可作为一个衡量的指标,可扩展性体现了灵活性,一个好的模型应该易于扩展.由上文中对新型网络环境下访问控制模型的总结,可以看到访问控制在网络环境中的应用已相当广泛,目前使用较多的有基于身份、基于语义 Web、基于上下文、基于位置及基于可信和信誉的模型.表 1 对以上模型是否能够保证机密性和完整性、是否有好的可扩展性进行了比较.

基于身份的访问控制可以应用到所有的网络环境中,但由于实现简单,其安全性和可扩展性不好;基于语义 Web 的访问控制实质上是非策略性的描述,具有良好的可扩展性,主要应用在智能信息检索、分布式计算、Web Service 和企业数据管理等方面,不仅可以应用在网格环境下,还可以应用在 P2P 网络、WWW 服务和信誉度模型等方面;上下文信息的概念非常广泛,包括用户自身的状态和周围的环境,如用户所处的位置、行为特征等.基于上下文的访问控制具有较好的可扩展性,可应用于所有网络,如网格、P2P、无线网络等;基于位置的访问控制适用于与位置信息相关的网络,如无线移动通信网络、传感器网络和互联网服务等;基于可信和信誉的模型能

够保证机密性和完整性,且具有较好的可扩展性,可应用于对可信要求较高的网络中,如 Ad Hoc 网络、P2P 网络和可信网络等.

Table 1 Comparing of access control models

表 1 访问控制模型比较

Access control model	Confidentiality	Integrity	Scalability
Identity-Based access control model	Yes	No	No
Semantic Web-based access control model	—	—	Yes
Context-Based access control model	No	Yes	Yes
Location-Based access control model	No	Yes	Yes
Trust and reputation-based access control model	Yes	Yes	Yes

3 可信网络访问控制研究

3.1 可信网络体系结构

随着计算技术的普及,计算机系统应用日益广泛.由于计算机系统处理的任务多样化,计算机系统的工作环境普适化,计算机系统也越来越复杂,面临的各种人为和非人为的威胁也越来越多,如恶意攻击、垃圾邮件、计算机病毒等,导致人们对网络产生了不信任感.计算机系统能否正确、安全、高效地完成指定任务,即能否提供可信赖的服务能力,将成为研究人员关心的主要问题之一.计算机系统这种提供可信赖服务的能力就是可信性,如何确保计算机网络的可信性是未来计算新的研究方向.可信网络是可信计算发展的必然趋势,是下一代互联网发展的必然目标.

可信网络的研究已远远超出信息安全的可用性、完整性和机密性的内涵,其目标是保护计算信息网络的安全性、可用性和可控性,抵抗计算机病毒、蠕虫、黑客的入侵和攻击,杜绝安全漏洞和隐患,保证计算的高服务质量,为高可信计算提供一个安全、可靠的网络环境[33].可信网络体系结构充分考虑到了网络的复杂异构性,从系统的角度保障安全服务的一致性.图 7 是可信网络体系结构,其中:数据传输平面负责承载业务,并保障协议的可信性;可信控制平面则包括一组可信协议,提供完备的控制指令,实现对用户和网络运行信息的分布式采集、传播和处理,支持信任信息在可信用户间的共享,并驱动和协调具体的行为控制方式.数据平面接受可信控制平面的监管,可信控制平面则向数据平面开放某些访问接口,从而使得业务能够获知网络运行是否可信,网络也可以根据用户要求为业务定制某种模式的运行方式,授予更高的信任级别,体现更高的可信保障水平.

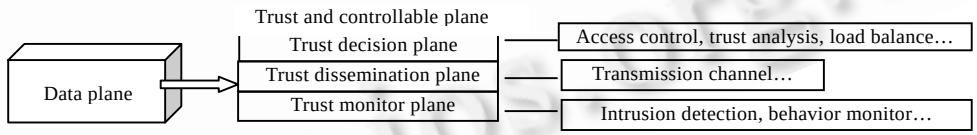

Fig.7 Trust network architecture

图 7 可信网络体系结构

其中,可信控制平面又分为可信监测平面、可信分发平面和可信决策平面.可信监测平面主要负责入侵检测、系统的行为监控以及网络组件行为可信性信息的收集,如身份、行为记录或信任推荐度等;可信分发平面为可信监测平面和可信决策平面提供有效的传输通道;可信决策平面根据访问控制策略对信息进行可信性分析,并将网络运行目标(可信度、路由可达性和负载均衡等)转化为控制信息,如行为接纳或拒绝、资源提供选择和包过滤等.

3.2 可信和信誉

很多文献中都提到了可信(trust)的概念,图 8 为文献[34]中提出的可信的分类.从图中可以看到可信行为产生的过程,可信是协同环境的基础,是一种连续的行为,而不是离散的,通常不具有继承性,但是通过学习过程可以对可信值进行动态更新.一般从两个方面来描述可信,即时间(time)和上下文(context),时间表现了可信的动态性,一个不可信的用户可能通过好的行为得到一个高的可信值,而一个可信用户也可能故意表现为不诚实的行

为;可信是上下文相关的,在不同方面得到的可信值是不同的.

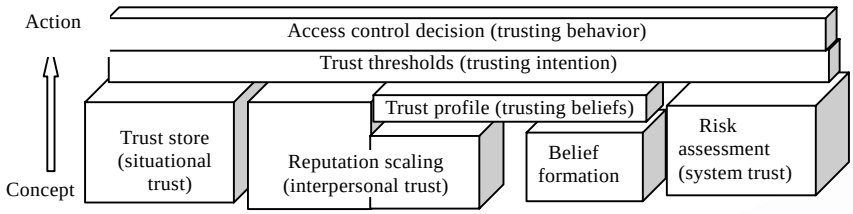

Fig.8 Trust classifications and structure

图 8 可信分类和结构

可信通常与信誉(reputation)相混淆,这里有必要将这两个概念加以区别:可信是主动的,它是一个用户对另一个用户某种能力的信任,建立在以往交易的满意度的评估上;信誉是被动的,是其他用户通过观察和交互过程对该用户的评价,一个用户的信誉值在不同情况和行为下都是不同的,且信誉是可信信息的集合,它是通过交互或资源共享的历史行为来预测该用户行为是否可信.虽然可信和信誉是两个不同的概念,但却都是上下文相关的,都具有多样性和动态性.

由于 Ad Hoc 网络主要应用在军事系统中,对可信和信誉的要求程度较高,因此对信誉系统的研究较多.目前信誉系统有 3 类:正信誉(positive reputation)、负信誉(negative reputation)和二者的结合.正信誉系统仅考虑节点正面的行为和反馈,如在 CORE[35]系统中节点之间通过协作建立正信誉值,其缺点是仅考虑了节点好的行为信息,而没有考虑负面的反馈.负信誉系统[36]仅考虑节点负面的行为和反馈,其前提是假设系统中节点是可信的,通过其行为反馈来更改节点的信誉值,其缺点是缺少惩罚机制,对那些信誉值较低且表现为恶意行为的节点无能为力.CONFIDANT 系统[37]同时考虑了正信誉和负信誉,并通过等级表(rating list)和权重(weighting)来计算节点的信誉值,使具有恶意行为的节点在网络中孤立,激励所有节点参与到网络中,提高了系统的通信效率.

近年来,对网络可信模型的研究已经引起关注,多数都是基于可信和信誉的模型,这些模型都可以应用到网络的可信访问控制研究中.文献[23,38]是为 P2P 系统提出的基于贝叶斯网络(Bayesian network)的可信和信誉模型,其信誉建立在推荐(recommendation)的基础上.由于在 P2P 系统中对等点的可信值是多方面的,即在不同的情况下对 peer 的可信值是不同的,贝叶斯网络为不同情况下的可信值提供了一个灵活的模型,可应用于 P2P 文件共享系统或其他 P2P 系统中.文献[39]为动态协同网提出了一个分布式基于可信的访问控制系统,该系统是一种以节点为中心的基于可信的访问控制,结合了信誉和风险(risk),具有动态性,能够激励节点之间的相互协作和共享资源,适用于移动 Ad Hoc 协同环境.

3.3 可信网络中可信和信誉机制

对可信网络访问控制的研究有助于提高网络系统的安全性,是可信网络安全性研究中的一个重要问题,必须将传统的访问控制方法与认证、授权、密钥管理等方法相结合才能实现可信网络的安全问题.虽然基于角色的访问控制本身具有很多优势,但是在可信网络中,仅通过基于角色的访问控制并不能实现网络的可信,必须通过适当的基于可信的访问控制策略,经过安全认证与授权后的用户才具有某种角色,可行使某种权限或执行某些安全操作,这样才能保证网络中用户的行为是可信的.

这里以 P2P 文件共享系统为例,说明可信和信誉机制的实现过程.在 P2P 系统中,可信是一个 peer 对另一个 peer 能力的信任,建立在直接经验的基础上;信誉是一个 peer 对另一个 peer 能力、诚实度和可靠性的信任,建立在其他点的推荐上,推荐值也称为参考值(reference).P2P 系统中的 peer 通过询问或节点之间的交互得到一些参考值,根据这些参考值动态更新对其他 peer 的可信值.可信分为两类:一类是对文件提供者在提供文件共享能力上的可信;一类是对那些提供推荐的 peer 可靠性上的可信.信誉值可以集中计算,如由可信第三方计算,也可以分散计算,即每个点通过询问推荐并各自计算出其他点的信誉值.

图 9 为 P2P 文件共享系统中的可信和信誉机制,图中,FP(file provider)为文件提供者.从图 9 可以看出,可信

和信誉机制的实现过程:当一个 peer 要选择一个可信 FP 时,如果历史上曾有过与 FP 交互的经验,则在自己的可信 FP 数据库中找到一个可信值最高的 FP 与之交互;如果以前没有过与 FP 交互的经验或对 FP 了解较少,则从其他 peer 的推荐中,通过综合计算选择一个信誉值高的 FP 进行交互.通过这次交互的满意度对该 FP 进行评估,并更新对该 FP 的可信值,同时更新那些提供推荐的 peer 的可信值.可信和信誉机制可以帮助区分好坏节点,并找到适合自己需求的 FP,提高了节点之间通信的效率,这种机制可以根据不同的需求应用于不同网络环境的可信访问控制模型中,可以提高网络节点间通信的效率和安全性.

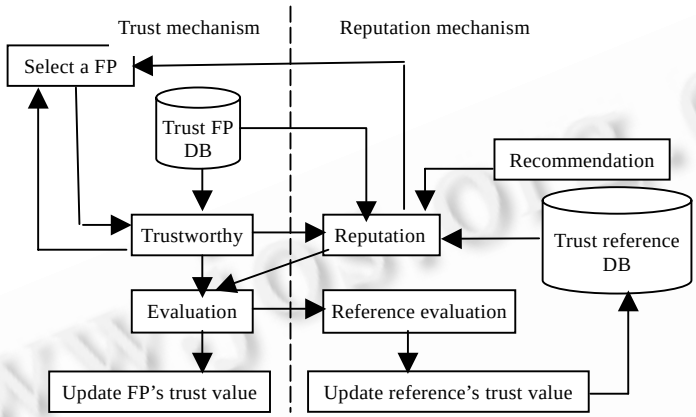

Fig.9 Trust and reputation mechanism in P2P file sharing system

图 9 P2P 文件共享系统中可信和信誉机制

可信网络的访问控制要求建立基于可信的访问控制模型,而可信访问控制主要是建立基于可信和信誉的模型,目前研究较多的是对 P2P 文件共享系统和 Ad Hoc 网络的可信模型,由于这两种网络都要求节点间共享资源,因而对可信的要求程度较高.可信网络作为可信计算发展的必然趋势,对可信访问控制的研究也必然成为热点,其中,对可信模型的建立和可信值的评估是两个重要的问题.此外,还有一些关键问题需要解决,如节点的搜索问题,即如何找到可信的节点并向它们询问推荐,如何保证系统免受各种攻击等.目前,可信模型正受到更多人的关注,可信值的评估方法在文献[40,41]中都有介绍,针对 P2P 系统中可信评估的研究也越来越多[42−45].这些可信模型和可信评估的方法都将为可信访问控制提供参考,并成为可信网络研究的一个重要内容.

4 结束语

随着 Internet 技术、无线通信技术、电子技术及计算技术的高速发展,计算机系统应用日益广泛.然而,面对如此庞大的系统,其脆弱性是不可避免的,网络正面临着严峻的安全性挑战,对网络安全的研究已引起人们的高度重视,访问控制作为网络安全的一个重要方面也日益受到关注,针对不同的网络环境已经提出了很多相应的访问控制模型,这些模型都为网络安全的实现提供了很好的解决途径.通过本文的综述可以看到,访问控制技术的研究呈现出以下几个发展趋势:

(1) 分布式系统中的访问控制技术将成为未来的研究热点,包括适用于分布式系统或工作流系统的动态访问控制及分层访问控制,基于角色的访问控制将会在大型分布式系统中得到更广泛的应用.

(2) 对网络信息系统、无线网络(如 ad hoc,sensor network 和移动网络)及 P2P 系统的访问控制技术的研究,将成为重要的研究方向,需要灵活、易扩展的、支持多种安全策略的访问控制技术的研究,而基于上下文、基于语义、基于位置等访问控制模型或者它们的相互结合,将会应用到更多的网络环境中.

(3) 可信网络是计算机网络发展的一个必然趋势,对可信模型、可信评估及基于可信的访问控制的研究将成为重要的研究方向.此外,可信网络的安全问题已经远远不止保密性和完整性的问题,单一的安全技术很难保证系统的真正安全,访问控制技术与其他安全技术进一步的结合将成为今后的研究热点,如访问控制与策略、域之间的隔离,密钥管理以及系统行为认证等技术相结合.

References:

[1] Lampson BW. Protection. Operating System Rev., 1974,8(1):18−24.

[2] Bell DE, Lapadula LJ. Secure Computer Systems: Mathematical Foundations, Vol. 1. Bedford: The Mitre Corporation, 1973.

[3] Harrison MA, Ruzzo WL, Ullman JD. Protection in operating systems. Communications of ACM, 1976,19(8):461−471.

[4] Department of Defense. Trusted computer system evaluation criteria (TESEC). Technical Report, DOD 5200.28-STD, 1985.

[5] Ferraiolo D, Kuhn DR. Role-Based access control. In: Proc. of the 15th National Computer Security Conf. 1992. 554−563. http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf

[6] Sandhu R, Coyne EJ, Feinstein HL, Youman CE. Role-Based access control models. IEEE Computer, 1996,29(2):38−47.

[7] Sandhu R, Bhamidipati V, Munawer Q. The ARBAC97 model for role-based administration of roles. ACM Trans. on Information and System Security (TISSEC), 1999,2(1):105−135.

[8] Sandhu R, Munawer Q. The ARBAC99 model for administration of roles. In: Proc. of the 15th Annual Computer Security Applications Conf. Washington: IEEE Computer Society, 1999. 229−238. http://www.list.gmu.edu/confrnc/acsac/acsac99(org).pdf

[9] Ferraiolo DF, Sandhu R, Gavrila S. Proposed NIST standard for role-based access control. ACM Trans. on Information and Systems Security (TISSEC), 2001,4(3):224−274.

[10] Thomas RK, Sandhu RS. Task-Based authentication control (TBAC): A family of models for active an enterprise-oriented authentication management. In: Proc. of the 11th IFIP Conf. on Database Security. California, 1997. 11−13. http://www.list.gmu.edu/confrnc/ifip/i97tbac.pdf

[11] Oh S, Park S. Task-Role-Based access control model. Information System, 2003,28(6):533−562.

[12] Park J, Sandhu R. Towards usage control models: Beyond traditional access control. In: Proc. of the 7th ACM Symp. on Access Control Models and Technologies. California, 2002. 57−64. http://www.list.gmu.edu/confrnc/sacmat/2002-UCON.pdf

[13] Park J, Sandhu R. The $UCON_{ABC}$ usage control model. ACM Trans. on Information and System Security, 2004,7(1):128−174.

[14] Sandhu R, Park J. Usage control: A vision for next generation access control. In Proc. of the 2nd Int'l Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security. LNCS 2776, Berlin: Springer-Verlag, 2003. 17−31.

[15] Condor high throughput computing. 2006. http://www.cs.wise.edu/condor/

[16] Legion Research Group of the University of Virginia. Legion, a worldwide virtual computer. 2005. http://legion.virginia.edu/

[17] Globus project: Globus toolkit. 2006. http:// www.globus.org/

[18] Yao H, Hu H, Huang B, Li R. Dynamic role and context-based access control for grid applications. In: Proc. of the 6th Int'l Conf. on Parallel and Distributed Computing: Applications and Technologies. IEEE Computer Society, 2005. 404−406.

[19] Luo JZ, Wang XP, Song AB. A semantic access control model for grid sevices. In: Proc. of the 9th Int'l Conf. on Computer Supported Cooperative Work in Design. Coventry: IEEE Press, 2005. 350−355.

[20] Ryutov T, Zhou L, Neuman C, Leithead T, Seamons K. Adaptive trust negotiation and access control. In: Proc. of the 10th Symp. on Access Control Models and Technologies (SACMAT 2005). New York: ACM Press, 2005. 139−146.

[21] Fenkam P, Dustdar S, Kirda E, Reif G, Gall H. Towards an access control system for mobile peer-to-peer collaborative environments. In: Proc. of the IEEE 11th Int'l Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2002). IEEE Computer Society, 2002. 95−102.

[22] Kim W, Graupner S, Sahai A. A secure platform for P2P computing in the Internet. In: Proc. of the 35th Hawaii Int'l Conf. on System Sciences (HICSS). Hawaii: IEEE Computer Society, 2002. 3948−3957.

[23] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks. In: Proc. of the 3rd Int'l Conf. on Peer-to-Peer Computing. IEEE Press, 2003. 150−157.

[24] Xing L, Liu L. A reputation-based trust model for peer-to-peer ecommerce communities. In: Proc. of the ACM Conf. on Electronic Commerce. New York: ACM Press, 2003. 228−229.

[25] Wang Y, Vassileva J. Bayesian network-based trust model in peer-to-peer networks. In: Proc. of the Workshop on "Deception, Fraud and Trust in Agent Societies" at the Autonomous Agents and Multi Agent Systems. LNCS 2872, Berlin: Springer-Verlag, 2003. 23−34.

[26] Wang Y, Vassileva J. Bayesian network-based trust model. In: Proc. of the IEEE Int'l Conf. on Web Intelligence. IEEE Computer Society, 2003. 372−378.

[27] Li Z, Dong Y, Zhuang L, Huang J. Implementation of secure peer group in peer-to-peer network. In: Proc. of the Information Conf. on Communication Technology (ICCT). IEEE Press, 2003. 192−195.

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

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

[30] Faria DB, Cheriton DR. DoS and authentication in wireless public access networks. In: Proc. of the 3rd ACM Workshop on Wireless Security. New York: ACM Press, 2002. 47−56.

[31] Wan ZG, Zhu B, Deng RH, Bao F, Ananda AL. DoS-Resistant access control protocol with identity confidentiality for wireless networks. In: Proc. of the 6th IEEE Wireless Communications and Networking Conf. IEEE Press, 2005. 1521−1526.

[32] Ray I, Yu LJ. Towards a location-aware role-based access control model. In: Proc. of the 1st IEEE Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks. IEEE Press, 2005. 234−236.

[33] Lin C, Peng XH. Research on trustworthy networks. Chinese Journal of Computers, 2005,28(5):751−758 (in Chinese with English abstract).

[34] Mcknight D, Chervany N. The meanings of trust. Technical Report, TR94-04, University of Minnesota, 1996.

[35] Michiardi P, Molva R. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks. In: Proc. of the 6th IFIP Conf. on Communications and Multimedia Security. Portoroz, 2002. http://portal.acm.org/citation.cfm?id=647802.737297

[36] Marti S, Giuli T, Lai K, Baker M. Mitigating routing misbehavior in mobile ad-hoc networks. In: Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking. Boston: ACM Press, 2000. 255−265.

[37] Buchegger S, Boudec JL. Performance analysis of the CONFIDANT protocol. In: Proc. of the 3rd ACM Int'l Symp. on Mobile Ah Hoc Networking and Computing. ACM Press, 2002. 226−236.

[38] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks. In: Proc. of the 2nd Int'l Workshop on Agents and Peer-to-Peer Computing. Berlin: Springer-Verlag, 2004. 23−34.

[39] Adams WJ, Davis NJ. Toward a decentralized trust-based access control system for dynamic collaboration. In: Proc. of the IEEE Workshop on Information Assurance and Security United States Military Academy. West Point: IEEE Press, 2005. 317−324.

[40] Griffiths N. Task delegation using experience-based multi-dimensional trust. In: Proc. of the 4th Int'l Joint Conf. on Autonomous Agents and Multi-Agent Systems. New York: ACM Press, 2005. 489−496.

[41] Srivatsa M, Xiong L, Liu L. TrustGuard: Countering vulnerabilities in reputation management for decentralized overlay networks. In: Proc. of the 14th World Wide Web Conf. New York: ACM Press, 2005. 422−431.

[42] Aberer K, Despotovic Z. Managing trust in a peer-to-peer information system. In: Proc. of the 10th Int'l Conf. on Information and Knowledge Management. New York: ACM Press, 2001.

[43] Cornelli F, Damiani E, Vimercati SDCD, Paraboschi S, Samarati S. Choosing reputable servents in a P2P network. In: Proc. of the 11th World Wide Web Conf. New York: ACM Press, 2002. 376−386.

[44] Kamvar SD, Schlosser MT, Molina HG. The EigenTrust algorithm for reputation management P2P networks. In: Proc. of the 12th Int'l Conf. on World Wide Web. New York: ACM Press, 2003. 640−651.

[45] Buchegger S, Boudec JL. A robust reputation system for P2P and mobile ad-hoc networks. In: Proc. of the 2nd Workshop on the Economics of Peer-to-Peer Systems. 2004. http://citeseer.ist.psu.edu/buchegger04robust.html

附中文参考文献:

[33] 林闯,彭学海.可信网络研究.计算机学报,2005,28(5):751−758.

林闯(1948－),男,辽宁沈阳人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为计算机网络,系统性能评价,随机 Petri 网,可信网络,可信计算.

封富君(1978－),女,博士生,主要研究领域为网络安全,Petri 网,访问控制.

李俊山(1956－),男,教授,博士生导师,CCF 高级会员,主要研究领域为图像处理技术,并行计算机体系结构,网络信息技术.