一种基于节点推荐可信度的 P2P 信任模型

周 岩,何如龙,吴学智
(海军工程大学 电子工程学院,湖北 武汉 430033)

摘 要:提出了一种基于节点推荐可信度的信任模型,通过对推荐节点的服务质量和推荐质量进行区分,实现节点推荐行为的量化评估,最大程度地降低虚假反馈对提供服务节点的诋毁或吹捧,有效保证服务节点全局信任值的真实可靠性。仿真分析表明,该模型可以有效抑制信任模型中不诚实反馈行为的危害性。

关键词:对等网络;推荐可信度;信任模型
中图分类号:TP **文献标识码**:A **文章编号**:1674-7720(2011)20-0057-04

Node's recommend credibility based on P2P trust model

Zhou Yan, He Rulong, Wu Xuezhi
(Electronic Engineering College, Naval University of Engineering, Wuhan 430033, China)

Abstract: To solve the problem in peer-to-peer network, a trust model is presented with node's recommend credibility. Through differentiating the quality of service and recommendation provided by node, quantization and evaluation about node recommend behavior is realized, discredit or flatter about service nodes lead by fake feedback is reduced in degree. These measure availably ensure service node's reliability of global trust value. Simulation analyses show that, this model can restrain harm of dishonestly feedback more effectively.

Key words: peer-to-peer; recommend credibility; trust model

由于具有开放、灵活与健壮等特性,P2P 网络逐渐成为互联网上重要应用之一。当前,P2P 网络仍然缺乏有效的信任机制来提高系统整体的可用性,这非常显著地表现为应用中大量欺诈行为的存在以及不可靠的服务。如何实现一种机制模型,从而将 P2P 网络中的不良用户进行有效识别,规避恶意用户带来的安全风险,是 P2P 网络安全面临的主要问题。

1 相关研究

近几年,国内外的众多学者借助社会关系中的人际模型对网络信任模型进行了深入研究,基于信誉机制的信任模型构建实现了节点间信任关系的建立,可见在模型中推荐节点在信任系统中起着至关重要的作用[1]。这种模型根据计算信任值的范围可划分为两类。

1.1 局部信任模型

局部信任模型中,节点通过询问有限数量的其他节点以获取对某个服务节点的推荐度,再综合自身和该节点交互的历史信息,最终确定服务节点的信任度,进而以此来决断是否接受服务。该类模型的典型代表是 P2Prep[2]。这种机制往往比较简单且通信代价小,但通过局部信任模型获取的信任值往往是片面的,因此也就无法抵制恶意节点协同作弊。

1.2 全局信任模型

全局信任模型中,所有的网络节点都具有唯一的全局信任值,该值通过整合网络中所有节点对该节点的信任评价得到,因此恶意节点不能仅仅通过少数不诚实同伙节点给出不实评价而获得本文高的信任值[3]。这种机制可以更准确地评估节点行为。该类模型的典型代表是 EigenTrust[4]。

虽然传统的信誉机制可以鼓励网络中的节点主动共享资源,有效提高节点的服务质量[5-7],但同时也带来特有的安全问题,如节点恶意诋毁其他信誉高的节点或夸大信誉低的节点。单个节点的恶意行为对整个网络的影响比较小,但多个节点联合起来进行恶意推荐就会破坏整个网络的公平性和稳定性。目前基于信誉的信任模型多数是将推荐节点信任度作为服务选择的依据,即系统根据节点提供的历史交易信息计算其信任等级。当存

在多个可选服务提供节点时，高信任等级节点的推荐将很大程度地影响请求节点对服务节点的选择。可见此类模型混淆了节点“服务质量”与“推荐质量”的区别，忽视了提供良好服务节点对其竞争者进行恶意诋毁现象的存在。因此基于上述原理的信任模型只能在一定程度上抑制节点的一般恶意行为，但在应付许多针对信任模型本身的一些攻击行为，如不诚实反馈和协同作弊等恶意行为表现出来的有效性和监管性仍然不足[8]。本文在研究现有信任模型的基础上，引入节点推荐可信度的概念来实现对推荐行为的量化和评估，并提出了基于节点推荐可信度的信任模型。

2 数学表示

2.1 直接信任值

定义 1 满意度函数 $S_{i\to j}^{k}$ 表示在节点 i 看来，在第 k 次交易过程中，节点 j 提供服务的满意度取值集合为 $\{0,1\}$，可定义为：

$$S_{i\to j}^{k}=\begin{cases}1 & \text{满意}\\ 0 & \text{不满意}\end{cases} \tag{1}$$

定义 2 信任向量 $TV_{i\to j}$ 记录节点 i 与节点 j 的交易历史情况，每次交易完成后，在向量中增加本次交易过程中 i 对 j 提供的服务满意度，可定义为：

$$TV_{i\to j}=\{S_{i\to j}^{1},S_{i\to j}^{2},\cdots,S_{i\to j}^{n-1},S_{i\to j}^{n}\} \tag{2}$$

其中 n 为节点 i 与节点 j 的交易次数。从定义中可以看到，在两节点未进行任何交易前，信任向量 $TV_{i\to j}$ 集合为空，随着节点间交易次数的不断增加，信任向量为一组二进制向量。通过信任向量概念的引入，大大简化了节点间直接信任值计算的复杂性，同时也利于在节点内存储历史交易信息的结构化。

定义 3 直接信任值 $DT_{i\to j}$ 表示在直接交易历史中，节点 i 对节点 j 的满意度综合评价，即直接信任评价，可定义为：

$$DT_{i\to j}=\begin{cases}s_{ij}-\alpha f_{ij}/s_{ij}+f_{ij}+1 & s_{ij}-\alpha f_{ij}\geqslant 0\\ 0 & s_{ij}-\alpha f_{ij}<0\end{cases} \tag{3}$$

其中，s_{ij} 表示信任向量 $TV_{i\to j}$ 中 1 的个数，f_{ij} 表示信任向量 $TV_{i\to j}$ 中 0 的个数，$\alpha>1$ 为交易失败惩罚因子，它确保了信任增加缓慢，而减少迅速，也就是说通过大量成功交易建立起来的信任值可以在下一次失败交易发生后得到大幅降低，这样极大地避免了恶意节点企图通过多次小金额成功交易骗取较高的信任值后，在大金额的交易中实施欺诈行为。这种信任值的增加和减少速度的不对称也有效加大了对节点摇摆行为的惩罚力度。由定义可知，两个节点的直接信任值 $DT_{i\to j}$ 取值范围为 $[0,1)$，当两个节点未发生交易时，$DT_{i\to j}$ 为 0。

2.2 推荐可信度

在 P2P 网络中存在着大量动态的节点，由于任两个节点之间在交互之前不可能都建立过信任关系，因而其交易发生的次数较少甚至是零，这就导致了节点间直接信任向量较为稀疏，此时仅凭直接信任值确定服务节点的信任度是不全面或是不可行的，因此推荐信任是必不可少的。推荐节点对某一个服务提供节点的评价真实程度或者准确程度如何来度量，是当前信任模型研究的重点。如前所述，当前众多信任模型只是基于如下假设：能够提供高质量服务的节点提供的推荐服务更可信；提供低质量服务的节点推荐的服务较为不可信。本文引入推荐可信度的概念代替推荐节点的服务信任度来描述其推荐真实程度，定义如下：

定义 4 推荐可信度 $Cr_{i\to j}$ 是用来描述推荐节点 i 向服务申请节点提供的针对服务提供节点 j 信任值真实性或者准确性的度量。

从定义可知，在进行信息评价过程中，具有较高推荐可信度的节点推荐的信息更为可信，因此其推荐过程将会被赋予更大的权值。通过分析，推荐可信度主要与以下两个因素有关：

(1)推荐节点与服务提供节点的交易次数。交易次数越多可以认为推荐节点对服务提供节点越了解，它所提供的推荐信息可靠性就越大；

(2)推荐节点对服务提供节点的信誉评价与大众评价的差异度。通常情况下，网络中的大部分节点都是诚信节点，它们提供可靠的服务，同时反馈诚信的推荐信息。在推荐过程中，大部分对节点信誉的评价应该是符合此节点的实际情况的，因此某一节点反馈的信誉评价与大众评价差异度越大说明此节点的推荐可信度越低。

由上述分析，本文定义推荐可信度 $Cr_{i\to j}$ 为：

$$Cr_{i\to j}=\beta^{1/num+1}\times Val_{i\to j} \tag{4}$$

其中，$\beta\in(0,1)$，num 为节点 i 向节点 j 申请服务后进行交易的次数，$Val_{i\to j}$ 为推荐节点 i 对节点 j 评价的推荐可信因子。由此可见，在 $\beta^{1/num+1}$ 的调节作用下使得在交易次数较多的情况下 $Cr_{i\to j}$ 值较大，也就相应地增加了节点的推荐权重。

节点 i 对节点 j 给出评价与大众评价的差异度定义为：

$$Dif_{i\to j}=\frac{|DT_i-DT_{av}|}{\sqrt{\sum_{k\in M(j)}\frac{(DT_{k\to j}-DT_{av})^2}{|M(j)|}}} \tag{5}$$

其中，DT_{av} 为与节点 j 进行过交易的所有推荐节点对其直接信任值的平均值，$M(j)$ 为与节点 j 进行过交易的推荐节点的集合。通过对上述公式分析，差异度 $Dif_{i\to j}$ 只要处于小于或者等于 1 的情况下，都可以认为节点 i 对节点 j 的信誉评价与大众评价差异在可接受范围内，则节点 i 推荐可信因子值越大，其推荐可信度越高。为此，可将 $Val_{i\to j}$ 定义为：

$$Val_{i\to j}=\begin{cases}Val_{i\to j}+\lambda(1-Val_{i\to j})(1-Dif_{i\to j}) & Dif_{i\to j}\leqslant 1\\ Val_{i\to j}-Val_{i\to j}(1-1/Dif_{i\to j}) & Dif_{i\to j}>1\\ 0.5 & i\text{ 与 }j\text{ 未发生交易}\end{cases} \tag{6}$$

将 $Val_{i\to j}$ 初始化值设为 0.5，也就是当节点向陌生节点提出推荐请求时，本文认为节点对其推荐的可信程度处于半怀疑状态。通过节点不断反馈诚实可靠的推荐信息，$Val_{i\to j}$ 的值会逐渐积累，因此其推荐可信度也会随之不断增加。相反，不实的推荐会导致推荐可信度的降低。为了防止推荐节点的推荐可信因子值过快变化，进而导致恶意推荐节点可以通过较少次数的诚意推荐来累积较高的推荐可信度，引入增长变量 λ $(0<\lambda<1)$，有效降低可信因子的增长幅度，增大节点恶意推荐的代价。

2.3 间接信任值

定义 5 RT_j 表示推荐节点集合 M 中的节点对服务提供节点 j 的汇聚的间接信任值，定义为：

$$RT_j=\frac{\sum_{k\in M(j)} DT_{k\to j}\times Cr_{k\to j}}{\sum_{k\in M(j)} Cr_{k\to j}} \tag{7}$$

2.4 全局信任值

通过以上计算，得到了节点 i 对节点 j 的直接信任值和间接信任值，下面将这两个信任值进行合成，给出节点 i 对节点 j 的全局信任值。

定义 6 网络中节点 i 对节点 j 的全局信任值为 $T_{i\to j}$，其定义为：

$$T_{i\to j}=\gamma\times DT_{i\to j}+(1-\gamma)\times RT_j \tag{8}$$

其中，$\gamma=1-\mu^n$，$\mu\in(0,1)$，n 表示节点 i 与节点 j 直接交易的次数。随着交易次数不断增加，直接信任的权值随之增大，说明节点 i 越来越相信自身对服务节点信任值的判断，符合人类社会交往的原则。

3 实现策略

信任模型的实现策略主要包含两个内容：各类信任信息的存储机制和求解过程的实现。

3.1 存储机制

信任模型采用完全的分布式结构，每一个节点都有一个信任存储模块，模块中存储本节点与其他节点进行交易后的信任向量、各节点的推荐可信因子以及对某一节点的全局信任值。节点每进行完一次交易，会根据具体交易效果更新与相应节点交易的信任向量，即在信任向量中添加一位二进制码。同时根据交易前获得各推荐节点给出的直接信任值，根据相应公式更新存储的各推荐节点的推荐信任因子，以便在下一次交易中直接使用推荐信任因子计算出各节点的推荐信任度。

3.2 求解过程

求解过程如下：

(1)节点 i 作为请求发起节点收到节点 j 的服务响应后，向网络广播信任查询消息并获取各推荐节点与节点 j 交易的信任向量，结合节点内存储的各推荐节点的推荐可信因子，使用式(4)计算出各节点的推荐可信度。

(2)使用式(3)计算节点 i 对响应节点 j 的直接信任值。

(3)使用式(3)~式(7)计算推荐节点集合对节点 j 的间接信任值。

(4)使用式(8)计算得到节点 i 对节点 j 的全局信任值，然后根据相应的服务节点选取法则，决定是否与节点 j 进行交易，如果不满足，返回步骤(1)，处理其他节点的服务响应，满足则进入步骤(5)。

(5)使用式(5)~式(6)对节点存储的推荐节点的推荐可信因子进行更新并存储。

4 仿真结果与分析

为了验证模型性能，本文设计了两组实验，并对实验结果进行详细分析。使用 Java SDK 1.6 构建一个适用于本方案的非结构化 P2P 仿真平台，仿真环境参数为 2.8 GHz Intel 处理器，2 GB 内存。

4.1 实验一

假设网络中节点的推荐行为表现为两种：一是诚信推荐行为，节点反馈的推荐信息真实可靠，既不会鼓吹也不会诋毁其他节点；二是恶意推荐行为，节点反馈的推荐信息的真实度根据具体策略的不同有所改变。本实验主要目的是为了分析模型在不同恶意推荐节点百分比的情况下，节点的推荐可信度的变化情况。实验假设恶意节点的推荐行为始终为恶意推荐，所有节点的推荐可信度初始值为 0.5，即认为全部节点相对于某一服务申请节点的可信权值相同。推荐轮数设为 30 次，λ 取值为 0.1，β 取值为 0.9。

如图 1 所示，在恶意节点占 10%的情况下，某一节点始终进行真实推荐，其推荐可信度如图中曲线 2 显示会不断增加，经过 30 轮的推荐之后其推荐可信度将维持在 0.9~1。如果节点周期性地出现恶意推荐，则其推荐可信度会在此次恶意推荐行为之后出现大幅度的下降，如曲线 1 所示，并且其下降的值需要多次真实推荐才可弥补回来，这样也就大大增加了节点的恶意推荐的代价。图 2 描述了在恶意节点占 20%的情况下，节点推荐可信度的变化情况。通过对图 1 和图 2 的比较，可以

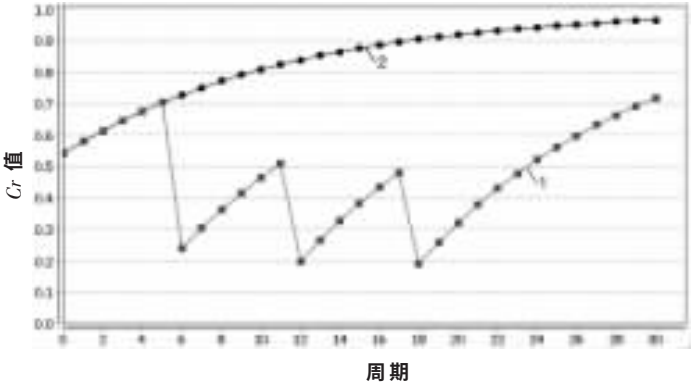

图 1 恶意节点为 10%情况下节点推荐可信度变化

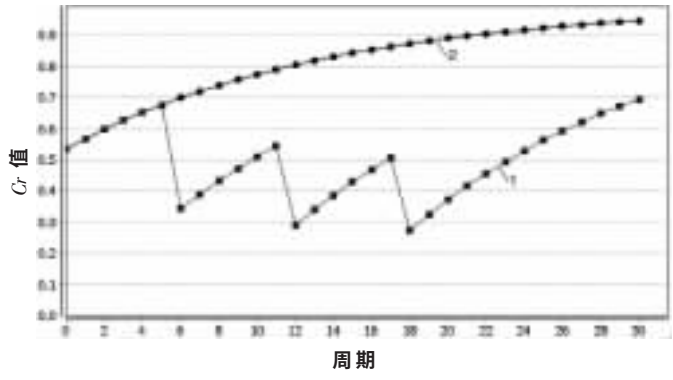

图 2 恶意节点为 20%情况下节点推荐可信度变化

得出恶意节点的比例虽然大幅增加，但是只是减缓了诚意推荐节点的推荐可信度的增幅，经过多轮推荐之后，模型仍然可以有效保证诚意节点的推荐可信度达到较为理想的状态。

实验一说明本模型对节点推荐可信度的计算可以较好地降低恶意推荐节点推荐可信度的值，进而有效抑制恶意推荐节点对其他节点的毁谤或吹捧。

4.2 实验二

主要目的是测试提供诚实服务的节点其全局信任值受恶意推荐节点比例的影响程度。实验假设恶意节点对某一服务提供节点的直接信任值均为 0，诚意节点根据与提供节点具体交易情况提供真实的直接信任值。推荐轮数为 40 次，μ 取值为 0.5。

如图 3 所示，当恶意推荐节点的比例在 10%和 30%的情况下，诚实服务提供节点的间接信任值会随着交易次数的增加而不断增加，恶意推荐节点所占比例越小，其在交易次数较少的情况下，增加的幅度越大。随着交易次数的不断增加，两种情况下的间接信任值会趋于一致。当恶意推荐节点的比例在 50%时，会对诚实服务节点的间接信任值造成很大影响，由于主流评价开始偏向于对此节点的不信任，其信任值会因为大量恶意节点的诋毁而不断降低。

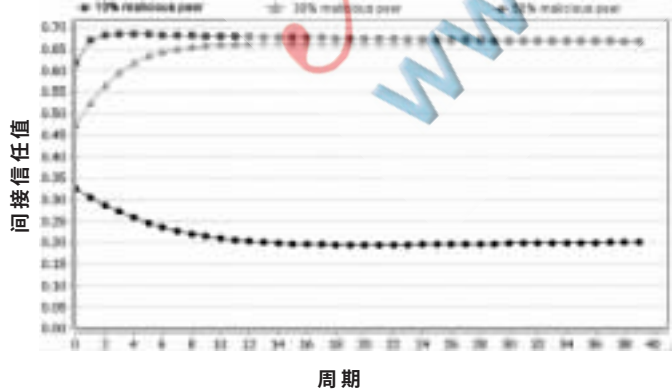

图 3 间接信任值

如图 4 所示，恶意推荐节点的比例增大在交易次数较小的情况下对全局信任值影响较大，随着交易次数的增加，节点计算出服务提供节点的信任值与实际情况相一致。

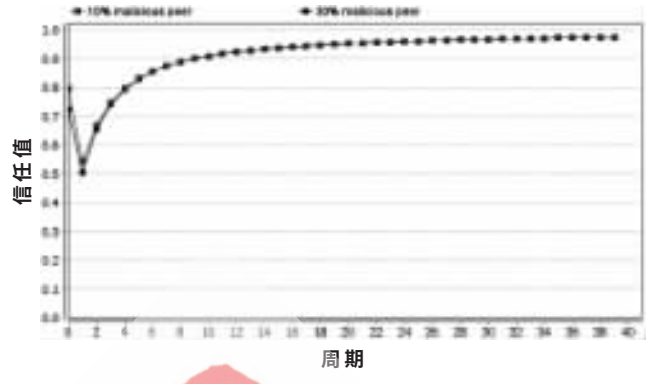

图 4 全局信任值

通过实验二说明本模型在一定程度上可以抑制恶意推荐节点对诚实节点的诋毁，同理也可以抑制其对同伙节点的吹捧。当恶意推荐节点在网络中不处于主导地位时，模型可以有效保证服务申请节点识别服务提供节点诚实与否的成功率。

本文设计提出了一种基于节点推荐可信度的信任模型，该模型通过区分节点资源提供和推荐节点两种行为，引入节点的推荐可信度来取代节点的信任值作为节点的推荐权重，从而有效避免了在 P2P 网络中存在的提供良好服务的节点对其他节点进行恶意诋毁行为所导致的推荐信任值不可靠的现象，在一定程度上提高了 P2P 网络抵御节点共谋攻击的安全性。

参考文献

[1] FARAG A, AHMAD R. The effect of behavior change on honesty checking in Peer-to-Peer systems[C]. Proc. of the 6th Annual Conference on Privacy, Security and Trust. Frederiction, New Brunswick, Canada: [s.n.], 2008.

[2] APOSTOLOS T, BARRY M G. Peer to Peer networks based on hierarchies of trust[C]. Proceeding s of the 5th IEEE International Conference on Peer to Peer Computing. Washington: IEEE Computer Society, 2005: 160-161.

[3] SELCUK A, UZUN E, PARIENTE M. A reputation-based trust management system for P2P networks[J]. International Journal of Network Security, 2008, 6(3): 235-245.

[4] KAMVAR S, SCHLOSSER M, GARCIA M H. The eigen trust algorithm for reputation management in P2P networks [C]. Proceedings of the Twelfth International World Wide Web Conference, 2003: 640-651.

[5] 金瑜，顾进广，赵红武，等. 一种新的超级节点对等网的声誉管理协议[J]. 华中科技大学学报(自然科学版)，2008，36(01)：44-48.

[6] 常俊胜，王怀民，尹刚. DyTrust：一种 P2P 系统中基于时间帧的动态信任模型[J]. 计算机学报，2006，29(08)：

1301-1307.

[7] 汪克文,谢福鼎,张永.基于惩罚机制的 P2P 电子商务模型[J].计算机工程,2010,36(12):265-268.

[8] 胡建理,吴泉源,周斌,等.一种基于反馈可信度的分布式 P2P 信任模型[J].软件学报,2009,20(10):2885-2898.

(收稿日期:2011-06-23)

作者简介:

周岩,男,1981年生,讲师,主要研究方向:信息网络、网络流媒体服务。

何如龙,男,1977年生,讲师,主要研究方向:信息网络。

吴学智,男,1962年生,副教授,硕士生导师,主要研究方向:网络化平台,军事通信。