·计算机工程与应用·

时空相关性的P2P网络信任模型

王 勇，黄科瑞，秦志光，吴 波

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】结合时间和空间特性，提出一个新的动态信任模型，该模型包含近期信任、长期信任、滥用信任和反馈信任等4个基本组件；针对P2P网络中节点动态性的问题，提出用社区信任度来表示物理位置相关的群体信任程度。模拟实验结果显示，该模型具有较好的动态适应能力和反馈信息聚合能力，能够有效地防止合谋、诋毁等恶意攻击行为。

关 键 词 P2P网络； 空间相关性； 时间相关性； 信任模型

中图分类号 TP393 文献标识码 A doi:10.3969/j.issn.1001-0548.2011.01.015

Time-Space Based Trust Model for P2P Systems

WANG Yong, HUANG Ke-rui, QIN Zhi-guang, and WU Bo

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract In this paper, we present a new time-space based trust model which integrates time and space factors, where short-term-trust, long-term-trust, abuse-trust and feedback-trust are the main consideration. Furthermore, the community-trust is proposed to solve the difficulty of binding between user and physical IP address. The community-trust indicates the integrative trust level of users' physical locations set in a specific range. Theoretical analysis and simulation results show that the time-space based trust model is effective on modeling dynamic trust relationship, aggregating feedback information, and resisting some attacks such as slander, peer collusion, and Sybil attacks.

Key words P2P network; space context; time context; trust model

近年来，P2P技术迅速发展，消耗着70%以上的Internet网络带宽。P2P网络的广泛流行给个人主机、Internet网络、乃至整个人类信息社会都带来诸多安全问题，阻碍着P2P网络的发展。

基于信任的P2P网络的研究目的是在分布式环境下建立P2P网络的节点信任机制，增强P2P网络中节点的可信性，从内在机制上解决P2P网络的安全问题。在P2P网络信任模型的发展中，主要出现了基于PKI的信任模型、基于贝叶斯的信任模型[1-3]、基于局部信任度的信任模型[4]、基于全局信任度的信任模型[5]以及基于资源的信任模型[6]5类模型。然而，现有的信任模型，由于计算复杂或者实现困难，还不能很好地应用于实际P2P系统。因此，本文提出了一种新的动态信任模型，该模型将时间和空间的上下文相结合，是基于时空相关性的信任模型，能够解决大多数P2P网络中存在的问题，并且与相应拓扑结构结合后，可使系统效率得以较大提高。

1 基于时间帧的DyTrust模型

DyTrust模型将时间上下文考虑在内，即将当前行为与历史行为联系起来，得出更准确、更符合真实交互行为的评价。该模型将时间因素细化，分为近期信任、长期信任、累计滥用信任、评价真实信任，进而达到抑制各类恶意行为的目的。DyTrust主要思想如下。

定义 1 R_{ij}^n 用于表示第n个时间帧时刻节点i对节点j的信任评价，且有：

$$R_{ij}^n = \lambda D_{ij}^n + (1-\lambda)\sum_{r\in I(j)} \frac{C_{ir}^n D_{rj}^n}{\sum_{r\in I(j)} C_{ir}^n} \tag{1}$$

式中，D_{ij}^n 表示在n时刻，节点i与节点j交互后，节点i对节点j的直接信任评价；C_{ij}^n 表示在n时刻，节点i对节点r所作出评价的信任程度，称为反馈信任。因此，当前的信任评价既考虑了本地的交互历史也考

收稿日期：2009－11－10；修回日期：2010－07－13
基金项目：国家863计划(2009AA01Z422)
作者简介：王 勇(1976－)，男，副教授，主要从事网络安全、对等网测量方面的研究.

虑了其他节点的评价。

定义 2　S_{ij}^n 用于表示第n个时间帧时刻节点i对节点j的短期信任度，且有：

$$S_{ij}^n=(1-\rho)S_{ij}^{n-1}+\rho R_{ij}^n,\ \ \rho=\begin{cases}\alpha & 0<R_{ij}^n-S_{ij}^{n-1}\leqslant\varepsilon\\ \beta & R_{ij}^n-S_{ij}^{n-1}\geqslant\varepsilon\\ \gamma & R_{ij}^n-S_{ij}^{n-1}<0\end{cases} \tag{2}$$

式中，α、β为信任度的增加因子；γ为信任度的减小因子。由于信任是需要长期的良好表现而建立的，而少量攻击行为便足以导致失去信任，因此取$\alpha<\gamma$且$\beta<\gamma$，即提升信任度比降低信任度更困难，两者是非对称的。

与DyTrust稍有不同的是，本文模型考虑了如下情况：当评价信誉度R_{ij}^n在短期内较上一短期信誉度S_{ij}^n有大幅度异常提升(即$R_{ij}^n-S_{ij}^n>\varepsilon$)时，很可能是节点$j$通过合谋欺骗迅速提升自身的信任度。此时，不能视为正常增加，而需要减小R_{ij}^n所占的比重，即$\beta<\alpha$，其中：

$$\alpha=\alpha\frac{c}{c+A_{ij}^n} \tag{3}$$

式中，A_{ij}^n定义见式(6)。

定义 3　LT_{ij}^n用于表示第n个时间帧时刻节点i对节点j的长期信任度，且有：

$$\mathrm{LT}_{ij}^n=\frac{(n-1)\mathrm{LT}_{ij}^{n-1}+R_{ij}^n}{n} \tag{4}$$

定义 4　T_{ij}^n用于表示第n个时间帧时刻节点i对节点j的最终信任度，且有：

$$T_{ij}^n=\min(S_{ij}^n,\mathrm{LT}_{ij}^n) \tag{5}$$

定义 5　A_{ij}^n用于表示第n个时间帧时刻节点i对节点j的滥用信任度，且有：

$$A_{ij}^n=\begin{cases}A_{ij}^{n-1}+(T_{ij}^n-D_{ij}^n) & T_{ij}^n-D_{ij}^n>\varepsilon\\ A_{ij}^{n-1} & \text{其他}\end{cases} \tag{6}$$

与DyTrust不同的是，考虑到获取与某节点所交互过的所有节点可能造成大的系统资源开销，本文模型并没有引入diff_{ir}^n以及$C_{r_{ir}}$，而是通过分层式的P2P拓扑结构，及有限的回复路径上的所有节点对评价者的评价来获取必要信息。虽然一定的局部性会导致安全性有所降低，但是与空间特性结合后，安全性得以升高。

2　基于时空相关性的信任模型

DyTrust模型充分利用了事件的时间相关特性。相应地，空间相关特性也可以被充分利用。据此，本文得出时空相关性模型。

在时空相关性模型中，时间特性主要是由DyTrust模型的时间帧构成。在计算机网络中，任何一个节点都隶属于一个社区，如学校、公司或政府机关；并且，节点在登录时其IP地址的变化是限定在一定范围之内的。利用该特性，将一定范围内的IP地址视为集合，对该集合进行整体评价，并对相关定义进行补充。

2.1　定义补充

定义 6　C_{ij}^n用于表示第n个时间帧时刻节点i对节点j所做出的对其他节点评价的信任度，且有：

$$C_{ij}^n=\frac{\sum_{r\in S}R_{rj}^{n-1}}{|S|} \tag{7}$$

式中，S是位于在j向i回复反馈报文的路径上且含有对j的信任评价R_{rj}^n的一类节点的集合；$|S|$为集合S中节点的个数。因此，C_{ij}^n是对评价者的评价，简称为二次评价。

定义 7　ML^n用于表示社区恶意程度：

$$\mathrm{ML}^n=\sum_{i\in S_1,\,j\in S_2}\mu_i(\omega-D_{ji}^n) \tag{8}$$

其中：

$$\mu_i=\alpha\cdot\mathrm{CP}_i+\beta\cdot\mathrm{TM}_i+\gamma\cdot\mathrm{TS}_i \tag{9}$$

式中，$\alpha+\beta+\gamma=1$；$S_1=\{i\,|\,D_{ji}^n<\omega\}$表示恶意节点的集合；$S_2=\{j\,|\,D_{ji}^n\neq\phi\}$表示与$i$交互过的节点集合；$\mu_i$表示节点$i$的破坏能力；$\mathrm{CP}_i$、$\mathrm{TM}_i$、$\mathrm{TS}_i$分别表示节点$i$的服务能力(如带宽)、在线时间和信誉度。注意到以下3点：1) 服务能力较强的恶意节点所造成的破坏较大；2) 长期在线的恶意节点所造成的破坏较大；3) 原本信誉度高的恶意节点所造成的破坏较大。因此，对每种因素赋予相应权重后，通过式(9)将不同破坏能力的节点加以区分；再将破坏能力与恶意程度($\omega-D_{ji}^n$)相乘后便得出该节点的恶意行为实际所造成的破坏；最后将节点的实际破坏累加，便得到社区最终的恶意程度ML^n。

定义 8　CB^n用于表示社区贡献程度；且有：

$$\mathrm{CB}^n=\sum_{i\in S_3,\,j\in S_2}[\varphi(D_{ji}-\omega)+\eta\cdot\mathrm{CP}_i+\sigma\cdot\mathrm{QT}_i](D_{ji}-\omega) \tag{10}$$

式中，$\varphi+\eta+\sigma=1$；$S_3=\{i\,|\,D_{ji}^n>\omega\}$表示受到好评的节点集合；$D_{ji}$、$\mathrm{CP}_i$、$\mathrm{QT}_i$分别表示节点$i$受到的评价、服务能力和含有资源的数量。注意到以下4点：1) 节点提供的资源质量越高越好；2) 节点服务

能力(如上传带宽)越强越好；3) 节点贡献资源的数量越多越好；4) 节点提供的资源越是网络上急需的越好。但是由于1)和3)只能由人为的评价体现，因此将该二因素统一用受到的评价 D_{ji} 来体现。与计算 ML^n 类似，得到准确的 CB^n 。

定义 9 CT^n 用于表示该社区整体信誉度，且有：

$$\mathrm{CT}^n=\begin{cases}0 & \dfrac{\mathrm{ML}^n}{\mathrm{CB}^n}\geqslant 1\\ \left(1-\dfrac{\mathrm{ML}^n}{\mathrm{CB}^n}\right)\mathrm{CT}^{n-1} & \theta<\dfrac{\mathrm{ML}^n}{\mathrm{CB}^n}<1\\ \mathrm{CT}^{n-1}+\dfrac{1}{\mathrm{CT}^{n-1}}\left(\theta-\dfrac{\mathrm{ML}^n}{\mathrm{CB}^n}\right)\sum_{i\in S_3}(D_{ji}^n-\omega) & \dfrac{\mathrm{ML}^n}{\mathrm{CB}^n}\leqslant\theta\end{cases} \tag{11}$$

2.2 抵御攻击能力分析

网络中的节点分为上层的超级节点和下层的普通节点两类。普通节点可以与多个超级节点相连，但不能与任何普通节点相连；超级节点可以与多个超级节点或普通节点相连，如图1所示。

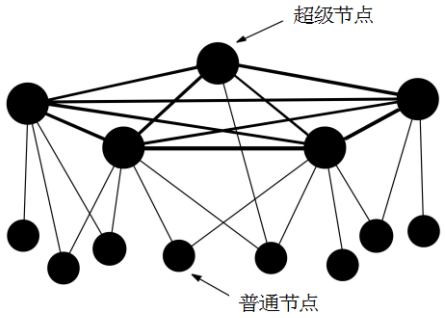

图1 P2P网络拓扑结构

2.2.1 抵御摇摆攻击

当节点j对节点i实行攻击时，根据式(6)可知 A_{ij}^n 升高，进而通过式(3)使得 α 下降，也就使之后的 S_{ij}^n 上升更加缓慢。节点j对节点i的攻击次数越多， S_{ij}^n 也就上升得越来越缓慢，由此可以看出对摇摆行为的惩罚。

2.2.2 抵御合谋欺骗

当节点j的信任度不高时，可能组织其他节点人为地提高其信任值，分为两种情况。

1) 长期信任度较低时抬高信任值，此时由式(4)和式(5)得知无法获得较高的 T_{ij}^n ；

2) 过快抬高自身信任值，当信任度上升速度过快且不符合正常的分布规律时，将被视为合伙欺骗而无法得到很快增长。由式(2)可知，节点不能过快地抬高其信任值。

2.2.3 避免对未交互节点赋予简单初始值

节点i对节点j的评价将被返回给j，由图1的拓扑可知，在返回过程中，该评价必将经过j的某个上层超级节点。当超级节点发现j是其下属节点时，该超级节点在转发报文时还将根据式(1)更新自身对节点j的评价。这样，即使在初次连接后没有进行直接交互的情况下，该超级节点也能够将其他节点对j的评价考虑在内，而不是简单地对j赋予一个初始值。

2.2.4 抵御反馈诋毁

当节点i对节点j进行反馈诋毁时，虽然在j的上层超级节点处会对j造成一定伤害，但是需要注意的是，节点j的上层是与多个超级节点相连的，而i对j的资源评价报文仅通过一条路径，因此最多在一个超级节点处对j造成伤害；而查询节点j的信誉度时，是j的上层的多个超级节点(甚至还有其他与j有过交互的普通节点)共同作出的，一个超级节点对j的不公正评价并不能导致j的被淹没。而只要节点j提供的是健康的资源，在同一时间帧内返回良好资源评价提高了j的信任度，也就抑制了节点i对节点j的反馈诋毁对j所造成的伤害。

2.2.5 缓解难以对节点进行绑定所带来的问题

由于节点的IP动态改变，因此无法将节点绑定。但IP地址变化存在范围限制，因此可将该范围内的IP集合视为一个社区(如学校、公司、机构等)，并通过整个社区的信任度判断该社区的健康程度。

社区信任度实际上反映的是与该社区成员交互而受到攻击的概率。当社区信任度较高时，即使社区内存在恶意节点，用户也可以选择与该社区内的节点交互，因为相比于良好节点的贡献来说，恶意节点的破坏微不足道。用户受到攻击的可能性小。当社区信任度较低时，即使社区内某节点信任度较高，用户也要对其提防，因为这很可能是节点通过非法手段构造的虚假信任度。

社区信任度缓存在社区对外的超级服务器上，超级服务器在转发报文的同时也更新自己社区的信任度。计算方法可参照本文2.2.2节的获取社区信任度算法。

另外，社区信任度可以与其他安全产品相结合加快社区本身的进化，如当社区发现其信任度有下降趋势时，启动入侵检测系统找出内部的恶意节点，及时对其进行清除。

3 实验结果以及仿真

根据P2P网络的测量分析结果[7]，在仿真实验中网络的规模为5 400个节点，选取的超级节点数为400，叶节点数为5 000。除普通节点不能与普通节点相连外，各节点之间均随机相连。

首先随机选取初始信誉度并不高的节点2 133模拟良好用户的行为；再选取初始信誉值较高的3 295模拟恶意行为。从图2可以看出，通过少数的恶意行为，节点3 259的信誉值就降低到了一个很低的水平；节点2 133则要通过多次的良好交互才能使信誉值明显提高，且呈减缓的趋势。因此信誉的上升和信誉的下降是非对称的。鼓励用户长期地保持良好行为。

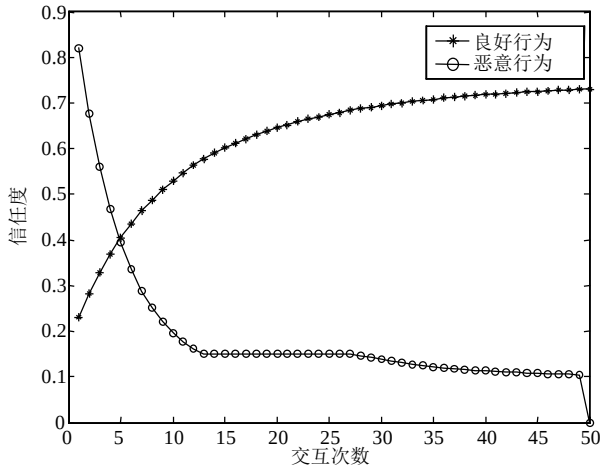

图2　信任度上升与下降对比

随后选取3 248节点再进行摇摆攻击。从图3可以看出，每次攻击后，上升速度呈递减的趋势，达到了惩罚摇摆行为的目的。

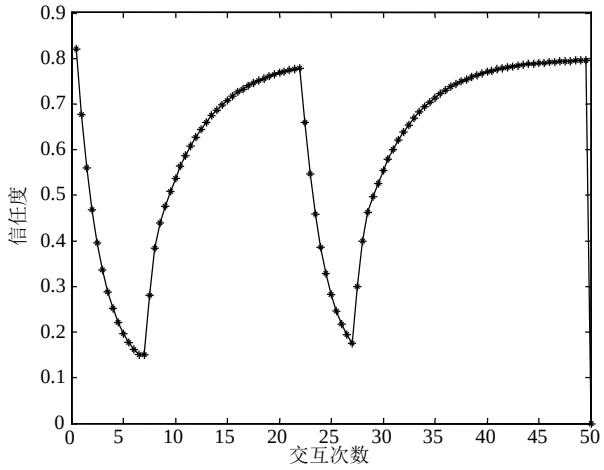

图3　摇摆行为信任度变化曲线

选取节点2 349，并且使某些特定的节点抬高其信誉值，其他的节点则给出诚实的交互值。从图4中可以看出，虽然该节点能够在一段较短的时间内保持较高的信任度，但是随着其他节点与该节点真实交互次数的增多，节点2 349的信任值将会立刻被降低到一个很低的数值，说明之前所做好评是虚假的，其信誉值依旧会被降低，使得其他节点不会因为该节点拥有虚假的较高的信誉值而选择与之交互而受到攻击，就对合伙欺骗起到了很好的抑制作用。

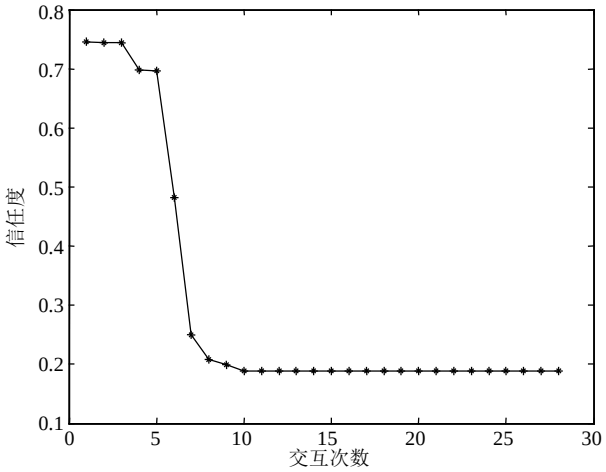

图4　合伙欺骗信任度变化曲线

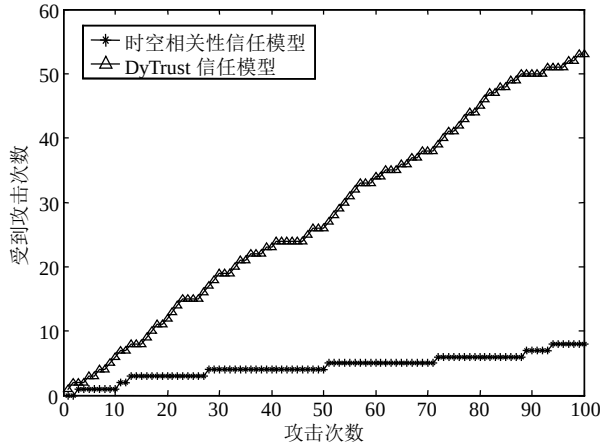

图5　DyTrust与时空相关性对比

最后，将DyTrust原型与在对DyTrust进行改进并融入空间因素后的基于时空相关性模型进行对比。由图5可以看出，在融入了空间因素后，网络所受到的攻击次数明显降低，说明基于时空相关性的信任模型能够更好地防止信誉攻击。在安全要求较高的场合下，采用基于时空相关性的信任模型比仅仅基于时间因素的DyTrust模型更加合适。

4 结 束 语

本文融合DyTrust的时间帧思想，对DyTrust进行改进，借助时间因素对攻击进行防御。此外，本文模型还将空间因素纳入一并考虑，针对IP地址动态变化而无法对节点进行绑定的问题，采用社区整体

信任度加以解决。该方式的主要优点在于：1) 可解决无法绑定用户的问题；2) 可与社区网络自身的安全设备结合自行净化社区网络；3) 可通过向用户显示受到攻击的概率抑制各种不良行为(如反馈诋毁、合谋欺骗等)；4) 可使得整个网络向着最优化的方向发展。仿真实验表明，本文模型可以成功地抑制各种恶意行为。

下一步的主要工作是进一步分析模型，并且结合ISP和用户行为特性，找出更好的的社区信任值计算模型，得到相关的最优参数值。

参 考 文 献

[1] 常俊胜, 王怀民, 尹刚. DyTrust: 一种P2P系统中基于时间帧的动态信任模[J]. 计算机学报, 2006, 29(8): 1301-1307.
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.

[2] WANG Y. Bayesian network-based trust model in peer-to-peer network[C]//Proceedings of Workshop on Deception, Fraud and Trust in Agent Societies at the Autonomous Agents and Multi Agent Systems 2003 Conference(AAMAS-03). Melbourne, Australia: ACM Press, 2003: 372-378.

[3] WANG Y, VASSILEVA J. Trust and reputation model in Peer-to-Peer networks[C]//Proceedings of the 3th International Conference on Peer-to-Peer Computing (P2P 03). Washington. D C, USA: IEEE Press, 2003: 150-159.

[4] CORNELLI F. Choosing reputable servents in a P2P network[C]//11th International World Wide Web Conference: WWW 2002. Hawaii, USA: IEEE Press, 2002: 150-157.

[5] KAMVAR S. The Eigentrust algorithm for reputation management in P2P networks[C]//12th International World Wide Web Conference: WWW 2003. Budapest, Hungary: ACM Press, 2003: 640-651.

[6] WALSH K, SIRER G E. Fighting peer-to-peer SPAM and decoys with object reputation[C]//Proceedings of SIGCOM-M'05 Workshop on Economics of Peer-to-Peer Systems. Philadelphia, USA: ACM Press, 2005: 138-143.

[7] 王勇, 云晓春, 李奕飞. 对等网络拓扑测量与特征分析实例[J]. 软件学报, 2008, 19(4): 981-992.
WANG Yong, YUN Xiao-chun, LI Yi-fei. Measuring and characterizing topologies of P2P networks[J]. Journal of Software, 2008, 19(4): 981-992.

[8] POUWELSE J, GARBACKI P, EPEMA D, et al. The bittorrent P2P file-sharing system: measurements and analysis[C]//Proceedings of IPTPS'05. New York, USA: [s.n], 2005.

[9] VECIANA G D, YANG X. Fairness, incentives and performance in peer-to-peer networks[C]//Proceedings of SIGCOMM'04. Portland, UAS: ACM Press, 2004.

[10] QIU D, SRIKANT R. Modeling and performance analysis of bittorrent-like peer-to-peer networks[C]//Proceedings of SIGCOMM'04. Portland, USA: ACM Press, 2004: 367-378.

[11] GUO L, CHEN S, XIAO Z. et al. Measurements, analysis, and modeling of bittorrent-like systems[C]//Proceedings of SIGCOMM'05. Philadelphia, USA: ACM Press, 2005: 4-4.

[12] IZAL M, URVOY-KELLER G., BIERSACK E, et al. Dissecting bittorrent: five months in a torrent's lifetime[C]//Proceedings of the 5th Annual Passive & Active Measurement Workshop: PAM 2004. Antibes Juan-Les-Pins, France: [s.n], 2004.

[13] POUWELSE J, GARBACKI P, EPEMA D, et al. The bittorrent P2P file-sharing system: measurements and analysis[C]//Proceedings of IPTPS'05. New York, USA: [s.n], 2005.

编 辑 蒋 晓