基于反馈相关性的P2P网络信任模型

王 勇 侯 洁 白 杨 夏 云 秦志光
(电子科技大学计算机科学与工程学院 成都 611731)

摘 要 用户对P2P网络安全性的需求刺激了信任模型的发展。在分析现有信任模型的基础上,提出了基于反馈相关性的动态信任模型——CoDyTrust。其在时间帧的基础上,采用虚假信任过滤机制和信任聚合机制,并在信任值计算中引入信任相关系数、信任遗忘因子、滥用信任值和推荐信任度等,通过反馈控制机制动态调节这些模型因子,在准确评价节点对不同资源信任的同时,实现网络中恶意行为检测。比较分析结果表明,CoDyTrust能够更好地反映网络中节点行为,准确检测恶意节点,有效抵御振荡、撒谎和合谋等攻击。

关键词 P2P网络,信任模型,虚假信任过滤,信任聚合
中图法分类号 TP311.11 **文献标识码** A

Survey on Feedback Correlation Based Dynamic Trust Model for P2P Systems

WANG Yong HOU Jie BAI Yang XIA Yun QIN Zhi-guang
(Department of Computer Science and Engineering, University of Electronic and Science Technology of China, Chengdu 611731, China)

Abstract Users' demands for the security of peer-to-peer network stimulate the development of trust model. By analyzing the previous trust and reputation systems, we proposed a novel feedback correlation based dynamic trust model for P2P systems, namely CoDyTrust. The trust model adopts fake trust filtering and trust aggregation mechanisms based on the time frames, and introduces several factors in the calculation of the global trust value, including correlation coefficient, trust forgetting factor, abused trust value and recommended trust. The factors can be adjusted dynamically through the feedback control mechanism. CoDyTrust can reflect the trust status of a node in the system, while providing the function of detecting malicious behaviors. The experimental results indicate that CoDyTrust can accurately detect malicious peers, which has the ability of defending strategic altering behavior, lying and collusive attack as well.

Keywords Peer-to-peer network, Trust model, Fake trust filtering, Trust aggregation

1 引言

随着P2P应用的日益流行,与之相关的各类安全问题威胁着用户数据安全,阻碍了P2P网络应用的快速发展。信任机制通过节点间的历史交易信息来评定节点信任高低,为后续交易选择提供依据。作为一种有效的节点行为度量体系,信任模型能够增强P2P网络的鲁棒性,提高网络整体性能和服务质量。研究者们相继提出了基于向量、基于群组、基于多因子以及基于Bayesian的信任模型,这些模型能够抵御不同的节点攻击行为,较准确地反映节点的真实信任状态,具有较好的可扩展性和健壮性。然而,随着P2P网络应用的发展和用户共享行为的转变,信任模型已经不能单纯地停留在加强系统对传统攻击的防御能力问题之上,如何解决节点自私行为带来的整体性能下降,如何检测并发现网络中这些自私行为,如何降低信任模型在计算和通信上带来的额外开销,这些问题还亟待进一步解决。

本文提出了基于反馈相关性的P2P网络信任机制——CoDyTrust,采用两层覆盖网络结构,引入节点反馈评价相关系数来过滤单个节点的虚假评价行为,聚合所有资源接收节点的真实反馈评价,引入团体信任和全局信任的概念,综合考虑时空因素的影响,结合历史信任状态和团体信任状态,建立全局信任度量体系。文中分析了该模型的通信复杂度和计算复杂度,以及CoDyTrust在各种典型攻击场景下的安全性。模拟实验结果显示,CoDyTrust具有复杂度不高、系统节点负载均衡的特点,能够准确地检测出网络中的恶意行为,有效抵御说谎、合谋等攻击。

2 相关工作

现有的信任模型可以归为集中式信任模型和分布式信任模型两类。其中集中式信任模型将网络中所有节点的信任值统一集中存储管理,这类模型需要认证服务器或少数的领袖节点来监督整个网络的运行情况,定期通告或惩罚违规节点。eBay[1]、淘宝等采用中心服务器存储管理用户的信任信息,每次交易完成后,交易双方相互评价,并将评价信息传到中心服务器上,评价信息分为正面评价(+1)、中性评价(0)、负面评价(-1),服务器将用户每次得到的评价累加形成最终用户信任值。eDonkey[2]等系统使用领袖节点(servers)管理网络中节点的信任数据,使用PKI技术通过认证服务器(CA)颁发证

到稿日期:2012-04-17 返修日期:2012-09-17 本文受国家242信息安全计划(2010A14),国家科技重大专项(2011ZX03002-002-03),四川省科技支撑计划(2010FZ0101)资助。

王 勇(1976-),男,博士,副教授,主要研究领域为网络信息安全,E-mail:cla@uestc.edu.cn。

书保障领袖节点的合法性。集中式信任模型易于管理，用户信任值计算高效，但依赖于少量中心管理节点，系统可扩展性较低，难以避免单点失效问题。

在分布式信任模型中，节点信任值的计算和存储都在本地进行，不需要中心服务器或领袖节点的参与，当前多数信任模型属于这一类型。分布式信任模型可以进一步分为两类，即全局信任模型和局部信任模型。

全局信任模型收集整个网络用户对某个节点的评价，并对这些评价进行分析，计算该节点惟一的信誉度。这里，信誉度是指一个节点在整个网络中具有的全局信誉值。EigenTrust[3]利用信任的传递特性，使用直接信任值计算全局信任值，认为直接信任值越高的节点推荐的信任值越可信，在计算全局信任时应赋予较大权重。该模型能抵御多种安全攻击，但普适性较差。Dou W 等人[4]在 EigenTrust 的基础上进行了改进，提出了 PowerTrust 模型，将得到评价数量显著多于其它节点的 Power 节点作为可信节点，在全局信任值计算过程中提出向前看随机游走(LRW)的策略，并借助 DHT 机制和 LPH(Locality Preserving Hashing)函数动态发现 Power 节点。这些改进方法使得 PowerTrust 抵抗恶意行为的能力相对 EigenTrust 有了显著的提高。然而，上述两种信任模型没有考虑时间维度，属于静态信任模型，对动态策略性行为的抵抗力较弱。L. Xiong 等[5]提出了一个动态信任模型 PeerTrust，其不仅将交易满意度反馈作为评估信任的参数，还考虑了交易总数目、反馈可信度、交易上下文因子、社区上下文因子等因素，分析实验结果表明，该模型具有较好的恶意行为抵御能力。针对节点的动态策略和不诚实反馈等恶意行为，Chang 等[6]提出了一个基于时间帧的动态信任模型 DyTrust，该模型使用时间帧标示出经验和推荐的时间特性，引入近期信任、长期信任、累积滥用信任和反馈可信度 4 个参数来计算节点信任度，通过反馈控制机制来动态调节这些参数。该信任模型具有很好的动态适应能力和反馈信息聚合能力，能有效地检测和惩罚恶意节点。Huang 等[7]提出了 DWTrust 模型，以降低信任建模和评估动态信任值的复杂性。DWTrust 采用了一个新的反馈控制机制，及时调整各因子的权重以反映信任环境的变化，该模型有效地降低了信任值的计算和节点通信开销。除了以上几种典型的信任模型以外，C Yang 等人[8]提出的基于声誉的信任模型 RepTrust、J Li[9]提出的 P2P 环境下基于相似度加权的信任模型、R Zhou 等人[10]提出的基于 Gossip 的信任值快速融合模型 GossipTrust 以及整合历史和当前节点信任数据的 PerformTrust[11]等都属于全局信任模型。全局信任模型考虑整个网络中节点的评价意见，能够较准确地反映节点的信任情况，但忽略了信任的私人化特征；此外，全局信任模型需要节点之间相互合作处理信任信息，随着网络规模的成长，计算和通信开销会显著增大，这类模型的可扩展性不高。

局部信任模型通过询问网络中有限个数的节点来获取某个节点的推荐度，综合自己和该节点交互的历史经验，确定节点的信任度，在这类模型中往往采取简单的局部广播手段。Y. Wang[12]提出了基于贝叶斯网络的信任模型，节点可以根据不同的场景来按需获取节点多方面的性能，该模型适用于节点间交互频繁的情况。NICE[13]使用全分布的用户信誉信息存储方式，节点存储的信任信息是其他节点对其所提供服务的满意度反馈，因此节点有动机存储信任信息。此外，PeerTrust 中的 PSM 度量体系以及石志国等人[14]提出的 TW-Trust 也属于局部信任模型。局部信任模型具有计算简便和计算结果收敛快的优点，但该类信任模型中得到的信任度比较片面，只结合了部分邻居节点的反馈，因此容易受到不可信节点和恶意节点的攻击。

此外，信任模型中的激励机制和隐私问题也是近年来关注的一个热点话题。文献[15]提出了一种基于节点信任度的的激励策略，胡建理等人[16]提出了一种具有激励效果的分布式 P2P 信任管理模型。在隐私保护方面，文献[17,18]分别提出了一种在计算分布式网络中信任值时保护隐私的方法，文献[19]提出了一种分布式的信任信息反馈隐私保护协议，Kinateder 等[20]提出了基于匿名网络的隐私信誉模型。

现有信任模型已经能较好地抵御 P2P 网络中的各种安全攻击，且已具有较高的效率，但仍存在很多问题和不足。如何提高系统恶意节点检测准确性，如何提高模型对节点振荡、撒谎以及合谋等安全攻击的抵御能力等问题还有待进一步的研究。本文针对这些问题进行了相应改进，提出了一个能准确检测系统恶意节点、有效抵御振荡、撒谎等攻击的信任模型——CoDyTrust。

3 基于相关系数的动态信任模型

3.1 网络结构

CoDyTrust 采用两层覆盖网络体系结构，如图 1 所示。其中，普通节点组成的下层网络为 Mesh 结构，普通节点间利用 P2P 机制实现资源共享，在每次共享交易完成后，将交易情况上报给超级节点组成的上层网络；超级节点所在的上层网络采用 KAD[21]结构，负责接收下层网络传递的交易评价信息，并存储和计算普通节点的信任值。这里，假设超级节点是相对稳定可信的。下层网络中的每个普通节点都与至少一个超级节点连接，每个超级节点负责管理指定 ID 范围的普通节点，当一个普通节点加入网络时，它随机地与不大于多个普通节点连接，接收并提供资源共享服务。网络中每个节点均拥有一个固定的 ID。

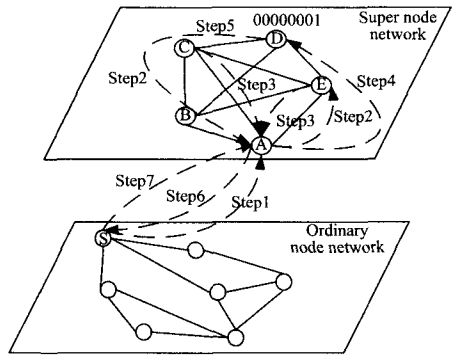

图 1 网络结构

当一个普通节点请求某个资源时，它向上层网络发送一个资源查询消息，上层网络返回拥有该资源的普通节点信息；请求节点接着向上层网络发送信任值查询消息，上层网络返回所有拥有该资源的节点信任值；请求节点选取信任值最高的节点发送资源请求消息，其接收到请求消息后根据对方的信任值决定是否提供资源发送服务，请求节点接收到所请求的资源后，根据服务的好坏给出该资源拥有节点的评价，将评价值发送给对应的上层超级节点。上层网络中的超级节点根据时间框架周期更新普通节点的信任值信息。

3.2 信任值计算

为了能及时反映一个节点最"新鲜"的信任状态，CoDyTrust 在计算过程中引入时间框架的概念：假设时间段$[t_{start}, t_{end}]$，将 $t_{start}\sim t_{end}$ 分为不同的子时间段$\{t_1, t_2, \cdots, t_n\}$ $(t_1<t_2, t_2-t_1=\Delta t)$。这里，将这些时间子片段称为时间框架，时间框架是从 0 开始的连续整数。假设在第 n 个时间框架中，节点 j 向网络中多个节点提供资源 R，i 是其中一个资源接收节点，第 3.2.1－3.2.5 节描述了时间框架 n 内节点 j 关于资源 R 的全局信任值计算过程。

3.2.1 直接评价信任值

在第 n 个时间框架内，节点 i 对节点 j 提供的资源 R 的直接评价信任 $D_{ij}^n(R)$值可表示为：

$$D_{ij}^n(R)=\frac{1}{m}\sum e_{ij}^n(R) \tag{1}$$

式中，m 是第 n 个时间框架内，节点 j 向节点 i 提供有关资源 R 的服务次数；$e_{ij}^n(R)$ 是第 n 个时间框架内，节点 i 给节点 j 的直接评价值，汇报时由接受服务节点 i 向 j 的监控节点发送，且 $e_{ij}^n(R)\in[0,1]$。

3.2.2 聚合信任值

定义 $Q_j^n(R)$为节点 j 在第 n 个时间框架内对于某一特定资源 R 的聚合反馈评价值。

假设 $Clt(j)$为时间框架 n 内接收过节点 j 提供资源 R 服务的所有节点的集合，m 为该集合元素个数，则节点 j 关于资源 R 的综合直接评价信任值 D_j^n 为：

$$D_j^n=\frac{1}{m}\sum_{b\in Clt(j)}D_{bj}(R) \tag{2}$$

引入皮尔森相关系数 $Corr_{ij}^n(R)$来评估单个节点 i 对节点 j 的直接评价信任值和节点 j 的综合直接评价信任值的相关性，即$[D_{ij}^1(R)\cdots D_{ij}^t(R)\cdots D_{ij}^n(R)]$和 $[D_j^1(R)\cdots D_j^t(R)\cdots D_j^n(R)]$之间的相关性，计算如式(3)所示。

$$Corr_{ij}^n(R)=\frac{1}{n-1}\sum_{t=1}^{n}\left(\frac{D_{ij}^t(R)-\frac{1}{n}\sum_{k=1}^{n}D_{ij}^k(R)}{\sigma_{D_{ij}^t(R)}}\right)\left(\frac{D_j^t(R)-\frac{1}{n}\sum_{k=1}^{n}D_j^k(R)}{\sigma_{D_j^t(R)}}\right) \tag{3}$$

式中，$\sigma_{D_{ij}^t(R)}$和 $\sigma_{D_j^t(R)}$分别是两个向量的标准差，其计算公式如式(4)、式(5)所示：

$$\sigma_{D_{ij}^t(R)}=\sqrt{\frac{1}{n-1}\sum_{t=1}^{n}\left(D_{ij}^t(R)-\frac{1}{n}\sum_{k=1}^{n}D_{ij}^k(R)\right)^2} \tag{4}$$

$$\sigma_{D_j^t(R)}=\sqrt{\frac{1}{n-1}\sum_{t=1}^{n}\left(D_j^t(R)-\frac{1}{n}\sum_{k=1}^{n}D_j^k(R)\right)^2} \tag{5}$$

特别地，当第 n 个时间框架内节点 j 提供的资源 R 只有一个节点 i 接收，则 $Corr_{ij}^n(R)=0$。

定义 $flag_{ij}^n(R)$为表示直接评价信任值 $D_{ij}^n(R)$是否有效的标志，则有：

$$corrThreshold_j^n(R)=\frac{1}{k}\sum_{t\in Clt(j)}Corr_{ij}^n(R) \tag{6}$$

$$flag_{ij}^n(R)=\begin{cases}0, & \text{if } Corr_{ij}^n(R)\leqslant corrThreshold_j^n(R)\\ 1, & \text{else}\end{cases} \tag{7}$$

定义体验信任度 Cu_{ib}^n为在第 n 个时间框架内，节点 i 对节点 b 的置信程度，特别地，$Cu_{ii}^n=1$。Cu_{ib}^n会根据交互双方的历史情况而更新，计算模式如式(8)、式(9)所示。

$$Cu_{ir}^n=\begin{cases}Cu_{ir}^{n-1}+\dfrac{1-Cu_{ir}^{n-1}}{2}, & \text{if } diff_{ir}^n<\theta\\ Cu_{ir}^{n-1}-\dfrac{Cu_{ir}^{n-1}}{2}, & \text{else}\end{cases} \tag{8}$$

$$diff_{ir}^n=\frac{\sum_{j\in CSet(i,r)}|D_{ij}^n-D_{rj}^n|}{|CSet(i,r)|} \tag{9}$$

式中，$CSet(i,r)$为节点 i 和 r 共同交互节点的集合。

结合式(2)－式(9)，可以得到节点 i 对 j 的聚合信任值计算：

$$Q_{ij}^n(R)=\frac{\sum_{b\in Clt(j)}flag_{bj}^n(R)*Cu_{ib}^n*D_{bj}^n(R)}{\sum_{b\in Clt(j)}flag_{bj}^n(R)*Cu_{ib}^n} \tag{10}$$

进而，节点 j 的综合聚合信任值可以表示为：

$$Q_j^n(R)=\frac{1}{k}\sum_{t\in Clt(j)}Q_{ij}^n(R) \tag{11}$$

3.2.3 当前信誉值

在第 n 个时间框架，节点 j 关于资源 R 的当前信誉值可表示为：

$$S_j^n(R)=(1-\rho)*S_j^{n-1}(R)+\rho*Q_j^n(R) \tag{12}$$

式中，ρ为信任遗忘因子，表示为：

$$\rho=\begin{cases}\rho_1, & \text{if } Q_j^n(R)-S_j^{n-1}(R)\geqslant-\varepsilon\\ \rho_2, & \text{else}\end{cases},\rho_2>\rho_1 \tag{13}$$

定义累积滥用信任 A_j^n 用以惩罚系统中的恶意行为。A_j^n 的初始值为 0，其更新函数表示为：

$$A_j^n=\begin{cases}A_j^{n-1}+(S_j^{n-1}(R)-Q_j^n(R)), & \text{if } Q_j^n(R)-S_j^{n-1}(R)>\varepsilon\\ A_j^{n-1}, & \text{else}\end{cases} \tag{14}$$

利用 A_j^n 可以得到 ρ_1 的计算公式：

$$\rho_1=\rho_1\times\frac{c}{c+A_j^n} \tag{15}$$

3.2.4 团体信任值

"抱团现象"是 P2P 等自组织网络的重要特性。计算节点服务的全局信任值时，将团体信任值考虑进来，可以减少团体自私行为对网络造成的影响。定义在时间框架 n 内，节点 j 所在团体 C 的信任值可表示为：

$$T_c^n=\frac{1}{k}\sum_{m\in e}\frac{1}{r}\sum_{l\notin c}\left[D_{lm}^n\times\frac{2E_m}{k_m(k_m-1)}\right] \tag{16}$$

式中，e 为团体 C 中边缘节点的集合；k 为团体 C 内的结点个数；r 为集合 e 的节点数目；k_m 为团体 C 中与边缘节点 m 连接的节点个数；E_m 为实际存在的连边数。

3.2.5 全局信任值

定义节点 j 提供资源 R 的全局信任值 $GT_j^n(R)$为：

$$GT_j^n(R)=\lambda*S_j^n(R)+(1-\lambda)*T_c^n \tag{17}$$

式中，λ为信誉度调节因子。

3.2.6 复杂度分析

本节将 CoDyTrust 与 EigenTrust、DyTrust、PeerTrust 以及 Xing[22] 等模型进行比较，分析模型的计算复杂度和通信开销，如表 1 所列。其中，在分析通信开销时，同时考虑消息传递和路由查找开销，由于 DyTrust 模型没有涉及网络应用环境，通信开销不适用于该模型。从表 1 的结果可以看到，CoDyTrust 在保障系统提供信任机制和恶意节点检测能力的同时，计算复杂度和通信开销均较低。

表 1 模型复杂度对比

信任模型	计算复杂度	通信开销
Xing's	O(MN)	O(N)+O(N)
PeerTrust	O(N³)	O(N)+O(logN)
DyTrust	O(N)	N/A
EigenTrust	O(N²)	O(MN)+O(logN)
CoDyTrust	O(N²)	O(N)+O(logN)

4 模拟实验分析

使用 Peersim[23] 进行模拟实验，检测 CoDyTrust 对恶意攻击的抵御效果，以验证模型的有效性。实验中使用的主要参数设置如表 2 所列。

表 2 模拟实验参数设置

参数名	描述	振荡攻击	撒谎	合谋攻击
S	当前信任值初值	0.5	0.5	0.5
Cu	推荐可信度初值	1.0	1.0	0.5
Q	聚合信任值初值	1.0	1.0	0.0
A	累积滥用信任初值	0.0	0.0	0.2
ϵ	评价误差最大容忍度	0.1	0.2	0.05
$\rho 1$	信任构建因子	0.09	0.09	0.1
$\rho 2$	信任损坏因子	0.3	0.3	0.5
c	惩罚控制因子	400	400	40
θ	评价差异最大容忍度	0.1	0.2	0.1
λ	自信度因子	0.8	0.8	0.8

4.1 信任值的构建和损坏

实验分别选择低初始信任值节点和高初始信任值节点，观察节点的良好行为和恶意行为对信任值的影响过程，结果如图 2 所示。可以发现，CoDyTrust 能够迅速对节点的恶意行为做出反应，同时，节点难以通过短时间内表现良好来提高信任值。即，CoDyTrust 使节点信任值上升速度慢于下降速度，节点重建信任需要付出比损坏信任更多的代价。

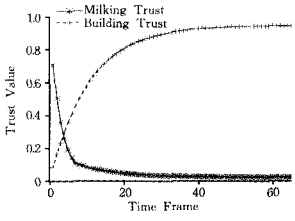

图 2 节点信任值构建与损坏

4.2 抵御振荡攻击

振荡攻击中，恶意节点首先表现良好，以获得一个较高的信任值，然后再发起恶意攻击，在信任值降到低于系统信任门限后，再次表现良好，进而恢复至较高信任值。

实验设置下层网络中节点数量为 80，恶意节点率为 0.3。假设恶意节点在其信任值达到 0.6 后开始进行恶意行为，当信任值下降到 0.2 后又开始表现良好，则 CoDyTrust 中振荡攻击恶意节点的信任值变化过程如图 3 所示。

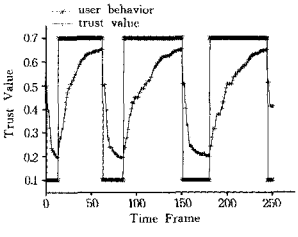

图 3 振荡攻击节点的信任值变化

从图 3 的曲线可以看到，恶意节点的信任值重建平均需要 58 个时间框架，而其信任值损坏平均需要 26 个时间框架，也就是说节点需要花两倍的时间来重建之前损毁的信任值。这一结果表明，恶意节点发起振荡攻击需要付出额外的代价，CoDyTrust 能够较好地抵御这类攻击。

4.3 抵御节点撒谎

撒谎攻击中，恶意节点作为资源接收节点以一定的概率给资源发送节点的监视节点发送虚假评价，这样监视节点计算出的普通节点的信任值不能真实地反映其信任情况。

这里定义误报率（False Positive Rate，FPR）和漏报率（False Negative Rate，FNR）作为模型检测恶意攻击节点能力的衡量指标，其中 FPR 是指被误评为恶意节点的非恶意节点占非恶意节点总数的百分比，FNR 是指被误评为非恶意节点的恶意节点占恶意节点总数的百分比。

对相同场景下的 CoDyTrust 和 DyTrust 模型进行了模拟比较实验，试验中设置下层网络规模为 120，撒谎节点比率为 25%，恶意节点比率为 80%，其它信任值计算过程中的参数设置参见表 2。两种信任模型中 FNR 值和 FPR 值的变化情况如图 4 和图 5 所示。

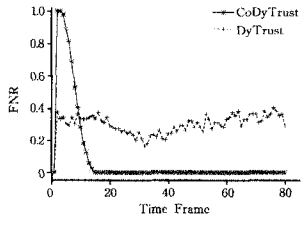

图 4 与 DyTrust 模型的 FNR 变化曲线的比较

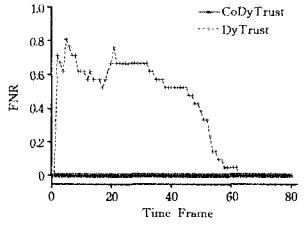

图 5 与 DyTrust 模型 FPR 变化曲线的比较

图 4 显示了相同参数下 CoDyTrust 与 DyTrust 模型 FNR 值变化趋势的比较。从该图可以看出，CoDyTrust 模型的 FNR 值经过 14 个时间框架就能降为 0，而 DyTrust 模型的 FNR 值一直在 0.3 上下波动，并没有下降趋势。这说明与 DyTrust 模型相比，本模型能很好地检测出恶意节点，被检测出的恶意节点将会逐渐从网络中孤立出来。

图 5 显示了 CoDyTrust 与 DyTrust 模型 FPR 值变化趋势的比较。观察该图可以发现，CoDyTrust 模型中 FPR 的值一直为 0，这表示 CoDyTrust 模型在恶意检测中不会将好节点误判为恶意节点，而 DyTrust 模型中的 FPR 值需经过 62 个时间框架才能降到 0，因此 DyTrust 在很长一段时间里都会有较高的误判率。

通过图 4 和图 5 中两种模型的对比结果可以看到，CoDyTrust 模型能很快地判断出节点是否进行不诚实反馈，并在信任值计算中将其不诚实的反馈值过滤掉，很好地减小了撒谎节点的影响。

4.4 抵御合谋攻击

合谋攻击中，恶意节点聚集成一个恶意团体，在团体内部，节点相互抬高服务评价，而对外它们可能共同陷害合法节点。因此，合谋攻击给系统带来的危害远远大于单个节点恶意攻击的危害。

实验设置下层网络中的节点数量为 80，恶意节点率为 0.3。图 6 显示了 CoDyTrust 模型在面临合谋攻击时系统 FPR 和 FNR 值的变化趋势。

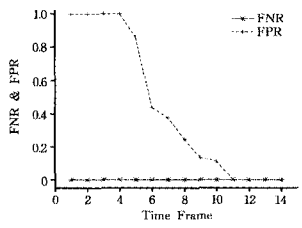

图 6 合谋攻击时 FNR 和 FPR 值的变化

观察该图可以看到，下层网络的 FPR 经过 10 个时间框

架后下降为 0，FNR 始终保持为 0。这一结果说明，CoDyTrust 能够有效检测出所有恶意节点，而对节点的误判会随着时间很快降低，系统能够快速进入稳定状态，并具有较高的恶意节点检测准确率。

4.5 负载均衡

图 7 比较了 CoDyTrust 和文献[22]模型在稳定状态下系统的负载分布情况。实验中设置普通节点数量为 9000，监视节点数量为 50。图 7 结果显示，Xing 信任模型的负载在 IP 地址的开头和结尾部分分布较少，而在中间部分分布较多，主要原因在于该模型中监视网络采用树形结构，网络的负载分布呈现出树形结构的自顶向下方式，即根据其相邻节点承载更高的节点监控任务；而 CoDyTrust 模型由于采用基于 KAD 的两层覆盖网络结构，上层网络节点的负载呈现出随机分布的特点，说明网络负载相对于树形结构更加均匀。

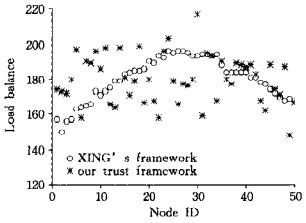

图 7 网络平稳时的负载分布

结束语 P2P 网络信任模型本质是提供更贴近节点行为特征的评价方式，以适应 P2P 网络节点动态性。近年来，如何建立一个能准确评价节点状态，有效抵御振荡、撒谎等安全攻击，检测恶意行为的信任模型成为人们关注的焦点。本文提出了一个 P2P 网络中基于反馈相关性的动态信任模型——CoDyTrust，采用虚假信任过滤机制和信任聚合机制，并在信任值计算中引入了信任遗忘因子、滥用信任值和推荐信任度等，通过反馈控制机制动态调节这些模型因子，在准确评价节点对不同资源信任的同时，实现网络中恶意行为检测。实验结果表明，CoDyTrust 能够较好地反映网络中节点行为，准确地检测出恶意节点，有效地抵御振荡、撒谎和合谋等攻击。

后续研究中将定义评价指标体系来定量分析 CoDyTrust 的安全性，进一步将信任激励机制相结合，使得网络系统在很好地抵御各类恶意攻击的同时，激励用户参与网络活动，促进网络向良好的运行模式成长。

参 考 文 献

[1] EBAY. Ebay feedback forum[OL]. http://pages.ebay.com/services/forum/feedback.html?_trksid=p3907.m36,2008

[2] Albrecht K, Ruedi A R, Clippee. A large-scale client/peer system[R]. TR-410. Swiss Federal Institute of Technology, 2003

[3] Kamvars, Schlosser M. The EigenTrust algorithm for reputation management in P2P networks[C]// Proceedings of the 12th International Conference on World Wide Web (WWW'03). Budapest, Hungary, 2003:640-651

[4] Dou W, Wang HM, Jia Y, et al. A recommendation-based peer-to-peer trust model[J]. Journal of Software, 2004, 15(4):571-583

[5] Li Xiong, Liu Ling. PeerTrust: Supporting reputation based Trust for Peer to Peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7):843-857

[6] Chang Jun-sheng, Wang Huai-min, Yin Gang. DyTust: A Time-Frame Based Dynamic Trust Model for P2P Systems[J]. Chinese Journal of Computers, 2006, 29(8):1301-1307

[7] Huang Chen-lin, Hu Hua-ping, Wang Zhi-ying. A Dynamic Trust Model Based on Feedback Control Mechanism for P2P Applications[J]. Lecture Notes in Computer Science, 2006, 4158:312-321

[8] Yang C, Liu N-Z. RepTrust: Reputation Based Trust Model in P2P Environment[J]. Computer Science, 2011, 38(3):131

[9] 李景涛，荆一楠，肖晓春. 基于相似度加权推荐的 P2P 环境下的信任模型[J]. 软件学报，2007，18(1)：158-166

[10] Zhou R, Hwang K, Cai M. Gossip Trust for Fast Reputation Aggregation in Peer-to-Peer Networks[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(9):1282-1295

[11] Fu Jian-mng, Xiong Hui-jun, Li Zhou, et al. PerformTrust: Trust model integrated past and current performance in P2P file sharing systems[C]// Proceedings of the 2008 IEEE/ACS International Conference on Computer Systems and Applications. 2008:718-725

[12] Wang Yao, Vassileva J. Bayesian Network-Based Trust Model [C]// Proceedings of IEEE WIC International Conference on Web Intelligence. Halifax, Canada, 2003:372-378

[13] Lee S, Sherwood R, Bhattacharjee B. Cooperative peer groups in NICE[C]// IEEE Infocom. San Francisco, USA, 2003:523-544

[14] 石志国，刘翼伟，王志良. 基于时间窗反馈机制的动态 P2P 信任模型[J]. 通信学报，2010(2)：120-129

[15] Lu Y, Wang X. Incentive strategy based on trust model in P2P network[C]// Proc 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR). vol. 3, Mar. 2010:192-195

[16] 胡建理，周斌，吴泉源. P2P 网络中具有激励机制的信任管理研究[J]. 通信学报，2011，32(5)：22-32

[17] Gudes E, Gal-Oz N, Grubshtein A. Methods for computing trust and reputation while preserving privacy[C]// Proc. of the IFIP Conf. on Data and Applications Security. 2009

[18] Hasan O, Bertino E, Brunie L. Efficient Privacy Preserving Reputation Protocols Inspired by Secure Sum[C]// Proc. Eighth Annual International Conference on Privacy Security and Trust (PST). 2010:126-133

[19] Hasan O, Brunie L, Bertino E. Preserving Privacy of Feedback Providers[C]// Decentralized Reputation Systems. Computers & Security, 2011

[20] Kinateder M, Terdic R, Rothermel K. Strong pseudonymous communication for peer-to-peer reputation systems[C]// Proc. of the 2005 ACM Symp. on Applied Computing. 2005

[21] Maymounkov P, Mazières D. Kademlia: A peer-to-peer information system based on the xor metric[C]// Lecture Notes in Computer Science. 2002, 2429:53-65

[22] Jin Xing, Chan S-H G. Detecting Malicious Nodes in Peer-to-Peer Streaming by Peer-Based Monitoring[C]// ACM Trans. Multimedia Comput. Commun. Appl. 6, 2, Article 9 (March 2010), 2010

[23] Lu J-l E, Jang Y-T, et al. PeerSim Cooker: A GUI IDE for PeerSim [J]. International Computer Symposium 2008 (ICS2008), 2008, 2:267-272