P2P 网络下分布式带激励的信任模型设计与研究①

Design and Research of a Distributed P2P Network Trust Model with Incentive

陈崇来　张瑞林　方志坚　毛景新　(浙江理工大学 软件工程研究所 浙江 杭州 310018)

摘　要： 由于 P2P 网络无中心、匿名性等特点，传统的基于 PKI 安全机制不能很好地保障其安全，设计一个有针对性的信任机制来保障 P2P 网络的安全是非常有意义的，在现有信任机制研究成果的基础上提出了一种更加完善的信任机制，基于模拟人类社会推荐信任评价安全策略，具有节点区分、严格奖惩的激励机制，通过模拟试验，与基于投票的信任机制相比，该信任机制能够更好地促进 P2P 网络的正常交易，抑制恶意的、破坏性的交易，确保 P2P 网络的安全性、稳定性。

关键词： P2P 激励 动态信任模型

1　引言

目前 Internet 网上流行的 P2P 文件共享系统，如 E-mule，BitTorrent，KaZaa 在传输音乐文件，视频文件，给大家交流文件提供了很好的平台，然而在这些 P2P 文件共享系统中，存在着恶意的行为模式，如搭便车行为[1](只是下载内容而不提供上载)，钓鱼式攻击(声称是网络中流行的有用文件，但实际上是一个假文件或恶意文件，不仅会影响下载用户，而且还浪费网络带宽，更有甚者，这个文件还会传播到其它的网络节点)。从文献[2]的研究来看，KaZaa 中有 80%的文件副本是被污染的。因此我们需要寻找一种解决方案来解决这个问题，即孤立网络中这些受污染的节点，并且鼓励这些节点把受污染的文件删除。

2　研究现状及信任模型的提出

已经有大量的文献试图解决这方面的问题，如文献[3－5]主要分析污染文件的机制，主要机制有伪元数据拷贝(插入一个污染文件副本，但是它拥有与正常文件相同的元数据描述)，伪 ID 对象拷贝(污染的文件对象的 ID 与正常的文件对象 ID 是相同的)，文件索引修改(破坏节点的文件索引，使之找不到原有的文件)，这些文献也给出了一些解决方案，但是这些方案还须进一步评价。

在已有的分布式信任机制中 Eigentrust，Xrep[6] 较有影响力。Eigentrust 是一个全局信任模型，每一个节点的信誉值是通过收集网内其它所有节点的评价而计算出来的，它需要网内事先有较高信誉的节点，但这是不现实的。Xrep 是一个基于投票的信任机制，从一个节点下载之后，认为内容是没有污染的，就给出一个评价值，但是它只使用节点本地的信誉信息来计算信任值，而且缺少奖惩机制。

为此，本文提出一种新的，带激励的分布式节点动态信任模型(下文用 New trust system 表示)，它能快速鉴别和严惩恶意节点，同时能让知错就该的节点一个恢复自己信誉的机会，在计算节点的信任值时，不仅考虑了节点本地的评价信息，同时也考虑了其它节点群的评价信息，类似人类社会中人们不仅会根据自己的经验信息而且还会考虑朋友的推荐信息来了解陌生人，进而评估陌生人是否可信。为了分析本方案的有效性，将它与基于投票的信任系统(Base vote system)[7]做比较。

① 收稿时间:2008-09-12

3 信任模型的设计

信任模型的设计主要从设计目标，以及涉及的相关概念及定义来介绍，最后用场景实例说明这个模型的工作过程。

3.1 设计目标

a)需要一个隔离和孤立受污染的节点机制，且鼓励被动受污染的节点删除污染的内容。

b)建立一套奖惩机制，惩罚节点在网络中有恶意行为，鼓励节点真实的行为。

c)系统初始化节点时，或新加入的节点没有较高的信任值。

3.2 概念及定义

在网络中，每个节点都可以对其它节点做评价，评价包括两部分：一个是个人评价，另一个是群体评价。

定义 I_{ij} 为节点 i 对节点 j 的个人评价，称个人评价，且

$$I_{ij}=\begin{cases}\max(0,I_{ij}-\alpha_d n)\\ \min(1,I_{ij}+\alpha_u n)\\ V_{init}\end{cases} \quad (1)$$

n 是节点 i 从节点 j 下载受污染内容的次数，主要目的是惩罚提供污染内容的节点。α_d和α_u分别为惩罚因子和奖励因子，调节奖惩程度的，并设定$\alpha_d > \alpha_u$，使得系统个人评价值升高的慢但下降的快，能有效严惩节点的恶意行为，V_{init} 为每个节点对其它节点评价的初始值。当下载的内容是是受污染时，I_{ij} 为 $\max(0,I_{ij}-\alpha dn)$，当下载的内容是真实的时，I_{ij} 为 $\min(1,I_{ij}-\alpha_u n)$，节点 i 对节点 j 一无所知时，$I_{ij}$ 为初始值 V_{init}。

定义 C_{ij} 为网络中与节点 i 有联系的其它节点们对节点 j 的评价，称群体评价，且

$$C_{ij}=\begin{cases}\dfrac{\sum_{k\in RL_{ij}} R_{ik}I_{kj}}{\sum_{k\in RL_{ij}} R_{ik}}\\ V_{init}\end{cases} \quad (2)$$

RL_{ij} 为节点 i 为了解节点 j 的群体评价，发出群体评价查询请求后有响应且对节点 j 有交往的节点列表。R_{ik} 为节点 i 对节点 k 的信任值，I_{kj} 为节点 k 对节点 j 的个人评价，V_{init} 为当有响应的节点列表为空时，C_{ij} 所设定的初值，即每个节点对其它节点评价的初始值。

定义 R_{ij} 为节点 i 对节点 k 的信任值，

$$R_{ij}=\beta C_{ij}+(1-\beta)I_{ij} \qquad 0\le\beta\le 1 \quad (3)$$

C_{ij} 为群体评价，I_{ij} 为个体评价，β为两者之间的权衡因子。当β大于 0 时，节点就可以通过群体评价来提高其它节点对自己的信任值了。

另外，为了孤立恶意节点，设置 Rthreshold(i) 节点 i 判断其它节点是否信任的一个阀值，且 0≤Rthreshold≤Vinit，当节点 i 发现对节点 j 的信任值小于 Rthreshold(i)，节点 i 就认为此节点 j 不可信任的节点，拒绝节点 j 从此节点下载内容，触发节点 j 删除受污染的内容，为节点 j 恢复信任值做好准备。为了使节点能更好地恢复信任值，每个节点可以根据自己的兴趣爱好设置不同的 $R_{threshold}$，但是必须要满足 $0\le R_{threshold}\le V_{init}$。

3.3 模型工作流程及场景举例

模型工作流程分 5 个步骤：信任初始化、信任查询、信任计算、信任评估和信任更新。如图 1 所示：

图 1　模型工作流程

信任初始化：主要完成节点的信任值初始化，如信任阀值、参数值设置，推荐节点的初始设置，查询协议时间间隔设置等；

信任查询：每隔一定时间发送信任查询，以取得推荐节点信任数据库的最新信任值；

信任计算：当节点发起下载请求时，根据自己的历史积累的经验和推荐节点的推荐信息，依照前文公式(3)计算出最终的信任值；

信任评估：将计算出的信任值与自己设定的信任

阀值相比较，大于阀值的，就从目标节点下载，否则就放弃。

信任更新：当节点下载完成后，发现内容是真实完整的或是受污染的，就用前文公式(1)计算新的个人评价值，并更新自己的信任数据库；

以下举个场景说明这个信任模型，假设 P2P 网络中，有三个节点，a，b 和 c，系统的参数设置是这样子的，$R_{threshold}(a)=0.35$，α_d和α_u分别为 0.3 和 0.2，β等于 0.4，$I_{ac}=I_{bc}=0.5$，$C_{ac}=0.5$，$R_{ab}=0.8$。

当节点 a 从节点 c 下载了个文件，发现是受污染的文件，则 $I_{ac}=0.5-0.3=0.2$，$R_{ac}=0.4*0.5+0.6*0.2=0.32$，而 $R_{threshold}(a)=0.35$，当节点 c 想从 a 节点下载时，节点 a 发现 $R_{ac}<R_{threshold}(a)$，节点 a 拒绝 c 下载，这触发了节点 c 删除受污染的共享文件，在接下来的两个时间单位内，节点 b 下载了 c 的一个健康文件，从而 $I_{bc}=0.7$，此后，当节点 a 发出群体评价查询时，节点 a 知道了 $I_{bc}=0.7$，从而 $C_{ac}=0.7$，$R_{ac}=0.4*0.7+0.6*0.2=0.4$，节点 a 认为节点 c 又是可信的了，这样就允许节点 c 下载节点 a 的内容了，从而鼓励系统中节点删除自己受污染的贡献文件，信任值的变化过程可以参见图 2。

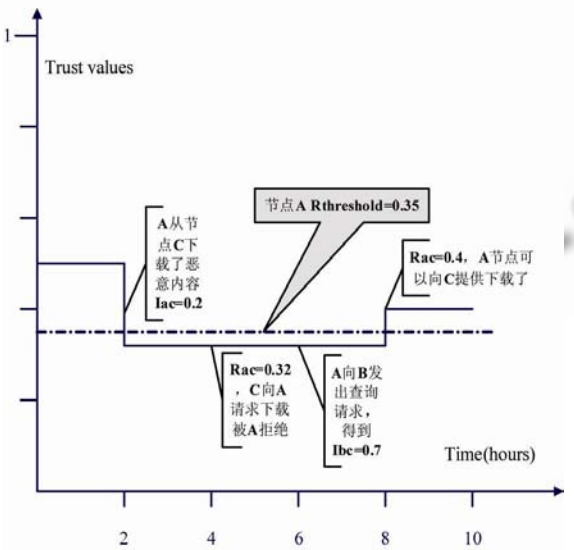

图 2　节点间信任值的变化情况

4　评价方法及实验

由于实际 P2P 网络环境比较复杂又较难以实验，本文通过程序来仿真实验，程序模拟器是一个基于事件驱动 P2P 文件共享系统，针对基于投票的信任系统和新的信任系统进行仿真，取得数据后，用健康文件的下载百分比(percents of health downloads)与稳定网络所用的时间(time)来衡量，以下是实验条件和实验结果。

4.1　实验假设条件

实验基于以下假定：

①网络的路由和对象发现是非常及时的，一个节点可以随机地从多个节点下载，而且各节点的共享内容一直都提供下载服务，且传输时间忽略不计。

②文件对象由 F 标识，每个文件的版本由 V 标识，节点随机选择下载时，遵循 Zip f 分布规律。

③节点的类型，假设有两种节点类型，提供健康文件的好节点和提供受污染文件的恶意节点，恶意节点仅仅提供受污染文件的下载，不下载别的节点的内容，也不退出这个网络。

④污染节点传播类型，这里考察伪元数据拷贝攻击和伪 ID 对象拷贝攻击[2]。

表 1　模拟节点类型行为参数表

参数	善意节点	恶意节点
各种类型节点数	1700	300
共享的文件对象数	200	900
下载的速率	40 个/天	0
平均下载时间间隔	8 小时	不下载

实验系统参数表见表 1，另外初始值约定如下：$\alpha_d=0.4$，$\alpha_u=0.2$，$V_{init}=0.5$，$R_{threshold}(a)$在 0.1 与 0.4 之间，群体评价查询间隔时间为一小时，在基于投票的信任系统(Base vote system)[7]中，我们假设所有的投票都是正确的，且在每次下载前更新节点相关性表，运行 GOOSIP 协议的间隔时间也设为一小时。

4.2　实验结果

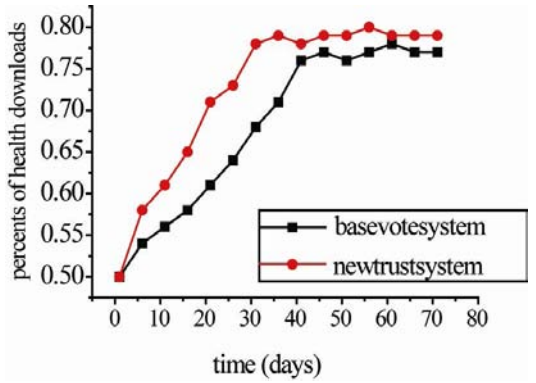

图 3　伪元数据拷贝攻击下的实验结果对比

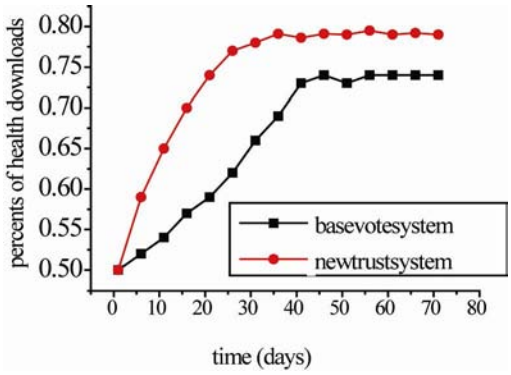

图 4 伪 ID 对象拷贝攻击下的实验对比结果

从图 3 和图 4 的实验结果中可以看出，在考察的这两种攻击(伪元数据拷贝攻击和伪 ID 对象拷贝攻击)下，与基于投票的信任系统(Base vote system)相比，起初，两个系统里健康文件的下载率都在不断地提高，最后两个系统都能在某个范围值上达到相对平衡，但本文提出的 New trust system，更具优势，效率更高，节点下载到的健康文件的几率也更大。

5 结论

本文提出了一个新的分布式带激励的节点动态信任模型(New trust system)，从伪元数据拷贝和伪 ID 对象拷贝这两种污染文件传播方面考察了这个系统和基于投票的系统，实验结果表明，在时间比较长的情况下，这两个系统都能遏制污染文件的传播，但是这个新系统更有效率，而且系统能较快地达到平衡稳定。但是该系统没有对别的攻击类型进行考察，有待于在接下来的工作中仔细研究其他攻击场景。

参考文献

1 Adar E, Huberman BA. Free riding on Gnutella.First Monday, 2000,5(10):6－8.

2 Liang J, Kumar R, Xi Y, Ross K W. Pollution inP2P File Sharing Systems. Proceedings of IEEE Infocom 2005.24th Aunual Joint Conference of the IEEE Computer and Communications Societies. Miami: FL, 2005:1174－1185.

3 Christin N, Weigend A, Chuang J. Content Availability, Pollution and Poisoning in File Sharing Peer-to-Peer Networks. Proc. 6th ACM Conf. on Electronic Commerce. Canada: Vancouver, 2005.

4 Kumar R, Yao D, Bagchi A, Ross K, Rubenstein D. Fluid Modeling of Pollution Proliferation in P2P Networks. Proc. ACM Sigmetrics. France: Saint-Malo, 2006.

5 Thommes R, Coates M. Epidemiological Modelling of Peer-to-Peer Viruses and Pollution. Proc. IEEE Infocom Spain: Barcelona, 2006.

6 冯真.P2P 环境下文件共享的声誉系统研究.郑州:解放军信息工程大学, 2006.

7 Walsh K, Sirer EG. Fighting Peer-to-Peer SPAM and Decoys with Object Reputation. Proc. Economics of P2P Systems, Philadelphia: PA, 2005.