

国家自然科学基金：无线传感器网络中高效的
虚假数据过滤方法研究，编号：61502057

对等网络下 基于局部信息的信任模型



黎梨苗 刘志雄 何可可 叶 晖 张志宏 / 著

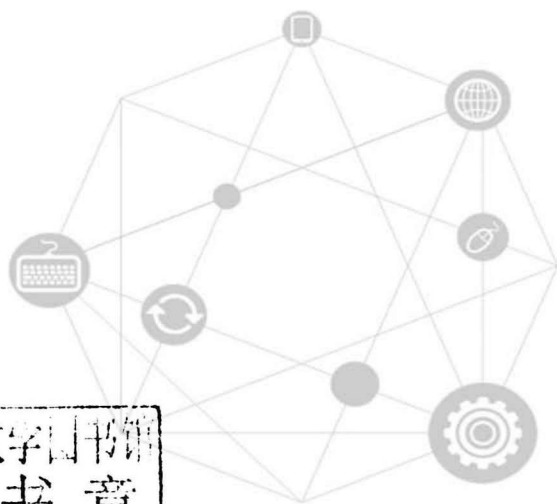
DUIDENG WANGLUOXIA
JIYU JUBU XINXI DE XINREN MOXING



电子科技大学出版社

DUIDENG WANGLUOXIA
JIYU JUBU XINXI DE XINREN MOXING

对等网络下 基于局部信息的信任模型



常州大学图书馆
藏书章

黎梨苗 刘志雄 何可可 叶 晖 张志宏 / 著



电子科技大学出版社

图书在版编目 (CIP) 数据

对等网络下基于局部信息的信任模型 / 黎梨苗等著.
—成都: 电子科技大学出版社, 2017. 1
ISBN 978-7-5647-4133-4

I. ①对… II. ①黎… III. ①互联网络—应用—借贷—研究 IV. ①F830.49

中国版本图书馆 CIP 数据核字 (2016) 第 319793 号

对等网络下基于局部信息的信任模型

黎梨苗 刘志雄 何可可 叶 晖 张志宏 著

出 版: 电子科技大学出版社 (成都市一环路东一段 159 号电子信息产业大厦 邮编: 610051)
策划编辑: 李述娜
责任编辑: 杜 倩 李 倩
主 页: www.uestcp.com.cn
电子邮箱: uestcp@uestcp.com.cn
发 行: 新华书店经销
印 刷: 四川永先数码印刷有限公司
成品尺寸: 140mm×203mm 印张 5.375 字数 190 千字
版 次: 2017 年 1 月第一版
印 次: 2017 年 1 月第一次印刷
书 号: ISBN 978-7-5647-4133-4
定 价: 36.00 元

■ 版权所有 侵权必究 ■

- ◆ 本社发行部电话: 028-83202463; 本社邮购电话: 028-83201495。
- ◆ 本书如有缺页、破损、装订错误, 请寄回印刷厂调换。

前 言

P2P (Peer-to-Peer: 对等) 网络已经发展成为 Internet 中最重要的应用系统之一, 它为人们提供了直接使用 Internet 进行交互的方法。网络中的任何节点, 可以随意加入与离开网络, 这样, 使得网络具有良好的灵活性与可扩展性。由于 P2P 网络中的节点具有高度的动态性和自主性, 由其引发的安全问题也越来越突出。如滥用资源、制造虚假信息、提供非法资源等恶意行为, 使得节点之间失去了信任, 严重阻碍了 P2P 网络的向前发展, 信任机制已成为解决 P2P 网络安全问题的重要手段。目前, 国内外学者已经研究出许多信任模型, 但是, 这些信任模型还存在着一些不足, 如评价信息的淹没, 信任评价语言信息处理不科学导致信任值偏离实际情况, 在不同领域不同层级的节点之间信任关系难以建立, 没有考虑不同节点参与评价优先权重的不同等。因此, 本书针对上述问题对 P2P 环境下的信任模型进行了深入研究, 主要成果如下。

(1) 提出了不等信任维度权重的信任评价模型。该模型以信誉与合作为轴, 建立了信任评价矩阵模型。依据相关文献, 分别给出了信誉评价指标与合作评价指标的定义, 并对指标进行了详细分析。依据指标性质的不同, 首次采用二元语义来处理信誉评价信息; 采用定性数据测量来处理合作评价信息, 解

决了评价信息淹没问题。因此，分别建立了节点的信誉评价模型与合作评价模型，从而得到节点之间的总信任评价模型。仿真与分析表明，该模型系统中的节点具有良好的任务执行成功率，且节点受恶意节点的影响较小。

(2) 提出了不确定性信息的信任评价模型。考虑主观信任评价信息的不确定性，采用模糊理论处理节点之间的信任评价。通过定义主体集、指标集、模糊评价集及属性集，来对信任评价问题加以描述。每个参与评价的主体对每个属性的指标进行评判，将所有的评判用特征向量矩阵来表示，采用无量纲原理来对属性指标进行处理，并且采用专家经验法来对各指标赋权值，构建信任评价模型。依据信任具有随时间衰退的特性，设计了与时间相关的信任更新算法。最后进行了实例分析与仿真，结果验证了该模型的科学性，体现了该模型系统中节点的信任值能较好地反映节点的真实情况，提高了节点之间的合作率与网络吞吐率。

(3) 提出了集成领域相似信息的信任模型。通过定义专家树建立了相似信息领域不同层级专家的相似度计算模型，定义了信任离散度与专家惩罚度，使信任模型具有抑制恶意节点行为的性能。提出了专家反馈算法使模型对节点之间的异常评价具有灵敏的反映。设计了基于 Kalman 滤波的信任更新机制，使信任能得到实时的、有效的更新。仿真与分析表明，模型能够有效抵抗不同恶意节点的攻击，具有较好的性能，使系统开销较小。

(4) 提出了推荐优先权的信任模型。首先依据现实生活中

的情况，给出了建立该模型的思想，设计了模型的工作流程。通过参考 Peer Trust 模型，引入直接信任度随时间衰减的因子与推荐信任度随时间衰减的因子，分别对节点的直接信任度与推荐信任度进行了数学建模。给出了随时间衰减的因子双向同步算法与优先权算法，解决了不同节点推荐信任优先权的分配问题，实现了实时更新与之交易过的节点各权重值。依据节点之间相互交易方式的不同，分两种情况建立了节点的总信任评价模型。仿真与分析表明，该模型能够很好地抑制恶意节点所带来的破坏，使系统中节点之间的信任普遍较好，具有较高的成功服务率与合作率，提高了系统的性能。

本书在编写过程中得到了陈志刚教授、邓晓衡教授、桂劲松副教授等的大力支持与帮助，在此表示衷心的感谢，借此机会向所有关心、支持和帮助本书编写、出版工作的同志们表示诚挚的谢意。

由于编者水平有限，书中难免存在不妥之处，恳请读者批评指正。

编 者

目 录

第 1 章 绪论	1
1.1 研究背景和意义	1
1.2 相关研究现状及分析	3
1.2.1 信任概述及分析	3
1.2.2 P2P 环境下的信任模型研究现状与分析	6
1.2.3 对研究现状的分析	13
1.3 本书的主要研究内容	16
1.4 本书的组织结构	17
第 2 章 信任建模的主要问题分析	20
2.1 信任值的表述	20
2.2 信任建模方法分析	22
2.3 信任评价数据的管理	27
2.3.1 信任评价数据的存储方法	28
2.3.2 信任评价数据的存储模式	29
2.3.3 信任评价数据的查询	30
2.3.4 信任评价数据的安全保证	31
2.3.5 信任评价数据的安全传输	33



对等网络下

基于局部信息的信任模型

2.4	信任模型的设计要求	34
2.5	信任模型仿真介绍	37
2.5.1	基于 OPNET Modeler 的仿真方法	37
2.5.2	基于 QueryCycle 的仿真方法 ^[47]	40
2.6	本章小结	43
第 3 章	不等信任维度权重的信任模型	44
3.1	引言	44
3.2	问题的描述	46
3.3	信任评价矩阵模型	47
3.4	基于二维度的相互信任评价模型	49
3.4.1	评价测量指标	49
3.4.2	二元语义模型	50
3.5	信誉与合作评价	52
3.5.1	信誉评价	52
3.5.2	合作评价	55
3.5.3	相互信任评价	56
3.6	仿真实验与分析	57
3.6.1	实验介绍	57
3.6.2	实验结果分析	58
3.7	本章小结	62
第 4 章	不确定性信息的信任模型	63
4.1	引言	63
4.2	问题的描述	65

4.3 基于模糊理论的信任评价模型	66
4.3.1 模糊评价的定量描述	67
4.3.2 模糊评价原理	69
4.3.3 信任评价的模糊决策	71
4.3.4 信任评价更新算法	73
4.3.5 恶意评价惩罚策略	75
4.4 实例分析	76
4.5 仿真实验与分析	77
4.5.1 实验介绍	77
4.5.2 实验结果分析	79
4.6 本章总结	82
第 5 章 集成领域相似信息的信任模型	83
5.1 引言	83
5.2 问题的描述	86
5.3 专家池模型基本概念	87
5.4 专家池模型设计思想及工作流程	90
5.5 基于专家池的信任模型	92
5.5.1 信任值的计算	92
5.5.2 专家信任反馈算法	94
5.5.3 专家节点信任更新	96
5.5.4 模型的安全性分析	99
5.6 仿真实验与分析	100
5.6.1 实验介绍	100



对等网络下 基于局部信息的信任模型

5.6.2 实验结果分析	103
5.7 本章小结	112
第 6 章 不等推荐优先权的信任模型	114
6.1 引言	114
6.2 问题的描述	117
6.3 基于推荐优先权的信任模型	118
6.3.1 模型设计思想	118
6.3.2 信任值的计算	120
6.4 优先权信任算法	124
6.5 模型安全性分析	125
6.5 仿真实验与分析	128
6.5.1 实验介绍	128
6.5.2 实验结果分析	131
6.6 本章小结	139
第 7 章 结论与展望	140
7.1 工作总结	140
7.2 展望	143
参考文献	147

第 1 章 绪 论

本章首先对本书的研究背景与意义进行了介绍,叙述了当前国内外相关领域的研究动态,然后对本书所做的研究工作与研究目标进行了介绍,最后给出了本书的主要研究内容与本书的组织结构安排。

1.1 研究背景和意义

Internet 的使用已走进了千家万户,用户享受着丰富的网络资源及不断增加的网络带宽,这使得传统的客户端/服务器 (Client/Server) 模式已无法满足社会的需求,从而使 P2P 计算技术发展成了当今及未来不可避免的互联网络计算模式。目前, P2P 网络应用已经成为互联网带宽应用最多的网络,其典型的网络系统有 NaPster、Gnutena 与 Kazaa 等,其中 Kazaa 网络系统已拥有 300 多万同时在线用户,并且发展趋势愈演愈烈,使得 P2P 技术已成为分布式计算领域的发展热点^[1]。

P2P (Peer-to-Peer) 网络即对等网络, Oram^[2]曾经把 P2P 网络简单地定义为: “P2P 是利用 Internet 网络边缘可用的存储空间、CPU 计算能力、信息内容以及人力等资源组织而形成



对等网络下 基于局部信息的信任模型

的一种网络应用形式。”其技术已经发展到了一定的程度，其特点是网络中的每一个节点即实体具有同等的地位，既是资源的提供者也是资源的消费者，体现了 P2P 网络没有中央节点控制的特点，使得资源相互共享，形成了开放式、自组织式的网络环境^[3]。P2P 网络中的节点具有高度的动态性和自主性，其可以自愿地、随机地加入网络，这样，导致了 P2P 网络的安全问题也越来越突出，使得 P2P 网络难以提供可靠的服务质量，影响了节点之间的信息共享与交互，大大破坏了正常的网络系统环境，降低了用户使用 P2P 网络的积极性。由于 P2P 网络本身所具有的匿名性与高度的开放性的特点，渐渐地 P2P 网络呈现出了一定的缺点。虽然 P2P 系统理论上具有最佳的性能状态，但实际情况下很难达到。出现此影响最主要的一个原因是 P2P 网络中的节点具有自主性，因此，节点在行为上出现了一些严重制约网络中节点之间合作关系的现象，如提供不可靠的服务、安全风险等。另外，到目前为止，P2P 网络系统中没有有效的激励机制去激励节点提供可靠的服务与进行良好的合作。P2P 网络系统中导致节点行为存在差异的因素包括两方面：一方面是 P2P 系统自身具有的高度开放性与匿名性；另一方面是系统中节点的地位、目的、类型等因素，从而使节点之间存在着严重的信任问题，最终影响了 P2P 系统的性能。按照节点自主行为的差异，可以将节点的行为分为自私行为和恶意行为两大类。自私行为通常包括 Free-riding^[4]与 Tragedy of the Commons^[5]。Free-riding 是指节点只请求资源而不提供自己资源的行为。典型的例子有 Gnutella 的文件共享系统，其中

Free-rider 节点占了 70%；在 eDonkey 的文件共享系统中，Free-rider 节点大约占了 80%。Tragedy of the Commons 是指节点无节制地使用公共资源的行为。恶意行为是指节点在网络中提供一些损害其他节点利益的行为。常见的恶意行为包括提供不可靠服务，进行欺诈蒙骗，散布病毒、木马等。恶意节点对系统攻击的形式多种多样，如诋毁、合谋、Dos 攻击、振荡、冒名等。在 P2P 系统中，一旦恶意节点形成规模，其行为将使系统崩溃。

虽然 P2P 技术在 Internet 网络中显示出明显的优势，但是，由于其本身的特点，系统中的节点存在相互信任问题，这样，严重影响了 P2P 技术的进一步发展。因此，在 P2P 环境下，建立安全可靠的信任管理模型是非常必要的。可是，大规模 P2P 环境下，基于全局信息的信任模型的实际使用代价非常大，甚至此类模型实现起来的可能性很小；而基于局部信息的信任模型，可有效降低实际使用成本，但模型精度受到诸多因素的影响。因此，研究如何基于局部信息改进来提高建模精度，并且研究相关信任模型具有科学意义和实用价值。

1.2 相关研究现状及分析

1.2.1 信任概述及分析

到目前为止，学科界对信任还没有统一的定义。20 世纪



对等网络下 基于局部信息的信任模型

70 年代末, Luhmann 采用社会学理论对信任加以描述, 将信任定义成是使社会复杂性简化的一种手段。1990 年, 计算机科学家 Gambetta 对信任进行了定义, 他认为信任并不是一个门限点, 而是一个概率分布式的概念, 可以用介于 $[0, 1]$ 之间的值来定量表示。后来, Grandison 与 Sloman 提出了信任的概念, 他们认为信任是一种坚固的信念, 用来描述某个个体在特定的情境下, 独立地、安全地且可靠地完成被其他个体所要求的服务或执行某特定动作的能力。文献[6-10]对信任的一些基本性质及概念进行了描述。信任是一个被多个学科所定义的概念, 它是一种主观判断, 描述了在特定的情境下, 主体 A 对主体 B 是否能完成主体 A 所要求的服务, 或者所执行特定的动作的一种度量。也指主体 A 依据自己跟主体 B 交往的经验, 以及其他主体提供的对主体 B 的评价信息, 得出的对主体 B 的一种可信程度的判断。信任分为直接信任与间接信任, 信任的一些基本概念定义如下。

定义 1-1 直接信任 (direct trust): 是指主体 A 与主体 B 直接交往后, 主体 A 对主体 B 所提供的服务或执行的动作进行评价, 从而得出对主体 B 的信任。

定义 1-2 间接信任 (recommendation trust): 也称推荐信任, 是指主体 A 根据第三方提供的对主体 B 的评价而形成的信任。

定义 1-3 信任度 (trust degree): 也称可信度, 是指衡量主体 A 对主体 B 信任程度的一种定量表示, 如完全信任用“1”表示, 信任用“0.5”表示, 不信任用“0”表示。

为了更清楚地说明上述定义之间的关系，我们用图 1-1 进行了描述。图中 T_{AB} 表示主体 A 对主体 B 的直接信任度。 T_{AC} 表示主体 A 通过主体 B 而获得的主体 C 的推荐信任度。从图中可以看出，由于主体 A 与主体 C 之间没有直接的交往历史，主体 A 只有通过主体 B 来获得对主体 C 的信任评价。

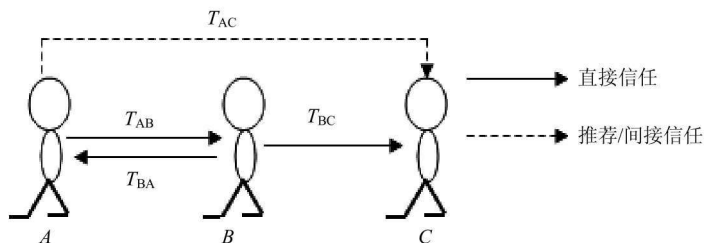


图 1-1 信任关系示例图

在信任机制研究中，与信任紧密相关又存在区别的一个重要概念是信誉。定义如下。

定义 1-4 信誉是对节点信任程度的一种全局度量，是网络中所有节点对所提供服务节点的质量与特性的一种综合评价，具有客观性。而信任是一个局部概念，只发生在两个主体之间，具有主观性。在一定的程度上，信任依赖于信誉，但并不完全决定于信誉^[11]。

在本书中，如果没有特殊声明，就不刻意区分信誉与信任，就把信誉归于信任的概念中，即信誉是 P2P 系统中所有节点对某个主体节点的信任。

信任具有以下属性。

1) 信任的衰减性。在对等信任模型中，节点相互之间不



对等网络下 基于局部信息的信任模型

存在不变的信任关系，信任值会随着时间的往前推移而逐渐减小。

2) 传递的局限性。传递的局限性可以表现为如下公式。

$$A \Rightarrow B \quad B \Rightarrow C \xrightarrow{\text{有限传递}} A \Rightarrow C \quad (1-1)$$

3) 信任关系的区间性。节点 A 对节点 B 是信任的，但并不表示节点 A 信任节点 B 所做的一切。信任存在一定的程度，我们把这种程度定义成区间。节点 A 对节点 B 的信任程度不同，则相互之间的信任就位于不同的区间，那么，节点 A 对节点 B 所做的一切就存在着信任差异，就不一定会信任节点 B 了。

4) 信任的无对等性。信任关系之间不存在对等性。

5) 信任的关联性。在节点之间的信任关系中，当节点 A 在一定程度上信任其他节点时，只是表示节点 A 对其他节点在特定内容上的信任，而不是对其他节点全盘内容的信任。

6) 信任关系的多样性。在信任模型中，节点之间的信任关系是多种对应关系，而不是单一对应关系。

1.2.2 P2P 环境下的信任模型研究现状与分析

在 P2P 网络系统中，节点可信任程度能力的体现受到一些客观因素的影响，例如节点数据的存储空间、计算速度、网络提供的带宽，并且节点之间的信任关系也受到许多因素的影响。因此，在计算信任值时，考虑全局知识的信任模型的实际使用代价很大，甚至不可能。所以，在 P2P 环境下的信任模型中，对信任值进行度量时，一般情况下都是基于局部知识来建立信任模型的，因为这样来计算信任值，可有效降低实际使用成本。

目前,就 P2P 网络系统而言,研究者们研究信任的关键技术是建立基于反馈信息的信任模型,该模型主要是采取节点与节点之间相互信任评价的方式来计算节点的信任值。采取该方法建立的模型分为两大类,一类是全局信任模型,另一类是局部信任模型。

全局信任模型是指网络中某个节点的信任值是通过网络中所有其他节点对其进行信任评价,并将评价信息采取迭代运算来进行处理,从而获得该节点的信任值的一种方式。在这种信任机制中,信任值的获得依赖于 P2P 网络中所有相关节点的评价信息,因此,这种机制相对来说可以更为准确地评价节点的信任程度。但是,简单的全局信任模型安全性与可靠性不高,容易受到恶意节点的攻击。而复杂的全局信任模型,需要网络中所有节点的相互合作来积极参与评价,使得处理的信息量非常大,再加上 P2P 系统的大规模特点和分散性,这种机制往往比较复杂且计算与通信代价较高。该类模型典型的有斯坦福大学开发的 EigenTrust 信任模型^[12]。

局部信任模型是指网络中某个节点的信任值是通过网络中所有与该节点进行直接交易后的节点给出对该节点的信任评价,并将评价信息进行一定的数学处理,从而获得该节点的信任值的一种方式。在这种信任机制中,信任值的获得仅仅依赖于有过直接交易的节点,相对来说,这样得出的被评价节点的信任程度与实际情况会有一定的差异。该类模型典型的有 Yuan Wan 等^[13]提出的 HBDTM (History-Based Distributed Trust Model) 模型。