

P2P网络中基于改进DyTrust的信任模型

赵治国,陈琼,谭敏生

(南华大学 计算机科学与技术学院,湖南 衡阳 421001)

摘要:为了动态提升P2P网络的适应性、可靠性和可信度,在DyTrust信任模型的基础上,考虑到风险因素和时间因素对P2P网络节点信任的影响,引入一个基于服务质量的风险函数和时间衰减因子 ω ,提出一种适合P2P复杂环境的信任模型。实验结果表明,相比现有信任模型,文中研究的P2P网络信任模型具有更好的动态自适应能力、更强的恶意节点检测能力,以及更优越的反馈信息聚合能力,对P2P网络的安全提供有力保障。

关键词:P2P网络;DyTrust信任模型;P2P网络信任模型

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2014)10-0174-04

doi:10.3969/j.issn.1673-629X.2014.10.042

Trust Model Based on Improved DyTrust in P2P Network

ZHAO Zhi-guo, CHEN Qiong, TAN Min-sheng

(School of Computer Science and Technology, University of South China,
Hengyang 421001, China)

Abstract: In order to dynamically improve the adaptability, validity and reliability of P2P Network, based on DyTrust trust model, considering the influence of risks and time on the trust of P2P network node, a risk function and a reduction time factor ω is introduced based on service quality, propose a trust model adapted to P2P network. The simulation experiment proves that compared with current model, P2P network trust model can provide safeguard with P2P network safety because it has better dynamic self-adaptability, better ability to check the malicious peers, and better advantage to aggregate feedback information.

Key words: P2P network; DyTrust trust model; P2P network trust model

0 引言

随着网络技术的发展,P2P网络的应用已非常广泛。由于P2P网络的分布性、开放性、动态性以及节点的匿名性和自治等特点,使得恶意节点可以随意滥用网络资源,传播木马和蠕虫,提供虚假信息,产生大量的欺骗行为和不可信任的服务,从而造成节点之间缺乏足够的安全信任,给P2P网络带来了许多安全问题,严重制约了P2P网络的进一步发展^[1-2]。可信度是衡量P2P网络安全问题的主要因素,也是客户节点选择服务节点的主要依据^[3]。可信度的计算主要通过构建相应的信任模型^[4],目前,P2P网络的安全可信问题正被越来越多的研究者关注,分别应用不同的理论和方法研究P2P网络的信任机制,提出一些信任模型以提高P2P网络的可信度^[5-6]。但网络的脆弱性不能完全消除,网络系统不存在完全安全,而可信网

络就是要主动检测攻击行为并能遏制其发生,增加网络行为可信,强化动态处理网络状态的能力。文中以DyTrust信任模型为基础,研究一种适应P2P网络复杂环境的信任模型,遏制P2P网络中的各种恶意节点行为,以提高P2P网络的可信度。

1 相关研究工作

为遏制P2P网络中的恶意节点行为、提高节点和服务的可靠性,近年来国内外学者在P2P网络的安全信任方面作了大量的研究工作,取得了一定的研究成果。文献[7]提出基于时间帧的动态信任模型DyTrust,使用近期信任、长期信任、累积滥用信任和反馈机制的动态调节,提高了信任模型的动态适应能力,对动态恶意节点的行为和虚假反馈的攻击能有效处理,增强了信任模型的动态适应能力和反馈信息有

收稿日期:2013-12-03

修回日期:2014-03-13

网络出版时间:2014-07-28

基金项目:湖南省高等学校科学研究优秀青年项目(12B110)

作者简介:赵治国(1977-),男,硕士,讲师,研究方向为计算机网络安全和P2P网络。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20140728.1226.031.html>

效聚合能力。为了提高 DyTrust 模型信任评价的准确性,解决信任模型的粗糙粒度与节点个体经验对信任评价带来的影响问题,文献[8]对 DyTrust 信任模型进行了改进,通过对节点所提供的服务进行细化和引入经验因子,精化信任算法的粒度,提高信任评价的准确度,体现了节点的个性化特性。文献[9]提出基于相似度加权的 WRTrust 模型,对于大型 Peer to Peer 网络中恶意节点的协同作弊行为有一定的识别和遏制力。文献[10]提出了基于品质和能力的信任模型,利用品质和能力的值作为模型中的评价向量,采用基于支持度的算法进行推荐信息的整合,有效地遏制共谋和诋毁等恶意行为。文献[11]提出了一种基于节点行为相似度的共谋团体识别模型,通过分析节点之间的行为相似度有效地检测出恶意行为共谋团体。文献[12]提出了一个基于时间窗的局部信任模型,通过反馈控制机制动态调节信任、信誉与激励三个参数,提高信任模型的动态适应能力和更好地处理恶意节点策略性动态变化行为和不诚实反馈对系统的攻击。文献[13]为解决 P2P 网络中节点的不合作行为和恶意攻击等问题,提出了一种分布式兴趣信任模型(DITM),通过划分兴趣域聚集兴趣相似的节点来解决节点间因兴趣不对称难以建立直接信任关系的问题,能有效抵御恶意节点针对特定兴趣域的攻击,并能激励好节点在多个域内贡献资源。文献[14]提出一种基于偏差因子的信任模型(TMDF),通过构造多维评价向量,参考社会网络中信任关系的建立方法,引入偏差因子计算推荐节点的可信度,再根据推荐信任和直接信任计算综合可信度,对抵制诋毁、共谋等恶意行为具有良好的抗攻击性能。

信任和风险有着非常紧密的联系,现有的研究工作大多忽略了风险因素对节点信任的影响。文中以 DyTrust 模型为基础,引入风险函数和时间衰减因子对其信任算法进行改进,能够较好地解决 P2P 网络信任问题以及有效地检测和惩罚恶意节点的行为。

2 P2P 网络信任模型

2.1 风险函数

在 P2P 网络中,节点所请求的服务质量越高,其风险可能就越大;所请求的服务质量越低,风险可能就越小^[15],因此,文中依据服务质量来定义风险函数。节点请求的服务质量分别定义为五个级别:服务质量最差的设为 I 级,服务质量值为 0~0.2;服务质量较差的设为 II 级,服务质量值为 0.2~0.4;服务质量一般的设为 III 级,服务质量值为 0.4~0.6;服务质量较高的设为 IV 级,服务质量值为 0.6~0.8;服务质量很高的设为 V 级,服务质量值为 0.8~1^[15],如公式(1)

所示:

$$S_{ij} = \begin{cases} s_5, & 0.8 < s_5 \leq 1 \\ s_4, & 0.6 \leq s_4 \leq 0.8 \\ s_3, & 0.4 \leq s_3 < 0.6 \\ s_2, & 0.2 \leq s_2 < 0.4 \\ s_1, & 0 \leq s_1 < 0.2 \end{cases} \quad (1)$$

风险函数如公式(2)所示:

$$\varphi_{ij}^n = \sum S_{ij} \times (1 - R_{ij}^n) \quad (2)$$

其中, S_{ij} 表示节点*i*对节点*j*在交互过程中所请求的服务质量值; R_{ij}^n 表示节点*i*对节点*j*在时间*n*-1内的信任评价; φ_{ij}^n 表示节点*i*对节点*j*在*n*-1时间帧内交互过程中所请求服务质量的风险值。

根据公式(1)和公式(2)计算节点所请求的服务质量的风险值,如果以前已获得了较高的信任值,那么现在所面临的风险就会较小。

2.2 直接信任模型

DyTrust 模型的直接信任算法用 D_{ij}^n 表示第 *n* 个时间帧 *i* 节点对 *j* 节点的直接信任值,用 e_{ij} 表示本次事务交互中 *i* 节点对 *j* 节点所提供服务的满意度评价,其值范围为 $0 \leq e_{ij} \leq 1$ ^[6]。当节点 *i* 与节点 *j* 在时间帧 *n* 内进行了 *m* 次交互,DyTrust 模型采用求平均值的方法计算节点 *i* 对节点 *j* 的直接信任值 $R(i,j)$ 。由于可信度的影响与服务满意度评价时间点离现在的时长紧密相关,那么这种计算方法会产生一定影响:当服务满意度评价时间点离现在越近,对可信度的影响会更大,越久的服务满意度对当前可信度的影响则非常小。所以,在 P2P 网络信任模型中,计算直接信任值不采用这种方法,而是引入一个时间衰减因子 ω ,使评价更有效性和准确性。其计算方法如公式(3)和公式(4)所示。

$$\omega = \frac{2 \times k}{m \times (m + 1)}, k = 1, 2, \dots, m \quad (3)$$

$$D_{ij}^n = \sum \omega \cdot e_{ij} \quad (4)$$

该直接信任值的计算方法充分考虑到信任值的时效性,即时间对信任值的影响,最近产生的服务评价对当前信任值的影响比较大,即第 *m* 次交互的服务评价在计算信任值时其权值最大,而时间久远的服务评价对当前信任值的影响较小,即权值也较小,从而提高 P2P 网络信任模型的动态自适应能力。

综合考虑近期信任函数 ST_{ij}^n 、长期信任函数 LT_{ij}^n 以及风险函数 $1 - \varphi_{ij}^n$,选择 $ST_{ij}^n, LT_{ij}^n, 1 - \varphi_{ij}^n$ 三个值中最小的作为最终信任评估结果 T_{ij}^n ,其公式为:

$$T_{ij}^n = \min(ST_{ij}^n, LT_{ij}^n, 1 - \varphi_{ij}^n) \quad (5)$$

3 实验及其结果分析

实验采用 PeerSim 仿真工具,实验参数设置与原模型相同,根据节点提供的服务方式将其分为三种:先不合作后合作交互方式、先合作后不合作交互方式、时而合作时而而不合作交互方式,其中,交互数目的阈值 H 设为 30。

(1) 先不合作后合作交互方式

这种交互方式是指节点在事务交互时,先不合作,在交互进行一段时间后打算通过合作来提高其信任值。对于这种交互方式,将 DyTrust 信任模型与 P2P 网络信任模型进行了对比实验,实验结果如图 1 所示。

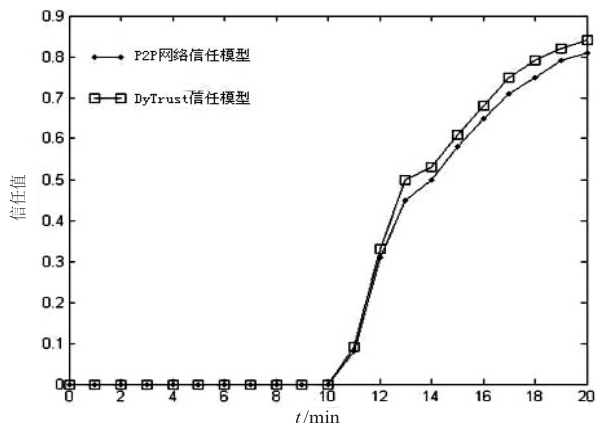


图1 先不合作后合作交互方式

实验结果表明:P2P 网络信任模型对于先不合作后合作交互方式的节点,其信任值提升速度比 DyTrust 信任模型慢,即其建立信任更加缓慢;P2P 网络信任模型比 DyTrust 模型需要更长时间的真实交互才能获得较高的信任。因此,P2P 网络信任模型检测该种恶意节点的能力更强。

(2) 先合作后不合作交互方式

这种交互方式是指节点在进行事务交互时,先通过合作,当拥有较好的信任关系而获得较高的信任值后马上不合作。对于此种恶意交互方式,将 DyTrust 信任模型与改进的 P2P 网络信任模型进行了对比实验,实验结果如图 2 所示。

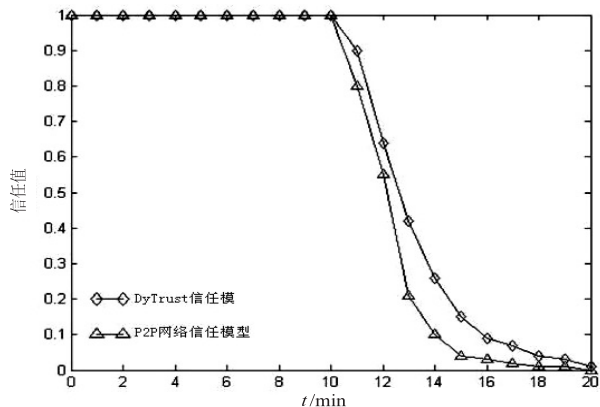


图2 先合作后不合作交互方式

实验结果表明:P2P 网络信任模型对这种交易方式的反应比 DyTrust 信任模型更为敏感,其信任值下降更快,使长时间不合作的节点想恢复其信任值到 1 需要更长时间,因此,能够有效地降低这种先合作后不合作的静态恶意节点带来攻击的危害。

(3) 时而合作时而而不合作交互方式

这种交互方式是指节点在事务交互进行时,时而而不合作,时而合作,表现出周期性规律,并在时间上存在约为 1:3 的比例关系。对于这种恶意摇摆交互方式,将 DyTrust 信任模型与 P2P 网络信任模型进行了对比实验,实验结果如图 3 所示。

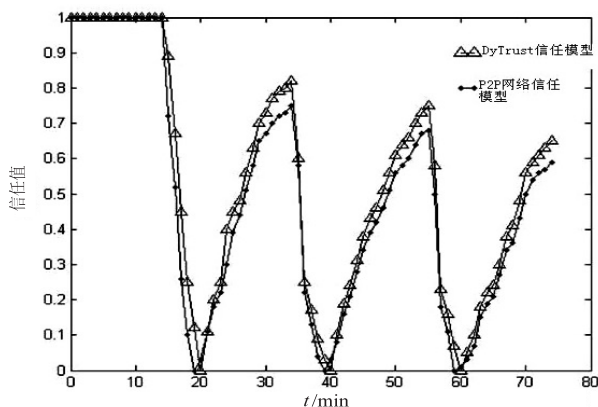


图3 时而合作时而而不合作交互方式

实验结果表明:P2P 网络信任模型能更快速响应与检测出节点恶意摇摆行为的变化。两种信任模型对节点不断摇摆的恶意交易行为都进行了惩罚,使其信任值的降低速度比增加速度快。由于 P2P 网络信任模型引入了风险函数,对有规律改变行为方式的动态恶意节点的惩罚更加快速和严厉,并随节点滥用信任的不断增加,原有信任值的恢复比 DyTrust 信任模型更慢,节点间需要更长时间的成功事务交易才能逐渐恢复其信任值。

针对两种模型的信息聚合能力,通过单个虚假反馈和协同虚假反馈对事务失败率的影响对两种信任模型进行对比实验。实验结果如图 4 和图 5 所示。

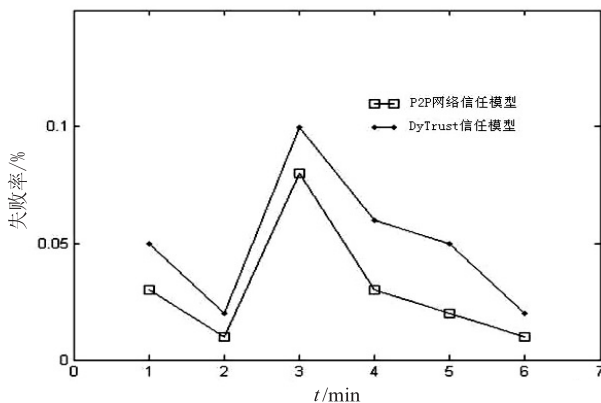


图4 单个虚假反馈的事务交互失败率

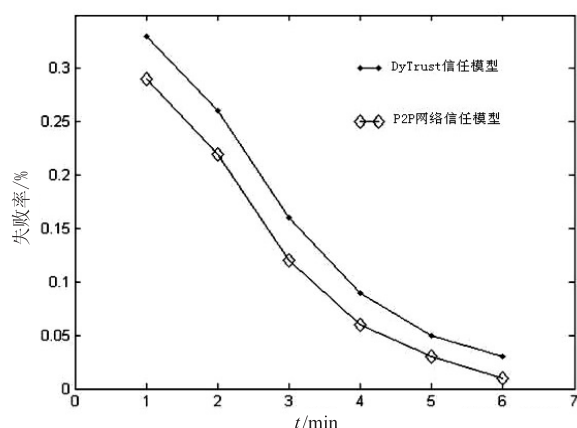


图 5 协同虚假反馈的事务交互失败率

无论是单个虚假反馈还是协同虚假反馈,两种模型节点的事务失败率下降得都比较快,但 P2P 网络信任模型的下降速度比 DyTrust 信任模型要更快,并随着时间的推移,二者的失败率都向 0 靠近。因此,可以看出,P2P 网络信任模型比 DyTrust 信任模型能极大地提高事务交互的成功率。同时,由于协同虚假反馈的隐蔽性高,需要较长时间的交互才能分辨出节点是否为恶意节点,因此,单个虚假反馈的事务失败率的下降速度都比协同反馈的事务失败率下降的更快。

针对节点先进行合作,后出现虚假反馈的协同虚假反馈的情况,对 P2P 网络信任模型与 DyTrust 信任模型进行了实验比较。实验结果如图 6 所示。

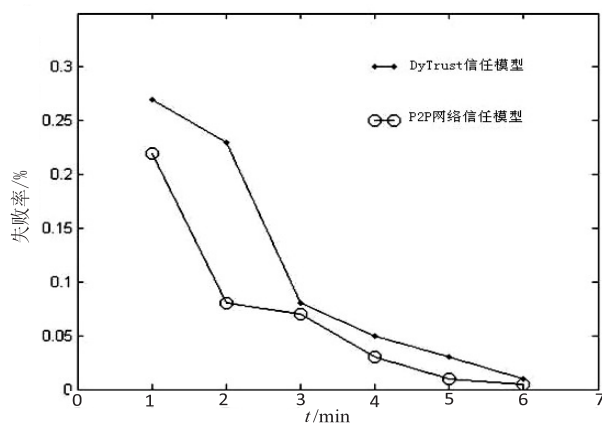


图 6 事务失败率

由图中可知,P2P 网络信任模型能更快地减少策略性提供反馈的虚假节点对事务成功率的影响,对虚假反馈灵敏度更大,适应能力更强。

4 结束语

文中在 DyTrust 模型基础上,结合 P2P 网络的复杂环境,考虑到风险因素和时间因素对 P2P 网络节点信任的影响,引入一个基于服务质量的风险函数和时

间衰减因子,对 DyTrust 模型进行了改进,提出了一种适应 P2P 网络的 P2P 信任模型。采用 PeerSim 仿真工具进行了仿真实验,实验结果表明,相比现有的信任模型,P2P 网络信任模型具有更好的动态自适应能力和更强的检测恶意节点的能力,为 P2P 网络的安全提供有效的保障。

参考文献:

- [1] Liang Zhengqiang, Shi Weisong. PET: a personalized trust model with reputation and risk evaluation for P2P resource sharing [C]//Proceedings of 38th international conference on system science. Hawaii, USA: [s. n.], 2005: 201-211.
- [2] Wang Yan, Lin Furen. Trust and risk evaluation of transactions with different amounts in peer-to-peer e-commerce environments [C]//Proc of IEEE international conference on e-business engineering. Shanghai: IEEE, 2006: 102-109.
- [3] 郑光勇,任晓慧,李肯立. P2P 中一种改进的可信模型[J]. 计算机工程与科学, 2008, 30(3): 7-10.
- [4] 李健,胡峰松,黄晗文,等. P2P 网络信任模型研究[J]. 计算技术与自动化, 2009, 28(2): 124-127.
- [5] Theodorakopoulos G, Baras J S. On trust models and trust evaluation metrics for ad-hoc networks[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 318-328.
- [6] Li Xiong, Liu Ling. PeerTrust: supporting reputation-based trust in peer-to-peer electronic communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857.
- [7] 常俊胜. 虚拟计算环境下基于信誉的信任管理研究[D]. 长沙:国防科学技术大学, 2008.
- [8] 王少杰,陈红松,郑雪峰,等. 一种改进的 DyTrust 信任模型[J]. 北京科技大学学报, 2008, 30(6): 685-689.
- [9] 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.
- [10] 田俊峰,蔡红云. 信任模型现状及进展[J]. 河北大学学报(自然科学版), 2011, 31(5): 555-560.
- [11] 苗光胜,冯登国,苏璞睿. P2P 信任模型中基于行为相似度的共谋团体识别模型[J]. 通信学报, 2009, 30(8): 9-20.
- [12] 石志国,刘冀伟,王志良. 基于时间窗反馈机制的动态 P2P 信任模型[J]. 通信学报, 2010, 31(2): 120-129.
- [13] 杨莉,张毓森,邢长友,等. P2P 环境下基于兴趣的分布式信任模型[J]. 东南大学学报(自然科学版), 2011, 41(2): 242-246.
- [14] 潘春华,朱同林,殷建军,等. 基于偏差因子的 P2P 网络信任模型[J]. 北京邮电大学学报, 2011, 34(3): 89-93.
- [15] 陈琼. 基于改进的 DyTrust 信任模型的网络信任度评估研究[D]. 衡阳:南华大学, 2012.

P2 P网络中基于改进DyTrust的信任模型

作者：赵治国， 陈琼， 谭敏生， ZHAO Zhi-guo, CHEN Qiong, TAN Min-sheng

作者单位：南华大学 计算机科学与技术学院, 湖南 衡阳, 421001

刊名：计算机技术与发展

英文刊名：Computer Technology and Development

年，卷(期)：2014(10)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjz201410043.aspx