

GBTM:一种 P2P 系统中基于群组的信任模型

张少娴, 俞 琼

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要:目前在 P2P 网络中,缺乏有效的机制来提高系统的安全性,存在许多恶意行为,信任模型已经成为 P2P 应用研究的一个重要课题。文中对基于信任机制的 P2P 网络进行研究,根据节点的兴趣、爱好建立不同群组,节点总体信任度由节点之间直接信任度、组与节点之间信任度、组间信任度以及多重参数合成,并通过针对诋毁恶意节点攻击、协同作弊攻击两种不同的攻击模式下的仿真实验表明,该模型具有较高的下载成功,并且能使节点负载处于可控范围内。

关键词:对等网络;信誉;信任模型;安全

中图分类号:TP393.07

文献标识码:A

文章编号:1673-629X(2012)03-0249-04

GBTM: A Group-Based Trust Model for P2P Systems

ZHANG Shao-xian, YU Qiong

(School of Computer, Nanjing University of Posts and Telecommunication, Nanjing 210003, China)

Abstract: Due to lack of effective mechanisms to improve the security performance of the system, there are a lot of malicious behaviors in P2P network. So, the trust model is an important research topic for the P2P application. It conducts the research on P2P network based on the trust model and divides different groups by the interest between peers. In this model, the global trust value can be computed by combining the trust value in direct peer, in interest group, between interest groups and multiple control factors. Through the simulation experiment, this model is verified to have high ratio of successful download, and the peer load can be controlled in a admissible range.

Key words: peer-to-peer; reputation; trust model; security

0 引言

P2P 网络因其资源共享、节点的对等通信及网络灵活自组织的特性得到了迅速地发展^[1]。但由于 P2P 网络的匿名性、开放性等本质特点,系统中不可避免地存在大量的欺诈等恶意行为,因此,建立一个有效的、安全的信任机制就显得尤为重要^[2]。可以这样下个定义,信任模型就是通过某种策略建立一整套量化的评价体系,给出欲交易节点的可信度地评价,并将这个评价告知给网络中其它的节点^[3]。

目前,国内外相关研究很多,比较著名的有斯坦福大学的 Kamvar 等人提出的显式管理 P2P 网络用户声誉的 EigenTrust 算法^[4],发表于 2003 年的服务与电子商务社群、基于声誉的 PeerTrust 信任模型^[5]以及文献[6,7]提出的信任模型。世界计算机领域最有影响力的几大组织和公司,比如 ACM、IEEE、Microsoft、IBM、HP 等都有人员从事这方面地研究。国内,南京大学的陈贵海教授^[8]、国防科学技术大学窦文^[9]等人也在此

领域做了大量的研究工作。

参考人类的社会管理方式,人不是单个存在的个体,都具有社会性,总是按照一定的策略(比如兴趣、爱好)形成一个个群组,再由这些群组构成人类社会。每个人在他所在的群组中都有一个被信任度,群组和群组之间也会相互评价对方的信任度。基于人类社会这种管理模式,文中提出了基于群组的信任模型 GBTM,根据节点的兴趣、爱好建立不同群组,节点总体信任度由节点之间直接信任度、组与节点之间信任度、组间信任度以及多重参数合成。

1 相关定义

参考文献[10~13]中信任模型的表示方法,定义如下:

定义 1 令 $Tr_{G_i G_j}$ 为群组 G_i 对群组 G_j 的信任值,则

$$Tr_{G_i G_j} =$$

$$\begin{cases} \beta^{S_{G_i G_j} + F_{G_i G_j}} \left(\frac{S_{G_i G_j} - F_{G_i G_j}}{S_{G_i G_j} + F_{G_i G_j}} \right), S_{G_i G_j} + F_{G_i G_j} \neq 0 \text{ 且 } 0 < \beta < 1 \\ Tr_{G_i G_j}^{reference}, F_{G_i G_j} + S_{G_i G_j} = 0 \text{ 且存在 Trust}_{G_i G_j}^{path} \\ Tr_{G_i G_j}^{strange} \end{cases}$$

其中 $S_{G_i G_j} \geq 0$ 为群组 G_i 中节点与 G_j 中节点交易成

收稿日期:2011-08-02;修回日期:2011-11-05

基金项目:江苏省高校自然科学基金项目(08KJB620002)

作者简介:张少娴(1972-),女,讲师,硕士,研究方向为数据库、信息安全。

功的次数, $F_{G_i} \geq 0$ 为 G_i 中节点与 G_j 中节点交易失败的次数, 当 $F_{G_i} + S_{G_i}$ 不等于 0 时, 说明两个群组发生过交易, $\beta \frac{1}{F_{G_i} + S_{G_i}}, 0 < \beta < 1$ 称为交易次数权重因子。当 $F_{G_i} + S_{G_i}$ 为 0 时, 如果两个群组间存在信任路径, 按照最强路径原则计算群组 G_i 对群组 G_j 的推荐值 $Tr_{G_i}^{reference}$; 否则, G_i 根据陌生群组的表现给定对 G_j 的信任值 $Tr_{G_i, strange}$ 。

定义 2 陌生群组信任值:

$$Tr_{G_i, strange} = \begin{cases} \frac{S_{G_i, strange} - F_{G_i, strange}}{S_{G_i, strange} + F_{G_i, strange}}, S_{G_i, strange} + F_{G_i, strange} \neq 0 \\ 0, \text{其它} \end{cases}$$

其中, $S_{G_i, strange} \geq 0$ 和 $F_{G_i, strange} \geq 0$ 分别表示 G_i 与陌生群组 $G_{strange}$ 交易成功和失败的次数。

定义 3 令 $Tr_i^{G_i}$ 为 G_i 对 i 的信任值, 则

$$Tr_i^{G_i} = \begin{cases} \frac{S_i^{G_i} - F_i^{G_i}}{S_i^{G_i} + F_i^{G_i}}, S_i^{G_i} + F_i^{G_i} \neq 0 \\ Tr_{strange}^{G_i}, S_i^{G_i} + F_i^{G_i} = 0 \end{cases}$$

其中, G_i 为节点 i 所属群组, $S_i^{G_i} \geq 0$ 和 $F_i^{G_i} \geq 0$ 分别为节点 i 与本群组内各节点交易成功与失败的次数, 由此可知 $Tr_i^{G_i}$ 仅在群组内部节点发生交易时改变。

定义 4 节点初始信任值:

$$Tr_{strange}^{G_i} = \begin{cases} \frac{S_{strange}^{G_i} - F_{strange}^{G_i}}{S_{strange}^{G_i} + F_{strange}^{G_i}}, S_{strange}^{G_i} + F_{strange}^{G_i} \neq 0 \\ 0, \text{其它} \end{cases}$$

$S_{strange}^{G_i} \geq 0$ 和 $F_{strange}^{G_i} \geq 0$ 分别为 G_i 内新加入节点与本群组内其它节点交易成功和失败的次数。

定义 5 令 Tr_{ij} 为节点 i 对 j 的信任值, 则

$$Tr_{ij} = \begin{cases} \beta \frac{1}{S_{ij} + F_{ij}} \left(\frac{S_{ij} - F_{ij}}{S_{ij} + F_{ij}} \right), S_{ij} + F_{ij} \neq 0 \text{ 且 } 0 < \beta < 1 \\ \frac{S_{strange}^i - F_{strange}^i}{S_{strange}^i + F_{strange}^i}, S_{ij} + F_{ij} = 0 \text{ 且 } S_{strange}^i + F_{strange}^i \neq 0 \\ 0, \text{其它} \end{cases}$$

Tr_{ij} 与群组间信任值定义类似: 其中 $S_{ij} \geq 0$ 和 $F_{ij} \geq 0$ 分别为节点 i 与节点 j 直接交易成功和失败的次数。同样地, Tr_{ij} 、 S_{ij} 和 F_{ij} 等均为由节点本地保存, β 值的设定可全局统一, 也可由节点自己设定以反映自己的选择取向。

2 信任信息更新

这里依然假设节点 i 与 j 发生交易, i 认为 j 提供服务成功和失败的次数分别为 S_{ij}' 和 F_{ij}' ; 则信任信息更新过程如下:

(1) 节点 i 与 j 属同一个群组时。

(a) 节点 i 本地信任信息更新: 如果在本地保存节点信任信息的数据结构 TList_i 队列找到 j 的有关信任值则按照前述定义直接更新; 如果找不到相应的信任信息, 就提交关于 j 的信任信息到该数据结构中, 更新 $S_{strange}^i$ 和 $F_{strange}^i$ 。然后按前述定义计算信任值; 在更新本地信任信息后, 节点 i 向 j 的档案节点汇报对 j 的反馈。

(b) 群组信任信息更新: j 的档案节点利用 TList 来保存相关节点信任信息, 根据上节过滤条件决定接受反馈信息后, 如 TList 已有 j 的信息, 则根据给出反馈信息的节点的可信度来加权更新信任信息:

$$S_j^{G(i)} = S_j^{G(i)} + Tr_i^{G(i)} S_{ij}', F_j^{G(i)} = F_j^{G(i)} + Tr_i^{G(i)} F_{ij}',$$

否则, 插入新的关于 j 的信任信息到队列中, 更新 $S_{strange}^{G(i)}$ 和 $F_{strange}^{G(i)}$ 。

(2) 节点 i 与 j 属不同群组时。

(a) 节点 i 本地信任信息更新: 方式与前述相同。

(b) $G(i)$ 群组信任信息更新: 根据过滤条件决定接受反馈信息后, 更新对 j 所在群组 $G(j)$ 的信任信息, 用队列 TList_{G_i} 来保存, 如 TList_{G_i} 已有 $G(j)$ 的信息, 则根据给出反馈信息的节点的可信度来加权更新信任信息:

$$S_{G(i)G(j)} = S_{G(i)G(j)} + Tr_i^{G(i)} S_{ij}',$$

$$F_{G(i)G(j)} = F_{G(i)G(j)} + Tr_i^{G(i)} F_{ij}'$$

否则, 插入新的关于 $G(j)$ 的信任信息到队列中, 更新 $S_{G(i)G(j)}$ 和 $F_{G(i)G(j)}$ 。同时向 $G(j)$ 发送 i 的交易反馈信息及本群组信任信息 $Tr_i^{G(i)}$ 。

(c) $G(j)$ 群组信任信息更新: 根据滤条件决定接受反馈信息后, 如 TList_j 已有 j 的信息, $G(j)$ 将根据 $Tr_{G(j)G(i)}$ 和 $Tr_i^{G(i)}$ 加权更新对 j 的信任信息:

$$S_j^{G(j)} = S_j^{G(j)} + C_i^{G(i)} S_{ij}', F_j^{G(j)} = F_j^{G(j)} + C_i^{G(i)} F_{ij}',$$

其中, $C_i^{G(i)} = \min\{Tr_i^{G(i)}, Tr_{G(j)G(i)}\}$ 。否则, 插入新的关于 j 的信任信息到队列中, 更新 $S_{strange}^{G(j)}$ 和 $F_{strange}^{G(j)}$ 。

3 仿真及结果分析

文中基于查询周期模拟器的原理对 GBTM 模型进行了仿真。同时, 为了对比, 文中也对传统的基于共享信息的信誉系统 (a Simple Reputation-Credit System, SRCS) 进行了仿真。在 SRCS 系统中, 结点 i 按下述定义计算节点 j 的信任值 Tr_{ij} 。

$$Tr_{ij} = \begin{cases} \left(\frac{S_{ij} - F_{ij}}{S_{ij} + F_{ij}} \right), S_{ij} + F_{ij} \neq 0 \\ Tr_{ij}^{reference}, F_{ij} + S_{ij} = 0 \text{ 且存在 Trust}_{ij}^{path} \\ Tr_{strange}, \text{其它} \end{cases}$$

其中, $Trust_{ij}^{path}$ 指节点 i 到节点 j 的信任路径, $Tr_{ij}^{reference}$ 为最强信任路径上的推荐信任值。 $S_{ij} \geq 0$ 和

$F_{ij} \geq 0$ 分别为节点 i 与节点 j 直接交易成功和失败的次数。 $Tr_{strange}$ 为一较小的正整数,全局统一,用来定义陌生节点的信任值。节点选择 Tr_{ij} 值最高的节点作为下载源。

文中在诋毁恶意节点攻击、协同作弊攻击两种不同的攻击模式下,对 GBTM 和 SRCS 这两种模型进行比较。

3.1 模拟实验

模拟实验包含了 1000 个节点,其中每个节点包含 10 个文件。在 GBTM 和 SRCS 系统中,本地可以保存最多十个节点的有关信任信息,节点所发出的信任请求消息的生存时间为 6。交易次数权重因子 β 为 0.8,另外,群组每隔 10 个周期对信任度进行衰减因子为 0.9 的衰减处理,使得信任度能比较真实地反映近期行为。

3.2 协同作弊攻击下的仿真及结果分析

恶意节点作为集团联合行动,协同作弊时,对网络会产生很大危害。在文中的仿真环境中,该类节点为与之有过交易的合作节点提供负面反馈,为请求下载的合作节点提供不可信文件,而夸大对特定节点的评价。在文中的仿真环境中,恶意节点可能彼此串通频繁提交对彼此过高的正面评价。

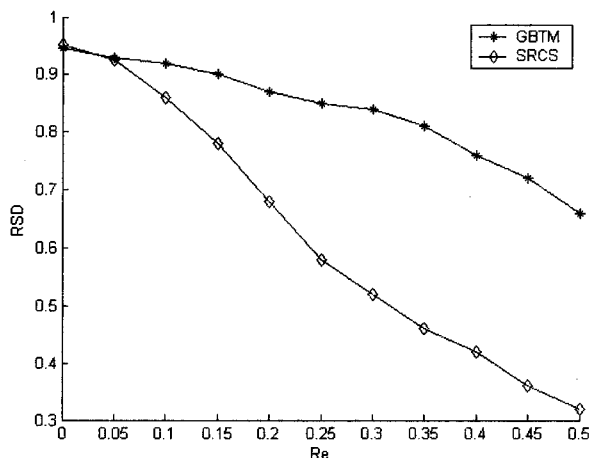


图1 不同恶意节点比例下的下载成功率(1)

如图1所示,给出了在不同恶意节点比例下,合作节点的下载成功率。可以看出,随着恶意节点比例地增加,下载成功率都有较为明显地下降,但 GBTM 要慢于 SRCS,当 Re 达到 0.5 时, RSD 仍保持在 0.67 附近。

图2给出了恶意节点比例 $Re=0.5$ 时, GBTM 和 SRCS 中的合作节点下载成功率随仿真周期的变化情况。可以看出 GBTM 仿真系统可快速进入稳定状态,系统性能还保持在一个可正常工作的情况,而 SRCS 的 RSD 则快速下降到 0.33 左右,系统基本被颠覆,这是因为 SRCS 简单地利用本地信任信息或节点推荐信息,并且对反馈信息不加甄别,在大量恶意节点的协同

作弊攻击下,节点已不能有效评估其它节点的信任信息,从而性能急剧下降。

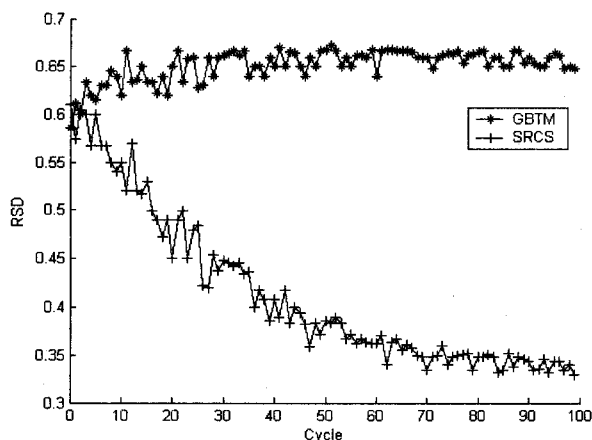


图2 $Re=0.5$ 时合作节点下载成功率(1)

3.3 诋毁恶意节点攻击下的仿真及结果分析

此类节点不仅提供不可信服务,而且对为其提供可信服务地合作节点做出不公正的负面评价,以期通过降低合作节点的可信度来破坏网络的可用性。

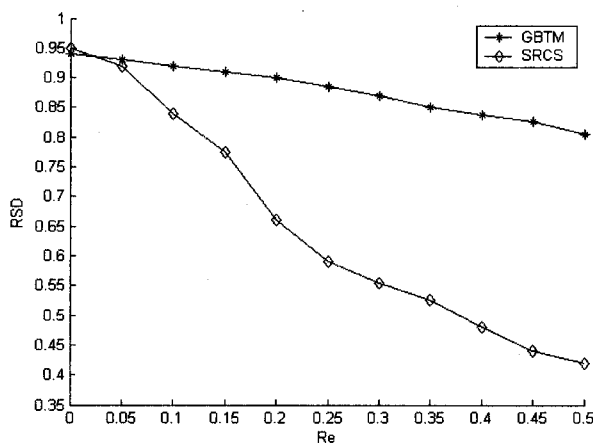


图3 不同恶意节点比例下的下载成功率(2)

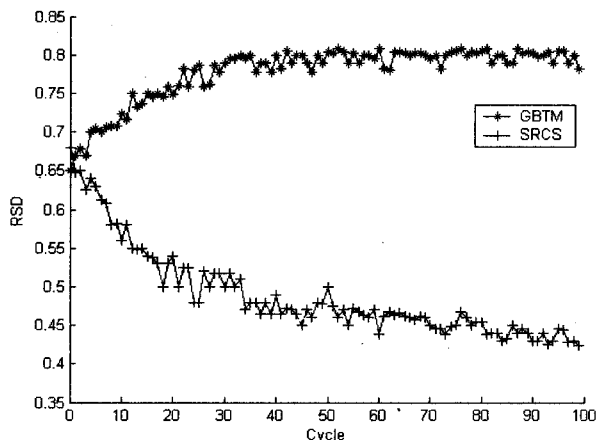


图4 $Re=0.5$ 时合作节点下载成功率(2)

从图3可以看出,随着恶意节点比例的增加, GBTM 的下载成功率下降缓慢,在 Re 达到 0.5 时, RSD 仍然维持在 0.8 左右,而 SRCS 系统的下载成功率则

随着恶意节点比例地增加迅速下降,说明诋毁恶意节点地攻击对 SRCS 系统影响较大,而 GBTM 模型对此类攻击则有较强地抵御能力。

图 4 给出了恶意节点比例 Re 达到 0.5 时,GBTM 和 SRCS 中的合作节点下载成功率随仿真周期变化情况,可以看出,GBTM 仿真系统随着仿真周期增加快速上升并保持稳定状态,SRCS 的 RSD 则快速下降,性能明显劣于 GBTM。

4 结束语

针对目前 P2P 网络中存在的恶意行为,文中提出了基于群组的信任模型 GBTM,根据节点的兴趣、爱好建立不同群组,节点总体信任度由节点之间直接信任度、组与节点之间信任度、组间信任度以及多重参数合成。对于资源或服务提供者,节点根据本地信任信息及群组地推荐来评估其信任值,并据此进行选择。因此,在 GBTM 中节点之间可以有效地建立信任关系。在不同恶意节点攻击模式下,模拟实验验证了 GBTM 模型的有效性。

参考文献:

- [1] Krishnan R, Smith M D, Telang R. The Economic of Peer-to-Peer Networks[J]. Journal of Information Technology Theory and Applications, 2003, 5(3): 31-44.
- [2] Aberer K, Despotovic Z. Managing Trust in a Peer-to-Peer Information System[C]//Proceedings of the 10th International Conference on Information and Knowledge Management. New York: ACM Press, 2001: 310-317.
- [3] Yu Bin, 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. [s. l.]: [s. n.], 2002: 294-301.
- [4] Kamvar S, Schlosser M, Garcia-Molina H. The EigenTrust Algorithm for Reputation Management in P2P Networks[C]//Proceedings of the 12th WWW Conference. Budapest: ACM Press, 2003: 640-651.
- [5] Xiong L, Liu L. PeerTrust: Supporting Reputation-based Trust in Peer-to-Peer Communities[J]. IEEE Transactions on Data and Knowledge Engineering, Special Issue on Peer-to-Peer Based Data Management, 2004, 16(7): 843-857.
- [6] Yao W, Julita V. Bayesian Network Based Trust Model[C]//Proceedings of the IEEE/WIC International Conference on Web Intelligence (WI'03). Los Alamitos, CA: IEEE Computer Society Press, 2003: 372-378.
- [7] Damian E, di Vimercati S D C, Paraboschi S, et al. Managing and Sharing Servants' Reputations in P2P Systems[J]. IEEE Transactions on Data and Knowledge Engineering, 2003, 15(4): 840-854.
- [8] 陈贵海, 李振华. 对等网络: 结构、应用与设计[M]. 北京: 清华大学出版社, 2007.
- [9] 宴文, 王怀民, 贾焰, 等. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. Journal of Software, 2004, 15(4): 571-583.
- [10] 徐锋, 吕建, 郑玮, 等. 一个软件服务协同中信任评估模型的设计[J]. Journal of Software, 2003, 14(6): 1043-1051.
- [11] 田慧蓉, 邹仕洪, 王文东, 等. P2P 网络层次化信任模型[J]. 电子与信息学报, 2007, 29(11): 2560-2563.
- [12] 孙知信, 唐益慰. 基于全局信任度的多层分组 P2P 信任模型[J]. 通信学报, 2007, 28(9): 133-140.
- [13] 郭晶, 吴国新, 李想. P2P 网络环境下信任模型的研究与实现[J]. 计算机技术与发展, 2009, 19(3): 102-105.

第三届全国服务计算会议暨 2012 年中国计算机学会服务计算学术会议

由中国计算机学会主办、中国计算机学会服务计算专业委员会和西安交通大学承办的 2012 年第三届中国计算机学会服务计算学术会议(CCF NCSC 2012)将于 2012 年 8 月 16-18 日在古都西安举行。会议现面向全国范围征集论文,诚邀服务计算、社会计算、云计算、物联网和信息安全等相关领域踊跃投稿、参加会议。会议将邀请国内外著名专家作专题报告,相关企业展示他们的最新技术成果。

重要日期: 投稿截止日期: 2012 年 4 月 15 日

论文出版: 录用论文中的约 30 篇优秀论文将推荐到 EI 检索期刊《计算机学报》、《计算机研究与发展》和《西安交通大学学报》上正式出版;其余录用论文将推荐到《小型微型计算机系统》(INSPEC, 中文核心)和《计算机技术与发展》(中国科技核心期刊)上正式出版。

投稿方式: 通过网站在线投稿: <http://ncsc2012.xjtu.edu.cn> 或电子邮件 NCSC2012@mail.xjtu.edu.cn 投稿(邮件主题注明:“NCSC 2012 投稿或服务计算会议投稿”)

联系电话: 029-82668096, 029-82668653 转 575 王老师 安老师 桂老师