广西科学院学报
Journal of Guangxi Academy of Sciences
2010,26(4):532~537
Vol. 26, No. 4 November 2010

信任模型中的激励机制研究进展
The Research Progress of Incentive Mechanism in Trust Models

罗柏发,蔡国永
LUO Bai-fa, CAI Guo-yong

(桂林电子科技大学计算机工程学院,广西桂林 541004)
(School of Computer Science and Engineering, Guilin University of Electronic Technology, Guilin, Guangxi, 541004, China)

摘要:介绍兼有激励机制的信任模型研究的问题以及信任模型的激励机制研究现状。目前信任的激励机制还没有一个解决信任的表述、度量、推导和综合运算等问题的统一标准,研究手段与方法仍比较单一,未能提供统一的敏感信息保护方案。建议根据当前国内外激励机制的研究现状和存在问题,继续对信任的激励机制展开更深入研究。

关键词:激励机制 信任 模型 安全
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2010)04-0532-06

Abstract: A problem of compatible-incentive trust model and the research state of the incentive mechanism in trust model are introduced. Presently, there is no consensus in the literature on the trust description, trust measure, trust collection and trust computation. The ways of trust research are still simply. A uniform protected scheme of sensitive information is not available. Based on research state and existed problems of trust, it is necessary to deeply research the incentive mechanism of trust in future works.

Key words: incentive mechanism, trust, model, security

信任是人类的特有现象,在社会网络中信任是人际关系的核心。目前人们对信任并没有一个统一的定义。但是,一般地,信任是指系统对对方在规定时间和环境内交付可信赖的服务能力的一种信赖或信仰,它表达了对合作伙伴提供服务的诚实、可信、能力、可靠性等品质的相信程度。目前,信任在安全系统和关键信息的管理访问中起着重要的作用,并被广泛地应用于各种领域,如电子商务、基于 Web 的访问、一些 p2p 应用等。然而,在大规模开放分布式网络环境中,由于节点的动态性和广泛分布性,信任管理开始变得非常困难。网络中少量恶意节点的不合理合作行为破坏了网络次序,所产生不公平现象严重损害了其他节点的积极性,同时也影响了信任网络的可信性。而激励机制能够促进节点间加强合作并积极参与网络活动共享资源信息,有效地抵制了信任管理中一些安全上的问题。因此,在信任模型中加入激励机制以提高节点的参与热情并防止少数恶意节点的不理性行为就显得非常的必要。

现有的信任模型主要有 3 类:(1)基于 PKI 的集中式信任模型。这类模型是以少数性能极好的节点作为领袖,负责监督整个网络,定期公告违规的节点。它的合法性通过 CA 颁发的证书加以保证。但是,这类模型往往容易受到攻击,有单点失效和可扩展等问题。Eugene Stab 和 Thomas Engel 在文献[1]中就提出了这样一种基于 CA 颁发凭证的信任模型,它可以应对一些可能攻击,但是不能解决这种方法的根本缺陷。(2)基于推理和规范的模型。这类模型对每个交互对象都进行推理,判断对方是否符合自己的条件;用逻辑来描述互动主体间的行为规范,从理论与实践的角度实现主体间的交互。文献[2,3]提出了一种新的方案去配合规范措施和执行惩罚那些违反禁止行为的措施,但是这种方法执

收稿日期:2010-09-20
作者简介:罗柏发(1985-),男,硕士研究生,主要从事社会计算和信任管理研究。

行效率低且不好管理信任。(3)基于历史记录的信任模型。这类模型通过用概率统计的手段量化历史经验,并预测对方做出同样行为的概率。这类模型的出现有利于信任的计算、传递和管理,但是同时也带来了风险,即如何激励节点给出真实评价和分享自己的经验。文献[4]合并直接经验和声誉共同构成一个信任的计算模型,该模型还考虑到了信任的多方面本体属性问题,比较全面地合成了对手的总体信任,但是它并不能使用于所有方案的实施。文献[5]认为传统信任机制过于呆板、僵硬,在不同的环境和情境下,处理信任应采取不同策略,为此,它将信任划分为不同的等级,建立了一个基于情景的信任评估机制。

本文希望通过介绍信任模型中的激励机制研究进展,为进一步研究更高效、实用的信任激励机制提供参考。

1 兼有激励机制的信任模型研究的问题

S. Marsh[6]最早结合社会学等学科的知识将信任形式化为计算的形式,从此信任就成了近年来的研究焦点。1996 年 AT&T 实验室的 Blaze 等人首先提出信任管理的概念,它为解决分布式环境中新应用形式的安全问题提供了新的思路。随着网络的增大,节点只从网络中获取自己想要的"利益"而并不贡献任何资源回馈网络,这种自利行为打破了平衡导致整个网络系统的崩溃[7]。另外,在一些信任的应用中节点可以用低成本反复注册多个身份以掩盖自己的实际身份,在匿名的环境中增加了网络的风险和事后惩罚的难度[8]。为了很好地解决这一难题,源于经济活动的激励机制观点为信任机制的进一步发展带来了新的活力。由于信任机制本身存在缺陷,有时它就像是一场赌博。激励机制能够促进节点间的合作并积极参与网络活动共享资源信息,有效地抑制"搭便车"现象,抵制了一些安全上的问题。因此,激励机制在一定程度上能够缓解信任机制上的不足,提高它的预测正确率。

兼有激励机制的信任模型主要研究两个问题:公共牧地问题(Free-riding problem)和节点抑制问题(White-washing problem)。

1.1 公共牧地问题

"公地制度"是英国以前的一种土地制度——封建主在自己的领地中划出一片尚未耕种的土地作为牧场,无偿提供给当地的牧民。然而,由于是无偿放牧,每一个牧民都想尽可能增加自己的牛羊数量,随着牛羊数量无节制地增加,牧场最终因过度放牧而成了不毛之地。从经济学角度分析,就是说个人在决策时只考虑个人的边际收益大于等于个人的边际成本,而不考虑他们的行动所造成的社会成本,最终造成一个给予他们无限制放牧权的经济系统的失败和崩溃。

在虚拟网络中,根据一份针对 Gnutella 的调查显示:70%以上的用户不共享任何资源,90%以上的用户不响应任何请求,网络中所有的资源仅由1%的节点提供[8]。网络中大量的服务仅由少数节点提供,滋生了大量的 Free-riding 行为。这样降低了整个网络节点的参与积极性,容易造成网络资源的崩溃并产生不安全因素。公共资源的不排他性是 Free-riding 产生的温床,各种节点可能由于自身资源的枯竭或基于自身安全的考虑,使用不要任何代价的公共资源当然是重要的首选。

为了解决 Free-riding 问题,Jurca 和 Faltings[9]提出一个兼顾激励的声誉机制去处理不积极和谎言,单独设置了一个经纪人角色从事信任信息的买卖。它规定任何资源的得到都需要付出一定的代价,任何假的资源都要受到经济上的损害,任何诚实的资源都要受到经济上奖励,试图用经济上的措施拉住处于囚徒困境的节点理性参与网络。在这种机制中,客户端会向一个命名为 R-agent 特殊的经纪人购买有关一个服务提供者的推荐;与提供者交互以后,客户端能够出售它的反馈信息到同一个 R-agent,但是只有当它的报告符合下一个客户端关于同一个服务提供者的反馈报告时才能获取报酬。但问题是:若来自 R-agent 的推荐是消极的,使得客户端准备去避免这个服务提供者,这时,客户端将没有任何的反馈能够出卖;而且由于投机取巧服务提供者的存在,并不能确保一个诚实反馈获得回报。这使得一个诚实的实体很可能会获得一个消极报酬从而使得它们不愿购买任何推荐信息。另外,它们工作的效率很大程度上取决于 R-agent 的诚实,而 R-agent 被假定由于是推理的、先验的而被信任。CFS[10]和 PAST[11]致力于存储配额(Storage Quotas)研究,CFS 系统中,提供存储资源的节点给每个消费其存储资源的节点限定了配额;而 PAST 系统中的配额依赖于为每个节点配置的智能卡(smartcard)。文献[12]描述了一种根据自身对公共资源的贡献值来分配资源,它认为贡献要与分配相一致,多劳多得,少劳少得,不劳不获。文献[13]提出用分布式声誉机制去认识普适计算环境下的服务可信

性，并激励节点积极分享诚实的推荐信息；为了解决节点信任信息的存储，它采取了组群分组管理的方法去积极地保护它们组的声誉，但是，对于节点真正身份的识别和抑制漂白方面，它并没有给出相关的措施。

1.2 节点抑制问题

假如节点A在多次交互后，由于不诚实或不积极地提供信任信息而受到了惩罚，它的声誉和资源比一些刚加入节点的还要少。这时，若注册一个新身份的代价不高，A很有可能去注册一些新的身份B、C、D等，用新面目加入网络。

一个节点多个身份的问题不仅使得恶意节点能够在匿名的情况下继续它的不理性行为，损害整体网络的性能并能逃脱惩罚制裁，而且还浪费了网络的资源，产生漂白问题，造成一些新的危害。比如合谋，身份B、C、D可以共同合谋推高A的声誉，为其谋取利益。

节点泛滥的根本原因在于信任机制本身需要各种节点积极地参与网络，因而放松对加入网络的限制。文献[14]认为White-washing问题的出现使得系统的等级下降，并认为提高节点准入条件和加强多身份节点的处罚力度有利于减少节点的滥用。然而，文献[15]认为White-washing问题解决的难点在于节点的识别，即如何辨别节点的多身份及其标识。

2 信任模型的激励机制研究现状

激励机制即为鼓励成员相互合作的模式。它包括向网络中引入激励机制所可能用到的一系列抽象策略。激励机制最早来源于人们的经济生活。在企业管理中，管理者为了提高被管理者的生产积极性，按照人们一般的心理制定了一些制度。这些制度除了刺激生产外，还有团结员工，增强合作等作用。

2.1 激励机制的社会心理学分析

美国社会心理学家、人格理论家和比较心理学家马斯洛在自己的研究中开创性地提出了人类价值体系存在的两类不同的需要，一类是沿生物谱系上升方向逐渐变弱的本能或冲动，称为低级需要和生理需要；一类是随生物进化而逐渐显现的潜能或需要，称为高级需要。人都潜藏着5种不同层次的需要，但是在不同的时期表现出来的各种需要的迫切程度是不同的。人的最迫切的需要才是激励人行动的主要原因和动力。人的需要是从外部得来的满足逐渐向内在得到的满足转化，低层次的需要基本得到满足以后，它的激励作用就会降低，其优势地位将不再保持下去，高层次的需要会取代它成为推动行为的主要原因。有的需要一经满足，便不能成为激发人们行为的起因，于是被其他需要取而代之。Deci则把激励因素分为内部的心理因素和外部的奖励因素两种。内部因素包括个人内心的各种感情愿望，外部因素则为物质或非物质的奖励因素等。Kollock指出可能激励个人向集体社区做出贡献的原因有4种：(1)个体做出贡献可以得到相应的回报，例如对其需求优先满足；(2)个体对集体的贡献可以提高自己的声誉；(3)自我成就感的满足；(4)对集体的依赖和对集体所承担义务。

社会心理学上分析也适用于网络上的节点。目前，社会网络日趋成熟，结合社会心理学，激励社会网络上节点的相互信任将是未来的一大研究热点。

2.2 激励机制的分类

目前，激励机制大体被分为两类：(1)货币支付模式，节点上每次信任的分享都需要明确的“货币”支付；(2)非货币模式(也被称为软激励模式)，除了使用明确的货币支付而采用其他的方法提供激励。

2.2.1 货币支付模式

2.2.1.1 真实货币支付

在网络中用户出售自己的资源，并通过银行利用用户资源的网格组织向该用户支付真实货币，同时在网络外进行付费。这种方式被广泛地应用于网格计算的经济模型中，目前的一些网格系统如Globus，Legion等，都提供了大量的、成熟的、可重复利用的中间件，例如资源协同分配服务、认证和安全服务GSI等。

2.2.1.2 微支付

在网络中所使用的并不能自由兑换成现实货币的货币称为虚拟货币。每个节点在分享其他节点的信任信息或资源之前，必须向服务提供节点支付相应价格的虚拟货币。为网络中其他节点提供服务可以得到相应的虚拟货币，所以为了能够持续的得到网络资源，节点必须不断的以自己的服务换回足够多的虚拟货币，其中货币的交易必须具备原子性、连贯性、孤立性和耐久性。现实中的系统包括The gojo Nation system、Maze等系统。

2.2.2 软激励模式

2.2.2.1 实物交换模式

在这种模式中，用户总是只有共享了资源，对系统做出了贡献才能从别人那里得到自己想要的资源。消费和提供服务的速率同样受到控制，即用户

使用一定的速率消费服务,也必须要提供相应的提供服务速率。使用这样的机制的目前有 eDonkey 和 BitTorrent 网络。但是由于基于实物交换的激励模型没有考虑到不合作行为还应该包含合理的不合作行为,它对所有的不合作行为都加以制约,并不能很好的体现网络的公平性。

2.2.2.2 差别服务质量模式

系统贡献的越多,则它从网络中就可以得到更好的服务,比如优先的访问权,更为稳定的传输,更高速的下载,更大的存储空间等。例如在文献[16]中所提出的基于节点服务情况和使用情况矩阵特征向量来决定是否向请求服务提供节点提供其所要求的服务。

2.3 激励机制的安全性研究

网络中存在大量的自私节点和少量的不理性节点,这些自私与不怀好意的自治端点将信任的可靠性推向危险的边缘,甚至威胁到整个网络的性能。因此,激励机制跟信任安全息息相关。

2.3.1 说谎

在网络中存在这样一类节点,它们希望以自己平凡平庸的表现去获取巨大利益或达到在网络中更好"社会地位"的目的,为此,它们不惜损害其他参与者的利益。例如,在评价或分享声誉时夸大自己的信任或诋毁竞争对手的声誉。解决这类问题的根本方法在于揭穿谎言,使其无法获得"非法利益"。目前,大多数的激励措施在于鼓励分享,对于说谎一般将谎言与历史记录进行对比,采用统计分析的方法找出偏差,对信任推荐进行甄别,采用好的诚实的推荐,弃用谎言[17]。文献[9]则直接采用双方对质的方法,例如节点 A 想要与 B 交互,C 与 B 已有过交互经验,它向 A 提供 B 的推荐信任,然后 A 再向 B 求证 C 的声誉两相对质进行真伪辨别。但是这样,有时会出现各说一词,真伪难辨的情况,比如,B 说 C 可信性小,C 说 B 可信性小。文献[18]则采取"兼听"的方法,它咨询大量与 B 有过交互经验的节点并综合得出自己对对手总体评价,根据总体评价再判断是否与对手节点进行交互。

2.3.2 背叛

在网络中,一些"地位"很高的节点由于以前的"功劳",它们可以得到一些特殊待遇,比如,优先使用和访问资源的权利等。但是如何防止"高地位"节点做一些背叛自己身份的行为一直是一个难点问题。对于此类问题,一般有 3 种解决的方法:(1)加大事后惩罚力度,使其等不偿失。这种方法尽管能够减少背叛行为的发生,但是一旦发生问题,即使惩罚了"高地位"节点,损失依然无法挽回。并且它的管理一般是集中式的,对于分布式系统往往加大了系统的复杂度[18]。(2)权利"阳光化"。享受特权的"高地位"节点在执行某些行为时必须在第三方的监督下执行。文献[19]独立设计了一个新的第三方角色,交互双方依靠第三方角色去交互,它们的行为受到第三方的监控;反过来,第三方也要受到交互双方的监控,最后按照各自的贡献来分配收益。(3)消去特权。在信任的计算模型中加入一些因子,使得信任随时间和环境等因素不断减少,让节点一直为高地位、高声誉来提供诚实的服务。文献[20]在社会网络的信任模型中加入时间衰减因子,每次诚实交互后增加的声誉值并不会大幅上升,但是若不积极或诚实交互那么它的声誉值将会大幅下跌。因此,节点为了维持自己的声誉和地位不得不努力地争取自己的利益。

2.3.3 合谋

合谋是在网络中多个节点合作共同抬高或贬低某一节点以达到它们共同目的的恶意行为。在信任机制中,合谋是一个非常复杂而难于解决的问题。节点身份的泛滥是其出现的主要原因之一。目前,合谋的出现不外乎以下两种情况:(1)由于 Whitewashing 的存在,节点注册身份的成本很低造成一个节点的大量身份对该节点的信任哄抬。(2)多个自私的恶意节点由于共同利益勾结起来共同哄抬某一恶意节点的声誉或诋毁某一高声誉节点的声誉。

对于情况(1)的解决办法,我们只需要控制节点身份的滥用,唯一标识并统一好节点和身份。任何节点都匹配唯一一个身份,任何身份都能识别出它是哪个节点。这时任何由于节点多身份合谋都会被识别。情况(2)中合谋的各个恶意节点是自私的,它们是为了共同目的才勾结在一起的,同时它们也处于囚徒困境之中,对此我们可以采取 NASH 均衡的方法进行解决[9]。最大流量算法是目前已知的最好的能够对付合谋的方法,其缺点是难于在网络中实现,其时间复杂性大约为 $O(V^3)$,V 表示边的个数。使用最大流量算法评估主观信任度几乎需要整个传输图的信息,每个节点计算的时候,通信量大,而且存在安全隐患[21],对应的实例图如图 1 所示。在图 1 的例子中,标记为 c 的节点为互相合谋的节点,边上权值为互相评估的信任值。我们可以看到合谋节点之间互相都给予对方很高的信任值。当 A 节点要主观评估 B 节点的信任度的时候,不管合谋节点

之间相互提供了多高的信任度，A 对 B 的主观评估总是 0。

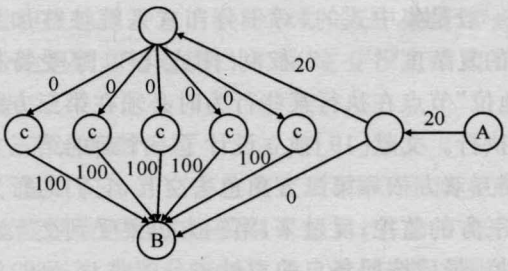

图 1 最大流量算法实例

2.3.4 敏感信息的泄露

在进行信任协商的时候，需要大量的通信服务和相关信任信息的交互，这时很容易出现敏感信息的泄露。对于使用信任证的信任机制，它有资源的内容敏感和资源的拥有敏感两类信任敏感信息。资源的内容敏感：信任证中的某些属性值属于显式敏感信息。资源的拥有敏感。协商方的响应和信息流动会隐式地暴露其保密信息，属于隐式敏感信息。文献[22]提出策略过滤和策略迁移的方法，分别用于解决信任证中可能涉及的两类敏感信息，其中，策略过滤是对信任证中的敏感属性设置一层新的访问控制策略；策略迁移的核心思想是将保护拥有性敏感信任证的策略迁移到其他可公开披露信任证之上。但是这对于那些不采用信任证的信任机制不能起到很好的作用。R. Jurca 等[9]提出使用基于非对称加密的密码机制来保护声誉信息的完整性和达到 agent 身份与声誉的紧密结合，重点确保下列 3 个属性：(1)一个 agent 的声誉是唯一地与它的身份联系的；(2)任何 agent 都不能自我不实地增加或降低自己的声誉；(3)在没有其他 agent 的同意，任何 agent 都不能篡改其他 agent 的声誉。

就资源体的拥有敏感保护而言，无论采用什么方案，其制订和应用过程都需要大量的额外工作。安全协议在信息安全领域占有主导地位，相应地，借助成熟的安全协议保护敏感级别高的信息，将成为值得推广的方法。

3 展望

目前，信任的激励机制研究成果很多，研究方法与手段也得到了不断发展，但是仍需进一步深入与拓展。首先，尽管目前的信任机制很多，但是这些机制基本是某个问题的具体解法，并没有一个解决信任的表述、度量、推导和综合运算等问题的统一标准。因此，探究一种综合式的信任模型将为激励机制跨域协作提供更有力的理论基础。其次，激励机制的研究手段与方法仍比较单一。现在大多数的信任激励机制都是采用经济激励的方法，基本上采取处于囚徒困境的 Nash 均衡理论作为研究手段。这对于那些并不在乎经济因素的信任机制起不到应有的作用。因此，探索一种基于普遍用户心理的更好的激励机制将为信任的激励机制的一般化提供必要的理论支持。第三，目前，针对典型敏感信息的保护已有密码保护的措施，它能有效提高激励机制的安全性与可行性。但是如何将经典的密码保护方案制定成安全协议并运用于激励机制中是一个值得关注的问题。此外，信任的激励机制具有与现实生活组织行为活动相一致的属性特征，既要维护信息的隐私性，又要促使资源的广泛共享和协作的顺利进行。

激励与计算机科学结合是典型的社会科学在自然科学中成功运用的实例，信任的激励机制消除了信任机制设计时所带来的缺陷危害，提高了协作安全性，抵制了各种恶意节点的不理性行为。伴随着 Internet 技术的发展、商务信息的全球化，其应用领域也将不断得到拓展。因此，了解动态、开放网络环境下协作的迫切需求，把握当前国内外激励机制的研究现状，继续展开深入的研究，将有助于提高信任协商双方贡献自我资源的积极性和安全性，有助于开放网络中基础设施的构建和完善。

参考文献：

[1] Eugene Stab, Thomas Engel. Tuning evidence-based trust models: proc of the IEEE, 2009 International Conference on Computational Science and Engineering [C]. Vancouver: IEEE Computer Society, 2009: 92-99.

[2] Felipe Meneguzzi. Norm-based behaviour modification in BDI agents: proceedings of the 8th International Conference on Autonomous Agents and Multi-agent Systems - Volume [C]. Budapest: International Foundation for Autonomous Agents and Multiagent Systems, 2009: 177-184.

[3] 郝晓云. 多智能主体系统的社会规范[J]. 重庆工学院学报：社会科学，2009，22(6)：75-78.

[4] Wang Ping, Zhang Zili. A Computation Trust Model with Trust Network in Multi- Agent Systems: proceedings of the 2005 International Conference on[C]. New York: ACM Press, 2005: 389-392.

[5] Osman N, Robertson D. A Contextualized trust model for distributed open systems: proceedings of the 20th International Joint Conference on Artificial Intelligence

[C]. New York:ACM press, 2007.

[6] James S Marsh, Leonard A Temme. Optical factors in judgments of size through an aperture[M]. Washington:Human Factors & Ergonomics Society Inc,1990: 109-118.

[7] Feldmany M,Laiz K. Quantifying disincentives in peer-to-peer networks: workshop on economics of p2p systems[M]. Berkeley:Springer,2003:117-122.

[8] EKrishna Gt Nmadi, Steven D Crribble. A measurement study of peer-to-peer file sharing systems: proceedings of the Multimedia Computing and Networking (MMCN)[C]. San Jose: Multimedia Systems Journal,2002.

[9] Jurca R, Faltings B. An incentive-compatible reputation mechanism:proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems[C]. Newport Beach: ACM press, 2003.

[10] Dabek F,Kaasheek M F, Karger D,et al. Wide-area cooperative storage with CFS: proceedings of the Eighteenth ACM Symposium on Operating Systems Principles[C]. Banff:ACM Press,2001:202-215.

[11] Rowstron A,Druschel P. Storage management and caching in PAST, a large-scale, persistent peer-to-peer storage utility: proceedings of the 18th ACM SymposiuTn on Operating Systems Principles[C]. Sanfrancisco: ACM press,2001:188-201.

[12] Feigenbaum J,Shenker S. Distributed algorithmic mechanism design: recent results and future directions: proceedings of the Discrete Algorithms and Methods for Mobile Computing and Communications [C]. Berlin:Springer,2002:1-13.

[13] Liu Jinshan. An incentive compatible reputation mechanism for ubiquitous computing environments [J]. International Journal of Information Security, 2007, 6(5):297-311.

[14] Michal Feldman,John Chuang. Overcoming free-riding behavior in peer-to-peer systems[J]. ACM SIGecom Exchanges, 2005,5(4): 41-50.

[15] Michal Feldman. Free-riding and whitewashing in peer-to-peer systems: proceeding of the ACM SIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems[C]. New York: ACM press,2004.

[16] Daniel Hughes. Free riding on gnutella revisited: the bell tolls[J]. IEEE Computer Society,2005,6(6):1-18.

[17] Seang Yi,Prasad Naldurg,Robin Kravets. Security aware ad-hoc routing for wireless networks:proc of the 2nd ACM International Symposium on Mobile AD Hoc Networking and Computing (MobiHoc'01)[C]. Texas:ACM press, 2001: 299-302.

[18] Wei Gong. Trust based malicious nodes detection in MANET[M]. Wuhan: IEEE Security & Privacy, 2009: 28-32.

[19] Kung H T, Wu Chunhsin. Differentiated admission for peer-to-peer system: Incentive Peers to Contribute their Resources[EB/OL]. [2010-08-12]. http://citeseerx. ist. psu. edu/viewdoc/download? doi=10. 1. 1. 14. 6920&rep=rep1&type=pdf.

[20] Ray I, Chakraborty S. A vector model of trust for developing trustworthy systems[J]. Computer Security,2004, 3193: 260-275.

[21] Boudec J Y. Rate adaptation, congestion control and fairness tutorial[EB/OL]. [2010-08-12]. http://citeseerx. ist. psu. edu/viewdoc/download? doi=10. 1. 1. 16. 3326&rep=rep1&type=pdf.

[22] Yu T. Automated trust establishment in open systems [D]. Illinois:University of Illinois,2003.

(责任编辑:韦廷宗)