第 35 卷 第 7 期 计 算 机 工 程 2009 年 4 月
Vol.35 No.7 Computer Engineering April 2009
·安全技术· 文章编号：1000—3428(2009)07—0150—03 文献标识码：A 中图分类号：N945

P2P 系统中一种基于声誉的混合抗污染机制

齐 梅，郭亚军，严慧芳
(华中师范大学计算机科学系，武汉 430079)

摘 要：提出一种新的基于节点声誉和目标声誉的混合抗污染机制。该机制由投票节点的声誉决定选定的目标文件的声誉。节点声誉通过引入严厉的惩罚策略及投票激励机制，有效孤立了污染者，刺激了用户对文件污染的警觉度，阻止污染的进一步扩散。仿真结果表明，与目标声誉系统相比，该机制收敛更快，抗污染性能更好。

关键词：P2P 系统；文件污染；混合声誉机制

Hybrid Anti-pollution Mechanism Based on Reputation in P2P Systems

QI Mei, GUO Ya-jun, YAN Hui-fang
(Department of Computer Science, Central China Normal University, Wuhan 430079)

【Abstract】This paper proposes a hybrid anti-pollution mechanism based on Peer reputation and object reputation where the reputation of selected object is determined by the reputation of voting Peers. Severe penalty strategy and polling incentive mechanism are introduced in computing Peer reputation, which can isolate the polluters effectively, stimulate users' awareness for file pollution, and avoid pollution further spreading. Simulation results show that compared with object reputation system, hybrid reputation mechanism converges faster, and has better performance of anti-pollution.

【Key words】P2P systems; file pollution; hybrid reputation mechanism

1 概述

现有的 P2P 文件共享系统由于充斥着大量的污染文件而极大地降低了系统的有效性。据调查，在 FastTrack/KaZaA 系统中，高达 80%的文件副本被污染[1]。而在 eDonkey 系统和 Overnet 网络中，被污染的主题也超过 50%。污染者的目标是篡改文件的内容，使其不可用，然后将污染文件注入到网络中，与具有相同元数据的非污染文件共存。下载了污染文件的用户不仅消耗了没必要的带宽，而且极有可能在未检查文件有效性的情况下共享这些污染文件，被动地进行污染传播。假如这些污染文件还携带病毒、木马或其他恶意程序，那么用户的损失将不堪设想。因此，有必要隔离污染者，同时激励用户删除下载的污染内容，最小化被动污染传播。

之前已有许多关于减少污染传播的研究，但都集中在分析不同污染传播的机制和建模上[2-4]，还有一些提出了减少污染的一般方法[1,3]。而文献[5-6]提出了实际的解决方案。目前存在 2 种基于声誉的抗污染机制，分别是基于节点声誉的抗污染机制和基于目标声誉的抗污染机制。Eigentrust[5]通过计算每个节点的全局声誉确立信任，是典型的基于节点声誉的系统，但是它需要已存在的信任节点集合，不能抵抗共谋行为。Credence[6]采用了基于目标声誉的方法。它的基本原理是使用一个网上投票方案对目标文件进行评价。用户在下载目标前，利用一个分布式的投票采集协议收集其他用户对目标的正面和负面评价。由于 Credence 关注的不是动态节点的声誉，而是目标文件的真实性，因此能够有效地隔离污染目标，但其收敛性很慢。而且它每一次的投票都通过加密解密来传递，计算量很大。同样，XRep 和 X^2Rep 系统引入了目标声誉机制。它们是用节点过去的投票行为作为其投票权重，但是声誉信息并没有在节点间传播，投票的计算和传播都需要节点在线，因此，不适用于动态的 P2P 环境。另外，以上基于目标的声誉系统都需要用户的投票参与，却没有相应的激励机制。

本文提出了一种基于节点声誉和目标声誉的混合抗污染机制。该机制结合了 2 种策略的优点，利用投票机制对目标文件进行投票，每一投票的权重由投票节点的本地声誉决定。节点的本地声誉引入了惩罚和奖励因子，对上传污染文件的节点给予严厉的惩罚，达到隔离恶意节点的目的。同时，促使用户节点尽快删除共享的污染文件，减少污染传播。而且，用户节点的投票参与行为会影响其本地声誉，这在一定程度上激励了它们的诚实投票行为，提高了非污染文件下载率。

2 混合声誉机制

混合声誉机制包括 2 个基础部分：目标声誉和节点声誉。目标声誉是对要下载的目标文件的真实性进行评价，是评价 P2P 文件共享系统可用性最直接的标准，也是用户的最终目的。而节点声誉则促进了对目标的准确评价。

2.1 目标声誉

用户在下载选定的目标 o 之前，先发布一个 Object-Voting-Query 消息来收集对目标 o 的投票。在对目标的投票过程中，消息的传递采用广播的形式：一个节点 p 发送一个

基金项目：中国博士后基金资助项目(20070410953)；湖北省自然科学基金资助项目(2005ABA243)
作者简介：齐 梅(1983－)，女，硕士研究生，主研方向：信息安全；郭亚军，副教授、博士后；严慧芳，硕士研究生
收稿日期：2008-06-20 **E-mail：**qimei1218@163.com

Query 消息给与它直接相邻的节点，该节点收到消息后检查是否有下载目标文件的经历：如果没有，则通过它拥有的所有连接将消息传递出去；如果有，则返回 Responds 的投票信息，再将消息传递出去。这样，系统中的每个节点都起到了路由器的作用。投票完成后，每个节点都会在本地数据库存储自己的投票信息。

假设 V_o^j 表示节点 j 对目标 o 的投票，那么

$$V_o^j=\begin{cases}-1 & polluted\\ 1 & unpolluted\end{cases}$$

表示污染文件与非污染文件。收集完投票后，用户节点 i 通过下式计算目标 o 的声誉：

$$R_o^i=\sum_{j\in N_o^i}(V_o^j\frac{R_j^i}{\sum_{j\in N_o^i}R_j^i})$$

其中，R_o^i 表示 o 的声誉值；N_o^i 表示节点 i 的 Object-Voting-Query 的 Responds 节点集。每一个响应节点 j 对目标 o 的投票权重由 j 的本地声誉 R_j^i 决定。为了抵抗对目标的共谋和诽谤攻击，用户根据自己的情况设置一个信任阈值 R_{thold}^i，只有当 $R_j^i\geqslant R_{\text{thold}}^i$ 时，j 的投票才有意义，反之则不予考虑。而且，用户只从本地声誉高于 R_{thold}^i 的源节点处下载目标文件。

2.2 节点声誉

节点的本地声誉由直接经验和其他节点的推荐构成，分别称为节点的直接信任和推荐信任。

2.2.1 直接信任

为了鼓励用户的投票行为，防止共谋和诽谤攻击，将节点 i 对节点 j 的直接信任分为 2 个部分：i 对 j 的直接交互经验以及 i 对 j 的投票相似经验。

假设 I_j^i 表示节点 i 对节点 j 的直接交互经验，即节点 i 从节点 j 处下载文件的信任度；

$$s=\begin{cases}-1 & polluted\\ 1 & unpolluted\end{cases}$$

表示每一次节点 i 从节点 j 处下载文件的评价。在每一次从 j 处下载文件后，i 会更新与 j 的直接交互经验：

$$I_j^i=I_j^i\mathrm{e}^{\left[\alpha(s+1)+\beta(s-1)n^2\right]} \tag{1}$$

其中，$E=\mathrm{e}^{\left[(s+1)\alpha+(s-1)\beta\right]}$ 是惩罚和奖励因子；n 表示到目前为止所有从 j 处下载的污染文件的数目；$\alpha<\beta$。当下载了污染文件时，$E=\mathrm{e}^{-2\beta n^2}$ 导致节点的信任值迅速下降；当下载的是非污染文件时，$E=\mathrm{e}^{2\alpha}$ 使节点的信任值增加。由式(1)可知，虽然节点上传非污染文件会提高信任度，但增长缓慢，而一旦节点上传的是污染文件，即使是偶尔的恶意上传行为，也会令信任度迅速降低。因此，长期上传污染文件的恶意节点能被有效地隔离开。

Credence[6]系统提出，如果 2 个用户节点对同一文件具有相似的评价，那么可以推断这 2 个节点之间存在某种直接信任关系。本文将这种信任关系转化为信任度表示，称为相似信任度 V_j^i。在节点 i 和节点 j 的投票经验中，如果存在对相同的 m 个文件的投票经验，N_{ij} 表示这 m 个文件集，那么

$$V_{ij}=1-\frac{\sum_{o\in N_{ij}}\left|V_o^i-V_o^j\right|}{2m}$$

显然，$V_{ij}\in[0,1]$。V_{ij} 越大，代表 i 与 j 对文件的评价越相似，因此，i 对 j 的信任度越高；反之，如果 V_{ij} 太小，j 的评价总是与 i 相悖，那么 j 可能是恶意诽谤。设定 $V_{ij}=0.5$ 为相似信任阈值，D_j^i 表示总的直接信任度，则

$$D_j^i=\eta I_j^i+\mu\left(V_{ij}-0.5\right) \tag{2}$$

其中，η 和 μ 是调整直接交互经验和投票相似经验的权重因子，$\eta+\mu=1$。由式(2)可知，节点的投票行为会影响直接信任度。当 $V_{ij}>0.5$ 时，i 对 j 的投票相似经验较高，直接信任度会增加；当 $V_{ij}<0.5$ 时，i 对 j 的投票相似经验较低，直接信任度反而会减少；当 $V_{ij}=0.5$ 时，投票相似经验不影响直接信任度。假定当 i 和 j 之间不存在对相同文件的投票经验时，V_{ij}=0.5。

式(2)从 2 个方面激励了用户节点的投票行为：

(1)激励了节点投票参与的热情；

(2)激励了节点的诚实投票。

因此，上传好的文件并且诚实又积极响应投票的节点，其直接信任度较高。每次交互后，积极的节点都会对下载的目标进行投票，然后更新 D_j^i，将投票信息存储在本地数据库中。

2.2.2 推荐信任

推荐信任捕捉了网络中与 j 交互过的其他节点对 j 的评价。节点 i 发送 Query 消息给与其交互过的其他节点，得到关于 j 的 Responds 信息，即推荐值。然后 i 计算关于 j 的推荐信任：

$$ID_j^i=\sum_{k\in N_j^i}(C_kD_j^k)$$

其中，N_j^i 表示响应节点列表；C_k 为节点 k 的推荐权重。

本文通过节点 k 的本地声誉来衡量其推荐权重：

$$C_k=\frac{R_k^i}{\sum_{k\in N_j^i}R_k^i}$$

其中，R_k^i 表示当前 i 对 k 的本地声誉评价。

同样，通过信任阈值 R_{thold}^i 甄选推荐。只有当 $R_k^i\geqslant R_{\text{thold}}^i$ 时，k 的推荐才有意义，反之，则不予考虑。如果未收到任何关于 j 的推荐，那么 $ID_j^i=0$。

2.2.3 本地声誉

节点 i 对节点 j 的本地声誉评价为

$$R_j^i=R_{\text{init}}+(1-\varepsilon)D_j^i+\varepsilon ID_j^i$$

对于刚加入系统的节点，设其初始本地声誉为 R_{init}。并设 $\varepsilon(0<\varepsilon<1)$ 是调整直接信任和推荐信任的权重因子。加入不久的节点由于直接交互信息少，更愿意相信来自其他节点的推荐信息，因此可以将 ε 设置大得些；有一定交互经验的节点更愿意相信自己的判断，ε 可设置得小些。

2.1 节和 2.2.2 节中提到的信任阈值 R_{thold}^i 表示节点 i 信任其他节点的最小声誉。设 R_{thold}^i 与 R_{init} 之间满足 $0<R_{\text{thold}}^i<R_{\text{init}}$。当节点 j 的本地声誉 $R_j^i<R_{\text{thold}}^i$ 时，显然 j 是恶意节点，i 将不会考虑它的投票意见以及推荐，也不会下载其提供的文件，同时拒绝上传文件给它。这样就完全孤立了恶意污染者。研究表明，有许多用户在下载完文件后并不会立即检查文件的真实性，而会继续保留在文件夹中共享。也就是说，如果下载了污染的文件，他们会在非恶意的情况下被动地进行污染传播。由于抗污染传播必须依赖用户下载后的检查删除意识，因此期望用户节点为了自己的声誉，会尽快删除共享的污染文件。

3 仿真实验与结果分析

3.1 仿真设置

本节模拟了一个无特殊结构的 P2P 文件共享系统来评估提出的混合声誉机制的抗污染性能。

在仿真实验中，假设有 50 个不同的文件主题，每个文件主题有 50 个不同的版本，而每个版本又有很多的复本，受欢迎程度越高的版本文件，其复本越多。仿真初始，系统中总文件数为 10 000。节点对文件主题的选择服从 Zipf 分布，Zipf 指数的取值在 $[0.63,1.24]$ 之间。选定主题后，节点挑选当前复本数最多的版本文件进行下载。

将系统中的节点分为 3 类：污染节点，非污染节点和搭便车(free-riding)节点。free-riding 节点只从其他节点处下载文件而不共享自己的资源。仿真初始，污染节点只共享污染文件，而非污染节点只共享非污染文件，free-riding 节点不共享任何文件。仿真过程中，非污染节点有可能被动地共享污染文件。节点可能在线，也可能不在线。

根据以上分析，仿真环境设置如下：

(1)网络环境

节点总数：1 000；

非污染节点：800；

污染节点：100；

free-riding 节点：100；

初始非污染节点：40；

初始污染节点：80；

在线时间大于 5 h 的节点：500。

(2)共享文件

共享文件总数：10 000；

共享文件主题 50；

每个主题的版本：50；

共享文件选择：Zipf 分布。

假设实验中混合声誉模型 Hybrid 的具体应用参数为：$R_{\text{init}}=0.4$，$\alpha=0.25$，$\beta=0.5$，R_{thold}^{i} 因节点而异，都设在 0.2~0.4 之间。

3.2 仿真结果分析

因为下载者只能靠自己手工检验才能判断文件是否污染，所以节点对文件污染的警觉度越高，污染效果越差。本文提出混合声誉机制的目的就是刺激用户对文件污染的警觉度，尽早删除污染文件，阻止污染传播。假设用户节点对文件污染的警觉度为 λ，根据 λ 的不同，分别比较了 Hybrid_1, Hybrid_2 与 Credence 的每日非污染文件下载率，仿真结果如图 1 所示。其中，Hybrid_1 表示应用混合声誉机制的最理想情况，即非污染节点的 $\lambda=100\%$，所有受到惩罚的非污染节点都尽快删除了所有共享污染文件时的下载情况。由于 free-riding 节点下载完文件后会立即检验文件的有效性，因此 free-riding 节点的 $\lambda=100\%$，在这里 free-riding 节点可以不予以分析。Hybrid_2 表示应用混合声誉机制的一般情况，考虑非污染节点的 $\lambda=50\%$ 时的下载情况。从图 1 可以看到，Hybrid_1 由于用惩罚机制刺激节点的警觉度达到最高，促使用户删除了所有共享的污染文件，因此收敛速度很快；Hybrid_2 虽然警觉度仅为 50%，但收敛速度也比较快；而 Credence 只是单纯的目标声誉系统，仅仅对下载目标进行了投票，虽然最终也能隔离所有的污染源，但由于没有对污染源节点的惩罚机制，其收敛速度缓慢。再者，Credence 没有对节点的投票激励机制，投票反馈行为也影响了下载率，所以，其效率最差。

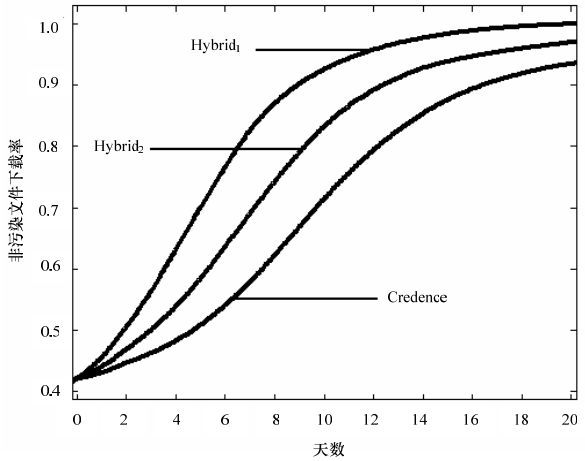

图 1 每日非污染文件下载率

4 结束语

本文提出了一种 P2P 文件共享系统中基于节点声誉和目标声誉的混合抗污染机制，通过节点声誉决定目标声誉。节点声誉中引入了惩罚和奖励因子及节点投票激励机制，目的在于提高目标声誉的准确性。仿真结果表明，该混合机制提高了非污染文件的成功下载率，有效减少了污染传播，与目标声誉系统 Credence 相比，由于提高了用户对文件污染的警觉度，引入了促进用户投票反馈的激励机制，因此其收敛速度更快。今后的研究将侧重于确立更精确、详细的用户模型以及攻击模型，考虑在各种具体的污染策略下对本机制的评估。

参考文献

[1] Liang Jian, Kumar R, Ross K W. Pollution in P2P File Sharing Systems[C]//Proceedings of IEEE INFOCOM'05. [S. l.]: IEEE Press, 2005.

[2] Benevenuto F, Costa C, Vasconcelos M, et al. Impact of Peer Incentives on the Dissemination of Polluted Content[C]//Proc. of ACM SAC'06. Dijon, France: ACM Press, 2006: 1875-1879.

[3] Thommes R, Coates M. Epidemiological Modeling of Peer-to-Peer Viruses and Pollution[C]//Proc. of IEEE INFOCOM'06. Barcelona, Spain: IEEE Press, 2006.

[4] Kumar R, Bagchi A, Ross K, et al. Fluid Modeling of Pollution Proliferation in P2P Networks[C]//Proc. of ACM SIGMETRICS'06. Saint-Malo, France: ACM Press, 2006.

[5] Kamvar S, Schlosser M, Garcia-Molina H. The Eigentrust Algorithm for Reputation Management in P2P Networks[C]//Proc. of Int'l WWW Conference. [S. l.]: IEEE Press, 2003.

[6] Walsh K, Sirer E G. Fighting Peer-to-Peer SPAM and Decoys with Object Reputation[C]//Proc. of ACM Workshop on Economics of Peer-to-Peer Systems. [S. l.]: ACM Press, 2005.

编辑 张 帆