P2P网络信任管理研究综述

张光华[1,2] 张玉清[1,3]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[1]
(河北科技大学信息科学与工程学院 石家庄 050000)[2]
(中国科学院研究生院国家计算机网络入侵防范中心 北京 100043)[3]

摘 要 建立信任管理机制对于确保P2P网络中用户的利益,确定资源或者服务的有效性具有重要意义。阐明了P2P网络信任管理中的基本概念,剖析了P2P网络信任管理系统的基本组成及各个部分中的关键问题,在此基础上介绍了P2P环境下的典型信任管理系统,讨论了和其他学科的融合发展。最后,对进一步研究方向如统一描述框架和分析评价标准作了展望。

关键词 P2P,信任管理,框架,标准
中图法分类号 TP393 **文献标识码** A

Survey of Trust Management on Peer-to-Peer Network

ZHANG Guang-hua[1,2] ZHANG Yu-qing[1,3]
(Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)[1]
(College of Information Science and Engineering, Hebei University of Science and Technology, Shijiazhuang 050000, China)[2]
(National Computer Network Intrusion Protection Center, GUCAS, Beijing 100043, China)[3]

Abstract Constructing a trust mechanism is very significant to benefit users in P2P network and verify validity of resource and service. Basic notions in P2P trust management was clarified in this paper and system constitution with key issues was analyzed in detail, which was followed by the introdcution of typical P2P trust management systems and the discussion about combination of P2P trust management and other subjects. In the end future research such as uniform framework and evaluation standard was expected.

Keywords P2P, Trust management, Framework, Standard

1 引言

随着P2P(Peer-to-Peer,点到点)技术的发展,它作为一种软件架构在电子商务、文件共享等方面得到了广泛应用。分布式、匿名性和自治性是P2P网络的本质属性,这也使它容易受到恶意用户的攻击[1]。因此,建立有效的信任管理机制,确定节点将要使用的资源或服务的有效性,对于确保P2P网络用户的利益具有非常重要的意义。然而,P2P网络和人类社会关系中的信任关系存在相似性,对等网络中节点具有高度的自主性,节点间的状态具有动态性和不确定性,这就决定了构建信任机制的复杂性。已有的工作表明[2-8],P2P网络信任管理已经引起了信任领域和P2P领域的研究团体极大的关注,但他们研究的侧重点又有所不同。目前,还没有一个通用的解决方案能够完全地解决P2P网络信任管理中的所有问题,进而部署在真实的P2P应用中。

将一个复杂的分布式算法在自治的、不可信赖的节点上运行,同时又期望它相对可靠、有效、安全,无疑是一个真实的挑战,这也正是P2P网络信任管理机制的任务。为了完成这个任务,必须把这个问题分解为更简单的问题,进而构造一个具有精确功能和良好特性的机制,从而实现P2P网络中的信任管理。我们的基本目标是阐明P2P网络信任管理中的基本概念,深入剖析P2P网络信任管理中的关键问题,并对已有的相关工作进行全面分类和总结,为P2P网络信任管理的进一步研究提供帮助和选择。

本文第2节介绍P2P网络信任管理中的基本概念;第3节讨论P2P信任管理中的关键问题;第4节列举具有代表性的信任模型;第5节总结P2P网络信任管理与其他学科的融合;最后指出了我们今后的研究方向。

2 P2P网络信任管理中的基本概念

P2P网络信任管理研究中,一些基本概念诸如节点、信任值、声誉值、可信度、可靠性等概念的表达有所差异,往往不利于信任统一框架的研究和建立,将它们构成信任模型中的主体元素,定义如下:

到稿日期:2009-10-10 返修日期:2009-12-17 本文受国家自然科学基金项目(60573048,60773135,90718007),国家高技术研究发展计划("863"计划)项目(2007AA01Z427,2007AA01Z450)资助。
张光华(1979—),博士生,讲师,CCF学生会员,主要研究方向为P2P安全和嵌入式系统,E-mail:xian_software@163.com;张玉清(1966—),教授,博士生导师,主要研究方向为网络安全和密码学。

定义 1(节点,peer,agent) 指 P2P 应用中的行为实体。在信任管理机制中,请求资源或者服务、进行信任评价的节点称为 trustor 或者 rater,提供资源或者服务、作为信任评价对象的节点称为 trustee 或者 ratee,为 trustor 或者 rater 提供信任信息的节点称为 witness。

定义 2(信任值,trust value) 指某一节点根据以往和其他节点发生直接的历史交互活动产生的结果,而得出的对其他节点的可靠程度高低的评估,是评估节点对相识或熟悉节点的直接主观评估,是一对多的关系,也称为直接信任。

定义 3(声誉值,reputation value) 指其他节点对该节点可靠程度的评估,是节点与未知或不熟悉节点交互活动前从其他信任节点得到的间接的主观评估,是其他节点的推荐值,是多对一的关系,也称为间接信任或者推荐信任。信任值和声誉值往往统称为信任信息。

定义 4(可信度,credibility) 一个查询节点对一个被查询节点的可信度,表示查询节点对从被查询节点处收集来的信任信息的真实性、准确性的信心指标,这个指标将直接影响对这些信息的使用。在信任管理机制中,一个查询节点收集到其他节点提供的声誉值时,常常需要根据自己对那些节点的可信度将信息加以筛选和修正。可信度是信任管理集中最难准确把握的方面之一。

定义 5(可靠性,reliability) 是指一个节点对另一个节点给与合作的把握量度,它或者是一个绝对数值,或者是一个与其他节点相比的相对值。可靠性是节点根据对某一节点的信任值和该节点自身的声誉值的综合而得出的对待评估节点的评估,是带权重比的评估。可靠性是一个节点考察另一个节点的最终指标,而对这个指标的评估则需要对收集的信任信息进行计算。

可靠性与声誉值、可信度之间存在如下关系。声誉值是一个客观总体看法,而可靠性是某个节点对另一个节点给与合作的把握量度。一个节点在某一时刻的声誉值是确定的,但其在不同的两个节点眼中,其可靠性却未必一致。可信度和可靠性都是一个节点对另一个节点的主观看法,都代表着一种信任,只不过可信度是对节点提供的信息的信任,可靠性是对节点在交易中的可能表现的信任。

在 P2P 网络中,节点的关系如图 1 所示,其中连线表示具有信任关系,箭头方向表示信任方向。节点 A 向节点 B 请求资源或者服务,此时节点 A 为 trustor,节点 B 为 trustee。节点 C 和节点 D 为节点 A 提供一些关于节点 B 的信任信息,称为 witness。

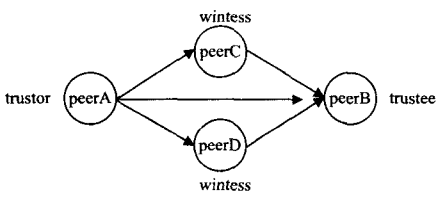

图 1 节点的关系

节点 A 分别对节点 C、节点 D 具有一定的可信度,同时节点 A 对节点 B 具有直接信任关系。节点 A 基于自身对节点 B 的直接信任以及节点 C、节点 D 对节点 B 的推荐信任,可对节点 B 进行信任评价。信任机制的基本流程如图 2 所示。

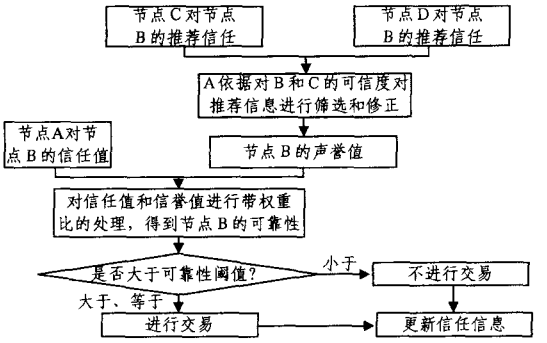

图 2 信任机制的基本流程

3 P2P 网络信任管理中的关键问题

P2P 网络信任管理的基本目标是设计并实现一个信任管理系统,当一个或者多个节点为某个节点提供服务或者资源的时候,信任管理系统能够为节点选择可靠的交易节点提供支持。为此,它必须实现以下 4 个功能:1)收集每个节点的信任信息;2)基于可靠性的期望值进行信任评价,选择一个可靠的交易节点;3)根据交易情形,更新相关的信任信息;4)对恶意节点进行惩罚,对善意节点进行奖励。

信任管理系统按照功能分解为 3 个主要部分,而激励和惩罚贯穿于信任管理的始终,如图 3 所示。每一部分的设计和实现应该考虑不同的机制,这些内容组成了 P2P 网络信任管理研究的核心问题。我们将讨论目前存在的研究和解决方案,阐明不同机制在已有的约束条件下如何有效运行。

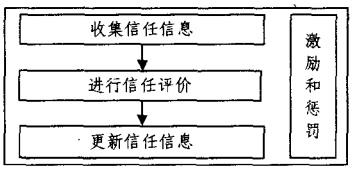

图 3 信任管理系统的基本组成

3.1 收集信任信息的关键问题

3.1.1 节点标识和信任初始化

某些节点在 P2P 网络中受到惩罚后,立即退出系统,然后以新标识再次登录到 P2P 网络,称为 Whitewashing 行为[9]。在一个纯粹的 P2P 网络中,限制一个节点使用一个标识是不切实际的。为了有效抑制 Whitewashing 行为,新标识节点应该被赋予较低的初始信任,使恶意节点无法轻易通过更换节点标识来达到欺骗的目的。Feldman 等人已经做了广泛的工作来分析 P2P 网络中陌生人策略和 Whitewashing 方面的问题[9-11],提出了一个陌生的动态策略。所有和陌生节点的第一次交易信息被聚合起来,使用一个基于陌生节点近期行为的度量,评估被下一个陌生节点欺骗的可能性,从而决定是否信任下一个陌生节点。这种可能概率的策略很适于系统中对 Whitewashing 的通用评价。

3.1.2 信任信息的存储和传输

由于 P2P 声誉系统中不存在单一控制点管理信任数据,因此系统中所有节点都要参与信任数据的管理。将各节点的信任信息分布冗余存储在分散于网络中的节点上,可以解决因本地存储节点不在线而导致的信任信息无法获取、信任信息更新不一致以及信任信息完整地存储在未知节点上可能存安全隐患的问题。同时,信任管理系统还必须防止存储节点

遭到恶意节点的攻击，确保得到的信任值是真实的，每个节点必须对自己提交的信任值负责，任何提交恶意评估的节点都能被识别。

文献[12]提交了一个完整的 P2P 安全传输协议 TrustMe，但该协议的安全是建立在引导程序的基础上的，若它被恶意用户攻击或者恶意用户自己执行引导程序，则其安全性就无从谈起。在此可引入分布式的密钥生成方案替代引导程序，以提高协议的安全性。文献[13,14]中采用基于 DHT (Distributed Hash Table，分布式 hash 表)的 P-Grid 存储机制构建一个虚拟二叉树，每个节点负责一个路径的数据存储，而文献[15-17]中的信息存储也都是基于 DHT 算法的。在文献[18]中，每个节点保存自己和一些邻居的信任信息，它也能向邻居请求一些推荐，广播、洪泛、概率洪泛的方法被用来发送请求推荐的查询或者分发自己的信任信息。P2PRep[19]提出了基于选举算法从分布于网络中的其他节点来获取待评估节点信誉值的传输协议，每个节点保留据自己直接经验所获得的信任信息，节点间通过请求和回答交流共享信息。EigenTrust[20]中信任信息数据通过一个“信任管理器”按某种方式统一管理，节点只需把存储在网络某处的信息查询出来。

3.1.3 行为类型

信任评价可以只基于积极的行为，如文件共享中的下载速率、文件大小；或者只基于消极的行为，如交易中的欺骗；或者是两者的结合。理想情况下，应该综合考虑节点交易中的积极行为和消极行为。文献[9]中阐述，节点可以根据用户对网络的贡献计算信任评价，贡献是一种只基于积极行为的信任评价。当能获得积极行为和消极行为的信息时，消极行为应该被赋予更高的权重，因为它比积极行为对一个节点的可靠性的影响更大。

3.2 进行信任评价的关键问题

3.2.1 信任信息的收集范围

一些信任系统[21,22]假设每个节点对存在的信任信息有相同的访问权，这样当不同的节点评价另一个节点的可信度时，它们的结果将会是一样的。在这些系统中，信任是全局的、客观的。另一些系统[23]中，信任评价是一个局部过程，建立在直接信任信息和来自节点邻居的间接信任信息的基础上，这种局部信任系统的可信度是主观的。

3.2.2 推荐者的可信度

当节点可能提供不正确的推荐时，推荐者的可信度应该被考虑，可靠性高的节点提供的推荐不一定是诚实的。有些节点提供虚假的信任信息，诋毁其他节点或者通过合伙欺骗来提升自身信任值[24]，造成信任度计算失真，影响信任系统的正常运作，破坏节点之间的信任关系。信任管理机制必须尽早识别此类信息并给予抑制，同时对提供虚假信息的节点实施必要的措施。

3.2.3 信任的模糊性和动态性

可靠性评价是在给定的上下文环境和时间内，基于初始信任的表示，节点对待评估节点做出的信任级别的预测。可靠性评价因为信任的模糊性和动态性而受到限制[25]。信任的模糊性和动态性的主要特性包括信任的隐含、信任的不对称、信任的传递、不同的上下文因素、时间因素。

例如，如果 A 信任 B，B 信任 C，B 推荐 C 给 A，A 就能够基于 B 的推荐和 A 对于 B 的信任来评估 C 的可靠性。A 在综合 B 的推荐时，必须处理传递的间接信任的级别。又如上下文因素，在一个电子商务应用中包括交易的数量和价格、交易的类型如提供服务还是提供推荐。一些信任系统[22,23]显示或者隐含地考虑了上下文，而其他一些则忽略了上下文，它们假定上下文对所有交易都是相同的。再如，当进行信任评价时，最近的交易行为应该比旧的交易行为具有更大的影响，近期经历应该被赋予更大的权重。文献[26]使用一个短期信任因子 st 来跟踪节点的行为变化，如果第 $n+1$ 个经历 e_{n+1} 与前面 n 个经历 st_n 的差值超过设定的阈值，st_{n+1} 随着它们差值的方向变化。文献[27]使用一种指数平均的方法合并多次交易结果，赋予最近的交易高权重，即近期交易结果对信任的影响程度要比早期的交易大。

3.2.4 可靠性的评价方法

当判断是否和一个节点交易时，最谨慎的节点只考虑他们自己的个人经验。由于缺少附加的信息，节点第一次交易时会有被欺骗的风险。但是，如果节点能够找到一些行为良好、经常提供良好服务的节点，本地的信任信息也就足够了[28]。有些节点会增加信息来源，收集系统中那些和它有信任关系的用户的推荐信息。这些用户包括他们个人生活中的朋友、商业伙伴或者他们信任的社会网络中的成员[29]。如果可信节点的数量很小，那么节点可能会要求那些可信节点递归地收集他们认为是可信的节点的推荐信息。每一次附加的递归查询都会以指数次幂提高信息来源。通过一个可传递的信任链收集的信息要比随机查询一个节点可靠得多[9,21,30]。最终，对一个节点的可靠性进行评价的时候，基于信息来源的可信度给予它们不同的权重。当然，个人经验往往是最有价值的[31]。EigenTrust[20]使用推荐节点的信任信息乘以推荐节点的可信度，为每个节点计算全局声誉评价。但是，这个算法被认为很容易受到合谋攻击。

3.2.5 可靠性的表示形式

可靠性的值可以是离散的或者是连续的，也可以是一个反映不同含义的变化范围。主要包括以下几种：集合{0,1}，0表示不可靠，1 表示可靠；多值评价，一个具体的间隔被分成更小的间隔，代表不同级别的可靠性[25]；[0,1]这样一个域，一个值代表一个可能性；多维评价。使用哪种表示取决于具体应用。

文献[13]是一种二元信任模型，认为节点要么值得信任，要么不值得信任。二元反馈模型太简单，在 P2P 文件共享系统可以很好地工作(因为文件要么是真实的，要么是不真实的)，但不能对节点的服务质量精确建模。多值的信任模型是将信任划分多个层次，每个信任层次对服务质量有不同的满意程度，范围包括从“很不满意”到“很满意”。在计算具体的信任值时，分别赋予每个层次一个数值，见文献[32]。多值的反馈模型较二元的有所改进，可以反映不同层次的服务质量，虽然其划分粒度比较粗，但仍足以反映复杂交易的交易质量。每个节点的可靠性用一个数值表示，使它可以和其他节点的可靠性或者交易设定的阈值进行比较。文献[27]用一个位于区间[0,1]的连续值来表示交易结果，是一种细粒度的划分，能够精确反映交易的服务质量。在一个所有节点都不可信的 P2P 环境中，从多方面对节点的可靠性进行评价也是有用的，许多系统提出维护每个节点的多维信任信息[33,34]。例如，TRELLIS[35]分别对交易中的节点可靠性和推荐的可信度进

行评价，文献[36]则建议分别对信任和不信任进行评价。

3.2.6 节点选择

一个节点的信任信息若被收集并被赋予合适的权重，则对该节点感兴趣的节点或者集中式的实体或者全体节点就会把该节点的可靠性计算出来。

计算可靠性的主要目的是帮助一个节点决定它应该与网络中哪个可用资源提供者交互。两个典型的情况是：(1)节点 B 提供给节点 A 一个资源或者服务，节点 A 可能根据节点 B 的可靠性大于还是小于一个设定的选择阈值做出决定[28]。(2)节点 A 请求一个特定的资源或者服务，多个服务提供者($B1$,$B2$…)响应。A 将使用每个响应者的可靠性按照他们提供正确服务的可能性对其进行排队，然后 A 选择可靠性最高的服务提供者。如果交易失败，A 可能和可靠性排在第二位的节点进行交易。如果它们的可靠性低于设定的选择阈值，用户也可能拒绝所有节点的交易请求。

3.3 激励和惩罚

信任评价完成后，节点将决定是否交易。之后，根据是否交易或者交易的结果修改自身直接信任，并修正对其他节点的可信度，至此完成了信息机制的基本流程。为了保证信任机制的有效性和安全性，针对自私行为和恶意行为的激励和惩罚贯穿于整个流程的始终。

搭便车现象与 P2P 通信模式提倡的协作共享理念背道而驰，在信任机制中必须激励这类自私节点参与网络活动，或者对它们进行隔离，避免与其他节点交互。大多数系统采取“随着提供服务的改进，相应获得改进的服务”的激励方案。例如在文件共享应用中，基于它从某个节点的下载速度，一个节点会降低或者提高对那个节点的上传速度；或者根据节点的贡献率，提供了不同质量级别的内容。一些解决方案鼓励节点为其他节点路由一些网络信息[37]，一些文献已经建议将低代价偿还机制应用在 P2P 系统中[38,39]。

在阻止自私行为时激励非常有效，但消除恶意行为则需要对恶意节点进行惩罚。如果信任管理机制能够主动识别恶意节点，网络中的邻居节点就能够断开与恶意节点的连接，立刻把恶意节点清除出网络。有些恶意节点会在一段时间后被踢出网络或者永远被禁止进入网络，为了重新进入网络，它们需要一个新的有效标识，这样的代价可能是昂贵的或者根本不可能实现。有的依赖索要报酬的金融结构的 P2P 系统对核实了恶意行为的恶意节点进行罚款。当然，这样一个解决方案应当谨慎使用，因为恶意节点也可能利用它们对表现善意的节点进行恶意评价，在系统中进行破坏活动。

4 典型的 P2P 网络信任模型

基于第 3 节中提及的关键问题，目前已有的 P2P 网络信任模型多种多样，主要分为两大类：非群组模型和群组模型。非群组模型较为丰富，按照关注领域的不同划分为 3 个方面：P2P 电子商务、P2P 文件共享、信任信息管理。

4.1 非群组模型

4.1.1 用于 P2P 电子商务的典型模型

1)PeerTrust[40]：PeerTrust 在可靠性评价中，考虑了 5 个因素：1)用户对完成交易的满意度的反馈；2)总交易次数；3)交易的可信度；4)交易上下文因素；5)团体上下文因素。需要考虑交易金额时，可增加交易金额的交易上下文因素；需要考虑节点的历史行为时，可将节点的历史行为作为团体上下文因素加入到信任公式中。同时，每个节点用 P-Grid 结构存储一部分信任数据，一个节点会根据需要收集必要的信任信息对另一个节点进行信任评价。但是，PeerTrust 没有给出信任因素的度量方法和权重因子的确定方法，难以对抗共谋行为。

2)FuzzyTrust[41]：指出信任是一个涉及多种动态因素的模糊概念，因而难以量化。依据影响电子商务交易的主要因素建立信任的模糊推理法则，基于 DHT 算法实现全局信任信息的聚合。节点根据本地的参考因素如服务质量、递送时间对交易过的节点做出一个模糊推断，产生一个本地评价。系统根据模糊推理规则设置聚合权重阈值，收集有效的本地评价。FuzzyTrust 仅能够对抗交易中的不诚实行为，计算代价和通信代价较大，未考虑影响信任评价的各种因素。

4.1.2 用于 P2P 文件共享的典型模型

1)P2PRep[19] 和 XRep[42]：基于局部信任信息的收集是建立在 Gnutella 协议基础上的，其特点是在判定一个节点是否可靠时，请求其他节点对这个节点进行投票，排除可疑和无效的投票后，再根据剩下的投票判断该节点是否可靠，在选择信任节点时同时考虑了节点的可靠性和节点提供的文件的可靠性。实现上也做了安全考虑，比如对敏感信息进行加密传输以确保信息的完整性和机密性，选择有效投票时考虑了投票人的 IP 地址以筛选掉可能的共谋节点。但是，这两种协议都会暴露投票节点的 IP 地址，削弱了 P2P 网络的匿名性；协议中公钥的传输是在不安全的信道上进行的，无法抵御中间人攻击；通过向朋友节点泛洪请求来获得信息，导致扩展性差，不适合大规模网络。

2)EigenTrust[20]：基于全局信任信息的收集，提出一种有效方式以最低耗费的消息交换来管理和使用本地信任值。它的核心思想是，当节点 i 需要了解任意节点 k 的全局可靠性时，首先从 k 的交易伙伴(曾经与 k 发生过交易的节点)获知节点 k 的可靠性信息，然后根据这些交易伙伴自身的局部可靠性(从 i 的眼光来看)综合出 k 的全局可靠性。该方法的优点是计算可信度时基于全局范围，得出的可信度计算结果没有遗漏。但是，该方法没有考虑计算过程结果的收敛性问题，未区分节点的可信度与可靠性，也未对可能存在冒名或诋毁的节点行为采取相应的策略。

3)SWRTrust[43]：Eigentrust[20] 作为全局信任模型，仅使用节点的全局可靠性作为推荐信任的权重，即假设具有高全局可靠性的节点其推荐信任也更加可信，但这个假设并不总是成立的。提出了一个基于相似度加权推荐的全局信任模型，以节点评价行为的相似度加权其推荐信任计算全局可靠性；引入一个简单算法优化相似度计算，以解决相似度计算中的稀疏性问题。

4) A Reputation-based Trust Management System for P2P systems[18]：文件下载请求节点存储信任向量，保存着与它交易过的节点的信任信息。对节点进行信任评价时，分别处理信任和不信任，不信任评价优先于信任评价，如果有非 0 的不信任评价就被认为是消极的。类似于人类社会，一次不诚实的交易会对人的可靠性产生很大的影响。安全扩展中考虑了关键字管理、身份鉴别、服务拒绝、伪造文件的下载、搭便车等问题。

4.1.3 用于信任信息管理的典型模型

1)Managing Trust[13]：关注信任信息的管理和获得。每个节点对其他节点的评价数据不是存放在自己节点上，而是存放于整个 P2P 网络中，具体存放地点由 P-Grid 存储规则确定。同时，为了防止网络故障以保证数据的健壮性，评价数据会冗余存放。当一个节点想要计算另一个节点的可靠性时，使用 P-Grid 中的算法查找该节点的投诉信息。一个节点的可靠性根据这些全局的投诉信息计算，若结果为负则该节点不可靠。但是，它只记录对节点的投诉评价，限于信任信息的二进制表达，没有量化信任值；同时，缺乏可信度的概念，无法防止污蔑行为的发生。

2)NICE[44]：关注信任信息的存储和查找，提出了基于 NICE 平台的不依赖于中心节点的分布式信任管理方案。在一次交易之后，每个节点针对交易质量签署它的 cookie，而 cookie 值表示为可比较的任意形式。如果签署的评价是正的，则评价会被存在另一交易方；如果签署的评价是负的，则评价会被存在本地。当一个节点 A 想要访问节点 B 的资源时，它必须呈献节点 B 签署的 cookie，以表明节点 B 对它的信任，这也激励节点存储交易中的 cookie。如果节点 A 没有这样的 cookie，A 可能会查找从 B 到 A 的链式 cookie，此时通过接收节点所有 cookie 的摘要来降低查找的开销。同时，关于节点 B 的负评价也会被节点 A 收集，从而做出是否交易的正确决定。

4.2 群组模型

从人类社会中的团体管理以及团体之间的合作得到启发，把 P2P 网络中的节点按照一定的策略划分为多个群组，实现信任管理。

1) A group based reputation system for P2P networks[45]：将信任关系划分为 3 个层次：群组之间的信任关系、群组与节点之间的信任关系和节点之间的信任关系。节点根据交易建立对其他节点的本地信任关系，并将交易结果向所在群组反馈。群组根据节点的反馈建立对群组内部节点的信任关系以及对其他群组的信任关系。节点要评估其他节点的可靠性时，如果本地没有相关信任信息，则询问群组。群组接收到来自组内节点的信任请求时，首先判断待信任节点是否属于本群组，如是则直接给出信任信息。如不是，则询问其所在信任群组获取推荐信任值。同时，根据陌生群组的行为调整陌生群组的信任值，以抵御恶意节点自组织为群组并不断更新群组 ID 进行的攻击。

2)An Adaptive Group-Based Reputation System in Peer-to-Peer Networks[46]：针对 Whitewashing 行为对于 P2P 网络效率的影响，每个群组保持一个 ITP(Initial Trust Probability，初始信任概率)。引入仲裁机制，3 个高可靠性节点依据新节点的随机信任值相对 ITP 的大小，对新节点的可靠性进行联合评判。群组的 ITP 也会基于新节点的行为和其他群组的 ITP 进行动态调节，以保护系统不受攻击。ITP 调节和节点可靠性计算的合理性有待进一步研究。

3)A Group-Based Trust Model in Peer-to-Peer Environment[47]：基于超级节点的群组信任模型，节点之间的信任关系被分解为群组内的信任和群组间的信任。根据交易节点是否处于同一个群组内，采用不同的可靠性评价方法。信任计算时，考虑时间因素，保证最近的交易信息被赋予更大的权重，信任信息保存在节点本身，以防止数据被篡改。但是，对于节点处于不同群组时，超级节点之间的信任关系没有给出明确定义；超级节点的性能要求也制约了群组的大小，而且存在单点失效的可能。

4) GARM: A Group-Anonymity Reputation Model in Peer-to-Peer System[48]：基于节点提供资源的类型划分群组，假设群组中由 pre-trust 节点负责选择服务节点和收集交易评价，实现提供资源的节点的匿名性，从而降低了虚假评价、合谋欺骗的不良影响；设置 CI(Continuing Interactions)记录节点提供服务的次数，基于一定的时间监控其提供服务与否，动态调节 CI 值，从而激励节点提供更多服务，抑制搭便车行为。

5 P2P 网络信任管理与其他学科的融合

从第 4 节中的模型可以看到，已有的非群组模型往往只针对电子商务、文件共享等某一特定应用环境，其中的全局信任模型为每个节点建立全局信任度是否必要和可行仍有待进一步研究，产生的网络流量以及迭代计算的计算量也会影响模型的可扩展性；基于局部信任的算法可扩展性差，不适合于大规模 P2P 网络，所反映的节点信任度具有片面性。同时，群组模型也不成熟，往往只关注于某个具体问题和特性的解决与实现。目前 P2P 信任管理系统还存在较多需要改进和完善的方面，它的研究也从最初的信息安全领域延伸到人工智能、神经网络、入侵检测等多个领域。

1)与人工智能的融合。准确性是信任机制的基本要求，信任模型应准确反映节点的可靠性。这里所说的准确性是一个相对的概念，因为信任本身就是无法准确定量的。对于这种利用不确定的条件得到不确定的结论，人工智能理论是一种理想的工具。有不少方案是建立在人工智能理论上的。萨斯喀彻温省大学的 YaoWang 等人利用 Bayesian 网络来建立信任棋型[33,49]。每个节点为所有与其交互过的节点建立一个 BN(Bayesian network)。通过 BN，请求者可根据自己关心的内容，计算服务提供者的可信概率，每种概率表达了节点在某一方面的可靠性。

2)与神经网络的融合。路易斯安那技术大学的 Weihua Song 等人提出基于神经网络的信任模型[50]。它的基本思路是通过神经网络聚合多个局部名誉来近似得到全局名誉。一旦一个用户的全局神经网络建立，当处于稳定状态时，只要将用户的多个局部名誉输入网络，就可以立刻得到全局名誉；当网络中发生状态变化时，监视进程将重新训练神经网络。

3)与入侵检测的融合。P2P 中的信任研究都是通过对节点历史行为的分析来预测下次行为。信任评价发生在交易之前，而信任信息更新发生在交易之后。也就是说，信任管理系统在交易前后发生作用，对交易过程中的恶意攻击无能为力，恶意攻击至少可以实施一次。可以考虑将信任管理研究与入侵检测结合起来，在交易过程中计算和评价信任，当监视到异常行为时，就开始削弱其可靠性，减到一定程度，就可以终止交易，以免给系统造成更大的伤害。

4)与博弈论的融合。博弈论是分析社会群体和经济活动中，个体和群体选择最优行为策略的有效数学工具。P2P 网络中的节点行为，也可以采用博弈论来进行分析。若利用博弈论方法建模，一个节点的行为选择就不再是自身的一个简单选择，它与同时在线的其他节点的行为选择密切相关。文

献[51]采用博弈论作为工具分析和抑制节点的搭便车行为。

5)与密码学的融合。节点间信任信息的安全传输能确保节点从网络中其他节点处获取待评估节点信任信息的真实性和完整性,采用密码学中的认证、数字签名等技术对信誉值进行加密传输,实现信任信息传输的安全性。文献[52]基于文献[19]协议中的不足提出了改进的传输协议,使用随机数抵御重放攻击,用数字签名保证信誉值的一致性和完整性。但在文献[52]中,公钥依旧在不安全的信道上传输,依旧无法阻止中间人攻击。

6)与其他理论的融合。基于信任的模糊性和动态性[25],Shanshan Song 等人提出基于模糊理论的信任模型[41]。为了有效隔离恶意节点,Hou Mengshu 等人提出基于确定性理论的信任模型[14]。文献[53]将节点的局部信任度表示为交易节点对其行为特征支持的证据,然后利用改进的 D-S 证据合成准则实施融合,得出节点的可靠性。

此外,其他一些研究成果也可以考虑引入 P2P 网络信任管理研究中,如数据挖掘和入侵容忍。对于推荐信息的过滤,可引入数据挖掘策略,以挖掘有用信息,降低无用甚至有害信息对于信任判断的影响。对于虚假评价问题,可融合入侵容忍技术,以确保信任信息保密性、完整性、真实性、可用性和不可否认性。

结束语 我们将 P2P 网络信任管理系统分解为 3 个主要部分,提出了每个部分需要考虑的基本问题,对已有的典型信任模型进行了分类和剖析,介绍了信任管理和其他学科的融合发展,这将有利于研究人员针对每一部分找到有效的解决方案,同时又不会忽略总体目标。

总体来说,现阶段信任模型层出不穷,证明 P2P 网络信任管理的整个研究态势呈现出分化的趋势,其研究也从最初的信息安全领域延伸到人工智能、神经网络、入侵检测等多个领域。各个子领域的研究成果和思想可以相互借鉴、互为补充。而且,每个子领域中的研究也在逐步细化,关注于某个具体问题和特性的解决与实现。如果各个子领域将分支研究成果融合起来,就有可能形成信任模型和信任政策的标准(如统一描述框架和分析评价标准),这也正是我们下一步努力和研究的方向。

参 考 文 献

[1] Papaioannou T G, Stamoulis G D. Effective use of reputation in peer-to-peer environments[C]// 2004 IEEE International Symposium on Cluster Computing and the Grid. Chicago, USA: Institute of Electrical and Electronics Engineers Inc., 2004: 259-268

[2] Khambatti M, Dasgupta P, Ryu K D. A role-based trust model for peer-to-peer communities and dynamic coalitions[C]// Proceedings of the Second IEEE International Information Assurance Workshop (IWIA'04). Charlotte, USA: IEEE Computer Society, 2004: 141-153

[3] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857

[4] Wang Y, Vassileva J. Trust-based community formation in peer-to-peer file sharing networks[C]// Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence. Beijing, China: IEEE Computer Society, 2004: 341-348

[5] Shi Z, He Y, Zhang H. Time self-decay trust management algorithm for P2P computing security [J]. Jisuanji Yanjiu yu Fazhan/Computer Research and Development, 2007, 44(1): 1-10

[6] Wu P, Wu G, Fang Q. Reputation-based trust model based on probability and statistics for P2P systems[J]. Jisuanji Yanjiu yu Fazhan/Computer Research and Development, 2008, 45(3): 408-416

[7] Selcuk A A, Uzun E, Pariente M R. A reputation-based trust management system for P2P networks[C]// CCGrid 2004. Chicago, USA: Institute of Electrical and Electronics Engineers Inc., 2004: 251-258

[8] Yamamoto A, Asahara D, Itao T, et al. Distributed pagerank: A distributed reputation model for open peer-to-peer networks[C]// Proceedings-2004 International Symposium on Applications and the Internet Workshops. Tokyo, Japan: Institute of Electrical and Electronics Engineers Computer Society, 2004: 389-394

[9] Feldman M, Lai K, Stoica I, et al. Robust incentive techniques for peer-to-peer networks [M] // Electronic commerce. New York, USA: ACM Press, 2004: 102-111

[10] Feldman M, Papadimitriou C, Chuang J, et al. Free-riding and whitewashing in peer-to-peer systems[J]. IEEE Journal on Selected Areas in Communcations, 2006, 24(5): 1010-1019

[11] Lai K. Incentives for cooperation in peer-to-peer networks[C]// Proceedings of Workshop on Economics of Peer-to-Peer Systems. New York, USA: ACM Press, 2003: 65-72

[12] Singh A, Liu L. TrustMe: Anonymous management of trust relationships in decentralized P2P systems[C]// Proceedings of Third International Conference on Peer-to-Peer Computing. New York, USA: ACM Press, 2003: 142-149

[13] Aberer K, Despotovic Z. Managing trust in a peer-2-peer information system[C]// Information and knowledge management. Atlanta, Georgia, USA: ACM Press, 2001: 310-317

[14] Hou M, Lu X, Zhou X, et al. A trust model of P2P system based on confirmation theory[J]. Operating Systems Review (ACM), 2005, 39(1): 56-62

[15] Sepandar D. Kamvar M T S H. EigenRep: Reputation Management in P2P Networks[C]// World Wide Web 2003. New York, USA: ACM Press, 2003: 123-134

[16] Dou W, Wang H, Jia Y, et al. A Recommendation-based peer-to-peer trust model[J]. Journal of Software, 2004, 15(4): 571-583

[17] Zhang Q, Zhang X, Wen X, et al. Construction of peer-to-peer multiple-grain trust model[J]. Journal of Software, 2006, 17(1): 96-107

[18] Tayabovorn C, Maneewongvatana S. A reputation-based system model for P2P networks[C]// ACST 2007. Phuket, Thailand: Acta Press, 2007: 188-193

[19] Cornelli F, Damiani E, de di Vimercati S C, et al. Choosing reputable servents in a P2P network[C]// World Wide Web 2002. Honolulu, Hawaii, USA: ACM Press, 2002: 376-386

[20] Kamvar S D, Schlosser M T, Garcia-Molina H. The Eigentrust algorithm for reputation management in P2P networks[C]// International World Wide Web 2003. Budapest, Hungary: ACM Press, 2003: 640-651

[21] Sherwood R, Lee S, Bhattacharjee B. Cooperative peer groups in NICE[J]. Computer Networks, 2006, 50(4): 523-544

[22] Li X, Liu L. A reputation-based trust model for peer-to-peer eCommerce communities [C] // Proceedings of the 4th ACM

Conference on Electronic Commerce. San Diego, USA: Association for Computing Machinery, 2003: 228-229

[23] Sabater J, Sierra C. Reputation and Social Network Analysis in MultiAgent Systems[C] // AAMAS'02. Bologna, Italy: ACM Press, 2002: 66-69

[24] Srivatsa M, Xiong L, Liu L. TrustGuard: countering vulnerabilities in reputation management for decentralized overlay networks[C] // World Wide Web 2005. Chiba, Japan: ACM Press, 2005: 422-431

[25] Chang E, Thomson P, Dillon T, et al. The fuzzy and dynamic nature of trust[C] // Second International Conference on Trust, Privacy and Security. Heidelberg, Germany: Springer Verlag, 2005: 161-174

[26] Duma C, Shahmehri N, Caronni G. Dynamic trust metrics for peer-to-peer systems[C] // 16th International Workshop on Database and Expert Systems. New York, USA: Institute of Electrical and Electronics Engineers Inc., 2006: 776-781

[27] Yu B, Singh M P, Sycara K. Developing trust in large-scale peer-to-peer systems[C] // 2004 IEEE 1st Symposium on Multi-Agent Security and Survivability. New York, USA: Institute of Electrical and Electronics Engineers Inc., 2004: 1-10

[28] Marti S, Garcia-Molina H. Identity crisis: anonymity vs reputation in P2P systems[C] // Peer-to-Peer Computing. New York, USA: ACM Press, 2003: 134-141

[29] Hogg T, Adamic L. Enhancing reputation mechanisms via online social networks[C] // Proceedings of the 5th ACM Conference on Electronic Commerce (EC'04). New York, USA: Association for Computing Machinery, 2004: 10-15

[30] Yu B, Singh M P. A Social Mechanism of Reputation Management in Electronic Communities[J]. Cooperative Information Agents IV, 2000, 10(2): 355-393

[31] Marti S, Garcia-Molina H. Limited reputation sharing in P 2 P systems[C] // Proceedings of the ACM Conference on Electronic Commerce. New York, USA: ACM Press, 2004: 91-101

[32] Azzedin F, Maheswaran M. Trust Modeling for Peer-to-Peer Based Computing Systems[C] // Parallel and Distributed Processing. New York, USA: IEEE Computer Society, 2003: 99-103

[33] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks[C] // Proceedings of Third International Conference on Peer-to-Peer Computing. New York, USA: ACM Press, 2003: 150-157

[34] Griffiths N, Sun S. Supporting peer-to-peer collaboration through trust[C] // 9th International Conference on Computer Supported Cooperative Work. Piscataway, USA: Institute of Electrical and Electronics Engineers Computer Society, 2005: 440-445

[35] Gil Y, Ratnakar V. Trusting Information Sources One Citizen at a Time[C] // Proceedings of the First International Semantic Web Conference. Heidelberg, Germany: Springer Verlag, 2002: 21-30

[36] Guha R, Kumar R, Raghavan P, et al. Propagation of trust and distrust[C] // World Wide Web 2004. New York, USA: ACM Press, 2004: 403-412

[37] Blanc A, Liu Y, Vahdat A. Designing incentives for peer-to-peer routing[C] // GECON 2004. Piscataway, USA: Institute of Electrical and Electronics Engineers Inc., 2005: 67-81

[38] Yang B, Garcia-Molina H. PPay: micropayments for peer-to-peer systems[C] // CCS 2003. Washington, USA: ACM Press, 2003: 34-40

[39] Horne B, Pinkas B, Sander T. Escrow services and incentives in peer-to-peer networks[C] // Proceedings of the 3rd ACM Conference on Electronic Commerce. Tampa, Florida, USA: ACM Press, 2001: 85-94

[40] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857

[41] Song S, Hwang K, Zhou R, et al. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing, 2005, 9(6): 24-34

[42] Damiani E, et al. A reputation-based approach for choosing reliable resources in peer-to-peer networks[C] // Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, USA: Association for Computing Machinery, 2002: 207-216

[43] Li J T, Wang X P, Chen Y Q, et al. A reputation management framework based on global trust model for P2P systems[C] // 7th International Conference on Advances in Web-Age Information Management. Hong Kong, China: Springer Verlag, 2006: 205-216

[44] Lee S, Sherwood R, Bhattacharjee B. Cooperative peer groups in NICE[C] // IEEE INFOCOM 2003. New York, USA: ACM Press, 2003: 1272-1282

[45] Tian H, Zou S, Wang W, et al. A Hierarchical reputation model for P2P networks[J]. Journal of Electronics and Information Technology, 2007, 29(11): 2560-2563

[46] Sun L, Jiao L, Wang Y F, et al. An adaptive group-based reputation system in peer-to-peer networks[J]. Internet and Network Economics, 2005, 3828: 651-659

[47] Xu F, Guo Y, Wang Q. A Group-Based Trust Model in Peer-to-Peer Environment[J]. IFIP International Federation for Information Processing, 2008, 251: 44-50

[48] Wen J, Shoubao Y, Dong W, et al. GARM: A Group-Anonymity Reputation Model in Peer-to-Peer System[C] // The Sixth International Conference on Grid and Cooperative Computing. New York, USA: ACM Press, 2007: 32-40

[49] Wang Y, Vassileva J. Bayesian Network Trust Model in Peer-to-Peer Networks[C] // AP2PC 2003. Melbourne, Australia: Springer Verlag, 2003: 23-34

[50] Song W, Phoha V V. Neural network-based reputation model in a distributed system[C] // Proceedings of the IEEE International Conference on E-Commerce Technology. San Diego, USA: IEEE Computer Society, 2004: 56-60

[51] Gupta R, Somani A K. Game theory as a tool to strategize as well as predict nodes' behavior in peer-to-peer networks[C] // Proceedings of the 11th International Conference on Parallel and Distributed Systems. Fukuoka, Japan: Institute of Electrical and Electronics Engineers Computer Society, 2005: 241-249

[52] Sieka B, Kshemkalyani A D, Singhal M. On the security of polling protocols in peer-to-peer systems[C] // Proceedings of the 4th International Conference on Peer-to-Peer Computing. New York, USA: ACM Press, 2004: 231-234

[53] Tian C, Zou S, Wang W, et al. A New trust model based on advanced D-S evidence theory for P2P networks[J]. Journal of Electronics and Information Technology, 2008, 30(6): 1480-1484