

文章编号:1001-9081(2008)12-3194-03

P2P 网络中一种可信访问控制模型

晏 樱^{1,2}, 李仁发³

(1. 湖南大学 软件学院, 长沙 410083; 2. 湖南交通职业技术学院 信息管理系, 长沙 410000;
3. 湖南大学 计算机与通信学院, 长沙 410083)
(hnyany@126.com)

摘要: 信任模型强调成员以及数据的可信性, 通过对网络中的不端行为进行通告和限制, 为用户能够更加合理地使用网络提供保证。提出了一个基于相似度加权推荐的全局信任模型(GSTrust)。在模型中, 信任值的请求者使用推荐者和自己之间的节点评分行为相似度加权推荐意见, 以节点评价行为的相似度加权其推荐度计算全局信任值, 并提出了基于群组的激励机制作为信任模型的有效补充, 仿真实验证明了模型的有效性。

关键词: 对等网络; 信任模型; 访问控制

中图分类号: TP393 文献标志码:A

A credible access control model in P2P networks

YAN Ying^{1,2}, LI Ren-fa³

(1. School of Software, Hunan University, Changsha Hunan 410083, China;
2. Department of Information Management, Hunan Communication Polytechnic, Changsha Hunan 410000, China;
3. School of Computer and Communication, Hunan University, Changsha Hunan 410000, China)

Abstract: Trust model emphasizes credibility of member and data. By proclaiming and restricting the misconduct of networks, it can provide guarantee for users to use the Internet more reasonably. A global trust model (GSTrust) was proposed based on similarity weighting recommendation. In this model, the trust value's requester weighted recommendation by using similarity behavior of the presenter and himself, and calculated the global trust value by using the similarity score to weight its recommendation. An incentive mechanism also was proposed based on group as the effective complement for trust model. Simulation experiment shows the good performance of GSTrust model.

Key words: Peer-to-Peer network; trust model; access control

0 引言

分布式、匿名性和自治是 P2P 网络的本质属性, 也是其成功的主要原因。在 P2P 环境下的信任模型要解决的核心问题是: 在不损失这些本质属性的前提下, 实现节点信任数据的计算、存储和分发在网络中分布式进行, 并且在上述各环节应占用很少的网络资源, 同时保证规模的可扩展性。所面临的首要挑战是协同作弊问题: 在恶意节点形成作弊的团体、协同伪造信任值时, 信任模型能否有效地识别并遏制作弊行为是评价模型的重要指标。

在 P2P 环境下, 全局信任模型综合整个网络对单个节点的信任评价, 得出该节点的全局信任值, 因此削弱了恶意节点团体协同作弊的效果。这类模型为获取全局的节点信任值, 综合整个 P2P 网络对于其中的某个节点的信任评价, 这样得到的信任评价综合了整个 P2P 网中所有节点的意见, 是比较准确的。

Eigen Trust^[1] 模型是全局信任模型中具有代表性的一种算法, 在此基础上, 文献[2]提出了基于推荐的 P2P 环境下的 trust 模型, 该模型也是全局信任模型的代表。在这两个模型中主要计算全局信任值方法如式(1)所示, 均以节点的全局信任值作为权重。

$$T_i = \sum_{k \in U_i} L_{ki} \cdot T_k \quad (1)$$

在该信任模型中, 全局信任值越高的节点其推荐意见的权重也越重要。然而在伪装的节点攻击下, 部分恶意节点通过伪装获得较高的全局信任值, 同时给其同伙给出非常高的推荐度。故而以上加权推荐的方法并不完全可行。基于此, 本文提出了基于群组和相似度的全局信任模型——GSTrust 模型。

1 GSTrust 模型

1.1 GSTrust 模型的主要构成

1) 提出了基于群组和相似度的全局信任策略, 信任值的请求者使用推荐者和自己之间的节点评分行为相似度加权推荐意见, 以节点评价行为的相似度加权其推荐度计算全局信任值。

2) 提出了基于群组的激励机制, 作为信任模型的有效补充, 激励 P2P 网络中的节点进行有效的协作并合理使用网络资源。

1.2 评分行为相似度度量方法

计算节点评分行为相似度比较有代表性的方法是余弦相似度^[3]。设节点 i 和节点 j 在 n 维项目空间上的评分分别表示为向量 $\mathbf{B}_i, \mathbf{B}_j$, 则节点 i 和节点 j 之间的相似度 $\text{sim}(i, j)$ 为:

$$\text{sim}(i, j) = \frac{\mathbf{B}_i \cdot \mathbf{B}_j}{\|\mathbf{B}_i\| \cdot \|\mathbf{B}_j\|} \quad (2)$$

收稿日期: 2008-06-19; 修回日期: 2008-09-08。 基金项目: 湖南省科技厅资助项目(20063342051)。

作者简介: 晏樱(1974-), 女, 湖南益阳人, 讲师, 硕士, 主要研究方向: 网络信息安全; 李仁发(1956-), 男, 湖南郴州人, 教授, 博士生导师, 博士, 主要研究方向: 嵌入式计算机与系统、无线网络、数字化实验。

由于该方法运算量较大,不具有良好的扩张性。故而本文在余弦相似度算法的基础上提出了一种简化算法,将余弦相似度计算转化成为对向量的分量按正负计数问题,从而减少了该方法的运算量。

该算法的基本思想是:比较向量 B_i 和 B_j 每个分量的正负符号,符号相同的分量个数越多,则说明 B_i 和 B_j 越相似。如式(3)所示:

$$\begin{cases} B_{ik} = 0, & i \neq k, G_{ik} + F_{ik} = 0 \\ B_{ik} = 1, & i \neq k, G_{ik} + F_{ik} > 0, \text{且 } G_{ik} \geq F_{ik} \\ B_{ik} = -1, & i \neq k, G_{ik} + F_{ik} > 0, \text{且 } G_{ik} < F_{ik} \end{cases} \quad (3)$$

其中 $B_i = [B_{i1}, B_{i2}, \dots, B_{in}]$, B_{ik} 是 i 对 k 的成功交易率评分,若在与 k 以往交互历史中,成功交互次数 G_{ik} 不少于失败交互次数 F_{ik} ,节点 i 令 B_{ik} 为 1,否则为 -1。

1.3 全局信任值的计算方法

全局信任值是从整个网络角度观察得到的节点 i 的信任值,它综合了网络中所有节点对 i 的全部评价。在 n 个节点的网络中,任意节点 i 具有全局唯一的信任值,记作 T_i 。在式(1)的基础上, GSTrust 模型提出了计算全局信任值的方法,如式(4)所示,其中 C_{ki} 标示节点 k 和节点 i 的评价行为的相似度,GSTrust 模型将其作为推荐度的权重。

$$T_i = \sum_{k \in U_i} L_{ki} \cdot C_{ki} \cdot T_k \quad (4)$$

全局信任值求解算法:网络中任意节点 i 同时具有两个角色,它既是用户节点,同时也是若干个用户节点的信任值管理节点。

引入信任值管理节点的全局信任值求解算法具有工程可行性,因为禁止任意节点 I 计算和提交自己的全局信任值有效地防止了作弊的发生。下面首先给出用到的两个原语语义以及相关的定义:

Submit($ID_i, (ID_j, ID_k), Value1, Value2$):将节点 j 对节点 k 的局部信任值等和信任计算相关的数据 $Value1, Value2$ 提交到 i 的信任值管理节点 M_i 。 $Value1$ 和 $Value2$ 的具体含义由上下文决定。

Query(ID_j, T_j, L_{ji}, B_j):基于 Chord 协议,查询节点 j 的全局信任值 T_j , j 对 i 的局部信任评分 L_{ji} 和 j 的成功交易率向量 B_j 。

定义 1 局部满意度 S_{ij} 是节点 i 对以往与节点 j 交互经验的总结, $S_{ij} > 0$ 说明 i 对 j 有正面的评价; $S_{ij} < 0$ 说明 i 对 j 有负面的评价。

定义 2 局部信任值 L_{ij} 是节点 i 根据直接交易历史对节点 j 做出的新人评分,也是 i 对 j 的推荐度。 L_{ii} 无实际意义,令其为 0,否则 i 可以伪造 L_{ii} ,为自己做出很高的信任评分。

定义 3 B_{ij} 是节点 i 对节点 j 的成功交易率评分,是节点 i 看来与节点 k 以往交互历史中,成功或失败交互数占其与节点 k 交互总次数的比率。

任意节点 i 作为一般用户节点和信任值管理节点的算法分别如下所示。

1) 节点 i 作为一般用户节点的算法:

```
UpdateAndSubmitTrustdata()
  // 节点 i 与 j 每次交互后更新并向 Mi 提交 G_ij 和 F_ij
  { If(成功交易) G_ij ← G_ij + 1;
    else F_ij ← F_ij + 1;
```

```
Submit (ID_i, (ID_i, ID_j), G_ij, F_ij);
  // 向 Mi 提交 G_ij 和 F_ij 并触发 Mi 的 UpdateLocaltrust() 过程
}
```

2) 节点 i 作为节点 u 的信任值管理节点的算法:

```
UpdateLocaltrust()
  // i 收到 Submit (ID_u, (ID_u, ID_v), G_uv, F_uv) 后,触发更新 L_uv, B_uv 的过程
  | 验证 G_uv, F_uv 的合理性;
    依定义 1,2,3 计算 S_uv, L_uv, B_uv ;
    Submit (ID_v, (ID_u, ID_v), L_uv, B_uv );
    // 向 M_v 提交 u 对 v 的评分 L_uv 和 B_uv,触发 M_v 将 ID_u 加入
    // 集合 U_v 的过程,并可选的触发 M_v 的 CalcGlobaltrust() 过程
}
CalcGlobaltrust()
```

```
// 代迭代计算 i 所管理的节点 u 的全局信任值
for( every j ∈ U_u (j ≠ u) )
  | Query (ID_j, T_j, L_ju, B_j);
    计算节点 j 和 i 的评分行为的相似度 C_ji;
    T_u ← T_u + L_ju * C_ji * T_j;
  |
return T_u;
```

有两种模式触发 CalcGlobaltrust() 过程:每当节点 i 收到其他节点对 u 的局部信任评分时,触发 CalcGlobaltrust() 更新 u 的全局信任值;或者每当网络运行一定的时间后触发(例如,设置门限值 p ,当 i 收到的对 u 的局部信任评分的数量大于 p 时触发)。

1.4 基于群组的激励机制

作为信任模型的有效补充,本文提出基于群组的激励机制 GIM,通过将感兴趣的节点组织成群组,实现个人贡献资源的群组化。采取互惠策略的节点根据个人历史交易信息或群组的互惠决策机制决定是否合作。群组根据历史交易保存成员节点或其他群组的信誉信息。对群组而言,群组内部节点发生交易时,根据节点对群组的友好程度决定是否合作;群组之间节点发生交易时,以群组为单位进行博弈(即根据群组的友好程度决定是否合作),提高了节点之间发生重复交易的概率。

接下来的问题是节点如何定义互惠决策函数。在传统的多次重复的博弈模型中,TFT 策略具有优良的性能。采用 TFT 策略的节点在第一次博弈中,总是合作。此后,重复博弈对方在上一次博弈中的行为。遵循 TFT 的设计原则,提出了基于节点友好程度(对节点参与等级和慷慨程度的总称)的互惠决策函数(式(5)):

令节点 i 的信誉信息为节点 i 参与到系统中的信息,记做 $R_i = (p_i, c_i)$,其中 p_i 和 c_i 分别为节点 i 提供的服务和消费的服务。如果没有 i 的信誉信息,令 $R_i = \emptyset$ 。那么群组 G_i 为节点 i 指定的信誉信息为:

$$R_i^{G(i)} = \begin{cases} R_i^{G(i)}, & i \in G_i = G(i) \\ R_{\text{strange}}^{G(i)}, & i \in G_i = G(i), R_i^{G(i)} = \emptyset \\ R_{G_i G(i)}, & i \notin G_i \\ R_{G_i G_{\text{strange}}}, & i \notin G_i, R_{G_i G(i)} = \emptyset \end{cases} \quad (5)$$

其中, $G(i)$ 是 i 所属的群组, $R_i^{G(i)}$ 为群组 $G(i)$ 保存的 i 作为其成员节点的信誉信息, $R_{\text{strange}}^{G(i)}$ 为群组 $G(i)$ 根据其群组成员首次提供或消费服务得出的陌生节点信誉信息, $R_{G_i G(i)}$ 为 G_i 根

据 $C(i)$ 的成员与自己的成员节点的交易历史得出的 $C(i)$ 信誉信息, $R_{C_i C_{\text{strange}}}$ 为 C_i 根据陌生群组的成员节点提供或消费服务得出的陌生群组信誉信息。

群组利用信息共享机制为成员节点或熟悉群组记录信誉信息。此外,群组根据成员节点或群组首次提供或消费服务的行为定义了陌生节点和陌生群组的信誉信息。这种信息共享机制克服了 P2P 系统中节点规模大且状态变化迅速,兴趣不对称以及零代价 ID 的问题。

在每个周期结束后,群组会对成员节点和熟悉群组的信誉信息进行衰减处理,群组对所保存的信誉信息进行衰减处理使得节点的近期行为对信誉信息有更重要的影响,可以防止节点累积信誉进行背叛,同时使得背叛节点在经过惩罚后,能得到其他节点的宽恕。

2 仿真实验及结果分析

为了验证 GSTrust 模型的性能,使用 Stanford 大学的 Query Cycle Simulator 软件包^[4],它仿真典型的文件共享式 P2P 网络。同时在该软件包中加入了自已的代码,实现了 GSTrust 模型,也实现了文献[1-2]的模型作为对照。

本仿真实验中,仿真周期为 1000 s,共仿真 3 次。在每个仿真周期内,P2P 网络中的节点可能处于活动状态或离线状态,每个节点随机地向整个网络广播一个文件下载请求,等待网络中其他节点的响应,当收到拥有文件的节点对本节点的响应后,建立响应节点列表。从列表中选取全局信任值最高的节点下载文件,若下载失败,则从列表中删除该节点,重复上述过程,直到文件下载成功。下载结束后,节点更新本地信誉信息,并向群组回报使其更新相应信誉信息。收集每个仿真周期内的数据得出不同策略性能,向成员节点通报,使这些节点进行策略调整,进行数据搜索,然后进入下一个仿真周期,不断重复收集过程,直到整个 P2P 网络中所有节点的信任值分布收敛到一个稳定状态。仿真实验开始时,假设每个节点信任值均为 $1/n$,其中 n 为网络节点数目。

2.1 基于相似度的全局信任策略 IM 类仿真及分析

IM 类仿真是指网络中的恶意节点均为孤立的恶意节点,调整网络中 IM 类节点的数量以观测实施 GSTrust, eigentrust 和窦文的模型的效果。图 1 给出了网络中 IM 节点数占 40%,并分别使用 4 种算法选择下载源时,失败下载次数 β 趋于 0 的速度。可以看到:使用 GSTrust 模型从第 6 个周期开始,几乎完全杜绝了失败下载的发生,这说明 GSTrust 遏制了恶意节点,使其无法获得较高的信任值。图中的 Random 是指不使用任何信任模型,节点每次随机选取下载源下载。

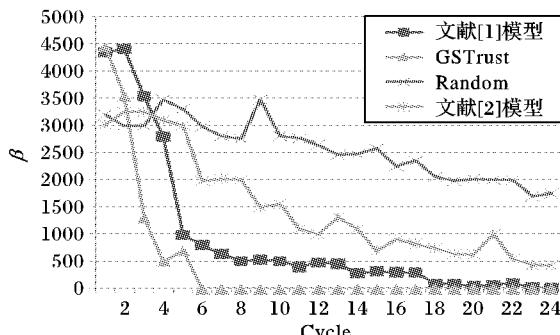


图 1 失败下载次数 β 随仿真周期的变化对比

2.2 基于相似度的全局信任策略 CM 类仿真及分析

CM 类恶意节点彼此“相识”,它们具有更强的协同作弊能力。GSTrust 中节点相信与自己行为相似的节点的推荐,相当于正常节点也形成了协作的团体。如图 2 所示在 CM 类仿真中,GSTrust 比其他模型更有优势。

2.3 基于群组的激励机制 IM 类仿真及分析

为了研究基于群组的激励机制的可扩展性,分别考察了基于群组的激励机制和 RIT 在不同网络规模下系统的性能。如图 3 所示,节点规模从 100 变化到 1000,基于群组的激励机制系统无论在节点对所属群组文件感兴趣概率 p_{interest} 为 0.6 还是 0.8 时,都具有较好的性能。本仿真运行 RIT 系统 $p_{\text{interest}} = 0.6$ 的情况,随着网络规模增加,RIT 系统的合作水平下降,系统性能下降。随着网络规模的增大,系统从初始状态演变到互惠合作状态所需的时间增长,故整个仿真过程中,系统的平均性能下降。

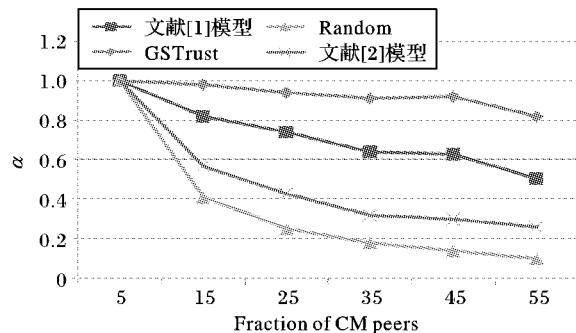


图 2 不同规模 CM 类节点存在时的下载成功率 α

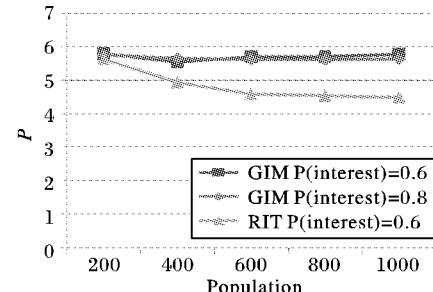


图 3 不同网络规模下节点对所属群组文件感兴趣概率 p

3 结语

本文提出了基于群组和相似度的安全信任模型 GSTrust,并利用基于群组的激励机制作为信任模型的有效补充,仿真实验表明在伪装的恶意节点模型中,GSTrust 模型的性能较高。

参考文献:

- [1] KAMVAR S D, SCHLOSSER M T, GARCIA - MOLINA H. The Eigentrush algorithm for reputation management in P2P networks [C]// Proceedings of the 12th International World Wide Web Conference. New York: ACM, 2003: 640 - 651.
- [2] 窦文. 信任敏感的 P2P 拓扑构造及其相关技术研究 [D]. 长沙: 国防科技大学, 2003.
- [3] CHARIKAR M S. Similarity estimation techniques form rounding algorithms [C]// Proceedings of the thirty - fourth annual ACM symposium on Theory of computing. New York: ACM, 2002: 380 - 388.
- [4] Stanford P2P sociology [EB/OL]. [2008 - 05 - 03]. <http://p2p.stanford.edu/index.html>.