

P2P 网络环境下信任模型的研究与实现

郭 晶, 吴国新, 李 想

(东南大学 计算机网络与信息集成教育部重点实验室, 江苏 南京 210018)

摘 要:在目前已广泛应用的 P2P 网络中, 由于缺乏严格的身份验证和信任机制, 存在着许多欺诈等恶意行为, 系统的有效性和可用性难以保证。介绍了信任管理思想的出现, 结合信任管理的概念和模型, 提出了一种结构化 P2P 系统的层次模型, 并详细设计了信任管理模块的组成。讨论了当前研究存在的问题以及今后的研究方向。

关键词:对等网络; 信任; 信誉; 信任模型

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2009)03-0102-04

Research and Design for Trust Model in P2P Network

GUO Jing, WU Guo-xin, LI Xiang

(Ministry of Education Key Lab. of Computer Network and Information Integration,
Southeast University, Nanjing 210018, China)

Abstract: Through lack of strict identification and trust mechanisms, there are a lot of malicious peers in current P2P network. Trust management is a hot topic of Web security research in recent years. In this paper, the emerging of trust management is presented. Its concepts and models are described in detail. A layered architecture is presented, which clearly separates the functional components of a structured P2P system. The existing problems of current works and futures research direction are discussed.

Key words: peer-to-peer; trust; reputation; trust model

0 引 言

当今世界 Internet 广泛普及, 端用户系统资源越见丰富, P2P 网络在协同工作、分布式信息共享、大规模并行计算等方面显示出的独特优势, 使其成为新的发展热点。P2P 网络是基于节点愿意共享资源这一基本假设的, 即每个节点共享自己的资源, 并从其他节点那里获取自己需要的资源。然而, 这种个人为公众提供资源, 且节点行为无约束的工作模式, 导致了 P2P 网络中的不可靠服务和欺诈问题以及“搭便车”的问题。因此, 必须设计有效的机制来规范 P2P 网络中的这些行为。

信任管理这一概念就是为了解决这一问题而提出的。文中首先介绍了信任管理的概念及其相关研究工作; 接着按照模块化思想, 对 P2P 系统按功能模块分层; 并研究其中的关键技术问题, 详细设计了信任模型的结构。

1 相关知识介绍

信任管理可以用来解决可信性和不确定性或风险的问题, 它的意义在于提供了一个适合应用系统开放分布和动态特性的安全决策框架^[1]。基本思想是承认开放系统中安全信息的不完整性, 提出系统的安全决策需要附加的安全信息, 从而将信任与分布式系统安全结合在一起。

研究信任和信任现象的领域很多, 如心理学、社会学、经济学、哲学以及计算机科学等等。文中研究的范畴是 P2P 计算环境下对等节点间的信任关系, 因此采用文献[2]给出的定义: 信任是一个对等节点基于与另一个节点的交互经验而产生的对该节点能力、诚信和可靠性的一种信心。

声誉是一个实体基于其他若干实体对另一个目标实体的信任评价而计算得到的对目标实体的一种可信程度的评估^[3]。在社会领域, 只有当过去的行为对将来有影响时, 人们才有动机去建立彼此间的信任关系。在 P2P 网络中也是一样, 如果节点 A 对其他节点有互惠行为, A 就有良好的信誉, A 会被其他节点信任, 并在交易中得到其他节点的互惠行为。信任模型与激励机制之间具有良好的互动关系, 可以有效促进 P2P 网

收稿日期: 2008-07-24

基金项目: 国家高技术研究发展计划(863 计划)(2007AA01Z422)

作者简介: 郭 晶(1986-), 女, 江苏泰州人, 硕士研究生, 研究方向为 P2P 网络、信任管理; 吴国新, 教授, 博士生导师, 研究方向为计算机网络。

络中节点之间的合作。

信任研究主要包括基于策略的信任框架、信任模型和特定应用领域的信任机制研究等三个方面。目前存在若干基于 Peer-to-Peer 环境的信任模型,有基于 PKI 的信任模型、基于局部推荐的模型、全局可信度模型和数据签名这几种。全局可信度模型是现在研究比较多的一种,为获取全局的节点可信度,每个节点通过邻居节点间的迭代,获取节点全局的可信度,一定的迭代周期过后,全局节点得到统一的信誉值总体。这个信任值是综合了全体节点对某节点的评价后得到的,可信度比较高,有比较强的指导意义。

信任机制是对传统网络中安全机制的有效补充,在整个网络体系中的地位有待明确^[4]。通常可将信任管理视为其他实体提供信任服务的服务中间件,信任管理系统的基本结构如图1所示。可以看到,通过各种各样的信息采集方式,比如集中式安全检测、分布式节点自检以及第三方通告等等,系统不断地收集输入,从信任信息存储处提取相关节点的信任值,经过信任分析算法之后,给出决策,从而提示系统应该采取怎样的行为控制手段,是接纳访问还是攻击预警或者进行免疫隔离等等。

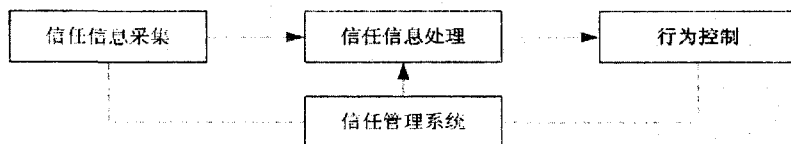


图1 信任管理系统基本结构

2 信任模型

目前围绕网络信任问题的研究集中在两个方面:一个是信任评价模型的研究,包括对信任概念模型的研究和对信任计算模型的研究。前者关注于理论模型,后者关注于信任的生成算法。另一方面的工作是信任管理框架的研究,主要研究在计算机网络环境下,信任的语义表达以及与信任评价相关的策略和证据的描述、收集、验证和管理等问题^[5]。下面着重介绍下信任的生成算法。

信任的生成算法主要涉及以下几个问题:(1)信任的表述和度量;(2)由经验推荐所引起的信任度推导和综合计算。几个有代表性的信任度评估模型在上述内容的处理上存在差异。纵观所有的基于全局的信任模型,主要涉及这几个概念和参数:本地信任、本地信任度、反馈可信度、全局可信度等等。下面分别给出定义和表达式^[6]。

2.1 本地信任值

两个节点间根据过去直接交往的历史行为而建立

起来的信任关系,就是本地信任值。其定义式为 $S_{ij} = G_{ij} - F_{ij}$ 。公式中 G_{ij} 为在节点 i 看来,与节点 j 交互成功的次数; F_{ij} 为在节点 i 看来与节点 j 交互失败的次数。本地信任值的评价,可以有多种方法,以二元评价为例的话,则取 $\text{tr}(i, j) = 1$ 或 $\text{tr}(i, j) = -1$ 。本地信任值也就是节点 i 对与节点 j 进行的所有交易满意和满意次数之差,即 $S_{ij} = \sum \text{tr}_{ij}$ 。

2.2 本地信任度

为了将本地信任度聚合,将其进行归一化是很有必要的。否则,恶意节点可以给它的同伴节点任意高的信任度,而给事实上表现良好的节点很低的信任度值,很容易就搅乱了整个系统。本地信任度 C_{ij} 就是归一化的本地信任值, C_{ij} 是这样定义的:

$$C_{ij} = \frac{\max(S_{ij}, 0)}{\sum_j \max(S_{ij}, 0)}$$

2.3 反馈可信度

反馈可信度是指2个节点之间没有进行过直接的交易,而是根据其邻居节点的推荐而建立起来的间接的信任关系。反馈可信度 C_r 有基于信任值、基于反馈相似度等几种判定方法^[5]。在不同的 P2P 环境下,

在系统恶意节点所占比重不同时,可以灵活选用适当的算法得到。

2.4 全局可信度

全局可信度,是指一个节点根据对另一节点的直接信任度和推荐信任度而综合得出的对该节点的信任程度^[7]。

全局信任模型下,迭代稳定之后,P2P 环境中所有节点对于某一节点的信誉度都是统一的。用 T 来表示,计算公式如下:

$$T = \alpha S_{ij} + \beta C_r, \text{ 式中 } \alpha + \beta = 1.$$

即根据可变化的权重分配,将直接交易关系得到的信任和他人推荐得到的信任相结合,得出对全网络对该节点的可信度评价。

2.5 信任生成算法的性能

对于信任生成算法的性能评估,有理论分析和实际验证两种方式。

由于大规模 P2P 网络这个实验条件比较难以满足,因此拟采用软件进行模拟 P2P 中的节点,包括大部分的正常节点和一部分的恶意节点。每个节点可以与其他节点进行交易,交易时触发另外一个节点的资源标志,采用全局计数器来统计成功次数、交易次数以及通信次数。对没有采用信任机制以及采用信任管理的网络,分别进行交易成功率和通信开销两方面的比较,来评价信任生成算法的性能优劣。

3 信任管理系统的结构模型

3.1 信任管理系统分层化模型设计

TCP/IP 分层模型使得各层之间相互独立,某层只要了解下一层通过接口所提供的服务,而不需要了解其实现细节。当某层内容发生变化时,只要接口关系不变,上下层均不会受到影响。鉴于这样的优点,把 P2P 系统中一些通用的功能模块化,给出如图 2 所示的 P2P 系统的层次模型。

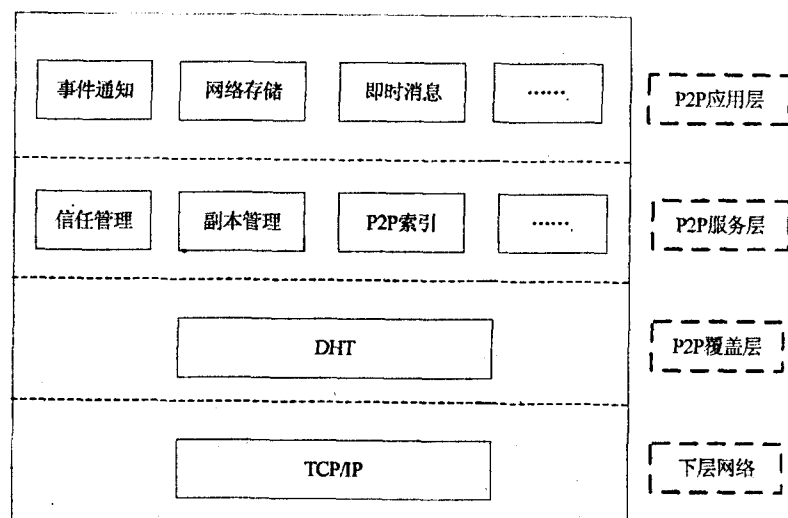


图 2 P2P 系统的层次模型

这个模型给出了 P2P 系统的一般性分层结构,是一种较合理的层次划分^[8]。最下层是底层网络,即现有的网络设施。第二层是 P2P 覆盖层,建立在底层网络之上,不论结构化 P2P 系统基于哪一种 DHT 来实现,它总是依赖于 DHT 提供的资源定位服务,这一部分功能应当独立成为一个模块。P2P 覆盖层主要的功能是构建和维护 P2P 覆盖网络。基于 DHT,节点和若干个邻居节点相连接,形成虚拟的覆盖网络。另外, DHT 还实现资源的定位功能。例如,对于采用 DHT 方式进行信任管理数据存储的系统来说, DHT 可以负责定位存放某节点的信任数据存储点。

第三层是单独的服务层。P2P 服务层提供 P2P 应用层通用的一些功能^[9]。例如,信任管理、副本管理、索引等。这些功能模块使用覆盖层所提供的一些接口,为上层提供一套 API, P2P 应用程序通过调用这些 API,来实现节点的信任评估、使用索引服务并实现数据对象的插入、删除、查找等功能。服务层提供的这些功能模块应当可以根据具体的 P2P 应用来定制。比如,用户可以灵活选择,是否需要采用信任管理机制来对系统进行维护。但信任管理和 P2P 覆盖网络的构建没有必然的联系,因此将信任管理作为服务层的一个功能。

最上层是 P2P 应用层,使用服务层提供的接口来

访问服务层和覆盖层为 P2P 应用提供的功能,这些功能的具体实现对 P2P 应用程序是透明的。具体的 P2P 应用有: P2P 数据存储;即时通信等等。

3.2 信任管理模块设计

P2P 服务层中的信任管理模块,主要功能是提供对指定的节点的信任评估。理想情况下,信任管理只应管理实体的抽象的信任属性,而不考虑实体的位置或者是来自哪个信任域,因而它是一个抽象的层次,它的下层才是具体的信任管理。另外信任管理作为服务中间件也为上层的用户合作提供信任支持以提高成功率。

图 3 是一种理想的情况,在 P2P、WSN、Adhoc 等网络之间都可以进行信任协商,事实上目前连针对单一网络环境如 P2P 中的信任模型,都还没达到可以通过协商互连的程度。面向多信任域的信任管理是进一步研究的一个课题,采取将信任管理与信任协商相结合的方法,以扩展信任管理的范围。例如在 P2P 环境中的 EigenTrust 和 PeerTrust 之间可以通过信任协商建立信任关系,这种方案的好处在于既保留了现有信任模型,又满足了在更大范围内建立信任关系的需求。

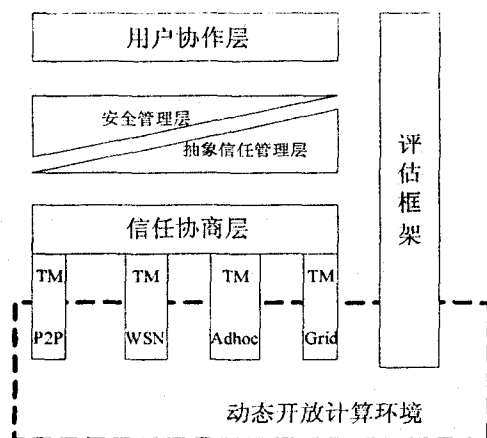


图 3 理想的信任管理模块

信任管理主要包括信任数据的采集、存储、传递、鉴别和评估几个环节^[10]。

(1) 采集:在信任相关的数据采集方面,引入关键的时间因素,提高信任评估的时效性,增强动态适应能力。

(2) 存储:在 P2P 环境下,信任数据应当分散存储到各个节点上。因此,每个节点需维护一定数量的信任评估所产生的数据。为此,将分析和研究现有的 DHT 结构的优势和不足,并考虑与现有的副本技术相结合,借鉴人类社会关系,构建基于社会网络的存储信

任数据的副本技术和拓扑结构。

(3)传递:依据分布式网络现有通信协议,确保信誉数据流经网络时完整性不受破坏。

(4)反馈激励:只有当过去的行为对未来有影响时,人们才有动机去建立彼此间的信任关系。只有当给出中肯的评价对自己的信誉值有提高时,节点才会积极主动地去对交易过的对象进行评估。因此,反馈激励机制就相当重要。对不同的对象行为,分布的应用环境,结合其他领域的合作理论,引入到激励模型中。

(5)信任值的计算:计算指定的节点的信任值,或配合其他节点的信任值计算。结合已有的信任评估算法,利用现代信息论最大熵原理,提出高效、快速收敛的自适应学习机制,改进信任系统的相关参数设置。

4 结束语

文中提出了信任管理系统的层次化设计模型,给出了信任管理的模块设计,讨论了当前研究需要着力解决的问题。

下一步,准备在多信任域的信任管理架构、信任模型建立和管理以及信任协商机制等方面进行研究,希望能将信任机制的可用性更为扩大。

参考文献:

- [1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust manage-

ment[C]//Proceedings of 17th Symposium on Security and Privacy. Oakland: IEEE Society Press, 1996: 164 - 173.

- [2] Wang Y, Vassileva J. Bayesian Network - Based Trust Model [C]//Proc. of IEEE/WIC International Conference on Web Intelligence (WI'2003). Halifax, Canada: [s. n.], 2003: 372 - 378.
- [3] 李景涛. P2P 环境下的信任模型与副本方案研究[D]. 上海: 复旦大学, 2006.
- [4] 林 闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005, 28 (5): 751 - 758.
- [5] 孟 魁. 虚拟社区环境下信任机制的研究[D]. 上海: 复旦大学, 2005.
- [6] Kamvar S D, Schlosser M T, Garcia - Molina H. The Eigen-Trust Algorithm for Reputation Management in P2P Networks[C]//Proceedings of the 12th international conference on World Wide. New York: ACM Press, 2003: 640 - 651.
- [7] Li Xiong, Liu Ling. PeerTrust: Supporting Reputation - Based Trust for Peer - to - Peer Electronic Communities[J]. IEEE Transactions on knowledge and data engineering, 2004, 16 (7): 843 - 857.
- [8] Chen R, Yeager W. Poblano: A distributed trust model for P2P networks[R]. Palo Alto: Sun Microsystems, 2002.
- [9] 徐 峰, 吕 建. Web 安全中的信任管理研究与进展[J]. 软件学报, 2002, 13(11): 2057 - 2064.
- [10] 赵 贵, 李 真, 张学杰. P2P 网络资源共享中基于信誉的访问控制[J]. 云南大学学报: 自然科学版, 2007, 29(S2): 238 - 240.

(上接第 101 页)

分辨出两个相干的宽带信号。在相同条件下,就 DOA 估计情况来看,TCT 算法的性能最好,估计结果最为精确,这是因为其聚焦矩阵是由去噪后的互谱密度矩阵进行特征分解得到的,但同时也提高了算法的运算量。

图 2 中,能更清楚地看到,估计性能最好的是 TCT 算法,其次是 RSS 算法,与这两种算法相比,对角聚焦矩阵法的方位估计性能稍差一些,但其聚焦矩阵的构造要简单一些。RSS 算法和 TCT 算法更真实地反映了信号位置,其 DOA 估计均方误差基本在 0.25° 以下(对角聚焦矩阵法均方误差最小值也在 0.3°),且谱峰较尖锐,其估计性能是优异的。

参考文献:

- [1] Agrawal M, Prasas S. Broadband DOA Estimation Using Spatial - Only Modeling of Array Data[J]. IEEE Trans, 2000, 48: 663 - 669.

- [2] Su Guanng, Morf M. The Signal Subspace Approach for Multiple Wide - Band Emitter Location[J]. IEEE Trans, 1983, 31: 1502 - 1522.
- [3] 王永良, 陈 辉, 彭应宁, 等. 空间谱估计理论与算法[M]. 北京: 清华大学出版社, 2004.
- [4] Yoon Yeo - Sun, Kaplan L M, McClellan J H. TOPS: New DOA Estimator for Wideband Signals[J]. IEEE Trans, 2006, 54: 1977 - 1989.
- [5] Wang H, Kaveh M. Coherent signal - subspace processing for the detection and estimation of angles of arrival of multiple wideband sources[J]. IEEE Trans, 1985, 33: 823 - 831.
- [6] Hung H, Kaveh M. Focusing Matrices for Coherent Signal - Subspace Processing[J]. IEEE Trans, 1988, 36: 1272 - 1281.
- [7] Doron A, Weiss A J. On Focusing Matrices for Wideband Array Processing[J]. IEEE Trans, 1992, 40: 1295 - 1302.
- [8] Valace S, Kabal P. Wideband Array Processing Using a Two - Sided Correlation Transformation[J]. IEEE Trans, 1995, 43: 160 - 172.