网络信任研究进展

刘建生[1] 游真旭[1] 乐光学[1,2] 王结太[2] 刘建华[2]

(江西理工大学理学院 江西 赣州 341000)[1] (嘉兴学院数理与信息工程学院 浙江 嘉兴 314000)[2]

摘 要 网络的迅速发展为人们提供了自由、开放的交互方式,互联网服务已经成为大众日常生活的重要组成部分,如何评价表征节点交互的可信度已成为网络应用的核心问题之一。由于开放式网络环境具有匿名性、随机性和动态性等特点,用户在网络中选择目标节点进行交互时面临诸多风险,因此基于节点交互行为的信任评价机制成为抑制网络恶意虚假行为的有效策略机制。首先,概述信任的相关性质,根据网络节点间的交互行为及其产生的信任关系特征,形式化定义与构建信任网络。其次,分析信任机制的框架体系,依次讨论信任机制在 P2P 网络、电子商务、社会网络中的研究要点与安全威胁。最后,重点对比分析不同领域中的典型信任模型,详述其抗攻击效用与不足,从改进模型算法、提高模型抗攻击能力等方面指出信任机制在未来的研究方向。

关键词 网络交互,恶意攻击,信任机制,信任模型

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.11.002

Research Progress of Network Trust

LIU Jian-sheng[1] YOU Zhen-xu[1] YUE Guang-xue[1,2] WANG Jie-tai[2] LIU Jian-hua[2]

(Department of Science, Jiangxi University of Science and Technology, Ganzhou, Jiangxi 341000, China)[1]

(Department of Mathematics and Information Engineering, Jiaxing University, Jiaxing, Zhejiang 314000, China)[2]

Abstract The rapid development of Internet provides people with a free and open way of interaction. Internet services have become an important part of populace's daily life. How to evaluate the trustworthiness of characterizing node interaction has become one of the core issues in network applications. Due to the anonymity, randomness and dynamic characteristics of open network environment, users face many risks in choosing the target node in the network for interaction. The trust evaluation mechanism based on node interaction becomes an effective strategy mechanism to suppress the malicious and fake behaviors of network. First of all, this paper outlined the related properties of trust, and formally defined and constructed the trust network according to the interactive behavior among network nodes and the characteristics of their trust relationship. Then, this paper analyzed the framework of trust mechanism, and discussed the research focuses and security threats of trust mechanism in P2P networks, e-commerce and social networks. At last, this paper focused on the comparison and analysis of typical trust models in different fields, detailed the effectiveness and shortcomings of anti-attack, and proposed the research direction of future trust mechanisms in terms of improving the model algorithm and enhancing the anti-attack capability of model.

Keywords Network interaction, Malicious attack, Trust mechanism, Trust model

1 引言

信任起源于社会学,是一种表征人类社会关系的维度,是评判人们交互风险的重要依据之一[1]。信任度由人们在进行社会活动时的个体表现决定,对交易或合作对象的信任度评估通常根据历史的直接交互经验或者多渠道的间接推荐信息进行。20 世纪 90 年代,网络技术的兴起与广泛应用,使得人类物理世界的社会关系迅速在虚拟网络世界中得以体现与扩展。因此,网络世界中节点交互关系的本质其实就是人类社会交互活动的一种映射,网络服务的主要特征也随之表现为类似社会活动中的协同服务和合作共享等。研究表明,社会学中的信任特征描述能很好地表征网络节点的信任度,建立有效的信任机制来评价网络中节点的信誉和行为,成为描述网络行为的关键技术之一。网络信任机制的研究已由静态信任向动态信任管理演化[2],业界基于不同的应用背景对信任机制进行了大量研究并取得了丰硕成果,已广泛应用于 P2P、

到稿日期:2018-01-05 返修日期:2018-04-17 本文受国家自然科学基金项目(61462036,61572014,61702224),浙江省自然科学基金项目(LY16F020028,LQ15F010008,LY15F020040)资助。

刘建生 男,副教授,CCF 会员,主要研究方向为深度学习;**游真旭** 女,硕士生,CCF 学生会员,主要研究方向为复杂网络理论;**乐光学** 男,教授,CCF 会员,主要研究方向为复杂网络、协同服务等,E-mail:guangxueyue@163.com(通信作者);**王结太** 男,博士,主要研究方向为无线网络技术;**刘建华** 男,副教授,主要研究方向为网络安全。

电子商务、推荐系统和社交网络领域。

在传统的 C/S 网络模型中，服务器是整个网络的核心节点，网络采用基于 PKI(Public Key Infrastructure)和 CA(Certificate Authority)的静态信任机制。服务节点是网络的中心，易造成网络性能和服务质量随服务节点的邻居节点聚集度的提升而下降的瓶颈问题。为了解决这一问题并提高网络性能，以 P2P 网络为代表的分布式技术得以兴起并迅速发展，信任机制的模式相应地从静态信任发展为动态信任管理。P2P 网络遵循“我为人人，人人为我”的宗旨构建网络，实现资源共享和协作服务，具有良好的健壮性、扩展性和服务能力。每个节点既是资源请求者，又是资源提供者，不同节点之间直接连接，交换数据和服务，从而弥补了因服务器拥塞而造成的网络性能下降的缺陷。P2P 技术被广泛应用于协同系统、资源共享、即时通信等环境，成为当前重要的网络应用技术。由于 P2P 网络具有匿名性、开放性和动态性等特点，理性和自私特征使得网络中出现了大量恶意和自私用户，从而造成 FreeRiding、服务欺诈、版权侵害、文件污染、病毒传播等安全隐患。此时的 P2P 交互双方是在缺乏可信第三方的情况下通过网络直接交互，传统 C/S 网络环境下基于 PKI 和 CA 的静态信任机制不再适用于 P2P 网络。在这样的环境背景下，信任机制的研究由静态信任向动态信任管理演化，针对大规模分布式网络应用的动态信任管理技术被提出，并取得了丰硕的成果，推动了网络可信的发展。

分布式网络技术的成熟与应用，以及移动计算技术和设备的发展，使得大众步入了一个全新的社交网络时代。中国互联网络信息中心(CNNIC)发布的第 40 次《中国互联网络发展状况统计报告》[1)] 显示，截至 2017 年 6 月，中国网民规模达到 7.51 亿，手机网民规模达 7.24 亿。网民通过流行的 Facebook、Twitter 以及新浪微博、淘宝网、微信等应用平台，以自组织方式构建了由复杂社会关系连接而成的在线社交网络(Online Social Network，OSN)。各类社交应用与服务颠覆了大众传统的社交模式，融合了即时通讯、电子商务和消费推荐等诸多领域。网络为大众提供了随时随地进行信息分享、产品交易、业务协作等社交活动的平台。大规模的在线社交网络具有复杂性与动态性，虚拟社交与在线交易存在不确定性和风险性，引发了虚假节点攻击、恶意信息感染、非授权用户访问、服务欺诈等安全问题。分析网络节点行为与挖掘节点关系成为在线社交网络的热点问题，建立有效的网络信任机制成为网络发展的关键技术之一。在大规模开放的社交网络交互环境下，针对用户的即时通信、社交应用、网络购物等服务，基于节点交互行为的信任评价机制可有效抑制恶意节点的虚假和欺诈等作弊行为。大量研究成果表明，有效的信任机制在保证网络可信发展的同时，还推动了基于信任的电子商务与推荐系统的发展。

本文首先概述信任的相关性质，根据网络节点间的交互行为及其产生的信任关系特征，形式化定义与构建信任网络；然后阐述信任机制的框架体系、应用领域和安全威胁，依序讨论信任机制在 P2P 网络、电子商务、社会网络中的应用与研究要点；最后重点对比分析不同领域中的典型信任模型，详述其抗攻击效用与在理论或算法实现方面存在的不足，从改进模型算法、提高模型抗攻击能力等方面指出下一步的研究工作。

2 信任

2.1 信任的定义

信任概念最初产生于社会学领域，是一个很难度量的抽象的心理认知。信任已成为一门广泛的跨学科的交叉性研究问题。不同学科或领域对信任的典型定义如表 1 所列，计算机领域对信任的典型定义如表 2 所列。

表 1 不同学科或领域对信任的典型定义

Table 1 Typical definitions of trust in different disciplines and fields

学科或领域	定义
社会学	信任是一种社会维度，被认为是文化道德规范与社会阶级制度的产物[1]。
心理学	信任是个人的心理实践、人格特质和行为，表现为对被信任者的一种心理期待[3]。
社会心理学	信任是个体在互动中对他人行为的一种期望与依赖[4]。
经济学	信任被描述为一种社会资本，对社会经济发展的模式与速度将产生重要影响[5]。
管理学	信任与企业的绩效、风险、交易成本等紧密相连[6]。
电子商务	对被信任者特定行为的主观可能性预期，该预期是以对方的历史交互为基础[7]。
社会网络	基于被信任者将来行为的正面期望的信念[8]。

表 2 计算机科学领域对信任的典型定义

Table 2 Typical definitions of trust in field of computer science

研究者	定义
Mayer	信任方基于对受信者某个行为的预测，不管能否监视或者控制受信方，信任方依然愿意接受相信受信方的风险[9]。
Jøsang	在给定的环境下给某方以一种相对安全的感觉，在即使可能会产生负面结果的情况下，某方仍然愿意依赖于另一方的程度[10]。
王晓峰等人	在特定时间段和特定上下文环境中，授信方(Trustor)对受信方(Trustee)的某种服务属性在诚实性、安全性、可靠性以及可依赖性方面的一种主观肯定[11]。
Huang 等人	信任是一种心理状态，包括 3 个方面：1)期望，即信任者希望从受信者获得服务；2)信念，即基于对受信者能力和意愿的判断，信任者相信期望是正确的；3)风险意愿，即信任者愿意承担抱有以上信念可能导致的失败后果[12]。

根据以上定义可知，信任是一个由可靠性、风险性、安全性等属性综合而成的概念，因此需要根据信任关系中的实体所处的具体上下文环境进行相应的考虑和定义。

在自由交互的开放式网络中，对信任属性的定义如下。

定义 1(信任，Trust) 信任是指信任评估者(也称主体、源节点)在开放的自由交互网络环境中，在有效时间域内根据自身的直接交互经验或者其他推荐者的推荐信息，对于被信任者(也称客体、目标节点)是否能够按照预期，诚实、安全、可靠地完成某种特定服务或者交易行为的能力的可信赖程度，是两个实体间的主观行为。

信誉是与信任密切相关的一个概念，但它们并不完全等价。Jøsang 描述的两句话充分体现了两者的区别与联系[10]：

I trust you because of your good reputation(因为你有很好的信誉，所以我信任你)。

I trust you despite your bad reputation(尽管你的信誉不好，但是我依然信任你)。

1) http://cnnic.cn/gywm/xwzx/rdxw/201708/t20170804_69449.htm

定义 2（信誉，reputation）　信誉也称为声誉。信誉是对实体已有服务能力与交易质量的综合度量，反映网络中其他与之有过历史交互的实体对其信任程度的总体期望值。信誉是全局的概念，表示网络中所有主体对某个主体的综合客观性评价。

2.2　信任的关键属性

在自由交互的开放式网络中，依据对信任属性的定义，结合相关文献[8]，归纳出信任的如下关键属性。

1）主观性（Subjective）：信任关系依赖于主体的认知、观念、信仰、经验等因素。信任者的偏见和偏好等主观因素直接影响信任关系的评估。

2）动态性（Dynamic）：信任的主观性决定信任关系的动态性，信任随主体的偏见偏好、直接交互经验的改变而动态增加或减少。

3）时效性（Time-sensitive）：长时间的冷却关系会导致信任衰减。交互经验具有时效性，表现为最新的交互经验对于信任评估更具有参考价值。

4）非对称性（Asymmetric）：由个体评价的主观性决定信任关系的非对称性。如图 1 所示，实体 C 信任实体 D，而实体 D 却不一定信任实体 C。

5）可传播性（Propagative）：信任的传播属性类似于人类口口相传（Word of Mouth）的信息传播模式[8]。信任可通过推荐方式在社会网络中沿某条关系路径进行传播，连接成信任链，形成信任网络。

6）有限传递性（Non-transitive）：信任随着传递用户数的增多而减弱，即传递路径越长，信任衰减越大。如图 1 所示，实体 A 对实体 D 的信任衰减程度大于实体 A 与 C 间的衰减程度，如果实体 A 信任实体 B，且实体 B 信任实体 C，则实体 A 仅在一定程度上信任实体 C 和 D。

7）可合并性（Composable）：利用信任链在两个陌生实体间建立部分信任关系，当存在多条信任链时，可将多条信任链的信任信息通过信任传递运算合并。

8）事件敏感性（EventSensitive）：信任关系的构建依靠一段有效时间的交互经验，是否因为一次重要的负面事件而毁于一旦，是信任机制奖惩算法需要考虑的问题。

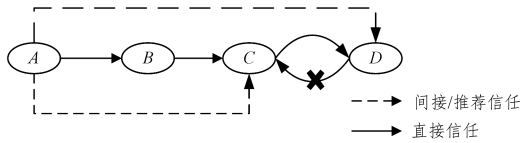

图 1　信任属性

Fig. 1　Trust attribute

信任极具不确定性。将信任动态变化的关键影响因素分为个体内因（endogenous factors，如个体的认知、性格、信仰、能力等）与外因（exogenous factors，如个体表现出的行为、策略、协议等）[13]。图 2 说明了个体信任动态变化的关键影响因素及引起的信任属性特征。

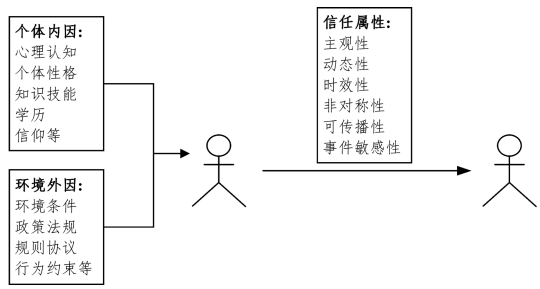

图 2　信任的关键影响因素

Fig. 2　Key influence factors of trust

2.3　信任值的表示方法

通过分析以上关键属性可知，信任极具抽象性和不确定性，需要采用合理的数学方法来量化信任的动态性，从而具体度量信任值的大小。已有文献中通常采用布尔变量、0 到 1 的实数或 −1 到 1 的实数、离散的等级或模糊逻辑值等。其表示方法有离散信任值、概率信任值、信念信任值、模糊信任值、灰色信任值以及信任云，后面 5 种表示方法反映了信任的抽象不确定性[14]。针对常见的 4 种表示方法进行举例分析，如表 3 所列。

表 3　信任值的表示方法

Table 3　Representation methods of trust values

分类	特点	文献定性描述	
离散信任值[15]	优点：简单描述，符合用户表达信任的习惯。 缺点：可计算性较差，需要借助映射函数把离散值映射成具体数值。	服务质量	描述
		好（G）	服务正确且服务质量好
		一般（L）	服务正确但服务质量欠佳，如服务不及时
		未响应（N）	拒绝服务
		不正常行为（B）	提供的服务是错误的甚至是恶意的
模糊信任值[16]	用模糊理论来研究主体的可信度，隶属度可以看成是主体隶属于可信任集合的程度。模糊化评价数据以后，信任系统利用模糊规则并基于这些模糊数据推测主体的可信任程度。	模糊集	描述
		T6	完全信任
		T5	特别信任
		…	…
		T1	不信任
概率信任值	优点：适用于很多与统计概率相关的推理算法。 缺点：把信任的主观性和不确定性等同于随机性。	实体 i 对实体 j 的信任度定义为 $a_{i,j}\in[0,1]$，$a_{i,j}$ 的值越大表示主体 i 对主体 j 越信任，0 表示完全不信任，而 1 则表示完全信任。概率信任值一方面表示了主体之间的信任度，另一方面也表示了主体之间不信任的程度。 如 $a_{i,j}=0.9$ 表示实体 i 对实体 j 的信任度为 0.9，不信任的程度为 0.1。	
信念信任值[17]	信念理论和概率论类似，差别在于所有可能出现的结果的概率之和不一定等于 1，信念理论保留了概率论中隐含的不确定性。	引入 *opinion* 表示信任度，把 *opinion* 定义为一个四元组 $\{b,d,u,a\}$。b,d,u 分别表示信任、怀疑、不确定。$b,d,u\in[0,1]$ 且 $b+d+u=1$。主体的可信任度为 $b+au$，其中 a 是一个系数，表示可信度中不确定所占的比例。	

3 信任网络

在自由交互的开放式网络中，节点间的交互关系本质上是人类物理世界中社会关系的一种映射，利用社会学中的信任关系能很好地反映网络节点的信誉与行为。通过形式化描述网络节点间的信任关系，以合理的信任值度量网络中的信任链可构造信任网络模型，为信任的传播机制和信任计算模型的研究提供理论基础。

3.1 信任关系

信任是网络中两个实体间的主观性行为，采用 0 到 1 的实数度量信任值大小，0 表示不信任，1 表示非常信任。

定义 3 设 I 为网络中交互实体的集合，$\exists i\in I$，$\exists j\in I$，且 $i\neq j$，以 $*$ 描述实体间的信任关系，T 表示信任值，则实体间信任关系的形式化定义如下：

$T: i*j\rightarrow[0,1]$

信任关系是研究信任机制的基础，已有许多学者依据不同的标准对信任关系做出不同的划分[18]，具体如表 4 所列。

表 4 信任关系的分类

Table 4 Classification of trust relationship

类别	含义
身份信任	利用加密、认证等传统安全机制，对网络实体身份的真实性进行授权和验证，也称静态信任。
行为信任	实体根据以往的交互经验及时调整相互之间的信任关系，也称动态信任。
直接信任	实体 A 根据与实体 B 的直接交互经验而形成的 A 对 B 的直接信任。
间接信任	当实体间无直接交互经验时，以其他实体提供的反馈信息为参考，根据自己的判断而形成的信任。
客观信任	基于凭证的，可以精确地描述、推理和验证，也叫身份信任。
主观信任	基于实体间的交互历史经验做出的主观判断，是基于信誉的信任关系。
域内信任	利用本域的管理策略评价域内实体的信任程度。
域间信任	以域为单位，通过其他域评价该域内所有实体的整体行为。
局部信任	源节点通过信任传播算法计算对目标节点的信任度，它表示源节点对目标节点的信任度。
全局信任	将信任网络中所有节点对某节点的局部信任度综合得到结果，表示节点在整个网络中的信任度。
一元信任	仅用信任程度这一个元素刻画信任度，一般采用经典的数学方法进行描述，如离散值、概率值、灰色值等。
多元信任	用信任、不信任和不确定等多个元素刻画信任度，如信念值、直觉模糊值、双格等。

3.2 信任网络的形式化模型

结合现实社会网络的认知理论和方法，通过对信任关系的相关属性进行分析和定义后，给出信任网络的形式化描述[19-20]。

定义 4(信任网络) 将网络节点间的信任关系以合理的信任值度量连接形成信任链，可构造一个信任网络。该信任网络可用一个加权有向图 G 来形式化表示，$G=(V,E,T_V)$。V 表示有向图的顶点集合(源节点、目标节点、中间节点)，$V=\{S,T,I\}$；E 表示顶点之间的关系集合，$E=\{e_1,e_2,\cdots\}$；T_V 表示顶点之间的信任值集合。

定义 5(源节点，source) 信任网络中发起信任评估请求的节点，也称服务请求节点(评估节点)，记为 s。源节点集合用符号 S 表示，$S=\{s|s\in S,s$ 为源节点$\}$。

定义 6(目标节点，target) 信任网络中被源节点进行信任值评估的节点，也称服务提供节点(服务/交易节点)，记为 t。目标节点集合用符号 T 表示，$T=\{t|t\in T,t$ 为目标节点$\}$。

定义 7(中间节点，internal) 信任网络中不属于源节点、目标节点的其余节点，记为 i。中间节点集合用符号 I 表示，$I=\{i|i\in I,i\notin S,i\notin T\}$。

信任网络是动态变化的，用于描述源节点 S 与目标节点 T 在某一时刻的信任关系。在某个时刻 τ，源节点和目标节点之间的信任网络可用 $G(\tau)$ 表示。如图 3 所示，$G(\tau)$：$V=\{i_1,i_2,i_3,i_4,i_5,i_6,i_7,i_8,i_9\}$；$I=\{i_2,i_3,i_4,i_5,i_6,i_7,i_8\}$，$S=\{i_1\}$，$T=\{i_9\}$；$T_v=\{0.2,0.6,0.5,0.8,0.9,0.4,0.5,0.7,0.6\}$。

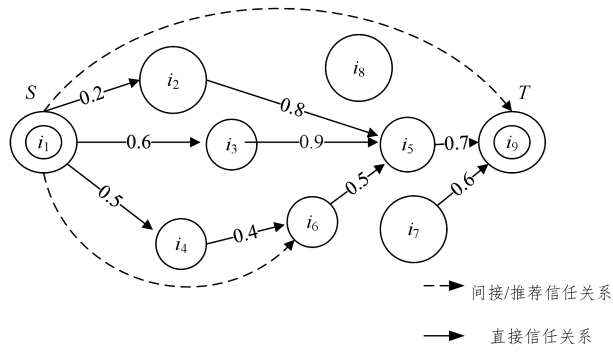

图 3 信任网络

Fig. 3 Trust network

定义 8(推荐节点，reference) 任意中间节点 $i\in I$，为帮助源节点 s 对目标节点 t 做出评价而提供自己与 t 的交易评价信息的节点，记为 r。推荐节点的集合用符号 R 表示，则 $r\in R$。

定义 9(信任度，trust worthiness) 信任度是评估节点对服务/交易节点信任值的一种量化。信任度 $T_{S,T}$ 表示源节点 S 对目标节点 T 的信任度。

定义 10(直接信任度，directed trust worthiness) S 对 T 的直接信任度 $DT_{S,T}$ 由节点间的直接历史经验计算，又称为局部信任度。

定义 11(推荐信任度，reference trust worthiness) S 对 T 的推荐信任度 $RT_{S,T}$ 是指 S 根据网络内其他推荐节点提供的其自身对 T 的直接信任度而计算得出的信任度。

定义 12(推荐可信度，credibility) 节点 S 对节点 R 的推荐可信度 $C_{S,R}$ 即为对节点 R 所提供的目标节点 T 的信誉值的信任程度的量化。

依据社会理论分析描述评估节点、推荐节点和服务/交易节点间的信任关系与推荐关系。推荐可信度取决于推荐节点和评估节点的熟悉度与亲密度，熟悉度与亲密度以交互频率来衡量。交互频繁的推荐节点的可信度高于无任何交互历史的推荐节点的可信度。以推荐方式传播的信任值在信任链中有限传递且逐层递减，表现为在推荐信任链上越靠近评估节点的推荐节点，其可信度相对越高。如图 4 所示，$node_1$ 和

$node_2$ 的推荐可信度高于 $node_3$ 和 $node_i$，而 $node_3$ 和 $node_i$ 的推荐可信度高于 $node_4$，$node_5$，$node_6$。

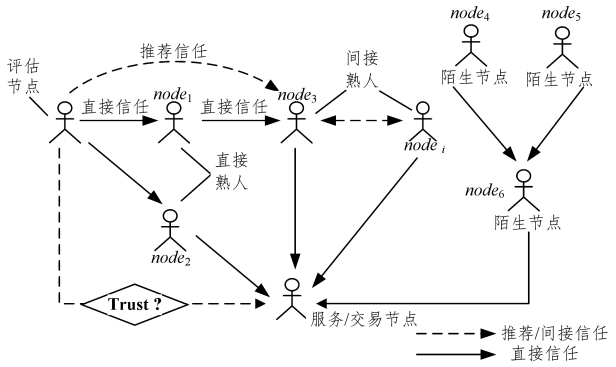

图 4　推荐信任关系

Fig. 4　Reference trust relationship

为了控制信任计算模型算法的时间复杂度与空间复杂度，对推荐节点 R 的层次给出如下定义。

定义 13（节点的层次，level of agent）　对于任意节点 u，$u\in I$。源节点 s 到 u 的信任链的最小跳数即最短距离 $d_{s,u}$ 称为节点的层次，记为 L。若 $d_{s,u}=N$，则称节点 u 为第 N 层节点，记 L_N 为第 N 层节点的集合，则 $u\in L_N$[20]。

定义 14（极限层次，ultimate level）　源节点 S 所能接受的推荐节点 R 所在的最远层次，即信任链传播跳数的极限值，记为 L_U[20]。

4　信任机制

4.1　信任机制的框架

由于开放式网络环境具有匿名性、自由性、随机性和动态性等特点，用户在网络中选择目标节点进行交互时面临诸多风险，基于节点交互行为的信任评价机制成为抑制网络恶意和虚假行为的有效策略机制。网络信任机制的研究已由静态信任向动态信任管理演化，按照动态信任管理的生命周期分为信任的产生、信任的建模、信任信息的收集、信任的计算、实体的交互与信任的更新 6 个部分[21]。信任机制的框架图如图 5 所示。

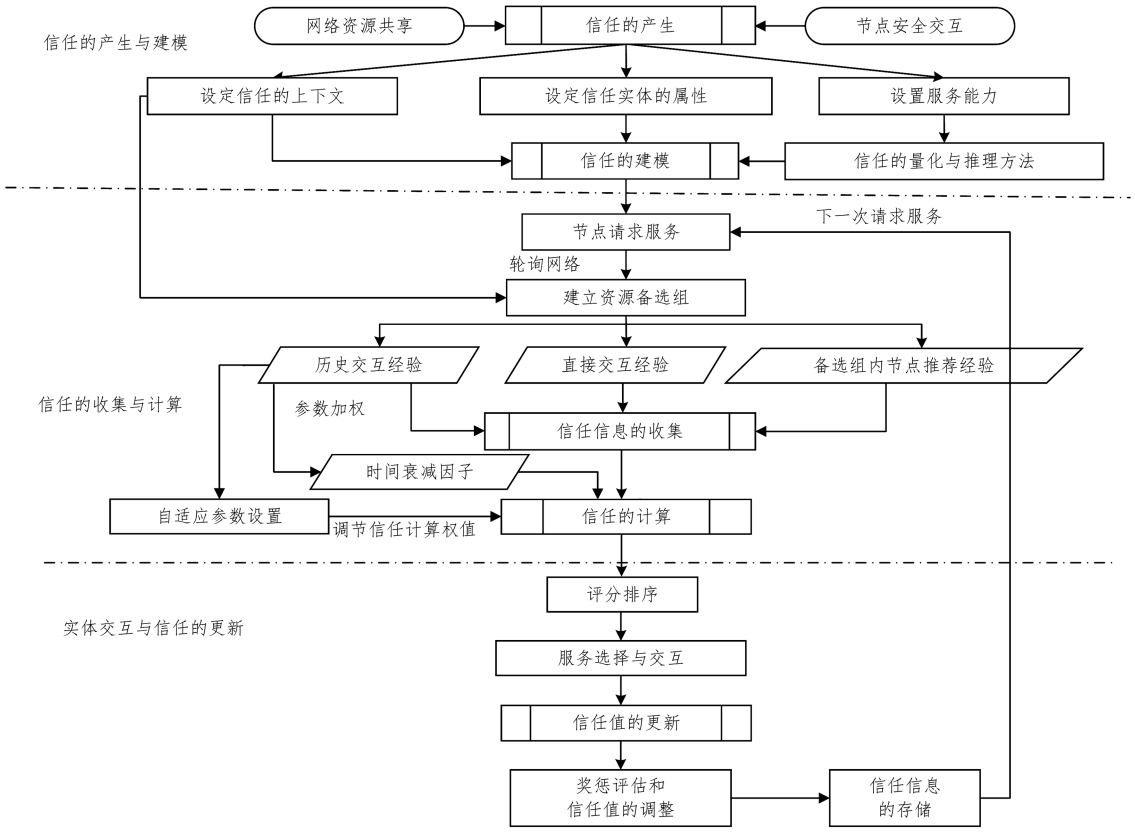

图 5　信任机制的框架

Fig. 5　Framework of trust mechanism framework

4.2　信任机制的应用领域

1994 年，Marsh 首次系统地论述了信任的形式化问题，为把信任机制应用到计算机系统中奠定了基础[22]。1996 年，BLAZE 提出并解决了 P2P 环境下信任管理存在的一些问题，是较早把信任引入到 P2P 系统的文献之一[23]。2000 年，自动信任协商（Automated Trust Negotiation，ATN）在传统的信任管理的基础上发展起来，它与信任管理的主要区别在于是否对外公布访问控制策略。在自动信任协商中，访问控制策略是对外公布的，其通过逐步向对方暴露数字证书，在陌生者之间建立信任关系，为合法用户访问资源提供安全保障，防止非法用户的非授权访问[24-27]。业界基于不同的应用背景对信任机制进行了大量研究并取得了丰硕成果，已将其广泛应用于 P2P、电子商务、推荐系统、社交网络领域。表 5 列出不同领域中信任机制的研究目的与内容。

表 5 信任机制的应用

Table 5 Applications of trust mechanism

应用领域	研究动机	研究要点
P2P 网络[13-14,30]	P2P 网络具有匿名性、动态性和开放性等特性，理性和自私特征使得网络中出现了大量恶意用户和自私用户，造成 FreeRiding、服务欺诈、版权侵害、文件污染、病毒传播等安全隐患。	信任与信誉机制： 1)信任与信誉的表示方法； 2)信任与信誉的计算方法； 3)信任与信誉值的存储方式。
电子商务[20,48,51]	在线网络虚拟交易存在不确定性与风险性，消费者往往难以评估网上陌生实体的可信度，更加无法辨别服务质量的好坏，经常面临交易的虚假信息发布、拒绝或延期交货、质量和售后服务，甚至是受到恶意欺诈等问题。	1)基于信誉的信任管理系统：代表性系统有 eBay 和 Amazon。通过构造科学的信任计算模型，客观度量卖家的可信度，降低用户交易风险。 2)基于信任的推荐系统。
社会网络[8,52,60-62]	开放、动态的大规模在线社会网络中存在大量陌生的交互对象，导致用户受到恶意和虚假节点攻击、感染恶意病毒、被非授权用户访问、服务欺诈等隐私泄漏与安全问题。	1)社会网络分析。 2)信任关系构建：①信任关系收集；②信任路径搜索；③信任传播；④信任评估。 3)社交网络中基于信任的推荐系统。

4.3 信任机制中的恶意攻击行为

针对信任机制在不同领域中的应用，信任计算模型应充分考虑不同环境抵抗恶意攻击行为的相应对策。网络恶意节点攻击行为的通常表现形式及解决方法见表 6。现有信任模型的抗攻击能力相对比较单一化，并没有实现较全面的抗攻击能力，大多都能识别与防范简单的恶意攻击与欺骗行为，但是对于复杂的共谋欺诈、女巫攻击和策略性攻击等恶意行为缺乏高效的识别和防护机制[21]；此外，现有的信任机制还缺乏行之有效的实体标签管理，导致恶意主体仍可轻易地洗白其“罪恶”历史，从而再次进入应用系统并重新进行恶意攻击。

表 6 恶意攻击行为的分类

Table 6 Classification of malicious attack behavior

恶意行为	表现形式	解决方法
摇摆攻击	1)m 次良好行为进行信任积累，然后使用 n 次交易进行攻击。 2)小金额交易或轻量级事务服务积累信任，对大金额交易或重要事务服务进行攻击。	奖励惩罚因子： 1)定义摇摆积累因子[28]； 2)定义事务影响因子[29-30]。
虚假反馈	1)诋毁攻击(nuke)：恶意的消极评价。 2)哄抬攻击(push)：言过其实的积极评价。	1)检测不诚实反馈：聚类技术[31]、基于 eta-function 过滤[32]、基于熵[33]等方法；信号模型[34]。 2)降低不诚实反馈的影响：用户反馈信誉；Laureti 等[35]提出迭代细化方法(反馈聚合算法中设置用户的反馈权重)；Zhang 和 Cohen[36]引入个性化的信任衡量反馈的可靠性。
“洗白”	重新注册一个账号，轻易地以新的身份重新加入系统以删除自己的历史恶意信息。	1)加标签； 2)增加注册账号代价。
共谋	1)简单的共谋行为。 2)复杂的共谋欺诈。	时域分析法[37]；时间和用户相关性分析法[38]； You 等[39]提出针对共谋欺诈的交易模式。

5 信任模型

在分析信任机制的框架、应用领域和安全威胁的基础上，重点研究信任机制的核心——信任模型。依序对目前国内外针对 P2P 网络、电子商务、社会网络 3 种应用场景的信任模型进行对比分析。从内容到优缺点角度深入研究不同领域中的典型信任模型，详述其在理论或算法实现方面、模型抗攻击能力方面的不足。

5.1 P2P 网络的典型信任模型

P2P 网络遵循“我为人人，人人为我”的宗旨构建网络，实现资源共享和协作服务，具有良好的健壮性、扩展性和服务能力。P2P 网络具有匿名性、开放性和动态性等特点，理性和自私特征使得网络中出现了大量恶意用户和自私用户，从而造成 FreeRiding、服务欺诈、版权侵害、文件污染、病毒传播等安全隐患。为解决 P2P 网络中节点的恶意行为问题，引入基于交互行为的节点信任与信誉评价机制。信任与信誉机制的主要内容包括收集节点间的历史交易记录，根据收集到的交易记录计算每个节点的可信度，依据节点的可信度决策是否进行交易。研究的要点[14]如下。

1)信任与信誉的表示方法：描述在系统中如何表示节点的信任和信誉；

2)信任与信誉的计算方法：利用节点的历史交易信息和推荐信息评估其信任与信誉；

3)信任与信誉值的存储方式：控制模型的时间和空间复杂度。

近十年来，国内外对 P2P 网络信任的研究已取得了丰硕的成果。文献[40]提出并解决了 P2P 环境下信任管理存在的一些问题，是较早把信任引入 P2P 系统的文献之一。文献[13-14,41]简要综述了 P2P 网络信任机制的国内外研究进展。

Kamvar 等[42]针对 P2P 文件共享系统，提出一种基于信

誉的全局信任模型 EigenTrust。该模型聚合与源节点发生过交易行为的每个节点对其的局部信任度，通过全局范围内信任链上的信任迭代，得到全局内每个节点的唯一信誉值，并使用此唯一信誉值来表示节点在此全局范围的信任值。该算法仅给出了一种迭代计算信任值的方法，没有考虑到其在计算信任值上的收敛速度，且由于采用迭代计算，通信代价太高，模型的抗攻击能力较弱。

PowerTrust[43]是在 EigenTrust 基础上提出的一种新的信任模型，具有较强的抗攻击能力。该模型采用了动态选举超级可信节点的算法，并使用一种名为“look-ahead”的随机行走策略，以改善全局声誉计算的迭代过程[14]。

Xiong 等[44]针对 P2P 在线社区，提出一种基于信誉的信任模型 PeerTrust。该模型类似于 EigenTrust 的推荐信誉构造原理，算法的优势在于引入反馈交易评价来评价节点的推荐信任值、交易时间因子和交易的激励机制等影响因子，增强了模型的抗攻击能力。但该模型没有给出信任因素及置信因子的度量方法，在具体的推荐算法上也更为复杂(5.1.1 节将对此算法进行详细分析)。

Wang 等[45]提出一种基于贝叶斯(Bayesian)的信任模型。该算法的贡献在于将贝叶斯网络引入到信任度的计算过程中，依据先前的交易反馈评价，利用 Bayesian 概率的方法来计算当前节点的信任度。计算前需对评价的样本空间进行处理，使其服从一定的概率分布，算法的复杂度较高。该模型忽略了恶意节点存在的安全威胁，导致抗攻击性能较差。

Beth 等[46]将经验分为肯定经验和否定经验，基于 agent 完成一次任务的可能性在[0,1]区间内服从均匀分布这一假设提出一种信任模型。但是该模型在度量信任关系时只利用了肯定经验，在计算信任度时无法很好地识别一些节点的恶意推荐。

Jøsang 等[10]引入观念空间与证据空间等概念，使用主观逻辑描述与度量信任关系，提出一个由信念建模和信念逻辑算子组成的信任度推导和计算模型，并提供了一套主观逻辑(subjective logic)运算用于信任度的推理和综合计算。但是，该模型没有明确区分直接信任和推荐信任，无法识别恶意推荐，因此抗攻击能力不足。

田春岐等[47]提出一种基于信誉与风险评价的信任模型 R²BTM(Reputation and Risk evaluation Based Trust Model)，该模型引入信任度的不确定性与风险性，并提出采用信息熵理论来量化风险。该模型突出体现了信任的风险性与不确定性。

刘义春等[30]提出一种基于上下文因素的 P2P 动态信任模型，结合考虑时间衰减、交互重要性和交互次数度量实体交互信任，基于 Dice 相似度给出信任相似度算法，设计一种多链路反馈可信度融合算法，聚合直接交互、评价相似度和信任链传递计算实体的推荐信任，综合直接信任和推荐信任进行实体信任的评估，并提出了一种新的信任更新和奖惩机制(5.1.2 节将对此算法进行详细分析)。

表 7 对上述典型信任模型进行对比分析。参考文献[13-14]列出以下模型评价指标：Context aware 描述模型是否引入服务上下文影响因子(比如 P2P 文件共享系统中文件的大小、类型和传输带宽等)；Multi-dimensional 描述模型是否将交易次数、交互事务的重要性等多维属性作为模型的影响因子；Reputation scoring 描述信任的量化方式；Arith-method 表示模型的构建理论；Decentralized 表示模型的控制方式是否为集中式；Evaluation scope 表示模型的评估范围，即局部或全局；Veracity 表示信任度的精确程度；Scalability 描述模型的扩展性；Robustness 表示模型的抗攻击能力，即鲁棒性；Overhead 表示模型的算法复杂度(时间和空间复杂度等)。

表 7　P2P 中典型的信任模型比较

Table 7　Comparison of typical trust models in P2P

Index collection	EigenTrust/ PowerTrust[42-43]	PeerTrust[44]	Beth[46]	Jøsang[10]	Yao[45]	R²BTM[47]	Liu[30]
Context aware	No	Yes	No	No	Yes	Yes	Yes
Multi-dimensional	No	Yes	No	No	No	No	Yes
Reputation scoring	0 or 1	[0,1]	[0,1]	[0,1]	−1 or +1	[0,1]	[0,1]
Arith-method	Linear iteration	Linear iteration	Probability distribution	Probability distribution	Bayes	Weighted mean	Weighted mean
Decentralized	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Evaluation scope	Global	Global /Local	Local	Local	Local	Global /Local	Global /Local
Veracity	Good	Better	Low	Lower	Good	Good	Good
Scalability	High	High	Low	Low	Low	Low	High
Robustness	Good	Good	Low	Low	Low	Low	Best
Overhead	High	Lower	Low	Low	Low	Low	High

5.1.1　PeerTrust

Xiong 等[44]借鉴 EigenTrust 的推荐信誉构造原理，针对 P2P 在线社区提出一种基于信誉的信任模型 PeerTrust。此模型是 P2P 网络中信任模型研究的关键奠基石之一，其算法思想一直被后续的信任计算模型沿用。

PeerTrust 的突出贡献是引入多维信任度影响因子：交易相关因素(交易时间、数量、交易额度等)，环境上下文，反馈交易评价，反馈评价节点的可信度，交易的激励机制等。结合以上多维度信任影响因子，提出任一节点 u 的信誉计算如式(1)所示：

$$T(u)=\alpha*\sum_{i=1}^{I(u)}S(u,i)*C_r(p(u,i))*TF(u,i)+(1-\alpha)*CF(u) \tag{1}$$

其中，$I(u)$为节点 u 在有效时间内的交易总数；$p(u,i)$，$S(u,i)$和 $TF(u,i)$分别为节点 u 的第 i 次交易对象、获得的反馈评价和相关的服务上下文；$Cr(v)$为节点的反馈可信度；$CF(u)$

为与节点 u 相关的环境产生的信任因素；调节因子 $\alpha(0<\alpha<1)$控制两部分信誉参数对节点信誉的影响。

PeerTrust 根据 $C_r(v)$评价算法的不同划分为两种，其中 $p(u)$为 u 的所有交易对象集合。

1)基于迭代的全局信任模型 PeerTrust-TVM：类似于 EigenTrust 采用节点的全局信誉度量节点反馈的可信度。PeerTrust-TVM 的计算公式如式(2)所示：

$$T_{TVM}(u)=\alpha*\sum_{i=1}^{I(u)}S(u,i)*\frac{T(p(u,i))}{\sum_{i=1}^{I(u)}T(p(u,i))}*TF(u,i)+(1-\alpha)*CF(u) \tag{2}$$

模型为全局迭代算法，其复杂度高达 $O(n^2)$(n 为系统规模)(具体参数属性见文献[44])。

2)基于相似度的局部信任模型 PeerTrustPSM：采用节点的反馈相似度 $Sim(v,w)$度量节点反馈的可信度。其计算公式如式(3)所示：

$$T_{PSM}(u)=\alpha*\sum_{i=1}^{I(u)}S(u,i)*\frac{Sim(p(u,i),w)}{\sum_{i=1}^{I(u)}Sim(p(u,j),w)}*TF(u,i)+(1-\alpha)*CF(u) \tag{3}$$

$$Sim(v,w)=\sqrt{\frac{\sum_{x\in IJS(v,w)}\left(\frac{\sum_{i=1}^{I(x,v)}S(x,i)}{I(x,v)}-\frac{\sum_{i=1}^{I(x,w)}S(x,i)}{I(x,w)}\right)^2}{|IJS(v,w)|}}$$

其中，$IJS(i,j)$表示同时与节点 i 与节点 j 交互过的节点集合。该模型看似比 PeerTrust-TVM 更具合理性，但是由于需要计算全局的反馈相似度，相应的计算代价大大增加，因此很难用于构造全局信誉。

PeerTrust 抵抗恶意行为的能力主要体现在以下方面：

1)归一化评价信息可以抑制恶意节点虚假的过高或过低评价的负面影响；

2)计算信任度时考虑交易数量、交易额度、交易时间因子等多维度信任影响因子，可避免节点利用多次交易、小额交易积累信任而掩盖其恶意摇摆的策略行为，能有效抵抗此类摇摆攻击；

3)依据评价相似度度量来评价可信度，在一定程度上可抵抗恶意节点的合谋攻击，因为恶意节点与正常节点间的评价相似度差异较大。

PeerTrust 模型在信誉描述方面比 EigenTrust 模型更全面、灵活，其优势主要体现在以下方面：

1)引入服务上下文信息作为信誉评价的参数，真实反映节点的实际贡献，节点信任度的准确性较高；

2)信任度的计算考虑交易数量、交易额度、交易时间因子，可以避免恶意节点的摇摆策略行为，抵抗虚假反馈、摇摆策略攻击的性能明显提升。

模型的不足之处如下：

1)在大规模的 P2P 系统中，模型的迭代收敛速度较慢，且算法的时间复杂度和空间复杂度较高。

2)未区分节点交易可信度与推荐可信度，不能有效识别并过滤虚假推荐，抵抗共谋团体攻击和策略性女巫攻击等隐蔽的协同作弊行为的能力较差。

3)缺乏节点的信任更新与奖励惩罚机制。

5.1.2 基于上下文因素的多维度 P2P 信任模型

刘义春等[30]提出一种基于上下文因素的 P2P 动态信任模型，与 PeerTrust 模型相比，该模型同样结合直接信任与推荐信任构建信任评价模型，也引入了上下文因素作为信任影响因子：时间衰减、交互重要性和交互次数等。但是，不同于 PeerTrust 模型的反馈可信度计算方法，该模型设计了一种多链路反馈可信度融合算法。该算法的主要贡献在于：1)抽象出基于直接交互经验的信任、基于共同评价相似度的信任和基于推荐信任链的信任三类推荐信任形成机制，并实现 3 类推荐信任的聚合；2)研究实体信任的奖励与更新机制，根据当前交互中实体表现的交互满意度分别提出信任奖惩更新算法与反馈可信度更新算法。

该模型综合直接信任 $DT(i,j)$和推荐信任 $RT(i,j)$评估实体的总体信任 $T(i,j)$，计算公式如式(4)所示：

$$T(i,j)=\begin{cases}\alpha DT(i,j)+\beta RT(i,j), & DT(i,j)\text{和 }RT(i,j)\text{都存在}\\ DT(i,j), & RT(i,j)\text{不存在}\\ RT(i,j), & DT(i,j)\text{不存在}\\ DT_0, & DT(i,j)\text{和 }RT(i,j)\text{都不存在}\end{cases}$$

$$\alpha=\frac{n_1^{\frac{3}{2}}}{n_1^{\frac{3}{2}}+n_2},\beta=\frac{n_2}{n_1^{\frac{3}{2}}+n_2} \tag{4}$$

式(4)利用节点 i 和 j 之间的直接交互次数 n_1 和其他节点的推荐次数 n_2，动态调整 DT 和 RT 的权重。$\alpha>\beta$ 表示直接信任对总体信任度的影响大于第三方推荐。

1)直接信任度 $DT(i,j)$

直接信任度的计算公式如式(5)所示：

$$DT_{ij}=\rho(n)\frac{\sum_{l=1}^{n}S_l\varphi(\Delta t_l)IF_l}{\sum_{l=1}^{n}\varphi(\Delta t_l)IF_l}+(1-\rho(n))DT_0 \tag{5}$$

节点 i 和 j 在一个时间窗口内 n 次交互，第 l 次的交互时间距今有 Δt_l 个时间片，第 l 次交互后节点 i 对节点 j 的评价值 $S_l\in[0,1]$。IF_l 为第 l 次交互的事务影响因子，$\rho(n)$为交互次数的影响函数(具体参数属性见文献[30])。

模型计算直接信任度时需考虑以下因素，并合理刻画信任的时效性、衰减性，以准确计算节点信任度。

①时间窗口：反映信任评价的时效性，引入动态时间窗口来刻画实体的有效交易记录。

②时间衰减度：$\varphi(\Delta t)=e^{\frac{-t_r}{\lambda}}$，表示第 l 次交互相对于当前时刻的信任衰减度。

③事务影响因子：避免恶意节点以小额交易积累信任，有效抵抗针对交易额的摇摆策略行为。

④交互活跃度：表示节点在网络中的稳定程度，只有长期稳定且频繁成功交易的节点才具有较高的信任度。

2)推荐信任度 $RT(i,j)$

模型按照节点与推荐节点间是否直接交互和信任传递规则的标准，将推荐信任划分为：基于直接交互经验的信任、基于共同评价相似度的信任和基于推荐信任链的信任。以不同权重聚合这 3 类推荐信任，提出 RT_{ij} 的计算公式如式(6)所示：

$$RT_{ij}=w_1RT_{ij}^{(1)}+w_2RT_{ij}^{(2)}+w_3RT_{ij}^{(3)} \tag{6}$$

其中，$RT_{ij}^{(1)}$，$RT_{ij}^{(2)}$，$RT_{ij}^{(3)}$ 分别对应以下 3 类推荐信任，各类

权重比与具体参数详见文献[30]。

①基于直接交互的推荐信任

当节点 i 与任一推荐节点 $k\in RS_1$（RS_1 为推荐节点集合）曾有过直接交互时，节点 k 将其对节点 j 的信任 T_{kj} 反馈给节点 i。此时节点 k 的推荐可信度 $Cr_{ik}^{(1)}$ 为直接信任 DT_{ik}，推荐信任的计算公式如式(7)所示：

$$Cr_{ik}^{(1)}=DT_{ik},RT_{ij}^{(1)}=\frac{\sum\limits_{k\in RS_1}DT_{ik}T_{kj}\varphi(\Delta t_k)IF_k}{\sum\limits_{k\in RS_1}DT_{ik}\varphi(\Delta t_k)IF_k} \tag{7}$$

②基于评价相似度的推荐信任

当节点 i 与任一推荐节点 $k\in RS_2$（RS_2 为推荐节点集合）没有过直接交互但都曾对多个相同对象进行过信任评价时，采用 Dice 相似度估算推荐节点反馈信任的反馈可信度。计算公式如式(8)所示：

$$Cr_{ik}^{(2)}=\eta\frac{2\sum\limits_{l\in CS}T_{il}T_{kl}}{\sum\limits_{l\in CS}T_{il}^2+\sum\limits_{l\in CS}T_{kl}^2}+(1-\eta)\frac{2|IS\cap KS|}{|IS|+|KS|}$$

$$RT_{ij}^{(1)}=\frac{\sum\limits_{k\in RS_2}Cr_{ik}^{(2)}T_{kj}}{\sum\limits_{k\in RS_2}Cr_{ik}^{(2)}} \tag{8}$$

③基于信任链的推荐信任

当节点 i 与推荐节点 k 没有过直接交互，但两节点之间存在一条或多条推荐链路时，综合考虑 NC 条信任传递链路计算推荐信任度。经由多条不同的链路进行信任传输时，由于每一节点传递的信任值皆可能具有误差或恶意风险，链路跳数越多，误差或恶意风险积累越大[30]。为了应对此问题，式(9)对多个链路的信任没有采取简单平均，而是考虑链路长度 $p(l)$，以 $1/lbp(l)$ 为权重，使得较短的信任链路具有较高的权重[30]。该类反馈的可信度与推荐信任的计算公式如式(9)所示：

$$Cr_{ik}^{(3)}=\sum_{l=1}^{NC}\frac{\dfrac{((\prod\limits_{q=0}^{p(l)-1}T(c_q^{(l)},c_{q+1}^{(l)}))^{\frac{1}{p(l)}})}{lb(p(l))}}{\sum\limits_{l=1}^{NC}\dfrac{1}{lb(p(l))}}$$

$$RT_{ij}^{(3)}=\frac{\sum\limits_{k\in RS_3}Cr_{ik}^{(3)}DT_{kj}}{\sum\limits_{k\in RS_3}Cr_{ik}^{(3)}} \tag{9}$$

3）信任更新与奖惩

模型设交互前评估的实体信任度为 $T_{i,j}$，本次交互中实体表现的信任值为 $S_{i,j}$，则交互结束后实体信任的更新如式(10)所示：

$$T_{i,j}\leftarrow\theta S_{i,j}+(1-\theta)T_{i,j}+\delta \tag{10}$$

其中，θ 为信任更新调节因子，δ 为信任奖惩分量，具体参数属性见文献[30]。

$$\theta=\begin{cases}1-\sqrt{\dfrac{\frac{S_{ij}}{T_{ij}}-0.5}{\frac{S_{ij}}{T_{ij}}+1}}, & \dfrac{S_{ij}}{T_{ij}}\geqslant 0.5\\ 1, & \dfrac{S_{ij}}{T_{ij}}<0.5\end{cases}$$

$$\delta=\begin{cases}(1-e^{-\frac{n}{2a}})T_{ij}(1-S_{ij})(S_{ij}-T_{ij}), & S_{ij}\geqslant T_{ij}\\ (1-e^{-\frac{n}{2a}})S_{ij}(1-S_{ij})(S_{ij}-T_{ij}), & S_{ij}<T_{ij}\end{cases}$$

奖惩机制中本次交互的满意度 S_{ij} 较 T_{ij} 上升时，升幅越大，奖励的比率反而越小，以防止出现摇摆攻击时因实体满意度遽升而给予过高奖励，从而降低摇摆攻击的影响；并且时间窗口内交互次数 n 越大，信任的奖励（或惩罚）值也就越大。通过该奖惩机制合理地抑制了摇摆节点的影响，并且很好地激励了积极、良性节点的交易。

该模型抵抗恶意行为的能力主要体现在以下方面：

1）归一化评价信息可以抑制恶意节点虚假的过高或过低评价的负面影响；

2）引入交互活跃度、事务影响因子、交易时间因子等多维度信任影响因子，可避免节点利用多次交易、小额交易积累信任而掩盖其恶意摇摆的策略行为，能有效抵抗摇摆攻击；

3）聚合直接交互、评价相似度和信任链传递 3 种类型来计算的推荐可信度可以有效降低恶意节点提供的评价在信任值计算过程中所占的比重；

4）依据基于 Dice 评价相似度度量评价的推荐可信度可抵抗恶意节点的合谋攻击；

5）信任更新与激励惩罚算法、信任推荐节点的反馈可信度更新算法，合理地抑制了摇摆节点的影响，并且很好地激励了积极、良性节点的交易。

与 PeerTrust 相比，该模型的优势主要体现在以下方面：

1）刻画信任度的准确性与合理性明显提高，引入时间窗口、时间衰减函数、事务影响因子、交互活跃度等多维信任影响因子；

2）合理分析常见的推荐情形，抽象出 3 类推荐信任形成机制，并且基于 Dice 相似度给出了一种新的信任相似度算法，设计出了一种新的多链路反馈可信度融合算法，模型推荐信任度的准确性得到提高；

3）提出信任更新与奖励惩罚算法、信任推荐节点的反馈可信度更新算法，模型的抗攻击性能大幅提升。

该模型的不足之处如下：

1）为了综合考虑影响信任计算的多维度上下文因素，模型的算法复杂度较大。

2）对于信任的奖惩机制，作者没有在仿真实验中体现同时面对多种恶意攻击行为时算法抗攻击能力与适应能力的效果。对于大规模复杂的网络情况，该算法的健壮性和鲁棒性还有待研究。

5.2　电子商务典型的信任模型

电子商务作为一种全新的信息化商业模式，有效地推动了网络服务的飞速发展。在线交易存在不确定性与风险性，消费者往往难以评估网上陌生实体的可信度，更无法辨别服务质量的好坏，经常面临交易的虚假信息发布等恶意欺诈问题。在开放的虚拟电子市场中，建立和评价交易实体间的信任关系是解决其交易安全控制机制的有效方法之一[48]。为了更好地管理在线网络交易，使用户建立对所处的电子商务平台更强的信心，目前已有大量的在线电子商务网站构建了各自的信誉管理系统，比如 eBay，Amazon，Taobao 等。这些电子商务网站大多数采用信誉评价机制，其核心思想是：买家完成一笔交易后，对卖家进行信用评分。但是在实际应用中，这种机制存在诸多弊端和系统信息不对称的虚假问题，如信用炒作、周期性行骗、评分方式过于简单，无法排除卖家自己

注册多个买家账户、多次购买并给予自己好评的欺诈行为[20]。因此,基于用户交互行为客观度量卖家的可信度,构建抗攻击能力强、信任度真实且准确的信任计算模型,已成为业界的研究热点。

马霄等[48]针对电子商务应用,提出一种潜在的信任关系预测算法,旨在挖掘陌生用户间潜在的信任与不信任关系。首先提出用户信任关系子网络和用户商品评价关系子网络的形式化描述;然后利用社会学理论,综合计算由用户相似度和全局声誉度的差异性产生的信任度。该算法在预测信任关系的准确度方面具有良好的性能,但是其仅考虑了离散的二值信任关系,信任关系的不确定性及信任值的细化有待进一步研究。此外,算法能否合理应用于基于信任的推荐系统还需进一步验证。

Yu 和 Singh[49]针对信任的不确定性问题,提出分布式信任管理的证据模型。该模型通过节点评分建立的基本概率分配函数来表示信息中的不确定性;分析了信任传递的有效性,并利用 D-S(DempsterShafer)证据合成规则聚合所有推荐者的证据,避免了不确定性在信任传递时丢失的问题。但是,该算法存在信任评估值武断而不渐变、可信门限值改变较敏感、将无证据等同冲突证据等不足。

张仕斌等[50]提出一种特殊的属性评价方法和基于价格的信任惩罚方法,以有效防止电子商务中的信用炒作和周期行骗问题。算法的特点是利用云模型的期望和超熵量化客体的信任程度和不确定程度,并集成各反馈属性云得到综合信任云,然后计算与各标准信任子云间的相似度,确定实体的信任等级。但是,该算法存在信任区间根据经验划分、属性权重须预先指定、对信任诋毁攻击抵抗性弱、实际应用推广不强等不足。

Zhang 等[29]针对电子商务服务环境提出了一种上下文感知的信任评估模型,其通过对比当前交易与历史交易的上下文相似度来推测计算信任度,能够识别、预防潜在的价值失衡恶意交易,抵御恶意节点的摇摆策略攻击(即用低价商品积累信任,以便于在高价商品上欺诈)。但是,文中上下文只关注商品服务的类别和交易额两个属性,且缺乏对推荐信任及推荐可信度的考虑。

甘早斌等[51]针对移动 Agent 电子商务环境,提出了一种基于声誉的多维度信任算法(Reputation-based Multi-Dimensional Trust,RMDT)。该模型较好地体现了个体偏好、风险态度等主观因素对信任计算的影响,增强了信任算法在交易单个属性上的敏感性,并且提出一种利用信任传递路径以概率计算推荐可信度的方法(5.2.1 节将对此算法进行详细分析)。

甘早斌等[20]还提出一种 C2C 电子商务环境下的动态信任算法 CDTA(C2C Dynamic Trust Algorithm)。该算法的优势在于采用评价相似度来衡量推荐者与信任接受者的主观偏好,以此过滤掉推荐信息,得到与用户主观偏好相近的推荐信息,使得推荐信息对用户更具参考价值(5.2.2 节将对此算法进行详细分析)。

表 8 对以上典型信任模型进行对比分析,部分评价指标属性与表 7 相同。电子商务的信任计算模型添加的评价指标如下:Risk evaluation,用于描述电子商务环境中模型是否考虑用户个人偏好、风险态度等;History awareness,用于描述模型是否考虑历史交易的具体信息;Transaction,用于描述模型是否考虑交易成功与失败的次数、交易金额、交易重要性等因素;Time attenuation,用于描述模型是否考虑信任的时间衰减性。

表 8 电子商务中典型信任模型的比较

Table 8 Comparison of typical trust models in e-commerce

Index collection	Ma[48]	Yu[49]	Zhang[50]	Zhang[29]	RMDT[51]	CDTA[20]
Contex taware	Yes	Yes	Yes	Yes	Yes	Yes
Multi-dimensional	Yes	Yes	Yes	Yes	Yes	Yes
Reputation scoring	[0,1]	[0,1]	Hybrid	[0,1]	[0,1]	[0,1]
Arith-method	Weighted mean	D-S	Cloud-Based	Weighted mean	Weighted mean	Weighted Mean
Decentralized	No	Yes	No	No	No	No
Evaluation scope	Global/Local	Global/Local	Global/Local	Global/Local	Global/Local	Global/Local
Risk evaluation	No	No	No	No	Yes	No
History awareness	Yes	Yes	Yes	Yes	Yes	Yes
Transaction	No	No	Yes	Yes	Yes	Yes
Time attenuation	No	No	Yes	No	Yes	Yes
Veracity	Low	Low	Good	Good	Best	Better
Scalability	Good	Good	Medium	Good	High	Good
Robustness	Low	Medium	Good	Good	Best	Better
Overhead	Low	High	Medium	Low	High	Medium

5.2.1 RMDT

甘早斌等[51]针对移动 Agent 电子商务环境,提出一种基于声誉的多维度信任算法。该算法主要解决已有的信任算法评价维度较粗、不适合 Agent 按照其主观需求做出信任决策的问题。将多维度机制引入信任算法,即按照交易的内容对历史交易的评价予以不同维度,则能帮助消费者做出满足个人主观偏好的信任决策[51]。RMDT 采用效用函数计算多维度评价,较好地体现了个体偏好和风险态度。

该模型综合直接信任 $DT(s,t)$和推荐信任 $RT(s,t)$来评估实体总体信任 $T(s,t)$,如式(11)所示:

$$T(s,t)=\lambda \cdot DT(s,t)+(1-\lambda) \cdot RT(s,t) \tag{11}$$

当交易次数 $N>0$ 时,调节因子 λ 以交易成功次数占比有效时间内的交易总次数来动态调节权重。

1)直接信任度 DT

直接信任度的计算如式(12)所示:

$$DT=\begin{cases} w_s\left(\frac{n_s}{N}\right)^{\frac{1}{2}}+w_m\left(\frac{\sum_{k=1}^{N}m_k\times O_m^k}{\sum_{k=1}^{N}m_k}\right)^{\frac{1}{2}}+w_t\left(\frac{\sum_{k=1}^{N}\Delta t_k\times O_t^k}{\sum_{k=1}^{N}\Delta t_k}\right)^{\frac{1}{2}}+w_q\left(\frac{\sum_{k=1}^{N}O_q^k}{N}\right)^{\frac{1}{2}}, & N\geqslant 1 \\ 0, & N=0 \end{cases} \tag{12}$$

模型利用 4 个主要的维度来评价节点的信任度，即交易成功与否、交易金额、交易时间和服务质量，亦即 $O=\{o_s,o_m,o_t,o_q\}$。式(12)以幂函数定义 4 个维度的效用函数，反映每次历史交易的具体情况和交易评价都会对 DT 的计算产生影响。随着交易的不断进行，DT 随之动态更新，并且越是最新的交易，对本次信任评估的影响越大(具体参数属性见文献[51])。

2)推荐信任度 RT

推荐信任度的计算如式(13)所示(具体参数属性见文献[51])：

$$RT=\begin{cases} \frac{\sum_{i=1}^{n_{L_1}}C_{S,R_{F_i}}\times Rep_{R_{F_i}}+\sum_{k=2}^{N_U}\sum_{j=1}^{n_{L_k}}C_{S,R_{PF_j}}\times Rep_{R_{PF_j}}+\sum_{l=1}^{n_{R_{S^o}}}C_{S,R_{S_l^o}}\times Rep_{R_{S_l^o}}}{\sum_{i=1}^{n_{L_1}}C_{S,R_{1F_i}}+\sum_{k=2}^{N_U}\sum_{j=1}^{n_{L_k}}C_{S,R_{PF_j}}+\sum_{l=1}^{n_{R_{S^o}}}C_{S,R_{S_l^o}}}, & N_R>0 \\ 0, & N_R=0 \end{cases} \tag{13}$$

模型首先根据推荐者与评估节点的亲疏程度，把推荐者依朋友关系分类为朋友节点、伪朋友节点、陌生人，再分别计算其推荐可信度。对推荐节点的信誉值与推荐可信度进行加权平均，从而计算得到推荐信任度。

将推荐节点细分为朋友节点 R_F、伪朋友节点 R_{PF}、纯陌生节点 R_{S^o}。推荐可信度 C 的计算如下：

①$C_{S,R_{F_i}}=\frac{1}{2^{d_{S,R_{F_i}}}}$，其中 $d_{S,R_{F_i}}\equiv 1$；

②$C_{S,R_{PF_j}}=\frac{1}{2^{d_{S,R_{PF_j}}}}$，其中 $d_{S,R_{PF_j}}\geqslant 2$；

③$C_{S,R_{S_i^o}}=\frac{1}{2^{\max(d_{S,R_{PF_j}})+1}}$。

以上推荐可信度的计算采用概率的方法，基于信任网络中的信任链传递层级 d，属于同层次即相同传递跳数的节点具有相同的推荐可信度。模型将源节点 S 与推荐节点 R 之间的最短路径长 $d_{S,R}$ 作为 R 的推荐可信度 $C_{S,R}$ 的决定因素及 R 的筛选参数，以有效控制算法的复杂度。

RMDT 抵抗恶意行为的能力主要体现在以下几方面：

1)归一化评价信息可以抑制恶意节点虚假的过高或过低评价的负面影响；

2)引入用户的主观偏好与风险态度，模型的敏感性较强，能较及时地反映节点的摇摆行为；

3)信任度的计算考虑交易成功的数量、服务质量、交易额度、交易时间因子，可以避免恶意节点的摇摆策略行为；

4)将 S 与 R 之间的最短路径长 $d_{S,R}$ 作为 R 的推荐可信度 $C_{S,R}$ 的决定因素及 R 的筛选参数，以推荐路径计算所得的可信度作为推荐信任权重，可降低抗恶意虚假推荐的影响。

RMDT 具有如下优点：

1)模型抵抗摇摆策略攻击的性能较好；

2)引入时间敏感函数以给予信任机制一定的奖惩机制，实现信任度的动态更新。

其模型不足之处如下：

1)模型不能有效抵抗复杂的共谋欺诈等攻击；

2)缺乏有效的信任奖惩机制，所提出的时间敏感函数在节点消极行为转积极行为时，信任增速过快，且提高幅度较大。

5.2.2　CDTA

甘早斌等[20]提出 C2C 电子商务环境下的动态信任算法。与 RMDT 相比，该算法考虑了交易的多属性及其相关性，信任评价的粒度更加细化，使得信任计算的结果更加客观[20]。该算法采用评价相似度来衡量推荐者与评估者的主观偏好，以此过滤掉推荐信息，得到与用户主观偏好相近的推荐信息，进一步体现了个体偏好并提高了对恶意虚假推荐的抵抗能力，但是模型没有考虑风险态度等。

模型综合直接信任 $DT(s,t)$ 和推荐信任 $RT(s,t)$ 来评估实体总体信任 $T(s,t)$，如式(14)所示：

$$\begin{aligned} &T(s,t)=\lambda\cdot DT(s,t)+(1-\lambda)\cdot RT(s,t) \\ &\lambda=\frac{n_s\cdot m_s^2}{n_s\cdot m_s^2+\overline{n_{R'}}\cdot\overline{m_{R'}^2}} \end{aligned} \tag{14}$$

不同于 RMDT，模型的调节因子 λ 以节点的交易次数和交易金额为参数，并且以交易金额的平方计算，反映了交易金额大的单笔交易对信任度具有更大的影响(具体参数属性见文献[20])。

1)直接信任度 $DT(s,t)$

直接信任度的计算如式(15)所示：

$$DT_{\tau_n}=\begin{cases} e^{-\alpha(\tau_n-\tau_{n-1})}\cdot\sum_{i=0}^{N}\theta_i\cdot K_i, & \text{other} \\ DT_{\text{default}}, & N=0 \end{cases} \tag{15}$$

模型考虑以下因素，以合理刻画信任的衰减性、时效性、主观性，信任计算的结果较 RMDT 更加客观、准确。

①时间衰减函数：$e^{-\alpha(\tau_n-\tau_{n-1})}$，$\alpha$ 为调节系数，反映有效时间内最近的交易记录对信任计算更具有参考价值。

②反馈评价值：$K_i=\sum_{j=1}^{n}w_j\cdot k_{ij}$。根据交易的 n 维评价向量，以个性化权重计算第 i 次交易反馈评价值，反映信任的主观性，体现个体偏好。

③评价影响因子：$\theta_i=\frac{m_i^2\cdot(\tau_i-\tau_0)}{\sum_{j=1}^{N}m_j^2\cdot(\tau_j-\tau_0)}$。以交易时间与交易金额作为参数，并使用 m^2 来提升金额在评价因子中的重要程度，反映距当前时间越近且金额越大的交易评价信息比其他交易的评价信息对节点间的直接信任影响更大。

2)推荐信任度 $RT(s,t)$

推荐信任度的计算如式(16)所示:

$$RT(s,t)=\begin{cases}\sum\limits_{i\in R'}(C(s,i)\cdot DT(i,t)\cdot\delta_i), & R'\neq\emptyset\\ 0, & R'=\emptyset\end{cases}\tag{16}$$

模型引入信任相似因子 δ_i,采用评价相似度 $\Delta_{i,j}$ 来衡量推荐者与评估者的主观偏好,以此过滤掉推荐信息,得到与用户主观偏好相近的推荐信息,提高了对恶意虚假推荐的抵抗能力,并且进一步体现了个体偏好。利用皮尔逊相关系数计算相似度,如式(17)所示:

$$\Delta_{i,j}=\begin{cases}\dfrac{\sum\limits_{n\in N_{i,j}}(DT(i,n)-\overline{DT_i})\cdot(DT(j,n)-\overline{DT_j})}{\sqrt{\sum\limits_{n\in N_{i,j}}(DT(i,n)-\overline{DT_i})}\cdot\sqrt{\sum\limits_{n\in N_{i,j}}(DT(j,n)-\overline{DT_j})}}, & \text{other}\\ 0, & |N_{i,j}|<\beta\end{cases}\tag{17}$$

CDTA 抵抗恶意行为的能力主要体现在以下几方面:

1)归一化评价信息可以抑制恶意节点虚假的过高或过低评价的负面影响;

2)信任度的计算考虑交易成功的数量、服务质量、交易额度、交易时间因子,可以避免恶意节点的摇摆策略行为;

3)引入时间敏感函数、基于评价相似度的推荐信任可有效抑制虚假评价与恶意推荐的影响。

CDTA 较 RMDT 具有如下优点:

1)考虑了交易的时间、交易额等多属性及其相关性,信任评价的粒度更加细化,能更加合理地反映信任的衰减性、时效性、主观性;

2)采用评价相似度来衡量推荐者与评估者的主观偏好,以此将推荐信息过滤,得到与用户主观偏好相近的推荐信息。

该模型的不足之处如下:

1)推荐可信度量化过于简单;

2)缺乏有效的信任动态更新与奖惩机制;

3)抗攻击性能较 RMDT 并没有明显提升,对摇摆策略行为的敏感性弱于 RMDT,模型依然未能有效抵抗复杂的共谋攻击等。

5.3 社会网络的典型信任模型

分布式网络技术的成熟与应用,以及移动计算技术和设备的发展,使得大众步入了一个全新的社交网络时代。各类社交应用与服务颠覆了大众的传统社交模式,融合了即时通讯、电子商务和消费推荐等诸多领域。网络为大众提供了随时随地进行信息分享、产品交易、业务协作等社交活动的平台。然而,在如此开放与动态的大规模在线社会网络中,人们常常面临着陌生的交互对象,这使得用户间的交互往往存在着不确定性和风险性。用户在享受社交网络带来便利的同时,更希望免受虚假节点的攻击,并实现对分享数据的控制,防止其被恶意信息感染、恶意节点攻击或非授权用户访问。信任机制作为一种有效的解决途径,近几年被广泛应用于社会网络,并取得了大量研究成果。

在社会网络环境中,信任关系的建立是一个复杂递进的过程,涉及交互历史、信任推荐和信任管理等多方面的信息,是一个基于多要素决策的复杂模型系统[52]。Sherchan 等将与社会网络相关的信任机制研究归类为 3 个方面:信任信息的收集、信任评估和信任传播[8]。

Al-Oufi 等[53]针对在线社会网络中的可信人员,提出一种扩展的集群信任评测方法,更好地确定出有序的可靠信任用户集,从而防止不可靠用户访问个人网络,较好地保护了用户的个人隐私。该方法是对 Advogoto 方法的扩展,它通过合并社会关系强度找出与每个用户相关的可靠用户群,其信任测度设计扩散机制使每个节点的能力沿着社会关系链有效地延展为连续节点,以能力最大流来识别本地可信用户,并对其进行信任级别的划分[54]。

乔秀全等[55]根据社会心理学,提出社交网络服务中一种基于用户上下文的信任度计算方法。利用信任的产生过程把信任度分为熟悉性产生的信任度和相似性产生的信任度,又根据所起作用的不同,把相似性分为内部相似性和外部相似性分别进行计算,充分提高了信任度计算的人性化、合理性和有效性。但是,这 3 部分权重的确定缺乏相关的理论依据。

王刚等[54]针对现有模型缺乏有效的激励策略以及协同作弊和信任推荐不可信等问题,提出社会网络中交易节点的选取及其信任关系的计算方法。算法引入交易影响力函数、推荐时间影响函数、交易内容相似度和推荐熟悉度等多维影响因子来保证推荐可信性,最后提出了基于多属性的节点推荐信任度更新方法[54](5.3.1 节将对此算法进行详细分析)。

田俊峰等[56]针对 Jøsang[10]只给出二项式观点的传递公式的不足,结合实体信誉环境对信任融合操作的影响,提出了基于多项式主观逻辑的扩展信任传播模型。Liu 等[57]将主观逻辑中的不确定性进一步区分为先验(没有证据)和后验(证据失真),从而提出一种 3 值主观逻辑(3VSL)方法并将其用于评估社会网络中实体间的信任关系。该方法能够明显提高 Jøsang 模型的准确度。Cerutti[58]等研究了基于主观逻辑的依赖上下文的信任决策和一系列折扣算子及其几何解释。

徐军等[59]针对信任传递中信任不确定性的丢失问题,提出一种基于直觉模糊理论的多维信任传递模型。该模型讨论了直觉模糊环境下基本的信任传播算子,并且综合考虑信任传播路径长度与信任质量对信任聚合的影响,给出了两种加权信任聚合算子。该模型计算信任度的准确性较高,但算法复杂度也较高,而且算法没有考虑恶意行为的影响。

Zhang 等[60]提出一种低成本的信任链路遍历机制(Trust Traversal)。该文主旨并不是建立一个完整的信任评估模型,而是根据用户间关系的可靠性与亲密度分类了 3 种信任链路,即强信任、弱信任和不可信,并且提出 3 种信任度的计算数学模型:信誉度、直接链路信任度和间接链路信任度;同时提出两个信任影响因子的计算方法:相互信任度和交互活跃度。模型的计算准确度高,复杂度较低(5.3.2 节将对此算法进行详细分析)。

表 9 对以上典型的信任模型进行对比分析,部分评价指标属性与表 7 相同。社交网络信任计算模型添加的评价指标如下:History Transaction,用来描述模型是否考虑历史交易信息;Time attenuation,用来描述模型是否考虑信任的时间衰减性。

表 9　社会网络中典型的信任模型比较

Table 9　Comparison of typical trust models in social network

Index Collection	Tian[56]	Liu[57]	Cerutti[58]	Qiao[55]	Xu[59]	Wang[54]	Zhang[60]
Context aware	No	No	Yes	Yes	No	Yes	Yes
Multi-Dimensional	No	No	Yes	Yes	No	Yes	Yes
Reputation scoring	[0,1]	[0,1]	[0,1]	[0,1]	−1 or +1	[0,1]	[0,1]
Arith-method	Subjective logic	Subjective logic	Subjective Logic	Weighted mean	Intuitionistic Fuzzy theory	Weighted mean	Weighted mean
History Transaction	No	No	No	Yes	No	Yes	Yes
Time attenuation	No	No	No	No	No	Yes	Yes
Veracity	Lower	Lower	Lower	Good	Better	Better	Best
Scalability	High	Medium	Medium	Medium	Good	Good	Good
Robustness	Medium	Medium	Medium	Medium	Low	Good	Good
Overhead	High	High	High	Low	High	Medium	Low

5.3.1　社会网络中信任关系的计算方法

王刚等[54]针对现有模型缺乏有效的激励策略以及协同作弊和信任推荐不可信的问题，提出社会网络中交易节点的选取及其信任关系的计算方法。模型有效区分了节点作为交易节点和推荐节点的可信度差异性问题，从而建立有效的奖惩策略来刺激节点积极交易与推荐。通过重点区分熟人与陌生人的推荐可信度，模型对单纯恶意节点的攻击和协同作弊推荐节点都具有较好的识别和抑制能力。

模型融合推荐信任 RT_{SP}（服务交易节点）和直接信任 DT_{SP}^{SR}（服务推荐节点）来评估目标节点（交易节点）的综合信任值 GT_{SP}^{SR}。计算公式如式(18)所示：

$$GT_{SP}^{SR}=(\lambda\ \gamma)\cdot\begin{pmatrix}DT_{SP}^{SR}\\RT_{SP}\end{pmatrix} \tag{18}$$

其中，$\lambda+\gamma=1$，$\lambda,\gamma\in[0,1]$。模型定义交易影响力函数 $\lambda(k)$，用于表示权重随交易次数 k 的动态变化情况。

1）直接信任度 DT_{SP}^{E}

直接信任度的计算如式(19)所示：

$$DT_{SP}^{E}=\frac{S_{SP}^{E}+1}{S_{SP}^{E}+F_{SP}^{E}+2}$$
$$DT_{SP}^{E}=f(N(t))\cdot DT_{SP}^{E} \tag{19}$$

以最简单、简明的交易成功与否指标计算：评估节点 E 与服务交易节点 SP 交易成功的次数 S_{SP}^{E} 与失败的次数 F_{SP}^{E}。模型公平地默认节点间无交互时的直接信任度为 1/2。同时，考虑信任的时间衰减性，引入时间-交易次数影响函数 $f(N(t))$。模型定义任意长度的时间区间 t 中，节点 E 与 SP 发生的交易次数 $N(t)$ 服从参数 $\lambda_t>0$ 的泊松分布（具体参数属性见文献[54]）。

2）推荐信任度 RT_{SP}

推荐信任度的计算如式(20)所示：

$$RT_{sp}=\sum_{i,j=1,i\neq j}^{n}Sim(C_{sp}^{i},C_{sp}^{j})\cdot\left(\sqrt[3]{\alpha\cdot\omega_{sp}^{i}\cdot DT_{SP}^{i}}+\sqrt[3]{\beta\cdot\omega_{sp}^{j}\cdot DT_{SP}^{j}}\right)/n \tag{20}$$

基于对服务内容的相似度进行计算，其中 $Sim(C_{sp}^{i},C_{sp}^{j})$ 表示 C_{sp}^{i} 和 C_{sp}^{j} 两个节点间的服务内容的相似程度，采用皮尔逊相关系数对服务内容的 5 个主要属性维度计算相似度。ω_{sp}^{i} 和 ω_{sp}^{j} 分别表示熟人推荐的权重和陌生人推荐的权重，其中 $\begin{cases}\omega_{sp}^{i}=DT_{SP}^{i}\\\omega_{sp}^{j}=0.5\end{cases}$，陌生人的权重初始公平设置为 0.5，即表示其可信或不可信的概率各为 0.5。α 是熟人推荐节点对服务交易节点的信任程度。β 是陌生推荐节点对服务交易节点的信任程度。

3）推荐可信度 RR_i

推荐可信度的计算如式(21)所示：

$$\begin{cases}RR_i=\sqrt[4]{f(t_0,t_i)Sim(C_{sp}^{i},C_{sp}^{j})\cdot\alpha\cdot\omega_{SR}^{i}}\\RR_i=\sqrt[4]{f(t_0,t_i)Sim(C_{sp}^{i},C_{sp}^{j})\cdot\beta\cdot\omega_{SR}^{i}}\end{cases} \tag{21}$$

其中，i 是熟人推荐节点，j 是陌生人推荐节点。模型引入交易影响力函数、推荐时间影响函数、交易内容相似度和推荐熟悉度多维影响因子，有效保证了节点的推荐可信度。

模型抵抗恶意行为的能力主要体现在以下几方面：

1）归一化评价信息可以抑制恶意节点虚假的过高或过低评价的负面影响；

2）针对信任的动态变化与衰减性，考虑服务成本、交易次数等，可避免恶意节点的摇摆策略行为；

3）通过计算服务相似度、推荐时间影响函数和推荐熟悉度等多维影响因子来提高推荐可信度，模型对单纯恶意节点的攻击和协同作弊推荐节点都有较好的识别和抑制能力。

模型具有如下优点：

1）引入时间-交易影响函数，表明服务交易节点需长期、频繁地进行稳定服务才可获取较高的信任度；

2）通过区分熟人节点和陌生人的不同推荐信任度，避免信任值越高的节点推荐越可信的假设；

3）有效区分了一个节点作为推荐节点和交易节点的可信度的差异性问题；

4）提出了基于马尔科夫的推荐能力进化度方法，更新节点的推荐可信度。

模型的不足之处如下：

1）直接进行信任计算时，为简化运算，只选择了交易是否成功作为计算指标，未考虑交易金额等其他信任影响因子；

2）算法在实现推荐可信度的更新时，在马尔科夫链中假设一步转移概率 p_w 是不变的，但是实际中其是在不断发生变化的。

5.3.2　Trust Traversal

Zhang 等[60]提出一种低成本的信任链路遍历机制（Trust Traversal）。该文根据用户间关系的可靠性与亲密度分类了 3 种信任链路，即强信任、弱信任和不可信，并且提出了 3 种

信任度的计算数学模型:信誉度、直接链路信任度和间接链路信任度;同时提出了两个信任影响因子的计算方法:相互信任度和交互活跃度。模型的计算准确度高,复杂度较低。模型的算法与思想在今后的研究工作中仍值得借鉴与采用。

1)信誉

模型根据信誉的形成机制,分别针对 3 个规则进行信誉计算。

①有效评价积累:算法定义评论者的资格 $qu(d_i)$来反映评论的有效性,将其作为信誉计算的权重,并且引入社交网络中的关键因素社团。信誉的计算如式(22)所示,其中,$C(d_i)$表示一个实体所属的社团数目,m 是评论实体(d_i)的实体个数,$J(d_j,d_i)$表示实体(d_j)对实体(d_i)的有效评论集合(具体参数属性见文献[60])。

$$qu(d_i)=reputation(d_i)\times\beta^{\frac{1}{|C(d_i)|}} \tag{22}$$

$$reputation(d_i)=\frac{\sum_{j=1}^{m}\sum_{k=1}^{|J(d_j,d_i)|}(judgment(d_j,d_i)_k\times qu(d_j))/|J(d_j,d_i)|}{\sum_{j=1}^{m}qualification(d_j)}$$

②时间衰减性:定义时间片 $T(n)$表示信誉的有效期,以一个时间片为单位时间更新信誉度,时间衰减因子 $\delta\in[0,1]$。信誉的更新计算如式(23)所示:

$$reputation(d_i)^k=\frac{\sum_{j=0}^{k-1}reputation(d_i)^{T(j)}}{\sum_{j}^{k-1}\delta^j} \tag{23}$$

③信誉置信因子:$\vartheta(d_i)$表示实体信誉的可靠,计算公式如式(24)所示:

$$\vartheta(d_i)=\frac{1}{2}\times[jc(d_i)+\mathrm{hr}(reputation(d_i))] \tag{24}$$

其中,评论一致性 $jc(d_i)$:以用户获得所有评价的偏差度表征信誉可靠性,若评价偏差度越小则用户信誉越可靠。命中率 $\mathrm{hr}(reputation(d_i))$:信誉可以用于预测实体的可靠性,可靠的信誉值应该在有效的容错范围内保持较高的命中率。

2)直接信任链路信任度

直接信任的计算公式如式(25)所示:

$$trust(d_i,d_j)=if(d_i,d_j)\times ctf(d_i,d_j)\times sf(d_i,d_j) \tag{25}$$

此方法合理刻画了信任度的动态性和主观性。式(25)反映了当共同信任相似性高、两个节点频繁且稳定互相交互时,信任度更高。模型计算直接信任度时,有如下 3 个影响因子。

①交互因子:$if(d_i,d_j)$反映交互实体间的主观感受与交互经验所产生的信任值。

②共同信任因子:$ctf(d_i,d_j)$表示若两个用户具有共同信任用户集,并且两个用户分别对共同信任对象均保持较高的信任度,则这两个用户彼此更加信任。

③稳定性因子:$sf(d_i,d_j)$反映用户彼此频繁、稳定交易或长期单向交互等的信任波动。

3)间接信任链路信任度

间接信任的计算如式(26)所示:

$$trust_{\phi(rs,rt)}=\{[trust(rs,r1)\times wr(r1)]+\sum_{i=2}^{n}[trust(ru_{i-1},ru_i)\times wr(ru_i)]+[trust(ru_i,rt)\times wr(rt)]\}\times K_{\phi(rs,rt)} \tag{26}$$

模型明确了在信任链中信任传递需要遵循的 3 个计算规则:信任累加规则、信誉权重规则、逐层递减规则。

文献[60]中计算信任度的数学模型的优势如下:

1)提出信任度计算中的影响因子(信誉度的有效累积量、时间衰减度和置信因子、信任传递性规则、信誉权重规则、信任链路上的逐层递减规则)。该信任度计算方法使得每个用户都能够测量大多数其他用户的可信度(直接交互用户的直接信任度、整体可信度声誉,以及任何陌生用户的间接链接信任度)。

2)在传统方法中,间接连接用户之间的信任是基于它们之间的所有可能路径(或者预先选择的高于信任阈值的路径)综合评估的,因此在时间复杂度和空间复杂度方面产生了巨大的开销。本文研究的是一种遍历策略,只在信任传递路径中检测强连接的链路,从而避免了链路中不可信或孤立的关系,有效降低了算法的时间复杂度和空间复杂度。

6 存在的问题与展望

6.1 当前研究存在的问题

近年来,为构建可信网络,业界基于不同的应用背景对信任机制进行了大量研究并取得了丰硕的成果。各领域的信任模型都较好地保证了互联网应用系统的安全性与协作性,但是在理论或者算法实现方面普遍存在以下问题。

1)理论与实践相分离。大多数模型都面临着技术可行性与经济可行性的问题,不能在具体的应用中真正实现应用部署,因此停留在理论学术研究阶段。评估模型的功能性与效用性时,大多通过实验仿真的手段作出分析判断,无法在实践中真正得到检验与优化。

2)模型的性能评估未标准化。基于不同的应用环境,现有模型所实现的功能各有侧重点,并且构建信任模型的方法和手段的多样性决定了信任模型的多样性。因此,需要标准化信任模型的功能评估参数,以便完善模型的扩展性与通用性。

3)模型的数据搜集与存储缺陷。在研究信任机制问题时,大多数模型重点实现了系统中节点信任度的评估,却缺少算法的完整实现部分,如数据存储与访问、数据传输协议等,忽略了这些影响算法性能与扩展性的因素。此外,关注的焦点多在信任算法本身,比如算法的有效性和健壮性等,轻视了算法数据集的重要性。

4)混淆推荐可信度与交易可信度。大多数模型很少针对推荐节点进行评价,多为默认信任值高的节点其推荐也更值得信任,然而这种假设在实际应用中并不总是成立。一个节点的信任度高,只能说明其作为服务/交易节点的可信度较高,并不能说明它的推荐可信度高。模型需要有效区分节点作为推荐节点和交易节点的交易可信度的差异性问题。

5)信任奖惩机制的研究相对不足。由于缺乏有效的激励策略,节点会逐渐失去服务交易的主动性和积极性,同时也会失去推荐动力,导致推荐节点的规模逐渐萎缩,影响综合信任

值的精确性；而对于共谋行为、协同作弊、策略性攻击等信任推荐不可信的问题，模型更需要建立高效的动态惩罚策略，以保证模型的安全性与准确性。

6）模型的抗攻击能力不足。现有的信任模型的抗攻击能力相对比较单一化，并没有实现较全面的抗攻击能力。大多已有模型对于简单的恶意攻击与欺骗行为都具有较好的识别与防范能力，但是对于共谋团体攻击、女巫攻击和策略性攻击等复杂的作弊行为缺乏高效的识别和防护机制[21]。此外，现有的信任机制还缺乏行之有效的实体标签管理，导致恶意主体仍可轻易地洗白其“罪恶”历史后再次进入应用系统并重新进行恶意攻击。

6.2　展望

根据以上分析，为了提出一种普适性、健壮性和可靠性更优的信任机制，未来可从以下方面来对信任模型进行研究。

1）改进信任模型的算法实现。研究信任数据的存储方式与访问策略，以及数据在节点之间的安全传输协议等；遵循有效的激励奖惩机制规则：信任慢增长、快降低，对长期频繁稳定服务/交易、推荐成功率高的节点进行奖励，对不同程度的攻击设置不同的惩罚力度；对于复杂的数学推导及模型收敛过程，合理控制算法的时间复杂度和空间复杂度。

2）提高信任模型的抗攻击能力。提高识别和过滤虚假评价的能力；提升对摇摆策略攻击行为的敏感度，并实现有效的抵抗策略；重点研究敏感识别并抵抗恶意节点的复杂联合欺诈、共谋团体攻击和策略性女巫攻击等隐蔽的协同作弊行为；考虑信任系统采用何种方式给节点分配标签，恶意节点的标签何时更改，以及其自身是否可以改变。

3）明确信任模型具备的功能参数。通过研究不同应用环境中的现有信任机制，提出模型的以下 9 个功能参数。①灵活性：信任机制动态调整与更新信任；②主观性：反映不同个体信任值的主观差异；③模糊性：反映信任的抽象模糊性；④时间衰减性：长时间的冷却关系会导致信任衰减；⑤传递性：基于信任链，以推荐方式计算两个陌生节点的信任度；⑥抗攻击性：识别并抵抗恶意攻击；⑦奖惩机制：鼓励良好节点交易与推荐，惩罚恶意节点，降低其信任值或禁止其交易；⑧敏感性：根据网络变化动态感知与调整信任关系；⑨可扩展性：模型稳定或低负载（计算复杂度、时间复杂度和查询机制）。

4）综合各领域进行理论与实践研究。结合心理学、社会行为学和社会网络分析方面的理论指导，进一步结合人工智能、机器学习等计算机技术手段构建更有效、更合理、更实用的信任模型；将理论研究的成果尽可能地应用于实际环境中；验证其合理性与效用性，以便进一步对其进行修正与完善。

结束语　目前对网络信任的研究依然是业界的热点，基于节点交互行为的信任评价机制已成为有效抑制网络节点恶意、虚假、欺诈行为的关键技术之一。借鉴不同领域已有的信任研究成果，今后的研究将向社交网络中基于信任的推荐系统[61-62]发展。

参 考 文 献

[1] BEATTY P，REAY I，DICK S，et al. Consumer trust in e-commerce web sites：A meta-study[J]. Acm Computing Surveys，2011，43(3)：1-46.

[2] YOU J，SHANGGUAN J L，XU S K，et al. Distributed dynamic trust management model based on trust reliability[J]. Journal of Software，2017，28(9)：2354-2369.（in Chinese）
游静，上官经伦，徐守坤，等. 考虑信任可靠度的分布式动态信任管理模型[J]. 软件学报，2017，28(9)：2354-2369.

[3] ROUSSEAU D M，SITKIN S B，BURT R S，et al. Not so different after all：Across-discipline view of trust [J]. Academy of Management Review，1998，23(3)：393-404.

[4] MCKNIGHT D H，CHERVANY N L. The meanings of trust [R]. University of Minnesota，1996.

[5] MCKNIGHT D H，CHOUDHURY V，KACMAR C. Trust in e-commerce vendors：a two-stage model[C]// Twenty First International Conference on Information Systems. DBLP，2000：532-536.

[6] MCKNIGHT D H，CHERVANY N L. What trust means in ecommerce customer relationship：an interdisciplinary conceptual typology [J]. International Journal of Electronic Commerce，2001，6(2)：35-59.

[7] GAMBETTA D. Can we trust trust [J]. Trust：Making and Breaking Cooperative Relations，2000，1(13)：213-237.

[8] SHERCHAN W，NEPAL S，PARIS C. A survey of trust in social networks [J]. ACM Computing Surveys (CSUR)，2013，45(4)：1-33.

[9] SCHOORMAN F D，MAYER R C，DAVIS J H. An integrative model of organizational trust：Past，present，and future [J]. Academy of Management Review，1995，20(3)：709-734.

[10] JØSANG A，ISMAIL R，BOYD C. A survey of trust and reputation systems for online service provision [J]. Decision Support Systems，2007，43(2)：618-644.

[11] WANG X F. Research on the tactics representation and quantitative model of trust management [D]. Changsha：National University of Defense Technology，2009.（in Chinese）
王晓峰. 信任管理的策略表示与量化模型研究[D]. 长沙：国防科学技术大学，2009.

[12] HUANG J，FOX M S. An ontology of trust：formal semantics and transitivity[C]// International Conference on Electronic Commerce：the New E-Commerce-Innovations for Conquering Current Barriers，Obstacles and Limitations to Conducting Successful Business on the Internet. DBLP，2006：259-270.

[13] LI X Y，GUI X L. Research on dynamic trust model for large scale distributed environment [J]. Journal of Software，2007，18(6)：1510-1521.（in Chinese）
李小勇，桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报，2007，18(6)：1510-1521.

[14] LI Y J，DAI Y F. Research on trust mechanism for peer-to-peer network[J]. Chinese Journal of Computers，2010，33(3)：390-405.（in Chinese）
李勇军，代亚非. 对等网络信任机制研究[J]. 计算机学报，2010，33(3)：390-405.

[15] LIANG Z Q，SHI W S. PET：A Personalized trust model with reputation and risk evaluation for P2P resource sharing[C]//

Proceeding of 38th Annual Hawaii International Conference on System Sciences. Piscataway: IEEE Computer Society, 2005: 201-211.

[16] TANG W, CHEN Z. Research of subjective trust management model based on the fuzzy set theory[J]. Journal of Software, 2003, 14(8): 1401-1408. (in Chinese)
唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报,2003,14(8):1401-1408.

[17] AUDUN J. Alogic for uncertain probabilities[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279-311.

[18] XU J. A Survey of Trust Modeling of Uncertainty Theory[J]. Microcomputer Systems, 2017, 38(1): 100-106. (in Chinese)
徐军. 不确定性理论的信任建模研究综述[J]. 小型微型计算机系统,2017,38(1):100-106.

[19] GAN Z B, ZENG C, LI K, et al. Construction and optimization of trust network in e-commerce environment[J]. Chinese Journal of Computers, 2012, 35(1): 27-37.

[20] GAN Z B, ZENG C, MA Y, et al. C2C e-commerce trust algorithm based on trust network[J]. Journal of Software, 2015, 26(8): 1946-1959. (in Chinese)
甘早斌,曾灿,马尧,等. 基于信任网络的 C2C 电子商务信任算法[J]. 软件学报,2015,26(8):1946-1959.

[21] WANG J P, SUN B, NIU X X, et al. Distributed trust model based on parameter modeling [J]. Journal on Communications, 2013, 34(4): 47-59. (in Chinese)
汪京培,孙斌,钮心忻,等. 基于参数建模的分布式信任模型[J]. 通信学报,2013,34(4):47-59.

[22] MARSH S P. Formalising trust as a computational concept [D]. Stirling: University of Stirling, 1994.

[23] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[C]// 17'th Symposium on Security and Privacy. IEEE Computer Society Press, 1996: 164-173.

[24] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated Trust Negotiation[M]. North Carolina State University at Raleigh, 2000.

[25] WINSBOROUGH W H, LI N. Towards practical automated trust negotiation[C]// Michael J B, ed. International Workshop on Policies for Distributed Systems and Networks. Washington: IEEE Computer Society Press, 2002: 92-103.

[26] LIAO Z S, JIN H, LI C S, et al. Automated trust negotiation and its development trend[J]. Journal of Software, 2006, 17(9): 1933-1948. (in Chinese)
廖振松,金海,李赤松,等. 自动信任协商及其发展趋势[J]. 软件学报,2006,17(9):1933-1948.

[27] LI J X, HUAI J P, LI X X. Research on automated trust negotiation[J]. Journal of Software, 2006, 17(1): 124-133. (in Chinese)
李建欣,怀进鹏,李先贤. 自动信任协商研究[J]. 软件学报,2006,17(1):124-133.

[28] DUMA C, SHAHMEHRI N, CARONNI G. Dynamic trust metrics for peer-to-peer systems [C] // Sixteenth International Workshop on Database and Expert Systems Applications, 2005. IEEE, 2005: 776-781.

[29] ZHANG H B, WANG Y, ZHANG X Z. Transaction similarity-based contextual trust evaluation in e-commerce and e-service environments[C]// Proc. of the 9th Int'l Conf. on Web Service. Washington: IEEE Computer Society Press, 2011: 500-507.

[30] LIU Y C, LIANG Y H. P2P Dynamic Trust Model Based on Contextual Factors [J]. Journal of Communication, 2016, 37(8): 34-45. (in Chinese)
刘义春,梁英宏. 基于上下文因素的 P2P 动态信任模型[J]. 通信学报,2016,37(8):34-45.

[31] DELLAROCAS C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior[C]// ACM Conference on Electronic Commerce. ACM, 2000: 150-157.

[32] WHITBY A, JOSANG A, INDULSKA J. Filtering out unfair ratings in Bayesian reputation systems [J]. The Icfain Journal of Management Research, 2005, 4(2): 48-64.

[33] JIANSHU W, CHUNYAN M, ANGELA G. An entropy-based approach to protecting rating systems from unfair testimonies [J]. Ieice Transactions on Information and Systems, 2006, 89(9): 2502-2511.

[34] YANG Y, SUN Y L, REN J, et al. Building trust in online rating systems through signal modeling[C]// IEEE ICDCS Workshop Trust Reputat. Manage, Toronto, ON, Canada, 2007.

[35] LAURETI P, MORET L, ZHANG Y C, et al. Information filtering via iterative refinement [J]. EPL (Europhysics Letters), 2006, 75(6): 1006.

[36] ZHANG J, COHEN R. A personalized approach to address unfair ratings in multiagent reputation systems[C]// AAMAS06 Workshop on Trust in Multi agent Systems. May 2006.

[37] YANG Y, SUN Y L, KAY S, et al. Defending online reputation systems against collaborative unfair raters through signal modeling and trust[C]// ACM Symposium on Applied Computing. ACM, 2009: 1308-1315.

[38] LIU Y, SUN Y. Anomaly Detection in Feedback-based Reputation Systems through Temporal and Correlation Analysis[C]// IEEE Second International Conference on Social Computing. IEEE, 2010: 65-72.

[39] YOU W, LIU L, XIA M. Reputation inflation detection in a Chinese C2C market [J]. Electronic Commerce Research and Applications, 2011, 10(5): 510-519.

[40] KARL A, ZORAN D. Managing trust in a Peer-2-Peer information system[C]// Proceeding of the 10th International Conference on Information and Knowledge Management. Atlanta, Georgia, USA, 2001: 310-317.

[41] HUANG J N, SONG J X, LIU W D, et al. A Survey of Peer-to-Peer Network Reputation Mechanisms[J]. Small Microcomputer Systems, 2006, 27(7): 1175-1181. (in Chinese)
黄金能,宋佳兴,刘卫东,等. 对等网络信誉机制研究综述[J]. 小型微型计算机系统,2006,27(7):1175-1181.

[42] KAMVAR S. The EigenTrust algorithm for reputation management in P2P networks [C]// 12th International World Wide Web Conference. 2003: 640-651.

(下转第 36 页)

[51] HAN R J, CAO Q L. Fuzzy chance constrained least squares twin support vector machine for uncertain classification[J]. Journal of Inteligent & Fuzzy Systems, 2017, 33(5): 3041-3049.

[52] XU Y T, YANG Z J, et al. A Novel Twin Support Vector Machine with Pinball Loss[J]. IEEE Transactions on Neural Networks and Learning Systems, 2017, 28(2): 359-370.

[53] CAO L, SHEN H. Imbalanced data classification based on hybrid resampling and twin support vector machine[J]. Computer Science & Information Systems, 2017, 14(3): 579-595.

[54] WANG H, ZHOU Z. An improved rough margin-based twin bounded support vector machine[M]. Elsevier Science Publishers B. V., 2017: 125-138.

(上接第 28 页)

[43] ZHOU R F, KAI H W. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing [J]. IEEE Transaction on Parallel and Distributed Systems, 2007, 18(4): 460-473.

[44] XIONG L, LIU L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge Data Engineering, 2004, 16(7): 843-857.

[45] WANG Y, VASSILEVA J. Bayesian network trust model in peer-to-peer networks[C]// Moro G, ed. Proc. of the 2nd Int'l workshop on Agents and Peer-to-Peer Computing. Berlin: Springer Verlag, 2004: 23-34.

[46] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open network[C]// European Symposium on Research in Security (ESORICS). Springer Verlag, 1994: 3-18.

[47] TIAN C Q, ZOU S H, TIAN H R, et al. A new trust model based on reputation and risk evaluation for P2P networks[J]. Journal of Electronics & Information Technology, 2007, 29(7): 1628-1632. (in Chinese)
田春岐, 邹仕洪, 田慧蓉, 等. 一种基于信誉和风险评价的分布式 P2P 信任模型[J]. 电子与信息学报, 2007, 29(7): 1628-1632.

[48] MA X, GAN Z B, LU H W, et al. A method of predicting potential trust relationships in e-commerce[J]. Computer Science, 2014, 12(41): 138-142. (in Chinese)
马霄, 甘早斌, 鲁宏伟, 等. 电子商务中的一种潜在信任关系预测方法[J]. 计算机科学, 2014, 12(41): 138-142.

[49] YU B, SINGH M P. An evidential model of distributed reputation management [C]// Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems: Part 1. ACM, 2002: 294-301.

[50] ZHANG S B, XU C X. Study on the trust evaluation approach based on cloud model[J]. Chinese Journal of Computers, 2013, 36(2): 422-431.

[51] GAN Z B, DING Q, LI K, et al. Reputation-based multi-dimensional trust algorithm[J]. Journal of Software, 2011, 22(10): 2401-2411. (in Chinese)
甘早斌, 丁倩, 李开, 等. 基于声誉的多维度信任计算算法[J]. 软件学报, 2011, 22(10): 2401-2411.

[52] MA Y. Research on trust network discovery and trust fusion in online social networks [D]. Wuhan: Huazhong University of Science and Technology, 2014. (in Chinese)
马尧. 在线社会网络的信任网络发现与信任融合研究[D]. 武汉: 华中科技大学, 2014.

[53] AL-OUFI S, KIM H N, SADDIK A E. A group trust metric for identifying people of trust in online social networks[J]. Expert Systems with Applications, 2012, 39(18): 13173-13181.

[54] WANG G, GUI X L. Selection of trading nodes in social networks and calculation of trust relationship [J]. Journal of Computer, 2013, 36(2): 368-383. (in Chinese)
王刚, 桂小林. 社会网络中交易节点的选取及其信任关系计算方法[J]. 计算机学报, 2013, 36(2): 368-383.

[55] QIAO X Q, YANG C, LI X F, et al. A Method for Computing Trust Based on User Context in Social Networks [J]. Journal of Software, 2011, 34(12): 2403-2412. (in Chinese)
乔秀全, 杨春, 李晓峰, 等. 社交网络中一种基于用户上下文的信任度计算方法[J]. 软件学报, 2011, 34(12): 2403-2412.

[56] TIAN J F, WU L J. Multinomial subjective logic based extended trust propagation model [J]. Journal on Communications, 2013, 34(5): 12-19.

[57] LIU G, YANG Q, WANG H, et al. Assessment of multi-hop interpersonal trust in social networks by three-valued subjective logic[C]// Proceedings of the International Conference on Computer Communications. IEEE, 2014: 1698-1706.

[58] CERUTTI F, TONIOLO A, OREN N, et al. Subjective logic operators in trust assessment: an empirical study[J]. Information Systems Frontiers, 2015, 17(4): 743-762.

[59] XU J, ZHONG Y S, ZHU W Q. A Multidimensional Trust Transfer Model Based on Intuitionistic Fuzzy Theory[J]. Journal of Chinese Computer Systems, 2015, 36(12): 2714-2718. (in Chinese)
徐军, 钟元生, 朱文强. 一种基于直觉模糊理论的多维信任传递模型[J]. 小型微型计算机系统, 2015, 36(12): 2714-2718.

[60] ZHANG B, ZHANG H, LI M Z, et al. Trust Traversal: A trust link detection scheme in social network [J]. Computer Networks, 2017, 120: 105-125.

[61] CHEN T, ZHU Q, ZHOU M, et al. Trust-Based recommendation algorithm in social network[J]. Journal of Software, 2017, 28(3): 721-731. (in Chinese)
陈婷, 朱青, 周梦, 等. 社交网络环境下基于信任的推荐算法[J]. 软件学报, 2017, 28(3): 721-731.

[62] WANG R Q, JIANG Y L, LI Y X, et al. A Collaborative Filtering Recommendation Algorithm Based on Multiple Social Trusts [J]. Journal of Computer Research and Development, 2016, 53(6): 1389-1399. (in Chinese)
王瑞琴, 蒋云良, 李一啸, 等. 一种基于多元社交信任的协同过滤推荐算法[J]. 计算机研究与发展, 2016, 53(6): 1389-1399.