◎网络、通信、安全◎

P2P 环境下的一种混合式信任模型

田祥宏[1],阎 浩[1],严筱永[1,2],邵 斐[1,3]
TIAN Xiang-hong[1],YAN Hao[1],YAN Xiao-yong[1,2],SHAO Fei[1,3]

1.金陵科技学院 信息技术学院,南京 211169
2.南京理工大学 计算机科学与技术学院,南京 210094
3.南京邮电大学 计算机学院,南京 210003
1.Department of Information Technology,Jinling Institute of Technology,Nanjing 211169,China
2.College of Computer Science and Technology,Nanjing University of Science and Technology,Nanjing 210094,China
3.College of Computer,Nanjing University of Posts and Telecommunications,Nanjing 210003,China

TIAN Xiang-hong,YAN Hao,YAN Xiao-yong,et al.Hybrid dynamic trust model in P2P environment.Computer Engineering and Applications,2009,45(31):73-76.

Abstract: This paper puts forward a hybrid dynamic trust model in P2P network which can resolve the problems of P2P network such as bad security,hard to management and so on.This model has integrated local trust,recommendation trust and global trust model,by this organic combination each model can take their respective advantage in the best measure.Meanwhile through the relative feedback mechanism,this model can effectively distinguish the change of node trust value,safety problems such as defense exaggeration,slander and so on.The simulation result indicates that this model can effectively distinguish the trust degree of node,at the same time it has the good safety.

Key words: Peer-to-Peer(P2P);network safety;trust model;trust degree

摘 要:提出了一种 P2P 环境下的混合式动态信任模型来解决当前 P2P 网络的安全性差、难于管理等问题缺陷。该模型融合了本地信任、推荐信任和全局信任模型,通过有机的结合能充分发挥各自模型的优点。同时通过相应的反馈机制能够有效地判断节点信任度的变化和抵御诋毁、夸大等安全问题。仿真结果表明,该模型能有效地判断节点的信任度,同时具有良好的安全性。

关键词:对等网络(P2P);网络安全;信任模型;信任度
DOI:10.3778/j.issn.1002-8331.2009.31.023 **文章编号**:1002-8331(2009)31-0073-04 **文献标识码**:A **中图分类号**:TP393.08

1 引言

P2P 网络(Peer-to-Peer 又称对等网络)是目前研究的热点方向。在 P2P 网络中各个节点的地位是对等的,每个节点既可以是服务器也可以是客户机。节点之间以这种松散的,相对独立的方式联系到一起,因此在分布式信息处理、协同工作、并行计算等方面比传统的 C/S 网络模式具有独特的优势。然而由于 P2P 网络自身的动态性、异构性和匿名性等特点,使得网络中恶性行为得不到有效的控制,服务质量得不到保障,因此在 P2P 网络中引入有效的信任模型机制是提高网络性能的重要步骤。

在研究现有的各种动态信任模型的基础上,提出了一种基于本地信任、推荐信任和全局信任的综合性的信任模型,能够准确地对网络节点的信任度给出评价,从而保证 P2P 网络中交易的安全性,提高网络服务质量。

2 基础知识

2.1 信任的定义

对信任的定义目前还没有统一的标准,结合相关文献[1-2],给信任一个描述性定义:

定义 1 信任就是相信对方,是一种建立在自身知识和经验基础上的判断,是一种节点与节点之间的主观行为,是一种主观判断,所有的信任本质上都是主观的。

定义 2 信任度就是信任的量化,表示相信的程度,可以是一个取值范围如[-1,1],也可以是一个有限集合如{不信任,不确定,信任}等。

定义 3 本地信任或称直接信任,主体节点根据彼此的交易历史和经验获取的对其他节点的信任度,用 DT 表示。

定义 4(推荐信任) 主体节点依据其余节点的间接推荐的形式获取的对某节点的信任度,用 RT 表示。

定义 5(全局信任) 无论是直接信任还是推荐信任,都是

作者简介:田祥宏(1971-),男,讲师,主研计算机网络;阎浩(1980-),男,助教,主研网络安全,可信网络;严筱永(1977-),男,助教,博士研究生,主研网络信息安全;邵斐(1978-),男,讲师,博士研究生,主研可信网络,信息安全。

收稿日期:2009-05-07 **修回日期**:2009-08-18

片面的,全局信任则是覆盖整个网络,由全网中所有节点共同给出的对某节点的信任度,用 GT 表示。

定义 6 综合信任度是直接信任、推荐信任和全局信任的综合计算结果,是三者在不同的网络环境下按照相应的策略综合后计算的信任度量。节点依据该信任度来决定是否与对方节点进行交易。

2.2 信任相关特点

信任是一种主观行为或者主观意识,并不是客观存在的定理或事实。对于信任的评价并不能给出准确是非标准,只能基于行为造成的结果来给出一个大致的对或错的判断,所以可信与否需要结合多种因素,经过综合后才能得到一个相对合理的结果。信任也是动态变化的,某一时刻对某个节点的信任度并不具备持续性,随着时间的推移或在其他因素的影响下,信任度会发生变化。所以以往的信任度量只能作为当前信任度判断的一个因素而不能对当前的判断起决定作用。信任模型的主要任务就是找出各种因素与信任度之间的关系,依据以往的经验和节点自身的行为或要求,综合各种影响因子,进行推理论证,来预测、量化节点的信任度[3]。

3 模型介绍

目前对 P2P 网络中信任模型的研究涌现出了很多优秀的成果,主要包括[4]:(1)基于 PKI 的信任模型;(2)基于局部推荐的信任模型;(3)数据签名;(4)全局信任模型。基于以上信任模型的优缺点,讨论了一种新型的综合信任模型,其中融合了本地信任、推荐信任和全局信任,使得三者有机结合为一个整体,能够很好地对 P2P 网络节点的信任度进行评估。其中信任值 $T\in[0,1]$数值越大表示信任度越高,数值越小表示越不信任。

3.1 本地信任

本地信任 DT_{ij} 的值根据节点之间直接交易的结果获取。每个 P2P 网络节点在本地保存一张表用于存储对其余网络节点的直接信任值。由于信任值受时间因素的影响,随着时间的推移信任度会逐渐趋向于 0,所以在计算本地信任时要把时间因素考虑在内。模型中将有效时间分为 n 个相等的时间段[6],以当前时间为基点,依次向后的时间段为 $TP_i\in\{TP_1,TP_2,\cdots,TP_n\}$ $1\leqslant i\leqslant n$,在每个时间段内计算出该时间段内的本地信任度 T_m,最后根据时间跨度的长短综合计算当前本地信任。

所以本地信任表的格式为:

交易节点 ID	时间段索引	成功交易次数	失败次数	其余说明
Node1	TP1	S1	F1	
Node1	TP2	S2	F2	
…	…	…	…	…

则本地信任度的计算方法为:

每个时间段的信任度:

$$T_m=\frac{S_{(m,ij)}}{S_{(m,ij)}+F_{(m,ij)}}$$

其中 $S_{(m,ij)},F_{(m,ij)}$分别表示在时间段 TP_m 内节点 i 与节点 j 交易成功和失败的次数。

每个时间段的信任度对当前信任度的影响是不同的,所以针对各个时间段 TP_m 设立衰减函数 $f(m)=\rho^{n-m}$,$0<\rho<1$,$1\leqslant m\leqslant n$。则节点 i 对节点 j 的本地信任 DT_{ij},其计算方法为:

$$DT_{ij}=\frac{\sum_{m=1}^{n}T_m\times f(m)}{\sum_{m=1}^{n}f(m)}$$

其中 $0<f(m)<f(m+1)\leqslant 1$。

3.2 推荐信任

3.2.1 推荐信任的原理

推荐信任就是依靠其余节点的反馈信息获取的间接信任度。如图 1 所示的网络中节点 A 要获取其余节点对节点 E 的推荐信任度来作为衡量节点 E 是否可信的依据。方法为:A 将向自己较信任的节点 B 和 C 发送查询信息。节点 B 收到查询信息后发现自己并没有对 E 的直接信任度,则 B 将查询信息转发到自己较信任的节点 D,D 经过查询将自己对 E 的直接信任发送给 B,B 通过计算后得到一个推荐信任值回传给 A。同时由于 C 保存有对 E 的直接信任,则直接将该值反馈给 A,A 在得到所有朋友节点的反馈后再综合得到总的推荐信任度。

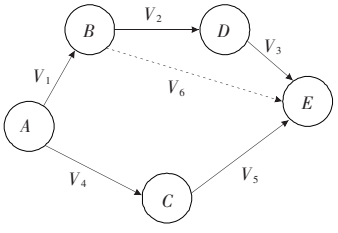

图 1 推荐信任原理

3.2.2 推荐信任的计算

推荐信任度用 RT_{ij} 表示。对于不同类型的推荐信任,其计算方法是不同的,具体的说如果推荐信任度为朋友节点的直接信任度,如 C 返回的 V_5,则计算方法为[5]:

$$RT_{ACE}=1-(1-V_5)^{V_4}$$

如果推荐信任度是朋友节点通过其余节点推荐回来的值,也就是说不是朋友节点直接信任度时(如图中 B 返回的虚线 V_6)则计算方法为:

$$RT_{ABE}=V_1\times V_6$$

则最终的推荐信任度为:

$$RT_{ij}=\frac{\sum_{p=1}^{q}RT_{ipj}\times DT_{ip}}{\sum_{p=1}^{q}DT_{ip}}$$

其中 RT_{ij} 表示节点 i 获取的对节点 j 的推荐信任度,q 表示节点 i 询问的朋友节点的总数,RT_{ipj} 表示 i 的朋友节点 p 返回的对节点 j 的信任度,DT_{ip} 表示节点 i 对朋友节点 p 的直接信任度。

在 P2P 网络中每个节点都选择自己相对比较信任的节点作为推荐节点,而不是遍历所有和该节点有直接关系的节点,这样可以在获取较准确的推荐信任度的同时把查询负担减低。

3.3 全局信任

全局信任的计算由整个网络中与节点交易的结果得出的。全局信任可以有效防止某些恶意团体或组织集中对某个节点进行诋毁事件的发生。全局信任值保存在网络中的某些超级节点中,超级节点并不作为服务器存在,而只是保存了全局信任信息。网络节点如果需要查询某个节点的全局信任值则需要把查询信息发送到相应的超级节点中,由超级节点将信任值返

回。为防止超级节点负载过量,在网络中设置多个超级节点,每个超级节点负载一定范围内的节点的全局信任度的保存工作。既减轻了超级节点的负担,有降低了查询信息造成的网络带宽的浪费,如图 2 所示。

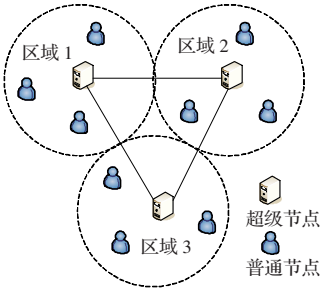

图 2　超级节点结构图

全局节点的计算方法与本地信任计算方法相同,也是划分为 n 个有效的时间段,每个时间段内保存着网络中所有节点对某个节点交易成功或失败情况的反馈记录(如表 1)。在计算全局信任度时首先将每个时间段的信任度计算出来,然后根据时间的衰减函数计算总的全局信任值,计算公式为:

$$GT_j=\frac{\sum_{m=1}^{n}T_m\times f(m)}{\sum_{m=1}^{n}f(m)}$$

3.4　综合信任

综合信任是本地信任、推荐信任和全局信任的有机结合,计算方法为:

$$T_{ij}=\alpha\times DT_{ij}+\beta\times RT_{ij}+\gamma\times GT_j$$

其中 T_{ij} 表示节点 i 对节点 j 的最终信任度,当 T_{ij} 大于设定的信任阈值时 i 可以信任 j 然后与 j 进行交易,否则可以拒绝与 j 交易。α,β,γ 表示本地信任、推荐信任和全局信任所占的比重,$\alpha+\beta+\gamma=1$,它们的值可以根据实际情况设置,如节点较自信则可以设置大一些。

4　其余问题说明

4.1　信任阈值

在动态信任的判断中必须要设置一个信任阈值当计算的综合信任度大于信任阈值时则表示该节点可以信任,否则表示节点不可信。节点可以根据自身情况设置信任阈值。信任阈值得计算可以采用公式[7]:

$$Threshold(i,j)=\frac{Risk(i,j)}{T_{ij}}\times I(i,j)$$

其中 $Threshold(i,j)$ 表示节点 i 对节点 j 的信任阈值,$Risk(i,j)$ 表示节点 i 与节点 j 交易时所承担的风险,$I(i,j)$ 表示节点 i 与节点 j 交易的重要性。

4.2　节点的加入与退出

当节点刚加入网络中时,所有的交易记录均为 0,如果严格按照公式计算则出现错误。此时规定对于新节点,必须首先到超级节点处注册,赋予初始信任度。此时新节点的信任度就是超级节点中保存的初始信任度。

如果节点退出网络,则必须先到超级节点处注销,超级节点将其记录删除,然后通知其余子节点删除其交易记录。

4.3　信任值的更新

节点交易完成后必须将交易的结果反馈,反馈的地方有两点,一是更新本地数据库中该时间段的交易次数,二是通知超级节点,更新其数据库中对应时间段中全局交易的信息。此时要注意时间段的处理,如果有新时间段产生,则需要根据信任有效总时长将无效的时间段的记录删除,同时调整时间段的索引号。

5　仿真结果

采用 Matlab7.0 对模型进行仿真,其中设置节点 200 个,一个超级节点;恶意节点约占 10%~15%,节点的初始信任值为 0.5。每个节点发出 200 次交互请求。每次交互的时间间隔为 1~2 s。其余参数设置如表 1。

表 1　参数表

参数	值
α	0.5
β	0.3
γ	0.2
ρ	0.9
τ	5 s
N	10

首先对节点信任值进行判断仿真。在真实网络中节点大致可以分为三类:(1)能提供可靠安全服务的优秀节点;(2)具有欺骗性或服务质量较差的劣质节点;(3)介于上面两者之间的提供不稳定的时好时坏服务的一般节点。所以仿真实验针对三种节点分别判断其信任值,仿真结果如图 3 所示。

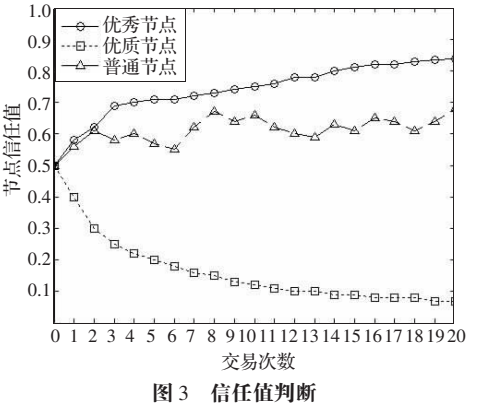

图 3　信任值判断

从仿真结果可以看出,优秀节点的信任值随着交易次数的不断增加,其信任值逐步上升,当交易次数到达一定程度时,信任值趋于稳定。由于参数设置的本地信任比重较大,所以初始阶段信任值增加较快,在交易次数增大时信任相对稳定与一定范围,增幅减缓。同样的劣质节点的信任值随着交易次数的增加不断减小,而一般节点的信任值则呈现不稳定的态势,忽高忽低的波动。

其次对模型的安全性进行仿真试验。在 P2P 网络容易出现节点间互相夸大和诋毁信任的情况,针对这两种情况分别进行仿真。在网络中任意选取一个节点,然后分别测试普通模型下和该模型下其抗夸大和抗诋毁的能力,测试结果如图 3 和图 4 所示。

从图中可以看出,无论是“夸大”还是“诋毁”攻击,随着交易次数的不断增加,受夸大或诋毁的节点信任值能够逐步接近

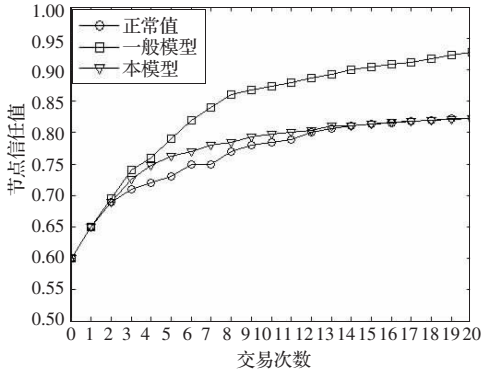

图4 抗“夸大”结果图

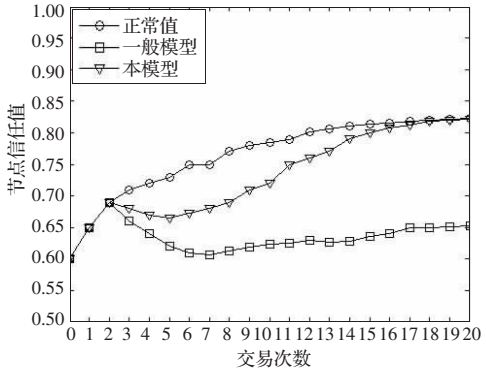

图5 抗“诋毁”结果图

正常值,说明本模型对“夸大”和“诋毁”都有较好的抵御能力。

6 小结

提出了一种混合式 P2P 环境下的信任模型,该模型将多种传统信任模型进行有机整合,其中对本地信任值、推荐信任值和全局信任值都给出了量化公式,而且提出了一种全局信任网络设计方案,同时在信任度量中引入了时间因子和反馈机制,从而对信任度进行的计算和评估能够更准确的和有效。该模型虽然在运算量上复杂了一些,但是却具有良好的信任值判断性能和较高的安全性。

参考文献:

[1] LI Xiao-Yong,GUI Xiao-Lin.Research on dynamic trust model for large scale distributed environment[J].Journal of Software,2007,18(6):1510-1521.

[2] 李雯,谢冬青,吴勇.P2P 环境下基于历史及推荐的信任模型[J].计算机应用研究,2008,25(3):915-919.

[3] 高铁杠,顾巧论,陈增强.可信网络的可信模型与算法设计研究[J].计算机应用研究,2007,24(6):142-144.

[4] 董西广,庄雷,常玉存.P2P 环境中的一种信任模型[J].微电子学与计算机,2008,6(25):137-139.

[5] 梁晨.基于评价的 P2P 网络信任模型研究[J].山东教育学院学报,2008(3):93-95.

[6] 袁巍,李津生,洪佩琳.一种 P2P 网络分布是信任模型及仿真[J].系统仿真学报,2006,18(4):938-942.

[7] 金兰芳,朱艳琴.基于信誉的 peer-to-peer 推荐信任模型[J].计算机工程与应用,2007,43(3):122-124.

(上接 62 页)

3 倍,且延迟抖动较小,可变延迟 d_{vari} 有确定的上限,作为航空电子统一网络的实现标准,FC 网络能够满足消息的实时性,只要网络工作在低负载的条件下。当网络负载继续增加,消息的延迟抖动急剧增加,延迟时间迅速恶化,在最坏情况下,消息的最大延迟时间接近最小延迟时间的 10 倍,这是由于大负载时 FC 网络的信道共享冲突解决机制不能够保证消息传输的确定性行为而导致的,应该在实际使用中避免这种情况。

5 结束语

通过性能测试得出:同等条件下,FC 交换网络较仲裁环拓扑延迟小,吞吐量大,而混合拓扑的性能处于二者之间;同等条件下,服务类 3 较服务类 2 延迟小,吞吐量大;FC 网络在均匀负载模式下,累积负载为网络最大吞吐量的 50%以下时,基本能够满足消息传输延迟上限。

一般来说,采用商用 COTS 网络协议作为航空电子统一网络可以采用两种方法,一种是确保网络工作在较低负载情况下,即保证消息在网络中传输时基本不发生冲突或冲突导致的延迟不确定性在可以接受的范围内;另一种方法是改进网络的介质访问控制方法,从理论上保证网络行为的确定性。而后者又可分为两种方法:对 FC 协议进行改进优化;通过 FC 的上层协议映射来保证网络的实时性。不论何种方法,FC 网络不同负载的性能测试为对其网络行为的研究提供了最为可信的参考数据;同时为 FC 网络仿真建模提供对比基础,为 FC 应用于航空电子系统提供技术储备。

参考文献:

[1] NCITS/Project 1331-D Fiber Channel Framing And Signaling[S].

[2] Cherkasova L,Kotov V,Rokicki T.Fibre channel fabrics:evaluation and design[C]//Proceedings of the 29th Annual Hawaii international Conference on System Sciences,1996:53-62.

[3] Thomas M R.Performance characterization of large and long fibre channel arbitrated loops[C]//Mass Storage Systems 16th IEEE Symposium,1999:11-21.

[4] Heath J R,Yakutis P J.High-speed storage area networks using a fibre channel arbitrated loop interconnect[J].IEEE Network,2000,14(2):51-56.

[5] Wang Chao-Yang,Zhou Feng,Zhu Yao-Long,et al.Simulation and analysis of FC network[C]//28th Annual IEEE International Conference,2003:285-288.

[6] 徐亚军,张晓林,郭蔡健,等.FC 网络性能测试与研究[J].计算机工程与应用,2007,43(15):137-139.

[7] 蔡昭权,秦磊华.光纤通道流量控制协议性能分析与应用[J].通信技术,2008,41(5):111-115.

[8] 徐亚军,张晓林,郭蔡健,等.一种光纤通道轻量 IP 上层协议[J].北京航空航天大学学报,2006,32(10):1246-1249.