网络环境下的个性化信任模型 PTM

廖新考 王力生 刘晓建 许晓洁

(同济大学电子与信息工程学院 上海 201804)

摘 要 信任是人类社会的基础,在科技、商业、日常生活等领域发挥着重要作用,一个健全的社会离不开信任。在研究现有信任模型缺陷的基础上,结合现实生活中的各种信任场景,提出了网络环境下的个性化信任模型。该信任模型能够针对不同实体识别出不同的信任意义,在特定的上下文环境中能为用户推荐满足其条件的所有信任路径,具有更好的动态适应性和上下文环境相关性。实验结果表明,该模型可有效提高信任模型的准确率。

关键词 个性化,信任模型,动态适应性

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.08.019

Personalized Trust Model in Network Environment

LIAO Xin-kao WANG Li-sheng LIU Xiao-jian XU Xiao-jie

(College of Electronics and Information Engineering, Tongji University, Shanghai 201804, China)

Abstract Trust is the foundation of human society, and plays an important role in the fields of science, technology, business, daily life and so on. A healthy society cannot keep well without trust. On the basis of studying the defects of the existing trust models and combining with all kinds of trust situations in the real life, a personalized trust model in network environment was proposed. This trust model can identify different trust meanings for various entities, and can recommend all trust paths for users which meet the whole conditions in specific context environment. Because of the better dynamic adaptability and context correlation, the model can effectively improve the accuracy of trust model, which is demonstrated by the experimental results.

Keywords Personalized, Trust model, Dynamic adaptability

1 引言

近20年来,随着计算机技术和网络的广泛使用,网络虚拟社会已并行于我们的真实世界而客观存在,网络正潜移默化地融入社会并改变着我们的生活方式。信任是人类社会的基础,在科技、商业、日常生活等领域发挥着重要作用,也是人们从事交易活动的最基本要求。信任系统能够结合互联网提供的信息获取方式对信任进行有效重新定义,因此在互联网特别是电子商务系统中占有十分重要的地位。目前,越来越多的研究者已经意识到信任机制在开放网络环境中的重要性,网络信任机制的存在将有利于提高网络交互的效率,促进网络环境的改善。随着开放网络中陌生实体交互规模的进一步扩大,对网络信任问题进行深入研究的重要性及迫切性日益显现。

随着信任问题的被关注度逐年递增,近几年在电子商务信任领域已聚集了诸多学者从事相关研究,并针对信任问题取得了一定的研究成果。Marsh[1]提出了一般被认为是第一个全面且正式的信任计算模型,通过用一组变量描述信任(包括重要性、效用、能力和风险等)给出了一种合成信任的方法,并强调时间也是合成最后信任值的一个关键变量。Abdul-Rahman等[2]将信任和声望归并后应用于虚拟团体的信任计算。在该模型中,信任依赖于节点过去的历史交互经验,声望通过其他节点的推荐和意见计算得出;随后,通过加权平均的方法将这两个参数合并成最终的信任评价,而加权平均的权重会对该模型信任评估的准确性产生影响。甘早斌等[3]将信任分为4个维度,针对电子商务社会网络环境提出了多维度的信任计算方法,利用效用函数构建直接信任的影响因子,通过推荐者关系网络区分推荐节点规模和可信度,有效提高了信任计算的准确性和客观性。Dong等[4]提出了FIRE计算模型,该模型能够在开放多智能体领域进行信任评估,并将多个信任组件集为一体,其中包括验证过的声望值、基于角色的信任值、直接交互信任值和基于观察的声望值这4个主要参数,最后采用加权平均的方法计算出最终的信任评价值。FIRE模型是一个静态参量模型,需要针对不同的领域重新设定所有参数,导致该模型的可扩展性和适应性较差。Zhou等[5]提出了基于"闲谈"进行信任计算的GossipTrust信任模

到稿日期:2017-02-08 返修日期:2017-06-07 本文受国家高技术研究发展计划(863计划)(2013AA040302)资助。

廖新考(1986-),男,博士生,主要研究方向为推荐系统、信任模型、激励机制等,E-mail:lxk861201@126.com;**王力生**(1954-),男,教授,主要研究方向为嵌入式系统、并行处理系统、GIS系统、电子商务系统、信息安全系统等;**刘晓建**(1982-),男,博士生,主要研究方向为云计算、访问控制;**许晓洁**(1982-),男,博士生,讲师,主要研究方向为计算机体系结构、嵌入式系统、信息安全、可信计算等。

型，通过利用节点之间相互传输的“闲谈信息”并行计算所有节点的信任值，可以通过快速收集每个节点的本地信任值来集成全局信任值。唐文等[6]在主观信任管理研究中应用了IF-THEN模糊规则，通过引入模糊逻辑和语言变量，对人类信任推理的一般知识和经验进行建模，提出了一种形式化、描述能力强且灵活直观的信任推理度量机制。李道全等[7]在深入研究电子商务相关信任模型的基础上，针对交易中可能存在的客观风险，提出了一种基于二层节点的综合信任度的计算模型；综合考虑了影响交易的金额及时间等多种因素，引入了可交易度的概念，并将其作为节点是否进行交易的决策依据，可有效提高交易的安全性。Teacy 等[8]提出了一种分层贝叶斯信任推理模型，该模型通过观察客体或信息源行为间的相关性来改善评估方法，并能防止不可信实体用“洗白”的方式隐藏其较差的信誉。张绍武等[9]从节点之间的相似性出发，结合贝叶斯条件概率公式，提出了一种概率信任传播模型，在分析信任传播模型中衰减系数影响的基础上，通过统计分析数据证明了贝叶斯理论的有效性。Kawser 等[10]根据概率论重新对逻辑符号进行了定义，提出了一种概率逻辑和模糊逻辑结合的信任模型，该模型可根据用户的平均评分得到更为精确的信誉值。Cerutti 等[11]通过考查主观逻辑对信任模型的影响，提出了一系列折扣及融合算子，并对其进行了详细解释。苏志远等[12]针对当前信任网络中节点间的信任关系过于稀疏和“冷启动”等问题，在基于服务质量方差计算节点局部信任、基于 k-hop“朋友圈”机制的信任传播策略、基于线性阈值的信任条件传播策略等基础上，构建了全局信任机制，并建立了一种基于混合策略的信任选择模型。徐军等[13]针对现有信任机制无法很好地表达信任的不确定性以及不能有效地处理分布式网络中存在的不诚实推荐和策略性欺骗等问题，提出了一种集成直觉模糊信息的信任评估模型。解云虹等[14]通过兼顾对多级别人员的静态和动态信任管理，根据异常的危险程度对信任值进行定义和划分，并结合用户信任值的动态变化情况来定义信誉值，由此建立了一种基于信任和信誉的全局网格信任模型。针对现有研究工作无法有效抑制虚假路由信息的产生和传播等问题，夏怒等[15]提出了一种面向域间路由系统的信任模型，以实现对自治域路由通告行为准确的可信评估。Hoogendoorn 等[16]将信任分成了独立信任和相关信任，并通过使用参数估算技术建立了较基准模型更易预测信任行为的相关信任模型。

综上所述，现有的信任模型存在如下问题：

(1)描述能力有待提高。目前，信任模型无法对信任关系的多属性、主观性以及动态性建模提供支持，在信任关系量化的形式和标准等方面未能达成一致共识，同时缺乏准确性和动态适应能力。

(2)应用于现实时遭遇困难。现有的信任模型由于存在适用范围小、实现代价大、安全性差、缺乏有效的模型评估手段等问题，应用于现实时依然具有许多限定和不足之处，如不适用于大规模网络环境、难以与应用集成、对欺骗行为的处理能力不足、难以发现信任路径等。

(3)需要在信任管理中加强对可信决策的支持。基于信任评价的传统信任管理系统仅根据安全策略来制定安全决策，由于缺乏信任、风险、访问控制策略等多方面的主观因素，可信决策的效果受到严重影响。

为了克服现有信任模型的局限性，本文提出了网络环境下的个性化信任模型(Personalized Trust Model)。该信任模型支持相对信任(信任在本模型中属于本地信任)，并采用量化的信任等级来标识信任程度。因此，该个性化信任模型能针对不同实体，通过量化其信任程度定义出不同的信任等级。由于信任对上下文环境敏感，因此该信任模型在特定的上下文环境中能为用户推荐满足其条件的所有信任路径。本文采用了不分层、不传递、分散的动态方式来表示信任，利用策略表示具有不同性质的实体直接信任的程度。描述能力方面，个性化信任模型具有较强的动态适应能力，用户可根据自身条件的不同设定各自的最小可信信任域、上下文环境和最大信任路径长度，并在实体间信任网络的基础上构建直接和间接信任路径；应用实现方面，个性化信任模型提出了基础理论模型以及关键构建算法，因而能应用于各种不同场景，并可适用于大规模网络环境；可信决策支持方面，个性化信任模型能根据上下文环境及最小可信信任域计算出个人的可信实体集和非可信实体集，用户可通过指定的策略在个性化信任服务中实现对各实体的信任决策。

本文第 2 节详细地描述了个性化信任模型；第 3 节介绍了个性化信任模型的构建过程；第 4 节通过实验对该信任模型的准确性和有效性进行了验证；最后进行总结并对下一步工作进行了展望。

2　个性化信任模型

个性化信任模型主要围绕个性化信任系统的概念进行设计，在一定程度上表达了用户与其他实体之间直接或间接的信任关系，其中的动态变化状态描述了在任何给定时刻的全局信任关系。在该信任模型中，使用一组特定的算法来发现并更新网络中的信任关系，利用直接关系来描述用户的直接经验，同时利用间接关系来描述用户之间的经验传递。下面对个性化信任模型中各个部分的定义及其相互关系进行详细描述。

2.1　实体

实体表示个性化信任模型中的任何可能，用 E 表示。例如，一个实体可以是一个用户、公钥、个性化信任系统、组织或概念等。

2.2　信任

在个性化信任模型中，信任是指在特定的上下文环境中，施信方对受信方交付约定服务和能力的信念，该信念为满足某一组特定标准的确定程度。在不同的上下文环境中，信任的标准也不同。

2.3　上下文环境

上下文环境是指在信任判断中的一组信息组合，统一用 C 表示。一个实体对另一个实体的信任以基于某种上下文环境为前提，因此在不同的上下文环境中，一个实体对另一个实体的信任程度是不同的。

2.4　个性化信任服务

个性化信任服务(PTS)是个性化信任模型中实现协议和方法的单个实例，用 PTS_i 来描述用户 i 的个性化信任服务。PTS 采用个性化信任模型的算法来确定有多少实体可以信

任，并能存储及解释策略和关系等信息。用户可以将 PTS 作为自己的信任决策代理，在 PTS 中使用指定的策略来做信任决策，在指定的环境中用户能自己实施信任决策。

2.5 信任等级

对于任意一组对象中的任何两个对象，要么它们为同一信任程度，要么一方比另一方更加可信。如果两个对象被信任为相同程度，则可以说两个对象具有相同的“信任等级”。因此，信任等级是一组对象在同一上下文环境中受信任的程度。此外，一个对象可能存在不信任另一个对象的关系。

$L=\{L_1,L_2,\cdots,L_n\}$ 表示信任等级的标识符，其中信任等级用 -1 到 1 之间的小数表示，即 $L_i\in[-1.0,1.0]$。当数值为正数时，表示其信任程度，数值越大表示越可信；当数值为负数时，表示其不信任程度，数值越小表示越不信任；数值为 0 时，表示不存在信任关系。$O=\{O_1,O_2,\cdots,O_m\}$ 表示对象的标识符，$Trust(O_i)$ 表示将信任等级分配给 O_i。

如果两个对象同样值得信赖，它们分配的信任等级也相同，则 $Trust(O_i)$ 的表达式如下：

$$Trust(O_i)=Trust(O_j)\rightarrow\{O_i,O_j\}\in L_m \tag{1}$$

如果一个对象比另一个对象更可信，那么两个对象将不能共用同一个信任等级，其中更可信对象的信任等级必然高于另一个对象的信任等级，则其表达式如下：

$$Trust(O_i)>Trust(O_j)\rightarrow O_i\in L_m,O_j\in L_n,L_m>L_n \tag{2}$$

对于任意的信任等级，在等级之上或者之下都允许重新插入新的信任等级，两个信任等级之间亦可。例如：B 对节点 98 的信任等级为 L_1，对节点 99 的信任等级为 L_2，L_1 略大于 L_2。当 B 对节点 97 的信任略大于对节点 99 的信任，而略小于对节点 98 的信任时，则 B 对节点 97 的信任等级 L_3 应介于 L_1 和 L_2 之间。因此，信任等级是可以动态扩展的。设已存在 O_i 和 O_j 对应的信任等级分别为 L_i 和 L_j，则新对象 O_k 的信任等级介于 L_i 和 L_j 之间，信任等级插入问题的形式化描述如下：$L=\{L_1,L_2,\cdots,L_j,L_i,\cdots,L_n\}$ 表示连续的信任等级，$Trust(O_i)>Trust(O_j)$，且 $L_i>L_j$。

$$Trust(O_i)>Trust(O_k)\rightarrow L_i>L_k \tag{3}$$

$$Trust(O_k)>Trust(O_j)\rightarrow L_k>L_j \tag{4}$$

则有：

$$Trust(O_i)>Trust(O_k)>Trust(O_j)\rightarrow L_i>L_k>L_j \tag{5}$$

最终信任等级 L 更新为 $L=\{L_1,L_2,\cdots,L_j,L_k,L_i,\cdots,L_n\}$。

2.6 直接信任关系

直接信任关系是指凭借直接经验而获得的信任关系，而非经过第三方或者传递信息获得。直接信任关系表示实体对另一方实体的直接信任程度，有时依赖于所测量实体的具体类型，直接信任关系中两实体之间的路径长度为 2。本文用 D_{RS} 表示直接信任关系，其形式化描述如下：

$$D_{RS}=f(E_R,O_R,E_S,C_i) \tag{6}$$

其中，D_{RS} 表示实体 E_R 对 E_S 的直接信任关系，其信任程度分布在信任域 O_R 上，上下文环境为 C_i。即直接信任关系有以下关系：

$$D_{RS}\rightarrow E_S\in O_i,O_i\in PTS_R \tag{7}$$

2.7 消息

两个实体之间通过消息互相传递数据，消息是从一个实体传送到另一个实体的任何数据。发起消息的实体被称为发送者，而最终目的接收实体被称为接收者。消息可以经过许多中间实体，但最终的目的接收者只有一个。这里的消息类似于一个典型的网络数据包或帧，并可以封装其他消息。

2.8 信任路径

消息从发送者传送到接收者之间，中间节点的连接过程组成了一条从发送者到接收者的信任路径。路径的起点为发送者，终点为接收者，且消息从发送者到接收者为单向传播，接收者只负责接收消息，接收者与发送者之间的直接关系不会受发送者与接收者的直接关系而影响。例如，A 从 B 处得到信任的消息，但 A 对 B 的信任程度不受 B 是否信任 A 的影响。信任路径的形式化描述如下：

$$Path=((PTS_1,O_1),(PTS_2,O_2),\cdots,(PTS_{n-1},O_{n-1}),(E_n,\varnothing)) \tag{8}$$

其中，PTS_i 为用户 i 的个性化信任服务，O_i 为用户 i 的信任域 O_i，则其中包含关系 $PTS_{i-1}\in O_i$，即个性化信任系统决定着消息的传递，而消息之间的传递过程即为用户自身的个性化信任系统中的传递过程，最终传递到接收者。令 $Pair_i=(PTS_i,O_i)$，即有：

$$Path=(Pair_1,Pair_2,\cdots,Pair_n) \tag{9}$$

定义路径长度为路径上的节点数量，即为 $|Path|$。当路径长度为 2 时，则为直接信任关系；当路径长度大于 2 时，则为间接信任关系。其中，间接信任关系利用信任的传递性，得到路径上的信任值如下：

$$Trust(Path)=O_1\times O_2\times\cdots\times O_{n-1} \tag{10}$$

例如：若实体 A 对实体 B 存在直接信任分布在信任域 $O_{0.9}$ 上，而实体 B 对实体 C 存在直接信任分布在信任域 $O_{0.6}$ 上，则实体 A 和实体 C 之间存在一条信任路径 $A\rightarrow B\rightarrow C$，实体 A 对实体 C 的信任路径的信任值为 $O_{0.9}\times O_{0.6}=O_{0.54}$，则实体 A 通过间接信任关系将实体 C 的信任程度更新到个人信任系统中的信任域 $O_{0.54}$ 上。

2.9 间接信任关系

间接信任关系是指通过第三方或者消息传递而获得的信任关系，而非经过直接经验获得。间接信任关系表示实体对另一方实体的间接信任程度，两实体之间的路径长度大于 2。本文用 I_{RS} 表示间接信任关系，$Path_{RS}$ 为实体 R 到实体 S 的路径，其形式化描述如下：

$$I_{RS}\rightarrow Trust(E_R,E_S,C_R)=Trust(E_R,Path_{RS},C_R) \tag{11}$$

其中，$D_{ij}\in Path_{RS}$ 表示实体 E_i 对 E_j 的直接信任关系，其信任程度分布在信任域 O_R 上，E_R 的上下文环境为 C_R。此处将对目标接收者的信任转换为对路径的信任。当存在多条路径到达接收者时，则对接收者存在多条信任路径，I_{RS} 则为多条信任路径的加权。

$$Trust(I_{RS})=\sum Trust(Path_{RS}) \tag{12}$$

例如：若实体 A 对实体 B 存在直接信任分布在信任域 $O_{0.6}$ 上，而实体 B 对实体 C 存在直接信任分布在信任域 $O_{0.5}$ 上，从而实体 A 和实体 C 之间存在一条信任路径 $A\rightarrow B\rightarrow C$，同时存在另一条信任路径 $A\rightarrow D\rightarrow C$，且 A 与 D 和 D 与 C 之间的直接信任分布分别为 $O_{0.4}$ 和 $O_{0.8}$，实体 A 对实体 C 的信任路径的信任值为两条信任路径的加权 $Trust(I_{AC})=O_{0.6}\times O_{0.5}+O_{0.8}\times O_{0.4}=O_{0.62}$，从而实体 A 通过间接信任关系将实体 C 的信任程度更新到个人信任系统中的信任域 $O_{0.62}$ 上。

2.10 最大路径长度

最大路径长度是指为了降低信任系统的时间复杂度而设置的最长有效信任路径，在该路径长度内能达到间接信任关系则被视为有效。根据“小世界原理”，该值默认设置为 6，不同用户的最大路径长度值不同。

2.11 最小可信信任域

最小信任域是指在特定的上下文环境中，目标用户在个人信任系统中对其他实体的最低可信任值。在目标用户的个人信任系统中，分布低于最小信任域标签的任何实体都可以被认为是不可信的实体；反之，分布高于最小信任域标签的任何实体则都可以被认为是可信实体。不同用户的最小可信信任域值不同。用 O_M 表示个人信任系统中的最小可信信任域，PTS_i 表示用户 i 的个人信任服务，C_i 表示特定的上下文环境，$O=\{O_{-1.0},\cdots,O_M,\cdots,O_{1.0}\}$ 表示用户 i 在特定的上下文环境中的信任域集合，则不可信的实体集合如下：

$$O_i<O_M\rightarrow Trust(E_i,O_i,C_i) \tag{13}$$

可信的实体集合如下：

$$O_i\geqslant O_M\rightarrow Trust(E_i,O_i,C_i) \tag{14}$$

例如：用户 A 设置其最小可信信任域值为 0.5，如果实体 B 和实体 C 分别分布在用户 A 的信任域 $O_{0.6}$ 和 $O_{0.45}$，则实体 B 对用户 A 而言是可信的；因实体 C 的信任程度低于其最小可信值，故实体 C 对于用户 A 是不可信的。

2.12 可信直接信任关系集

将实体 E_1 对实体 E_2 的可信直接信任关系集合定义为 E_1 和 E_2 之间存在直接信任关系，且 E_2 对 E_1 而言是可信的。O_M 表示个人信任系统中的最小可信信任域，PTS_i 表示 E_1 的个人信任服务，C_i 表示 PTS_i 下特定的上下文环境，$O=\{O_{0.0},\cdots,O_M,\cdots,O_{1.0}\}$ 表示 E_1 在上下文环境中的信任域集合，则可信直接信任关系集的形式化描述如下：

$$D^{+}_{E_1E_2}\rightarrow D_{E_1E_2}\wedge E_2\in O_j\wedge O_j\in[O_M,O_{1.0}] \tag{15}$$

不可信的直接信任关系集合的形式化描述如下：

$$D^{-}_{E_1E_2}\rightarrow D_{E_1E_2}\wedge E_2\in O_j\wedge O_j\notin[O_M,O_{1.0}] \tag{16}$$

类似地，可信的间接信任关系和不可信的间接信任关系的形式化描述分别如下：

$$I^{+}_{E_1E_2}\rightarrow I_{E_1E_2}\wedge E_2\in O_j\wedge O_j\in[O_M,O_{1.0}] \tag{17}$$

$$I^{-}_{E_1E_2}\rightarrow I_{E_1E_2}\wedge E_2\in O_j\wedge O_j\notin[O_M,O_{1.0}] \tag{18}$$

2.13 可信实体集

可信实体集包含可信直接信任关系集和可信间接信任关系集，其形式化描述如下：

$$T^{+}_{E_1E_2}\rightarrow D^{+}_{E_1E_2}\vee I^{+}_{E_1E_2} \tag{19}$$

同样地，不可信实体集包含不可信直接信任关系集和不可信间接信任关系集，其形式化描述如下：

$$T^{-}_{E_1E_2}\rightarrow D^{-}_{E_1E_2}\vee I^{-}_{E_1E_2} \tag{20}$$

3 个性化信任模型的构建过程

具有不同上下文属性背景的用户之间产生的信任关系具有较大差异，同一用户在不同兴趣领域内的信任关系强度也存在差异。本文针对个性化信任模型提出的各方面的定义是抽象的，旨在帮助各个实体能根据各自的环境特征确定可信实体集合。在该个性化信任模型中，不同的实体可以根据特殊环境设定各自的最小可信信任域、上下文环境和最大信任路径长度。个性化信任模型在实体间信任网络图的基础上进行构建，其构建过程包括路径发现过程和间接信任关系更新过程。

3.1 路径发现算法

本文采用路径发现算法来发现目标用户在特定上下文环境中的所有信任路径信息集合。在路径发现算法中，消息传递的数据格式如下：

PTS_L：本地 PTS；

PTS_R：目标用户的 PTS，初始化查询条件 Q_R；

O：信任域集合；

C：目标用户的上下文环境；

E：待评价的实体集合；

N：目标用户的最大路径长度；

N_C：当前路径剩余的最大长度，$Length_{RL}$ 表示 PTS_R 到 PTS_L 的路径长度，则 $N_C=N-Length_{RL}$。

故路径查询消息的格式包含 N_C 头信息和一个六元组签名信息$\langle PTS_L,PTS_R,O,C,E,N\rangle$。

路径发现算法主要用于寻找信任系统中的间接信任关系，如果信任关系中包含环的结构，则可能导致路径发现陷入死循环状态。因此，需要通经过环检测来过滤存在环的情况，然后通过消息 Q 抽取从 PTS_R 到 PTS_L 的路径 $Path_{RL}$，并寻找出所有的 $Path_{RL}$ 子路径。由于需保证最终的路径长度不超过 N，因此每次递归要计算出最小剩余路径长度 N_C，并过滤路径长度超过 N 的信任路径。此外，当间接信任关系低于该节点 PTS 系统中设置的最低信任域 O_M 时，不再继续往前延伸路径，该节点即为该路径的接收者。路径发现算法的伪码及文字描述如算法 1 所述。

算法 1 路径发现算法伪码及文字描述

输入：目标节点查询消息 Q，最大路径长度 N，信任域集合 O

输出：所有满足条件的路径

1. 检测是否存在环形结构。
2. 从消息 Q 中创建所有的子路径。
3. 遍历所有的子路径信息，并针对每个子路径重复以下操作。
4. 计算当前路径剩余的最大长度 N_C，若 $N_C<1$ 则返回结果，否则保存该节点信息并继续向其直接信任关系的节点延伸。
5. 计算与目标节点的间接信任关系，若计算结果低于 PTS 系统中设置的最低信任域 O_M，则返回结果，否则保存该节点信息并继续向其直接信任关系的节点延伸。
6. 结束循环。
7. 遍历所有的保存路径。
8. 返回路径信息。

3.2 间接信任关系更新算法

间接信任关系更新的过程中系统通过间接信任更新算法来维持最新的信任域关系。当直接信任关系改变时，将导致间接信任关系中的路径也发生改变，之前能到达的接收者有可能因为路径发生改变而导致无法到达。如原有间接信任路径(A,C,D)中，假定 A 系统中的最小信任值为 0.4，若在某一时刻 C 对 D 的直接信任发生变化，由原来的 0.5 变为 0.3，小于 A 中的最小信任值，则 D 在 A 的信任路径中将被舍弃；或者 C 对 D 的直接信任转变为 C 对 F 的直接信任时，也会导致原有的间接信任路径发生变化。在信任路径中，发生改变的节点的前面部分的路径不会随之变化，其后的路径才会发生

变化。因此，如果增加或者改变 S 的直接信任关系，那么必然要更新其后的路径所有间接信任关系中包含 S 但并非以 S 为接收者的路径。间接信任更新算法的伪码及文字描述如算法 2 所示。

算法 2 间接信任更新算法

输入：改变的直接信任关系，原路径信息

输出：更新路径信息

1. 当 PTS_i 与实体 E 的直接信任关系发生改变时，重复执行步骤 2 和步骤 3。
2. 将实体 E 重新加入其个性化信任系统中。
3. 更新实体 E 与 PTS_i 的直接信任关系。
4. 对于任意的查询路径信息 Q，若其中包含 PTS_i 并且 PTS_i 不作为其接收者，则执行步骤 5 和步骤 6。
5. 从查询路径信息 M 中取出最后一条查询信息。
6. 对查询路径信息 Q 重新执行路径发现算法，重新构建新路径。
7. 结束循环。

4 实验与结果分析

4.1 信任模型仿真实验与结果分析

本节主要通过模拟仿真实验来评价 PTM 个性化信任模型的性能，在该模拟仿真平台上采用多主体的建模仿真工具 NetLogo[17] 进行实验。仿真模型中的基本参数设置和默认详情参见表 1，设置该网络节点数量的范围为 100～1000，其中恶意节点的比重范围为 10%～50%。对于诚实节点，初始的信任值服从 $u_r=75$ 和 $\sigma_r=10$ 的标准正态分布；对于恶意节点，初始的信任值服从 $u_r=25$ 和 $\sigma_r=10$ 的标准正态分布。初始信任关系网络服从随机标准正态分布，如图 1 所示，网络复杂度 $D=6$ 表示初始节点的入度服从 $u_D=6$ 和 $\sigma_r=1$ 的标准正态分布。此外，阈值 $\theta_v=35\%$ 表示该网络中若有 35% 的可信节点认定目标节点为恶意节点，则该节点能被标识为恶意节点。

表 1 仿真模型参数的设置(PTM 个性化信任模型)

符号	说明	默认值
N	网络节点数量	100～1000
D	网络复杂度(平均节点入度)	3,6,9
α	恶意节点比例	10%,30%,50%
u_r	初始信任比例分布均值	0.75,0.25
σ_r^2	初始信任比例分布方差	0.1
u_D	平均节点入度分布均值	3,6,9
σ_D^2	平均节点入度分布方差	1
θ_v	恶意节点支持比例阈值	35%
ε	聚合阈值	0.02

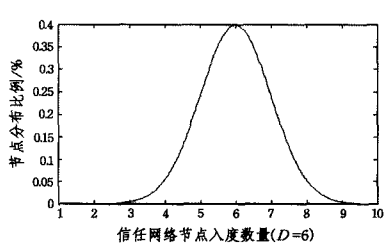


图 1 初始信任关系节点分布图($D=6$)

模拟仿真实验先按表 1 中设置的参数进行初始化，产生网络拓扑结构，根据已有的信任分布生成局部信任，随后逐步执行 PTM 个性化信任模型的聚合过程，直到所有节点的信誉都趋于稳定状态。为了模拟动态过程，随机在节点间产生交易，每次交易后双方节点都会返回一个 1～5 的数值作为对对方的服务评分。

通过有效信任评价比率来测量个性化信任模型预测的准确度，结果如图 2 所示。有效信任评价主要认为预测的信任值与实际的真实值(预设的评价分)之间的方差小于预设阈值。从图 2 可以发现，PTM 个性化信任模型的整体准确度基本在 90%左右，说明 PTM 信任模型不仅能有效识别直接信任，还能有效识别间接信任。

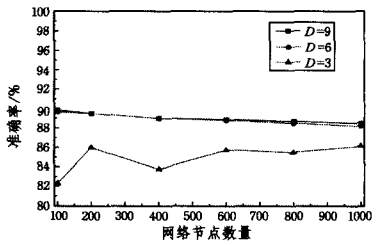
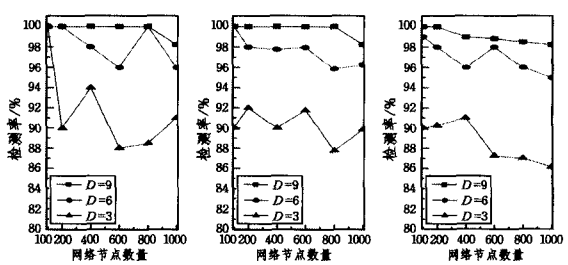


图 2 个性化信任模型的准确率

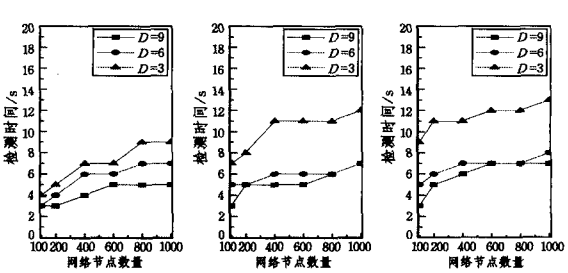
主要通过恶意节点检测率和检测时间来对恶意节点检测进行衡量。本文中，恶意节点主要指在交易中产生欺骗行为、在信任传输过程中发送错误的信任信息给下一节点或者在信任反馈评分中进行虚假评价的节点。在该模拟仿真环境下，恶意节点采用混合策略来传递消息。混合策略为可能传递的消息中既包含部分虚假信息，也包含部分真实消息。如果虚假消息概率比例为 50%，则表示传递的消息中有 50%是假的；当超过阈值 θ_v 的可信节点认定目标节点为恶意节点，则该节点能被标识为恶意节点。初始的恶意节点比例分别为 10%，30%，50%。

不同恶意节点比例的检测率如图 3 所示，在一个正常的网络环境下($D=6,9$；$\alpha=10\%,30\%$)，95%以上的恶意节点都能够被识别出来；即使在低复杂网络环境($D=3$)下，该检测的正确率仍能达到 90%左右。不同恶意节点比例的检测时间如图 4 所示，可以发现 PTM 个性化信任模型能够有效地识别恶意节点；随着恶意节点比例的增长，PTM 个性化信任模型检测性能降低的幅度很小；此外，在越复杂的网络环境下，恶意节点越容易被检测出来。



(a)恶意节点 10% (b)恶意节点 30% (c)恶意节点 50%

图 3 不同恶意节点比例的检测率对比图



(a)恶意节点 10% (b)恶意节点 30% (c)恶意节点 50%

图 4 不同恶意节点比例的检测时间对比图

4.2 对比实验结果与分析

本节主要将所提模型与 EigenTrust 信任模型及 PeerTrust 信任模型进行对比，其基本参数设置和默认值详情参见表 2。设置该网络节点数量的范围为 1000～10000，其中恶意节点比重范围为 10%～50%。对于诚实节点，初始信任值服从 $u_r=75$ 和 $\sigma_r=10$ 的标准正态分布；对于恶意节点，初始的信任值服从 $u_r=25$ 和 $\sigma_r=10$ 的标准正态分布。网络复杂度为 $D=10,20,30$。

表 2　对比实验仿真模型的参数设置

符号	说明	默认值
N	网络节点数量	1000～10000
D	网络复杂度(平均节点入度)	10,20,30
α	恶意节点比例	10%～50%
u_r	初始信任比例分布均值	0.75,0.25
σ_r^2	初始信任比例分布方差	0.1
u_D	平均节点入度分布均值	10,20,30
σ_D^2	平均节点入度分布方差	1
θ_v	恶意节点支持比例阈值	35%
ε	聚合阈值	0.02

(1)EigenTrust 信任模型

EigenTrust 模型通过将信任值进行简单的加权平均，综合不同方面的意见形成信任评价。该信任模型进行信任评估的核心是获取交易实体的全局可信度，主要利用交易网络中逻辑相邻的交易实体之间的相互信任评价进行迭代，进而获取交易实体的全局信誉度。EigenTrust 模型中信任值的聚合过程借鉴了应用最为普遍的加权平均方法，其计算方法如下：

$$T(i,j)=\alpha*(\lambda*D(i,j)+(1-\lambda)*F(i,j))-\beta*R(i) \tag{21}$$

其中，$T(i,j)$表示交易主体 i 对交易主体 j 的总体信任值，$D(i,j)$是交易主体 i 根据与交易主体 j 之间已有的交互记录得出的直接信任值，$F(i,j)$是交易主体 i 根据第三方主体的反馈推荐而形成的对主体 j 的反馈信任值，$R(i)$是交易主体 i 认为交易可能带来的风险值，α,β,λ 为归一化的权重因子。

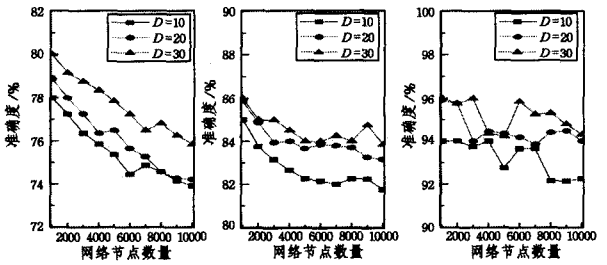
(2)PeerTrust 信任模型

Xiong 等[18]认为当前信任模型中信任计算时考虑的影响因素不够全面，尤其是忽略了交易上下文因素对信任评估的影响；通过分析交易过程中的上下文因素，提出了包含更多上下文因素的 PeerTrust 信任模型。该模型力图描述信任评价的全面性与合理性，5 种评价因子模型的数学描述如下：

$$T(i)=\alpha*\sum_j S(i,j)*Cr(p(i,j))*TF(i,j)+\beta*CF(i) \tag{22}$$

其中，$p(i,j)$是第 j 次历史交易中与服务提供者进行交易的节点集合，$S(i,j)$是 $p(i,j)$中消费者集合元素在第 j 次交易后分别对服务提供者给出的信任评价，$Cr(i)$是节点 i 所给信任评价的可信度，$TF(i,j)$是与节点的第 j 次交易过程中由交易上下文因素所产生的信任度，$CF(i)$是环境上下文因素产生的信任度，α 和 β 分别是归一化时交易上下文的信任值权重和社区上下文信任值权重因子。

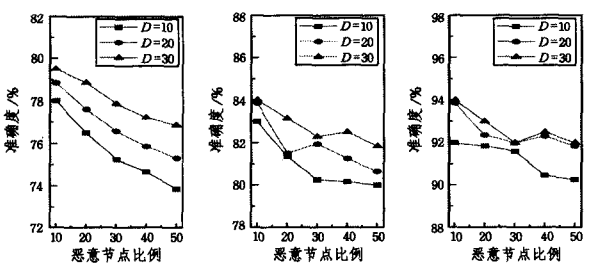
EigenTrust 信任模型、PeerTrust 信任模型和 PTM 信任模型的准确度与网络节点数量关系的对比实验结果如图 5 所示，其中恶意节点的比例均为 10%。准确度与之前实验定义的相同，即预测的信任值与实际的真实值(预设的评价分)之间的方差小于预设阈值。PTM 个性化信任模型整体的准确度基本可达到 90%以上，而 EigenTrust 信任模型和 PeerTrust 信任模型整体的准确度分别仅为 78%和 83%。由于 PTM 个性化信任模型中的信任值不仅通过直接经验，还通过间接经验以及上下文环境获取，因此信任评价的准确度得到了大幅提升。而当网络复杂度较低时，PTM 信任模型的准确度也随之降低，因为网络复杂度越低，会导致信任路径长度越长，从而需要传输的消息也越多，这必然会降低信任反馈信息在传输过程中的准确度。



(a)EigenTrust 准确度　(b)PeerTrust 准确度　(c)PTM 准确度

图 5　准确度与网络节点数量关系对比图

EigenTrust 信任模型、PeerTrust 信任模型和 PTM 信任模型的准确度与恶意节点比例的对比实验结果如图 6 所示，其中网络节点数量均设置为 5000。在该环境下，PTM 个性化信任模型的准确度均能维持在 90%以上，而 EigenTrust 和 PeerTrust 信任模型的准确度仅能维持在 75%～84%之间。实验发现，准确度随着恶意节点比例的上升而逐渐降低；当网络复杂度降低时，3 种信任模型的准确度也随之降低。



(a)EigenTrust 准确度　(b)PeerTrust 准确度　(c)PTMTrust 准确度

图 6　准确度与恶意节点比例关系对比图

综合图 5 和图 6 的实验结果，可以得出以下结论：PTM 信任模型的性能优于 EigenTrust 信任模型和 PeerTrust 信任模型的性能。

结束语　在总结现有信任模型缺陷和不足的基础上，本文提出了网络环境下的个性化信任模型。该模型通过量化不同实体的信任程度，能对不同实体定义出不同的信任等级，并在特定的上下文环境中为用户推荐满足其条件的所有信任路径。本文描述了个性化信任模型的基本形式以及关键的构建过程，最后通过相关实验对该信任模型的有效性进行了验证。本文仅提出了个性化信任模型的形式化描述及理论基础，模

型的应用场景还有待继续挖掘，如应用于个人服务等；此外，该信任模型中间接信任关系的非传递性和非对称性也有待进一步优化。

参 考 文 献

[1] STEPHEN M. Formalising trust as a computational concept [D]. Scotland: University of Stirling, 1994.

[2] ABDUL-RAHMAN A, HAILES S. Supporting trust in virtual communities[C]// Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. IEEE, 2002: 6007.

[3] 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.

[4] DONG H T, JENNINGS N R, SHADBOLT N. Developing an integrated trust and reputation model for open multiagent systems[C]// Proceedings of the 7th International Workshop on Trust in Agent Societies. 2004: 65-74.

[5] ZHOU R F, KAI H. Gossip-based reputation aggregation for unstructured peer-to-peer networks[C]// International Parallel and Distributed Processing Symposium. 2007: 1-10.

[6] TANG W, HU J B, CHEN Z. Research on a Fuzzy Logic-based Subjective Trust Management Model[J]. Journal of Computer Research and Development, 2005, 42(10): 1654-1659. (in Chinese)
唐文，胡建斌，陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展，2005，42(10)：1654-1659.

[7] LI D Q, WU X C, GUO R M. Electronic Commerce Transaction Trust Model Based on Two Layers Nodes and Objective Risk [J]. Computer Science, 2016, 43(5): 117-121. (in Chinese)
李道全，吴兴成，郭瑞敏. 一种基于二层节点和客观风险的电子商务交易信任模型[J]. 计算机科学，2016，43(5)：117-121.

[8] TEACY W T L, LUCK M, ROGERS A, et al. An efficient and versatile approach to trust and reputation using hierarchical bayesian modeling[J]. Artificial Intelligence, 2012, 193: 149-185.

[9] ZHANG S W, LIN H F, LIU X X, et al. Trust Propagation Based on Probability[J]. Computer Science, 2014, 41(8): 90-93. (in Chinese)
张绍武，林鸿飞，刘晓霞，等. 基于概率的信任传播模型[J]. 计算机科学，2014，41(8)：90-93.

[10] KAWSER W N, TONNY S K, AMJAD H, et al. A fuzzy and probabilistic logic based representational model of certain trust model[C]// International Conference on Informatics, Electronics & Vision. 2012: 1000-1005.

[11] CERUTTI F, KAPLAN L M, NORMAN T J, et al. Subjective logic operators in trust assessment: an empirical study[J]. Information Systems Frontiers, 2015, 17(4): 743-762.

[12] SU Z Y, LI M C, FAN X X, et al. LT Trust: a trust management model based on hybrid strategy[J]. Journal of Chinese Computer System, 2014, 35(7): 1464-1469.

[13] XU J, ZHONG Y S, WAN S P. Incentive Adaptive Trust Model Based on Integrated Intuitionistic Fuzzy Information[J]. Journal of Electronics and Information Technology, 2016, 38(4): 803-810. (in Chinese)
徐军，钟元生，万树平. 一种集成直觉模糊信息的激励自适应信任模型[J]. 电子与信息学报，2016，38(4)：803-810.

[14] XIE Y H, HE Y J, XIANG Y. A Secure Grid Trust Model Based on Trust and Reputation[J]. Journal of Xi'an University of Posts and Telecommunications, 2016, 21(3): 69-73. (in Chinese)
解云虹，何永健，向阳. 一种基于信任和信誉的安全网格信任模型[J]. 西安邮电大学学报，2016，21(3)：69-73.

[15] XIA L, LI W, LU Y, et al. A Trust Model for the Inter-Domain Routing System[J]. Journal of Computer Research and Development, 2016, 53(4): 845-860. (in Chinese)
夏怒，李伟，陆悠，等. 一种面向域间路由系统的信任模型[J]. 计算机研究与发展，2016，53(4)：845-860.

[16] HOOGENDOORN M, JAFFRY S W, VAN MAANEN P P, et al. Design and validation of a relative trust model[J]. Knowledge-Based Systems, 2014, 57: 81-94.

[17] WILENSKY U. Netlogo[OL]. http://ccl.northwestern.edu/netlogo.

[18] 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.

(上接第 81 页)

[10] BRAUN T, TRINH T A. Energy Efficiency Issues In Information-Centric Networking[M]// Energy Efficiency in Large Scale Distributed Systems. 2013: 271-278.

[11] GUAN K, ATKINSON G, KILPER D C, et al. On the Energy Efficiency of Content Delivery Architectures [C]// IEEE International Conference on Communications Workshops. IEEE, 2011: 1-6.

[12] CHOI N, GUAN K, KILPER D C, et al. In-network caching effect on optimal energy consumption In content-centric networking[C]// IEEE International Conference on Communications. IEEE, 2012: 2889-2894.

[13] FANG C, YU F R, HUANG T, et al. An energy-efficient distributed in-network caching scheme for green cont ent-centric networks[J]. Computer Networks, 2014, 78: 91-96.

[14] BICKSON D. The emule protocol specification[J]. Emule Project, 2005, 4(1): 17-30.

[15] BARROSO L A, HÖLZLE U. The Case for Energy-Propo rtional Computing[J]. Computer, 2007, 40(12): 33-37.

[16] LIANG X M, ZHU C, YAN D H. Novel genetic algorithm based on species selection for solving con strained non-linear programming pro problems [J]. Journal of Central South University (Science and Technology), 2009, 40(1): 185-189. (in Chinese)
梁昔明，朱灿，颜东煌. 基于物种选择的遗传算法求解约束非线性规划问题[J]. 中南大学学报(自然科学版)，2009，40(1)：185-189.