移动 P2P 环境下基于社会信任补充的信任模型

王 健[1,2,3],曹晓梅[1,2,3]
(1. 南京邮电大学 计算机与软件学院,江苏 南京 210003;
2. 江苏无线传感网高技术研究重点实验室,江苏 南京 210003;
3. 宽带无线通信与传感网技术教育部重点实验室,江苏 南京 210003)

摘 要:随着移动终端的普及,移动 P2P 网络中所面临的虚假文件传播,恶意节点共谋攻击等安全问题日益严重,因此,需要有效的信任机制来保证移动 P2P 网络的安全性。文中提出了一种基于社会信任补充的信任模型。该模型针对移动 P2P 网络中节点的高度动态性,参考人类社交网络,在节点历史交易信息不能获取时采用节点的社会信任作为补充,以此来评估节点的可信程度;同时引入交易速率作为交易失败的风险因子;并且利用向量描述节点之间的熟悉程度,通过计算向量余弦相似度,筛选出可靠的推荐节点,随后综合所有可信推荐节点的交易次数和交易满意次数,从而保证评价的稳定性。通过仿真的实验结果表明,该模型能够有效提高文件下载成功率并能够抵抗恶意节点的共谋攻击。

关键词:移动 P2P;社会信任;高度动态性;余弦相似度;共谋攻击
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2015)09-0134-05
doi:10.3969/j.issn.1673-629X.2015.09.029

A Trust Model Based on Social Trust Supplement for MP2P Networks

WANG Jian[1,2,3], CAO Xiao-mei[1,2,3]
(1. College of Computer and Software, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3. Key Lab of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing 210003, China)

Abstract: With the popularity of the mobile devices, the security problems about the spread of the false documents and the attack of malicious nodes in the Mobile P2P networks become more and more serious, then need an effective trust mechanism to protect the MP2P network. A trust model based on social trust as supplement is proposed. This model aims at the high dynamic characteristic of nodes in MP2P network and consuls social networks. While the trading history information of the nodes cannot be acquired, the model will use the social trust of the nodes as supplement to evaluate the node's reliability. The model also introduces the rate of transaction as the risk factor of the transaction failure. Use vector to describe the degree of the familiarity between the nodes and compute the cosine similarity to screen out reliable nodes, and then compute the trade times of the reliable nodes to ensure that the evaluation is stable. The simulation result proves that the model can promote the success rate of file downloads and defend the collusion attack of malicious nodes effectively.

Key words: Mobile P2P; social trust; high dynamic; cosine similarity; collusion attack

1 概 述

移动终端的普及和 3G 应用环境的逐渐成熟,使移动蜂窝网络和宽带无线网络上的对等网络(Peer to Peer,P2P)需求日渐强烈。与传统的 P2P 网络相比,移动 P2P 网络具有更高的开放性,因而更容易受到恶意节点的攻击,例如发布虚假恶意文件滥用资源等行为,影响网络的运行。信任管理作为一种“软安全”技术,能够有效解决这一问题信任机制从语义层次上对合作对象的行为进行建模来避免交互风险和辅助决策,相对于传统的安全技术具有更好的灵活性[1]。因此,需

收稿日期:2014-11-01 **修回日期**:2015-02-05 **网络出版时间**:2015-08-26
基金项目:国家自然科学基金资助项目(61202353);国家“973”重点基础研究发展计划项目(2011CB302903);江苏高校优势学科建设工程资助项目(yx002001)
作者简介:王 健(1990-),男,硕士,研究方向为无线网络安全;曹晓梅,博士,副教授,研究方向为计算机通信网与安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150826.1558.042.html

要有效的信任机制来保证移动 P2P 网络的安全性。

关于 P2P 网络中的信任机制已有大量的研究,文献[2]提出了基于相似度加权推荐的信任模型 SWRTrust,该模型以节点评分相似度加权其推荐信任值。文献[3]提出一种基于推荐证据的有效抗攻击的信任模型,该模型解决了汇聚推荐信息时无法处理不确定性推荐信息以及强行组合矛盾推荐信息引起的性能下降问题。文献[4]提出一种激励相容的 P2P 信誉模型 ICRM,该模型使用时间区间来表示经验和推荐的时间特性,利用直接信任度、推荐信任度及推荐可信度精确描述节点的信任等级,从而识别与抑制恶意节点。文献[5]提出一种基于信誉和风险评价的分布式 P2P 信任模型,该模型考虑到节点的动态行为影响信任度计算的不确定性,引入风险因素,并提出采用信息熵理论来量化风险。文献[6]提出基于反馈相关性的 P2P 网络信任模型 CoDyTrust,该模型引入信任相关系数、信任遗忘因子、滥用信任值和推荐信任度等,通过反馈控制,实现恶意行为检测。但是移动 P2P 网络与 P2P 网络相比,一个重要的特点就是移动 P2P 网络中节点的移动性强,P2P 网络的信任模型大多基于请求节点能够在有限跳数内获取其他节点的信任值,但是由于移动 P2P 网络的高度动态性,节点频繁加入和离开网络,经常会出现无法获取其他节点的信任信息的情况,从而无法建立节点之间的信任关系;其次受限于移动终端的资源和运算能力,P2P 网络中复杂的信任值计算方法并不适用,因此 P2P 网络中信任模型不能完全适用于移动 P2P 网络中。

目前针对移动 P2P 网络的信任模型研究还处于起步阶段,在移动 P2P 环境中,信任可以简要地分为 3 个类别,分别是社会信任、相似性信任和服务质量信任[7]。社会信任依据社会关系判断一个用户是否可靠;相似性信任则是认为具有相似兴趣的节点更为可靠;服务质量信任则是判断节点是否能够以规定的质量完成服务。现有的信任模型大多考虑的是服务质量信任,即评价一个节点是否可靠依据的是节点是否提供了高质量的服务。文献[8]提出一种多粒度信任模型 MGT,该模型引入聚类思想,从多方面的因素考量节点可信程度,但文章认为节点终端相似度越高,则节点的推荐信息可靠性越高,这样不足以筛选出可靠的推荐节点。文献[9]提出一种移动 P2P 网络环境下的动态安全信任模型 DSTM_MP2P,该模型针对节点信息未知和已知两种情况,提出两种方案。节点的信任信息已知时,提出基于节点行为的节点类型识别机制;对于节点信任信息未知时,提出基于贝叶斯博弈的节点概率选择策略。然而在移动 P2P 网络中,节点之间的交易很可能是少次短期的,而博弈策略发挥作用却必须依赖于长期多次的交易。文献[10]提出一种移动 P2P 分布式信任模型 SD^2 Trust,该模型区分了服务可信度和推荐可信度,依据社会距离确定推荐节点集和推荐信任的计算权重,但是该模型不能有效地对抗恶意节点的共谋攻击。文献[11]提出一种移动 P2P 环境下的分布式信任模型 MobTrust,该模型通过分布式存储机制,将节点转发的评价数据备份于 K 桶中,扩充了评价数据的存储范围。但是由于移动 P2P 网络中节点的高度动态性,伴随着节点的移动,评价数据存储的范围会越来越大,当节点离开网络时,其他节点存储的关于其的评价信息便会无用,造成终端的资源浪费。文献[12]提出一种基于代理的安全反馈信任模型 PSTM,该模型采用不同类别的代理服务器接入不同类型的终端,在多粒度计算中引入全局节点贡献度和评价可信度,同时将直接信任度分为面向节点的与面向资源的来激励节点提供真实的反馈。文献[13]为了聚合可信的推荐信任,将具有相似兴趣节点组成群组,群组中节点的推荐更为可靠,由于移动 P2P 网络中节点的移动性强,群组内节点不能实时有效地获取到反馈信息。文献[14]利用 M-Trust 方法对信任信息进行融合,节点保存周围节点的信任信息。然而节点移动性强,网络结构不断变化,保存周围节点的信任信息意义不大。

上述信任模型均是基于服务质量和相似性的信任模型,它们能够判断节点是否可靠的前提是节点之间有过交易或者能获得其他节点的推荐信息,从而得到直接信任值和推荐信任值进行计算。而在移动 P2P 网络中,由于其高度的动态性,节点移动或加入退出网络频繁,节点并不能在每次交易时都能获取到信任值。在信任值缺失时,不能有效评估节点是否可靠。此时便可利用社会信任作为补充,原因在于社会信任不依赖于节点的交易历史,即使节点之间未有过交易,节点也能通过节点间的社会关系对节点做出一定的可靠性评估。

文中针对移动 P2P 网络中节点移动性强,节点历史交易信息易缺失的特点,提出一个基于社会信任补充的信任模型 STTM(Social Trust as supplement to the Trust Model)。首先,考虑到移动 P2P 网络动态性强的特点,在 STTM 中,在对资源节点的信任信息未能获取的情况下,将利用节点之间的社会关系,计算请求节点对资源节点的社会信任作为补充来评价节点是否可靠其次在计算直接信任值时,引入交易速率作为风险因子,以此评估交易失败的风险;计算推荐信任值时,并非简单综合各推荐节点的推荐信任值,而是构造向量描述节点之间的熟悉程度,计算余弦相似度筛选出可信节点,综合所有可信推荐节点的交易次数和交

易满意次数,从而保证评价的稳定性;分配直接信任值与推荐信任值的权重时,利用变异系数法,使得稳定的评价信息具有更高的权重。最后分析和实验结果表明,该模型能够有效提高在信任值未知时资源的下载成功率,并能有效抵御恶意节点的共谋攻击。

2 基于社会信任补充的移动 P2P 信任模型

文中在计算信任值时分为请求节点对资源节点的交易信息可以获得和不能获得两种情况,在不能获取时,通过计算社会信任来判断节点是否可靠;可以获取时则综合节点对资源节点的直接信任值和其他节点对资源节点的推荐信任值。

2.1 节点历史交易信息缺失

在资源节点的交易历史行为信息未能获取时,STTM 采用社会信任评价节点是否可靠。该方案的优点在于社会信任不依赖于节点的交易历史,而是利用节点之间的社会关系。衡量社会信任的方法很多,结合人类社会关系,文中考虑在移动 P2P 网络中,一个节点可能会经常遇到一些其他节点,但是它们之间是没有过交易的,这种情况是比较常见的。可以称那些经常遇到但没有过交易的节点为“熟悉的陌生节点”。在信任值缺失的情况下,会觉得“熟悉的陌生节点”比很少相遇的陌生节点更加值得信任。同时在特定的环境中遇到过的节点会更加可靠,例如在校园或办公室遇到的会比在地铁上遇到的节点更加值得信赖。因此文中利用节点之间相遇的时间和相遇的环境来衡量节点之间的社会信任。计算社会信任值时,用户节点需要记录自己曾经到过的环境以及停留时间,同时对环境需进行划分,划分环境可以有多种方法,例如按照地理位置、网络接入点进行区分等等。

定义用户在环境 j 中与节点 i 相遇持续时间为 $t^{e}_{i,j}$,同时考虑到节点对不同环境的重视程度不同,在某些特定的环境中即使节点之间相遇时间很短,例如在家中,但是节点对其信任值也应很高。定义用户在环境 j 中所停留的总时间为 t^{s}_{j},那么环境 j 在用户所有定义的环境中所占比重 F_j 为:

$$F_j = \frac{t^{s}_{j}}{\sum_{j=1}^{n} t^{s}_{j}} \tag{1}$$

式(1)表明了环境 j 对于用户的重要程度,即一个用户在一个环境中时间越久,那么他就会对这个环境更加熟悉,同时对这个环境中的节点也会更加信任。

则用户节点对节点 i 的社会信任计算公式如下:

$$T_i = \sum_{j=1}^{n} \frac{t^{e}_{i,j}}{t^{s}_{j}} \times F_j = \frac{\sum_{j=1}^{n} t^{e}_{i,j}}{\sum_{j=1}^{n} t^{s}_{j}} \tag{2}$$

2.2 资源节点历史交易信息已知

当节点信任值可以获取时,文中通过以下两个信任值得到对节点的综合评价:依据本地存储的交易记录得到的直接信任值;依据其他节点提供的交易记录得到的推荐信任值。最后对两者进行综合得到对节点的评价。

2.2.1 直接信任值

直接信任值来自于节点之间直接的交互经验,节点通过与其他的节点直接进行交易并对其进行评价,采用一种方法计算出一个数值表示对其的信任程度。

大多数信任模型在计算直接信任值时仅采用用户满意度作为参数,文中考虑到移动 P2P 网络中节点移动或加入退出网络频繁的特性,若交易时间过长,便会存在节点移动出通信范围或退出网络的可能,从而导致交易失败。因此文中将节点资源传输速度作为交易的风险因子。节点 i 对节点 j 的直接信任值 Dt_{ij} 的计算公式如下:

$$\mathrm{Dt}_{ij} = \sum_{I(d)} \frac{T_n S_n(i,j)(1 - R_n)}{\sum_{I(d)} T_n} \tag{3}$$

其中,$S_n(i,j)$ 表示第 n 次交易时,节点 i 对节点 j 的满意程度,取值范围为[0,1];$I(d)$ 表示节点之间的交易次数;T_n 为第 n 次交易时的时间衰退因子,$T_n = \alpha^{\frac{t_c - t_n}{\Delta t}}$,$\alpha \in (0,1)$,$\Delta t$ 为两节点之间第一次交易时间与现在时间间隔,t_c 为当前交易的时间,t_n 为第 n 次交易的时间;R_n 为第 n 次交易时的风险因子,$R_n = \mathrm{e}^{-V_n}$,V_n 为第 n 次交易时资源提供节点的资源传送速率。

2.2.2 推荐信任值

在计算信任值时若只依据节点之间的直接信任值具有一定的片面性,甚至节点之间有可能是第一次交易,并不存在直接信任值,所以需要参考其他节点的推荐信任值。在大多数信任模型中,节点对于所获取的推荐信任值大致分为两种处理方式:依据推荐可信度剔除可信度低的节点的推荐信息;依据推荐信任值的相似性程度,相似性程度低于一定阈值的推荐信息不予考虑。然而在移动 P2P 网络中,这两种方式存在着一定的弊端。对于第一种方式,由于移动 P2P 网络中节点移动性强,很有可能发生节点之间交易次数非常有限的情况。若在这种情况下,假设节点 A 与 B 的推荐可信度均很高,但是如果节点 A 仅与节点 C 交易过一次,交易失败,A 对 C 信任值为 0;同时节点 B 与节点 C 交易 100 次,交易成功 99 次,B 对 C 的信任值会很高。由于两节点的推荐可信度均很高,两者的推荐信息均会被考虑,那么在计算推荐信任值时便会出现较大分歧。对于第二种方式同样存在上述情况,而且对于移动终端来说计算开销较大,同时在对抗共谋攻

击时容易失效。出现上述情况的主要原因是由于评价的不稳定性,在交易次数较少的情况下,虽然节点如实评价,但是评价并未稳定。在节点移动性强的移动 P2P 网络中,这种情况更是常见。所以文中采用的方法是综合所有节点的交易次数和交易满意次数,而不是仅仅综合所有节点的推荐信任值,即

$$\mathrm{Rt}_{ij} = \frac{\sum_{m \in s} n_{mj}}{\sum_{m \in s} N_{mj}} \tag{4}$$

其中,n_{mj} ,N_{mj} 分别是节点 m 与节点 j 之间交易满意次数和交易总次数;S 是与节点 j 有过交易的节点集合。

上述算法在理想情况下是完美适用的,即节点均如实报告自己的交易情况。但如果有恶意节点虚报交易次数(例如提高交易次数),便会主导推荐信任值的计算结果。所以文中首先需要确定可信推荐节点集,文中参考在社交网络中,人们倾向于相信与自己身份相近的人的评价信息。假设 A 与待评价的 B 为陌生人关系,那么 A 会更相信与 B 为陌生关系的其他人的评价,而不是 B 好友对其的评价,即两者与待评价节点之间的熟悉程度差异越小,评价信息越易被接受。文中选取节点之间的交易次数、交易频率、交易环境作为衡量节点之间熟悉程度的因素,例如节点 i,j 之间的熟悉程度可形式化定义为 $\boldsymbol{C}_{ij} = < N_{ij}, t_{ij}, s_{ij} >$,节点 m,j 之间的熟悉程度则为 $\boldsymbol{C}_{mj} = < N_{mj}, t_{mj}, s_{mj} >$,则节点 i,m 与节点 j 之间的熟悉度差异 σ_{im} 可以用向量的余弦相似度表示,公式如下:

$$\sigma_{im} = \frac{\boldsymbol{C}_{ij} \cdot \boldsymbol{C}_{mj}}{\| \boldsymbol{C}_{ij} \| \cdot \| \boldsymbol{C}_{mj} \|} \tag{5}$$

其中,$\boldsymbol{C}_{ij} \cdot \boldsymbol{C}_{mj}$ 表示 $\boldsymbol{C}_{ij}$ 和 $\boldsymbol{C}_{mj}$ 的内积;$\| \boldsymbol{C}_{ij} \|$ 和 $\| \boldsymbol{C}_{mj} \|$ 是取模运算;σ_{im} 表示节点 i,m 对于节点 j 的熟悉程度的差异。N_{ij} 和 N_{mj} 分别是节点 i,m 与节点 j 之间的交易次数;t_{ij} 和 t_{mj} 是节点 i,m 与节点 j 的交易频率;s_{ij} 和 s_{mj} 表示与节点 j 交易时环境对于节点 i,m 的重要程度。则对于节点 i 来说,可信推荐节点的集合为 $T_i = \{ m \mid \sigma_{im} \geqslant \lambda \}$,其中 λ 为常数。推荐信任值计算公式更新为:

$$\mathrm{Rt}_{ij} = \frac{\sum_{m \in T_i} \sigma_{mj} n_{mj}}{\sum_{m \in T_i} N_{mj}} \tag{6}$$

式(6)表明,当节点 i,m 对于节点 j 的熟悉程度越相似时,节点 m 的推荐信息越易被 i 所接受。

2.2.3　综合信任值计算

根据前文计算得到的直接信任值和推荐信任值进行综合,便可得到综合信任值,计算公式如下:

$$\mathrm{Ct}_{ij} = \alpha\ \mathrm{Dt}_{ij} + \beta\ \mathrm{Rt}_{ij} \tag{7}$$

其中,Dt_{ij} 为直接信任值;Rt_{ij} 为推荐信任值;$\alpha + \beta = 1$,α,β 分别反映了服务请求者对直接信任和推荐信任的采信比重。

参考在人类社会中人们更倾向于相信稳定的信息,文中利用变异系数来衡量信任值的稳定程度。首先计算直接信任值和推荐信任值的变异系数 $V = \sigma/\chi$。其中,σ 为信任值的标准差;χ 为信任值的平均数;V 值越大代表信任值差异越大,越不稳定,则权重的计算公式如下:

$$\alpha = \frac{V_{\mathrm{T}}}{V_{\mathrm{D}} + V_{\mathrm{T}}} \tag{8}$$

$$\beta = \frac{V_{\mathrm{D}}}{V_{\mathrm{D}} + V_{\mathrm{T}}} \tag{9}$$

其中,V_{D},V_{T} 分别是直接信任值和推荐信任值的变异系数。上式表明当直接信任值差异较大时,则推荐信任值占较高权重;推荐信任值差异较大时,则直接信任值占更高的权重。

3　仿真与分析

3.1　仿真环境及参数设置

为了评估模型在信任信息缺失情况下的性能及抵抗共谋攻击的作用,文中采用 PeerSim 软件,以文件共享为场景进行仿真,同时选择在抗共谋攻击方面效果较好的 MGT 模型进行比较,仿真参数设置见表 1。

表 1　仿真参数

参数	描述	参数值
N	网络节点总数	100
n	网络环境区分种类	4
F_j	不同环境所占权重	{0.1,0.2,0.3,0.4}
R_{s}	恶意节点对陌生节点表现恶意行为的概率/%	100
R_{f}	恶意节点对友好节点表现恶意行为的概率/%	0
λ	可信推荐节点集的阈值	0.5
V	节点传输数据速度/(kB/s)	[300,400]

3.2　仿真实验及分析

3.2.1　节点历史交易信息未知仿真

首先对模型在节点信任值未能获取时文件的下载成功率进行仿真,在本次仿真中模型假设节点与恶意节点越熟悉,恶意节点对其进行攻击(例如诋毁、传送虚假文件等)的可能性越低。则仿真实验结果如图 1 所示。从图中可以看出,在恶意节点比例在 30% 和 50% 的情况下,STTM 下的文件下载成功率均维持在一个较高水平,而 MGT 则是下载成功率较低且差异较大。原因在于 MGT 模型是多粒度的,节点对其他节点的信任值计算不仅依赖于交易历史,还依赖于终端相似性、终端能力等方面。在节点之间未有过交易经历时,节点的直接信任值则是依赖于对方节点的终端能

力等客观因素,恶意节点便有可乘之机。STTM 模型则是不依赖于客观因素,利用人类社会中社会信任的概念选择节点进行交易,而节点间的社会信任则是恶意节点难以伪造的。

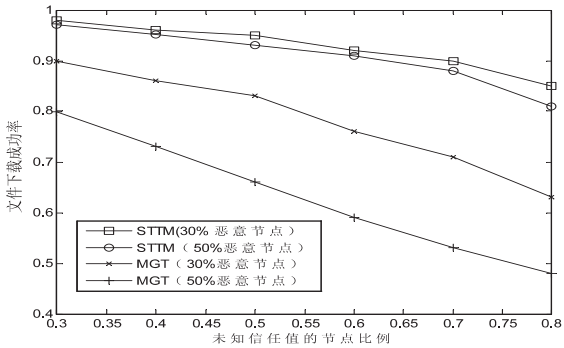

图 1 未知信任值节点的比例变化下文件成功率

3.2.2 恶意节点共谋行为仿真

共谋行为指的是恶意节点之间互相串通,对共谋团体内节点给予正反馈,而对其他节点进行诋毁。仿真实验结果如图 2 所示。

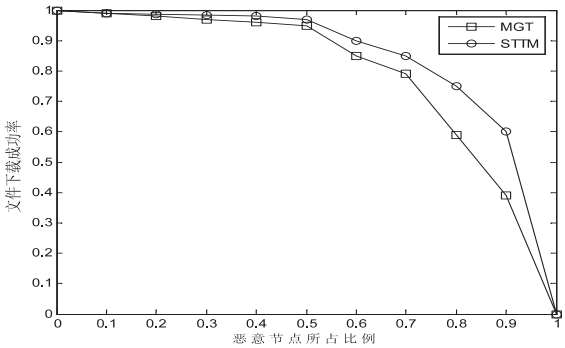

图 2 恶意节点(共谋)比例变化下文件下载成功率

从图 2 中可以看出,当恶意节点的比例低于 40% 时,两种模型的交易成功率均维持在较高水平。当恶意节点比例高于 50% 时,STTM 对恶意节点的共谋行为的抑制作用更加明显,交易成功率更高。原因在于 MGT 依赖于推荐可信度筛选可信节点,但是推荐可信度计算公式不能够阻止恶意节点通过多次小额交易提高自身的推荐可信度。STTM 则是通过计算节点间的熟悉程度差异筛选出可信推荐节点,恶意节点无法获知请求节点与待评价节点的熟悉程度,因此恶意节点不能通过虚报自身信息进入可信推荐节点集,便无法干预推荐信任值的计算。同时本模型在计算推荐信任值时不依赖于推荐节点提供的推荐信任值,而是统计可信节点的交易记录,这样可以避免由于交易次数较少而导致推荐信任值的不稳定,从而使得推荐信任值更加精确。

4 结束语

文中提出一种基于社会信任补充的信任模型 STTM。该模型在资源节点信任信息未能获取时,利用社会信任作为补充来判断节点的可靠性;在信任信息能够获取时,将信任值分为直接信任值和推荐信任值两部分,计算直接信任值时考虑交易速率作为风险因子;计算推荐信任值时使用向量定义节点之间的熟悉程度,通过余弦相似度计算出节点之间的熟悉度差异,依此筛选出可信推荐节点,最后统计可信推荐节点的交易记录;综合信任值时,利用变异系数法使得更为稳定的信任值具有更高的权重,从而保证综合信任值的稳定性与可靠性。STTM 在计算推荐信任值时利用熟悉程度差异来筛选可信推荐节点,而节点之间的熟悉程度只有节点自己可知,所以恶意节点很难通过伪造交易信息来进入其他节点的可信推荐节点集,从而避免了恶意诋毁和共谋行为的出现。

参考文献:

[1] 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.

[2] 李景涛,荆一楠,肖晓春,等. 基于相似度加权推荐的 P2P 环境下的信任模型[J]. 软件学报,2007,18(1):157-167.

[3] 田春岐,邹仕洪,王文东,等. 一种基于推荐证据的有效抗攻击 P2P 网络信任模型[J]. 计算机学报,2008,31(2):270-281.

[4] 胡建理,周 斌,周 瑜,等. 一种激励相容的 P2P 信誉模型[J]. 计算机科学,2011,38(9):59-63.

[5] 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.

[6] 王 勇,候 洁,白 杨,等. 基于反馈相关性的 P2P 网络信任模型[J]. 计算机科学,2013,40(2):103-107.

[7] Rathnayake U,Sivaraman V,Boreli R. Environmental context aware trust in mobile P2P networks[C]//Proc of IEEE 36th conference on local computer networks. [s. l.]:IEEE,2011:324-332.

[8] 任 艳,任平安,吴振强,等. 移动 P2P 网络中的多粒度信任模型[J]. 计算机工程与应用,2009,45(6):137-140.

[9] 李致远,王汝传. 一种移动 P2P 网络环境下的动态安全信任模型[J]. 电子学报,2012,40(1):1-7.

[10] 杨志兴,汤红波,柏 溢,等. 移动 P2P 分布式信任模型设计[J]. 计算机工程与应用,2013,49(23):75-80.

[11] 冯景瑜,张玉清. 构造移动 P2P 环境下的分布式信任模型[J]. 网络安全技术与应用,2011(4):73-76.

[12] 曹晓梅,朱海涛,沈何阳,等. MP2P 网下一种基于代理的安全反馈信任模型[J]. 计算机科学,2014,41(7):200-205.

[13] Wu Xu. A distributed trust management model for mobile P2P networks[J]. Peer-to-Peer Networking and Applications,2012,5(2):193-204.

[14] Basit Q,Geyong M. A distributed reputation and trust management scheme for mobile Peer-to-Peer networks[J]. Computer Communications,2012,35(5):608-618.

移动P2P环境下基于社会信任补充的信任模型

作者： 王健， 曹晓梅， WANG Jian， CAO Xiao-mei
作者单位： 南京邮电大学 计算机与软件学院，江苏 南京 210003；江苏无线传感网高技术研究重点实验室，江苏 南京 210003；宽带无线通信与传感网技术教育部重点实验室，江苏 南京 210003

刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(9)