

# P2P 网络中基于激励机制的信任模型

于 伟, 吴国文, 罗 辛

(东华大学计算机科学与技术学院, 上海 200051)

**摘 要:** 针对 P2P 网络提出一种信任模型。通过区分直接信任和间接信任, 使推荐信任度主要依赖节点以往的成功推荐次数而非直接信任度, 以抵御拥有较高直接信任度的节点对正常节点进行诋毁或欺骗。为避免非恶意节点因为网络延时等原因导致服务失败而被孤立出网络, 引入激励机制和信任重建机制, 定期提高非恶意节点的信任值, 使其能重新加入网络, 从而加强网络的容错性。实验结果表明, 该模型能有效保护非恶意节点, 孤立恶意节点, 使网络具有更好的健壮性。

**关键词:** 信任模型; 激励机制; P2P 网络; 信任重建; 直接信任; 间接信任

## Trust Model Based on Encouragement Mechanism in P2P Network

YU Wei, WU Guo-wen, LUO Xin

(School of Computer Science & Technology, Donghua University, Shanghai 200051, China)

**【Abstract】** This paper proposes a trust model for P2P network. By distinguishing direct trust and indirect trust, recommend trust value is got according to the past successful recommendation number but not direct trust, which resists behaviors that some Peers with high direct trust cheat others. In order to avoid non-malicious nodes to be isolated out of the network because of failure to offer services, incentive and trust construction mechanisms are introduced, which improves trust value of non-malicious nodes regularly, so that those nodes can rejoin the network and fault-tolerance of the network is strengthened. Experimental result shows that the model can better protect non-malicious nodes and isolate bad nodes, so that the network has better robustness.

**【Key words】** trust model; encouragement mechanism; P2P network; reconstruction of trust; direct trust; indirect trust

DOI: 10.3969/j.issn.1000-3428.2011.17.028

### 1 概 论

P2P 网络中的节点既是服务的提供者, 又是服务的获得者。每个节点在享受获得服务权利的同时, 也应该充分尽到向其他节点提供高质量服务的义务。但 P2P 网络具有的动态性、异构性、匿名性又为节点的恶意行为提供了便捷。如此下去会使网络变得不可用, 因此, 必须采取有效的机制让节点乐于提供优质服务。在以往的模型中, 恶意节点常利用较高的直接信任度诋毁正常节点, 一些非恶意节点又常因各种原因导致服务失败而被隔离出网络。针对上述问题, 本文将直接信任度和间接信任度分开考虑, 使拥有较高直接信任度的节点并不一定得到较高的间接信任度, 并引入激励机制和信任重建机制, 使非恶意节点能重新加入网络, 从而更好地保护非恶意节点, 孤立恶意节点, 使网络具有更好的健壮性。

### 2 相关工作

Beth 信任模型<sup>[1]</sup>首先将信任分为直接信任和推荐信任, 采用经验来度量信任关系, 并基于经验给出推导公式和综合公式, 但 Beth 模型只考虑肯定经验, 信任演化过于简单, 不能识别恶意节点, 将其孤立出网络。文献[2]提出基于贝叶斯网络的信任模型, 用主观逻辑描述和度量信任关系, 用观点表示主观信任, 通过综合推荐信息降低信任的不确定性, 但它同样没有考虑节点的恶意行为, 无法抵御恶意推荐所带来的影响。文献[3]提出动态推荐的信任模型来模拟社会网络的人际交互过程, 结合上下文动态选择推荐节点, 在推荐因子的计算上融入聚类分析结果, 提高了推荐的可靠度。但动态推荐涉及到信任传递的可信问题, 如 a 不信任 b, b 不信任 c, a 和 c 的信任关系并不确定。文献[4]提出的全局信任模型

EigenTrust 通过归一化本地信任值使网络中任意 2 个节点之间的推荐度均在 0 和 1 之间, 恶意节点无法伪造大于 1 的推荐度来夸大其同伙节点, 在此基础上得到  $n$  状态的 Markov 链的转移矩阵, 迭代计算全局信任值向量。但此模型迭代有一定的困难, 且不能很好地抵御不共享、冒名、诋毁等恶意行为。窦文针对此问题提出了改进的 EigenTrust 模型, 通过在基于推荐的全局信任度算法模型中引入新的推荐度函数, 采用社会网络分析中基于节点入度的中心性测量方法来求解网络中节点的全局信任值向量, 并在评价机制中引入 SHA 密码算法, 给出了该模型的数学分析和分布式实现方法。但其惩罚机制并不完善, 反而会加重诋毁行为的危害, 虽然采取了一些反诋毁的补救措施, 但没有从根本上改变。而且这 2 个模型有一个共同的缺陷: 仅使用节点的全局信任值作为推荐度的权重, 即假设具有高全局信任值的节点其推荐也更加可信。但这个假设并不总是成立的。本文为此提出一种间接信任不依赖于直接信任的可信模型, 并在演化过程中挽救非恶意节点, 提高网络的可用性。

### 3 信任的量化

若节点  $A$  信任节点  $B$ , 则  $A$  与  $B$  之间存在信任关系。信任关系就是评估实体确信评估对象能够以一定的概率正确地进行交互。信任分为直接信任关系和推荐信任关系。

#### 3.1 直接信任

节点  $A$  对节点  $B$  的直接信任度定义为:

**作者简介:** 于 伟(1985—), 男, 硕士研究生, 主研方向: 信任模型, 网络安全; 吴国文, 博士; 罗 辛, 讲师、博士

**收稿日期:** 2011-02-02 **E-mail:** yuweibdf201@163.com

$$D_{AB} = S_{AB} / I_{AB} \quad (1)$$

其中,  $S_{AB}$  为节点  $A$  与节点  $B$  交互成功的次数;  $F_{AB}$  为  $A$  与  $B$  交互失败的次数;  $I_{AB}$  为  $A$  和  $B$  总的交互次数。

### 3.2 推荐信任

推荐信任是一个节点对另一个节点所推荐的经验信息的可信程度。在现有信任模型中, 推荐信任的初始值一般与直接交互的经验相联系。直接交互成功次数多即直接信任度高的节点被赋予较高的推荐值; 反之, 直接交互成功次数少即直接信任度低的实体被赋予较低的推荐信任。但这样的机制基于以下假设: “好” 节点提供的推荐信任都是可靠的。但是如果恶意节点在直接信任较高的情况下对其他节点进行诋毁, 则很难被识别出来。因此, 将推荐信任和直接信任分开考虑, 在赋予直接信任初始值时, 同样赋予间接信任初始值, 使得间接信任不再依赖于直接信任。

如表 1 所示, 假定两节点可分为朋友、陌生人和黑名单 3 种关系。每种关系通过直接信任度和间接信任度来衡量。

表 1 节点的 3 种关系

节点关系	直接信任度 $D$	间接信任度 $R$
朋友	可交互, 提供优质服务	可推荐, 且推荐权值为 $\varepsilon=1$
陌生人	可交互, 提供一般服务	可推荐, 但推荐权值为 $0 < \varepsilon < 1$
黑名单	不可交互	$R > T_L$ 时方可推荐

当多个节点向一个节点请求服务时, 被请求的节点选择先为它的朋友节点提供服务, 然后为陌生人节点提供服务, 屏蔽黑名单。即为朋友提供优质服务, 为陌生人提供一般服务, 不为黑名单提供服务。同样, 朋友节点推荐的权值为  $1 (\varepsilon=1)$ , 陌生人节点推荐的权值为  $\varepsilon (0 < \varepsilon < 1)$ , 黑名单推荐的权值为  $0 (\varepsilon=0)$ 。节点  $A$  对节点  $C$  的间接信任度定义为:

$$R_{AC} = \sum \varepsilon_{AB} \times R_{BC} \quad (2)$$

其中,  $R_{BC}$  为节点  $B$  对节点  $C$  的间接信任值;  $\varepsilon_{AB}$  为节点  $A$  对于节点  $B$  推荐节点  $C$  的信任权值。

### 3.3 直接信任与间接信任的合成

节点  $A$  对节点  $B$  的总信任度  $T$  可定义为:

$$T = \alpha D_{AB} + \beta R_{AB} \quad (3)$$

其中,  $\alpha$  和  $\beta$  分别为直接信任度和间接信任度在总信任度中所占的比重,  $\alpha + \beta = 1$ ,  $\alpha, \beta \in [0, 1]$ 。

## 4 信任的演化

本文将信任的演化分成了 3 个时期: 初始化时期, 更新时期和重建时期, 如图 1 所示。其中, 实线为直接信任的演化曲线; 虚线为间接信任的演化曲线。直接信任和间接信任的演化在初始化阶段表现不同, 而在更新和重建阶段相同。并且  $(T_a, T_b) \in$  黑名单,  $(T_b, T_c) \in$  陌生人,  $(T_c, T_d) \in$  朋友。

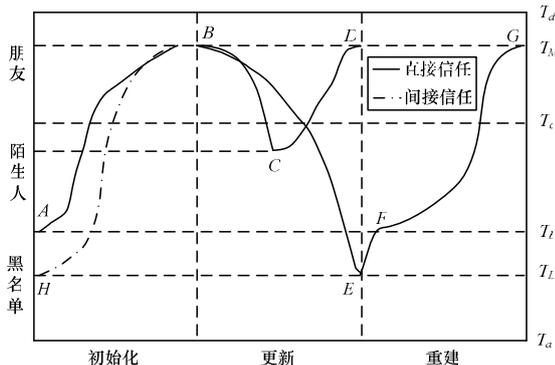


图 1 信任演化过程

### 4.1 信任初始化时期

一个新节点开始时并没有与其他任何节点进行过交互, 它没有可以推荐的信任信息。同样, 其他节点也不能推荐新节点。因此, 新加入的节点可以与别的节点进行交互, 但是不可以进行推荐 ( $\beta=0$ )。

如图 1 所示, 新节点直接信任的初始值为  $A$  点, 通过与其他节点的成功交互, 其直接信任值会上升, 考虑到时间衰减因子的作用, 即历史数据的参考性在降低, 因此, 定期降低其直接信任值, 使节点更加珍惜得到的信任值。如果此节点诚心交互, 直接信任值整体上还是上升的, 如  $AB$  段, 最终会逼近最高信任值。如果此节点没有恶意行为, 那么直接信任值会一直保持在  $T_M$  附近。由于新节点没有可以推荐的信任值, 因此初始值定义为  $H$  点, 如图 1 所示。在正常推荐其他节点的情况下, 节点的间接信任值会迅速上升, 如  $HB$  段。如果该节点是非恶意节点, 间接信任值会一直保持在  $T_M$  附近, 如  $B$  点附近。

### 4.2 信任更新时期

节点由于一系列原因在  $\Delta t$  时间内没有进行任何交互, 那么它的信任值就会发生衰减:

$$D' = \psi \cdot e^{-c\Delta t} \cdot D$$

$$R' = \psi \cdot e^{-c\Delta t} \cdot R$$

其中,  $\psi$  是常量;  $c$  是衰减因子。不交互的时间越长, 信任值下降得越多, 由此鼓励节点更多地参与到正常交互中, 为别人提供服务。

只要信任值没有降低到  $T_b$  之下, 就允许节点通过后期的交互和推荐提升信任值, 如  $BCD$  段。节点一旦处于黑名单范围内, 且信任值不小于  $T_L$ , 就需要进行信任重建以补救, 如  $BE$  段。

### 4.3 信任重建时期

一些节点会因为网络延时、偶然中断等非恶意原因导致交互失败而被认为存在不良行为, 现有的模型很少考虑到这些节点, 一般都会把它们孤立出网络。而对于此类节点, 更需要激励机制使其重新获得交互与推荐的权利, 从而增强网络的健壮性。

为了防止黑名单节点也通过此途径重新获得交互和推荐的权利, 本文规定, 只有直接信任值和推荐信任值都大于  $T_L$ , 直接信任或者间接信任才能被激励机制重建。重建函数如下:

$$D' = D + \lambda \cdot \Delta t$$

$$R' = R + \lambda \cdot \Delta t$$

其中,  $D'$  和  $R'$  是激励机制提升后的直接信任值和间接信任值;  $\lambda$  为常量, 表示信任值提升的速率。

参考图 1, 节点在信任值提升到  $F$  点之后才能重新加入网络, 继续提供服务和被服务, 如  $EFG$  段。

## 5 激励机制算法

激励机制算法前提条件为: 节点  $i$  新加入网络  $\Omega$ , 向网络发出请求服务  $A$ ;  $\Omega$  中已经存在节点  $j, k, l, m, n$ 。

首先给出算法步骤中的原语及其语义:

$RServe(i, A)$ : 节点  $i$  向网络发出服务  $A$  的请求。

$FServe(i, A, j)$ : 节点  $j$  查看本地记录, 判断自己能否向节点  $i$  提供服务  $A$ , 并将结果反馈给节点  $i$ 。

$FindOthers(i, A, j)$ : 节点  $j$  向  $A$  推荐可以服务  $A$  的其他节点。

$GDTrust(i, j)$ : 节点  $i$  查找本地记录, 读取节点  $i$  对节点

$j$  的直接信任值。

$GRTrust(i, j)$ : 节点  $i$  通过其他节点的推荐和自身的记录, 求得节点  $j$  的间接信任。

$CVal(i, j)$ : 节点  $i$  通过节点  $j$  的直接信任值和间接信任值利用式(3)计算综合信任值  $T$ 。

$UDLocal(i, j)$ : 节点  $i$  与节点  $j$  交互后, 更新本地关于节点  $j$  的直接信任值记录。

$URLocal(i, j, k)$ : 节点  $i$  与节点  $j$  交互后, 更新本地关于节点  $j$  推荐节点  $k$  的间接信任值记录。

$Save(i)$ : 如果  $T_L < D_i < T_c$  且  $T_L < R_i < R_b$ , 提升  $D_i$  和  $R_i$ , 让节点  $i$  重新加入网络。

$Judge(i, A, \Omega)$ : 节点  $i$  根据计算的信任值, 从网络  $\Omega$  中选择信任值高的节点为其提供服务。

假设节点  $i$  加入网络  $\Omega$ , 请求服务  $A$ , 成功交互后, 节点  $j$  向  $\Omega$  请求服务  $B$ ,  $\Omega$  中只有节点  $i$  可以提供服务  $B$ , 但节点  $i$  因为网络延时没能成功提供服务, 导致信任值下降, 需要激励方能重新加入网络。具体算法如下:

```

Procedure
  RServe(i, A);
  while(existpeer)
    FServe(i, A, x(x ∈ Ω));
    FindOthers(i, A, x(x ∈ Ω));
    GDTrust(i, x(x ∈ Ω));
    GRTrust(i, x(x ∈ Ω));
  CVal(i, x(x ∈ Ω));
  If( $T_L < D_i < T_c$  &  $T_L < R_i < R_b$ )
    Save(i);
  end while
  Judge(i, A, x(x ∈ Ω));
  UDLocal(i, x(x ∈ Ω));
  URLocal(i, x(x ∈ Ω), k);
End Procedure

```

## 6 仿真结果与分析

本文采用演化周期模型进行仿真, 每次仿真由若干个信任演化周期组成。在每个仿真网络中, 节点可以发起服务请求并对其他节点的服务请求进行响应。服务请求广播到网络中后, 收到服务请求的节点对其进行转发并查看是否对其应答, 发起请求的节点等待接受响应并从响应中根据信任度值选择某个节点进行提供服务, 交互结束后更新信任值, 然后查看本地信任值, 根据激励规则判断是否提升某些节点的信任值, 使其重新加入网络。

作为参照, 本文对 EigenTrust 模型在同一实验环境下进行了实现。在实验中, 节点个数为 100, 任何一个节点可以平等地与其他节点进行交互。假定网络中存在 30 个恶意节点, 其服务提供成功的概率接近 0; 正常节点有 30% 的概率由于非恶意原因造成交互失败。可以提供的服务为 10 种, 随机地分布在节点上, 并设定节点间交互的次数达到 1 万次就停止仿真。如图 2 所示, 恶意节点在开始阶段都遵循网络的

规定, 认真提供服务以及对其他节点进行推荐, 而非恶意节点还在正常交互以换得较高的直接信任值, 可用节点数还是可观的。但在一段时间后, EigenTrust 模型中的可用节点数迅速下降。因为经过恶意节点的诋毁, 正常节点也会被孤立出网络, 网络变得不可用。但本文模型因为激励机制的作用, 可用节点数会定期地提升一部分, 这部分正是那些被拯救的无辜节点, 同时因为抵御了大部分恶意节点, 正常节点可以正常交互。而 EigenTrust 模型没有采用激励机制, 绝大部分非恶意节点被孤立, 网络中可用的正常节点减少, 因此, 网络所能提供的服务质量也有一定程度的下降, 直接导致一些交互不成功。可见, 本文信任模型能够更好地让绝大多数非恶意节点重新加入网络, 并孤立大部分恶意节点, 从而更好地保持网络的健壮性、可用性。

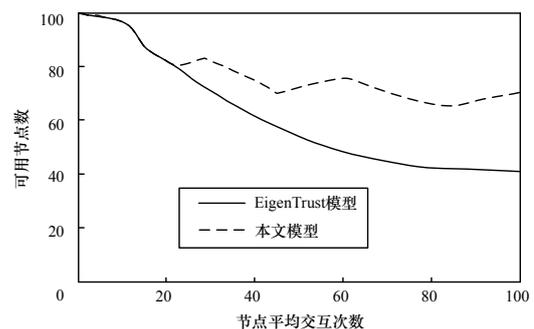


图2 EigenTrust模型与本文模型可用节点数比较

## 7 结束语

本文提出一种 P2P 环境下带激励机制的信任模型, 其可以防止恶意节点通过较高的直接信任值诋毁正常节点, 并拯救大部分非恶意节点, 实验结果证明了该模型的健壮性和可用性。但激励机制只能提升绝大部分非恶意节点的信任值, 有一些正常节点仍会被网络孤立, 而且偶尔还会有恶意节点混杂在网络中未被孤立。如何最大限度地让非恶意节点留在网络中参与服务而让恶意节点退出网络还有待解决, 这也是下一步的研究内容。

### 参考文献

- [1] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Network[C]//Proc. of ESORICS'94. Brighton, USA: Springer-Verlag, 1994: 3-18.
- [2] Josang A. An Algebra for Assessing Trust in Certification Chains[C]//Proc. of Internet Society Symp. on Network and Distributed System Security. San Diego, USA: [s. n.], 1999.
- [3] 张景安, 郭显娥. P2P网络中基于动态推荐的信任模型[J]. 计算机工程, 2010, 36(1): 174-176.
- [4] Kamvar S D, Schlosser M T. EigenRep: Reputation Management in P2P Networks[C]//Proc. of the 12th International World Wide Web Conference. New York, USA: ACM Press, 2003: 123-134.

编辑 张帆

(上接第74页)

- [3] Prathaban M, Kohlenberg J. Dynamic NAK Timer Algorithm to Improve Delivery Latency of CCSDS File Delivery Protocol in Deferred NAK Mode[C]//Proc. of AICT'09. [S. l.]: IEEE Computer Society, 2009.
- [4] 姜月秋, 张文波, 孙滨. 基于卫星网络的 TCP 拥塞控制算法[J]. 计算机工程, 2009, 35(5): 15-18.

- [5] Jacobson V. Congestion Avoidance and Control[J]. ACM Computer Communication Review, 1988, 18(4): 314-329.
- [6] Baek W, Lee D C. Expected File Delivery Time of Immediate NAK ARQ in CCSDS File Delivery Protocol[J]. IEEE Trans. on Aerospace and Electronic Systems, 2005, 41(2): 503-524.

编辑 顾姣健



