第33卷 第18期 计 算 机 工 程 2007年9月
Vol.33 No.18 Computer Engineering September 2007
·安全技术· 文章编号：1000—3428(2007)18—0145—03 文献标识码：A 中图分类号：TP309

一种自约束信誉更新模型

张明武[1]，杨 波[1]，张文政[2]
(1. 华南农业大学信息安全研究所，广州 510642；2. 现代通信国家重点实验室，成都 610041)

摘 要：在分析信誉计算模型的基础上，提出了一种自约束的信誉更新模型，由于节点的信誉主要反映历史信誉，信誉变化主要表现在新的评价分与以前信誉的变化上，因此通过自约束因子来表达这种变化。对该模型与Bayesian模型作了仿真分析比较。结果显示：信誉评估模型体现恶意行为的惩罚思想，当一个可信节点连续出现交易失败或不可信行为时，信誉值会指数级下降，恢复其信誉则是缓慢上升。
关键词：信任；信誉更新；Bayesian概率模型

Self-constraint Reputation Updating Model

ZHANG Ming-wu[1], YANG Bo[1], ZHANG Wen-zheng[2]
(1. Institute of Information Security, South China Agricultural University, Guangzhou 510642;
2. National Laboratory for Modern Communications, Chengdu 610041)

【Abstract】 Encounter or interactions between nodes unknown to each other are inevitable in Internet transaction. Reputation mechanism is to facilitate the entities trust relationship in decentralized environments. This paper provides a computational model based on directed trust and recommender trust, introduces a self-constraint reputation updating model, which focuses on the reputation rating fluctuating factor. It puts forward an idea about malicious user's reputation punishment. By comparing with Bayesian probabilistic trust model, it shows some benefits from simulation result: in the model, reputation rating will drop off fast whenever continuous failure transactions.
【Key words】 trust; reputation updating; Bayesian probabilistic model

基于分布式网络环境的应用，如电子商务、P2P文件下载、MANET和网格计算，给Internet上的服务带来了巨大的商机，但Internet的分布广泛性和动态性给网络安全带来了巨大挑战，恶意的攻击和不良企图用户给网络服务带来影响，共谋攻击和有预谋攻击是分布式网络中交易安全性的重要危险因素。信誉是对网络用户可信度进行评价的重要方面之一。

信誉是一个实体对另一实体的未来交易行为的主观期望[1,2]，它建立在已有的交易记录情况下的分析模型。信誉系统通过信誉模型来表达用户交易的信誉值，并通过它来激励信誉好的用户，约束信誉差的用户，同时也要对信誉差的用户作信誉惩罚处理，根据信誉的变化情况，推断网络预谋攻击和共谋攻击行为。信誉值的稳定分布和更新存储效率是信誉系统性能的重要因素。文献[3]将现有常见的信誉更新算法作了比较，对Rahman[2]、Bayesian、带遗忘因子 w_{age} 的Bayesian[4]、UniTec和ReGreT[5]等信誉更新算法进行了比较，算法仿真结果显示在5种算法中，Rahman算法由于信任值是离散的区间值，不利于连续信任度的表达；ReGreT需要存储大量的历史信誉值，开销较大；UniTec对最新信任值最敏感，当初值为0.5时1个不成功交易即使信誉为0；Bayesian具有较好的更新速度，但对于信任值的变化不敏感；带遗忘因子 w_{age} 的Bayesian算法对信任值的敏感度得到一定提高，但是 w_{age} 遗忘因子对于信任值的范围产生影响，当 w_{age} =0.3时，信任值范围缩减为[0, 2, 0, 8]。

1 信任模型及计算

1.1 信任表达

一个实体对其他节点的信任由两方面组成，一是直接信任，另一个是推荐信任，见图1。

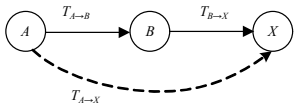


图1 推荐信任

如果节点A欲与节点X进行交易，若A曾与X有过交易并存储相关的信任值，称A与X有直接信任关系，信任值是 T_D。如果A与X的交易次数较少，T_D 并不能完全真实表达A对X的信任关系，推荐信任是A向其他节点 $\{M_1, M_2, ..., M_k\}$ 查询X的信任值 $\{T_{M_1\to X}, T_{M_2\to X}, \ ..., T_{M_k\to X}\}$，根据模型求出$A$对$X$的交易的间接信任值$T_R$。$A\to X$ 的总体信任值计算

$$T_{A\to X}=\alpha T_D+(1-\alpha)T_R \quad 0\le\alpha\le 1 \tag{1}$$

其中，T_D 是直接信任值；T_R 是A对X的推荐信任值；α 和 $1-\alpha$ 分别是直接信任和推荐信任的权重。

1.2 间接信任

一般来说，节点A并不能向所有其他节点寻求对节点X的间接信任，而是应当向自己认为可信的相邻节点提出[4]。

x_{AB}是用户A对B提供的交易的结果的评判，0表示交易成功，1表示交易失败。信任是在基于历史交易记录集 $D_{AB}=\{x_{AB}(1), x_{AB}(2), ..., x_{AB}(n) \mid x_{AB}(i)\in\{0,1\}\}$ 的情况下，一个实体对另一个实体的未来交易行为的主观期望。Bayesian方法

基金项目：国家自然科学基金资助项目(60372046，60573043)；现代通信国家重点实验室基金资助项目(9140c1108010606)
作者简介：张明武(1970－)，男，副教授、博士研究生，主研方向：网络与信息安全；杨 波，教授、博士生导师；张文政，研究员
收稿日期：2006-09-26 **E-mail：**zhangmw@scau.edu.cn

研究了两个实体间进行成功交互的概率估计。

定义 $\hat{\theta}_{AB}$ 是 A、B 间交易成功的可能性

$$T_{A\to B}=E[\hat{\theta}_{AB}\mid D_{AB}] \tag{2}$$

若 B 是 A 与 X 信任关系的推荐者，

$$T_{A\to X}=T_{A\to B}\times T_{B\to X}=E[\hat{\theta}_{AB}\mid D_{AB}]\times E[\hat{\theta}_{BX}\mid D_{BX}]$$

$A\to X$间有k条推荐路径的多并行推荐路径的信任计　算[1]，可用式(4)计算各路径的推荐信任 $T^{(1)}_{A\to X},T^{(2)}_{A\to X},\ldots,T^{(k)}_{A\to X}$　$A\to X$ 的信任值 $T_{A\to X}=\sum_{i=1}^{k}T^{(i)}_{A\to X}\times\overline{w_i}$，$\overline{w_i}$ 为链的权重，$\sum_{i=1}^{k}\overline{w_i}=1$。

2　信誉值的更新

实体 A 对 X 的评价信誉即与本次交易的评估分有关，又与历史信誉有关，实体间的信誉是以新得出的信誉分和历史信誉为主要依据，根据信誉更新模型进行新的信誉值计算。

2.1　Bayesian 模型信誉更新

Bayesian 概率模型是根据现有交易结果集 *Observation*，用概率公式来表达信任，将节点 $A\to B$ 的信任表达为在现有信任值 R_{AB} 对下一次交易的可成功的概率

$$R'_{AB}=\frac{p\{D_{AB}\mid R_{AB}\}\times R_{AB}}{\sum p\{D_{AB}\mid R_{AB}\}\times R_{AB}} \tag{3}$$

$D_{AB}=\{x_{AB}(1),x_{AB}(2),\ldots,x_{AB}(n)\mid x_{AB}(i)\in\{0,1\},i\le n\}$。设节点的交易成功与不成功服从 β-分布，在 n 次交易中有 p 次成功，节点间在第 n+1 次交易中成功的概率为

$$p(\hat{\theta}\mid D_{AB})=Beta(\alpha+p,\beta+n-p) \tag{4}$$

式中，$\alpha,\beta>0$，它决定交易的基础信任，$\alpha=\beta=1$ 时，$\hat{\theta}=0.5$，表示信任和不信任各占一半。节点的信任值可描述为

$$R'_{AB}=E[\hat{\theta}\mid D_{AB}]=E[p(x_{AB}(n+1)\mid D_{AB})]=\frac{\alpha+p}{\alpha+\beta+n} \tag{5}$$

信誉更新表达式为

$$R_{AB}=Beta(\alpha^{new}{}_{j},\beta^{new}{}_{j})=Beta(\alpha_j+r,\beta_j+s)$$
$$\alpha^{new}{}_{j}=\alpha_j+r,\beta^{new}{}_{j}=\beta_j+s \tag{6}$$

其中，r 和 s 分别是在更新时新产生的成功交易与失败交易次数。为提高最近的信息的权重，文献[2]中提出加权的信誉更新策略，引入遗忘因子 W_{age}，使得：$\alpha'_j=(w_{age}*\alpha_j)+r$，$\beta'_j=(w_{age}*\beta_j)+s$，但 W_{age} 是静态的固定值，主要依靠经验获得，引入遗忘因子后信任区间缩减到一定的范围。该模型中交易发起方对服务方的交易满意度只有 0(满意)或 1(不满意)两种情况，不能对满意度作定量表述，该模型也不能直观反映信誉的动态变化情况。

考虑到信誉值的变化有如下规律：

(1)新加入的节点无初始信誉值 $T_0=0$，经过少量的几次成功的交易后，应当很快得到较真实的信誉值；

(2)在节点间交易过程中，一次失败交易导致信誉值的下降幅度应大于成功交易导致信誉值的上升幅度。根据以上思想本文引入一种自约束信誉更新模型。

2.2　自约束更新模型

设计中，对目标节点的更新的信任值 T_i，除了当次评价分 S_i 和以前的信任值 T_{i-1} 有关，还与二者之间的抖动程度 θ_i 有关，通过约束限定因子 θ_i 来表达信誉的前后变化，并通过对此因子的自约束，以使信誉趋于稳定[5]。更新信任值公式表达为

$$T_i=\theta_i S_i+(1-\theta_i)T_{i-1} \tag{7}$$

其中，S_i 是当前的评价分；T_{i-1} 是 $i-1$ 时刻的信任值；θ_i 是影响因子，θ_i 定义如下：

$$\theta_i=\frac{\lambda e^{\Delta t_i}-1}{\lambda e+1}\ ,\ \Delta t_i=\left|S_i-T_{i-1}\right| \tag{8}$$

其中，$S_i,T_{i-1}\in[0,1],\Delta t_i\in[0,1]$；$\Delta t$ 和 θ 反映信任值的抖动情况；$\lambda\in[0,1]$ 是抖动调节因子。通过式(7)、式(8)，可得如下性质：

性质 1 若 $S_i,T_{i-1}\in[0,1]$，则 $T_i\in[0,1]$，T_i 表达函数封闭。

性质 2 $\lambda=1$ 时，θ_i 的最大值 $\theta_{\max}=(e-1)/(e+1)=0.459$，最小值 $\theta_{\min}=0$，θ_i 越大表示信任值的抖动越大。抖动调节因子 λ 变小时，抖动性变慢，即 $\theta_{\max}$ 会变小，可通过 λ 来调节信任值抖动程度。

性质 3 $\lambda=1$ 时，若 $\Delta t_i=|S_i-T_{i-1}|=1$，$\theta_i=\theta_{\max}$ 有两种情况：

(1) $S_i=1,T_{i-1}=0$。$T_{i-1}=0$ 表示信任初值为 0 是最新加入的新节点，$S_i=1$ 表示进行了一次成功交易，根据前面所述，$T_i=0.459$；

(2) $S_i=0,T_{i-1}=1$。$T_{i-1}=1$ 表示是经过很多次成功交易后信誉非常高的节点，$S_i=0$ 表示进行了一次不成功的交易，根据上述公式，有 $T_i=0.541$。

性质 4 若 $\Delta t_i=|S_i-T_{i-1}|=0$，则 $\theta_i=\theta_{\min}=0$，它表示当前次的信任分与以前的信任值相同，$T_i=T_{i-1}=S_i$，因而节点的信誉值不会变化，此时信誉值不需要更新。

由以上性质可以得出：更新表达式表述了节点间的信誉，它与上一次的信誉 T_{i-1} 和本次交易给出的得分 S_i 有关，同时表达式通过 θ_i 反映了节点信誉的变化幅度。

3　仿真结果

本方案进行信任值分布、信誉区间分布、信誉值稳定性以及不可信行为对信誉的影响等几方面模拟，并与 Bayesian 方案进行比较。为使信誉变化较快，本方案中设抖动调节因子 $\lambda=1$。

3.1　成功交易信任值分布比较

图 2 显示本方案与未加权的Bayesian方案[6]的比较曲线。在Bayesian方案中，$\alpha=\beta=1$，初值 $R_{AB}=0.5$，对于本方案设初值 $T_0=0,S_1=1$，两种方案均进行连续成功交易的评估公式叠代。

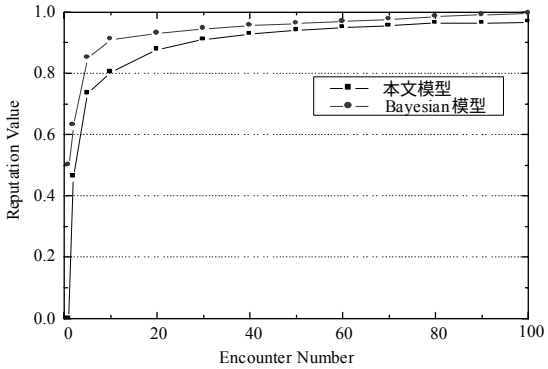


图 2　信誉分布比较

结果显示两种方案都可通过少数几个成功的交易，很快达到基本稳定的信任值。本方案需要 16 次连续的成功交易使信任值达到 0.85，Bayesian 方案的信任值收敛更快，在 4 次成功交易后信誉值达到 0.85，因而信誉区间比较集中。信任

值上升太快，会使一个节点容易骗取信任，通过极小的代价获取较高的信任值。

3.2 不可信行为对信誉影响

当一个完全可信的用户 $T_i=1$，若经过连续的不成功交易，两种模型的结果见图 3。由图知，Bayesian 模型在连续不成功交易时信誉值的下降趋近于线性下降，在经过 30 次不成功交易后，信誉值仍有 0.6 以上。本文模型中的下降则是指数级下降，连续 3 次不成功信誉值已小于 0.4，进入不可信区，连续 9 次不可信行为后，信誉 $T_i \le 0.2$。根据一般信誉原则，一个完全可信的用户如果连续有不可信行为，信誉值会急剧下降，本模型在不成功交易信誉下降影响优于 Bayesian 方案。

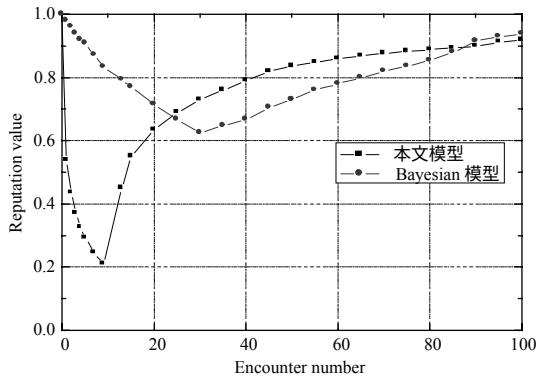


图 3 信誉的下降与恢复

在信誉恢复阶段，采用连续成功交易来提高信誉。根据实验仿真结果，本方案中一个处于不可信区域的用户，要想重新回到可信区域 0.9，需要连续成功交易 23 次，Bayesian 方案的信誉恢复也近似为线性递增，恢复速度更慢，从 0.6 达到 0.8 需要约 30 次成功交易。两种方案都实现了信誉的慢恢复。

4 结论

本文在分析信誉模型的基础上，给出了一种具有自约束因子的信誉更新评估模型，通过实验仿真结果显示，它具有快速零启动(信任初值为 0 可以通过省量交易达到信誉稳定)、信誉的快速下降慢速恢复的惩罚等特性，Bayesian 模型对信誉变化敏感度比本模型对信誉值变化敏感度小，在对不可信行为的信誉惩罚和信誉值的分布等方面显得不足。

参考文献

1 Mui L, Mohtashemi M, Halberstadt A. A Computational Model of Trust and Reputation[C]//Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Maui, Hawaii. 2002-01.

2 Abdul-Rahman A, Hailes S. Supporting Trust in Virtual Communities [C]//Proceedings of the 33th Hawaii International Conference on System Sciences, Maui, Hawaii. 2000-01.

3 Kinateder M, Baschny E, Rothermel K. Towards a Generic Trust Model — — Comparison Various Trust Update Algorithms[C]// Proceedings of Trust Management. 2005: 177-192.

4 Yu B, Singh M. A Social Mechanism for Reputation Management in Electronic Communities[C]//Proceedings of the 4th International Workshop on Cooperative Information Agents, Berlin. 2000.

5 Kinatede M, Rothermel K. Architecture and Algorithms for a Distributed Reputation System[C]//Proceedings of the lst International Conference on Trust Management, Crete, Greece. 2003.

6 Wang Y, Varadharajan J, Vijay. Interaction Trust Evaluation in Decentralized Environments[C]//Proc. of the 5th International Conference on Electronic Commerce and Web Technology, Zaragoza, Spain. 2004: 144-153.

(上接第 144 页)

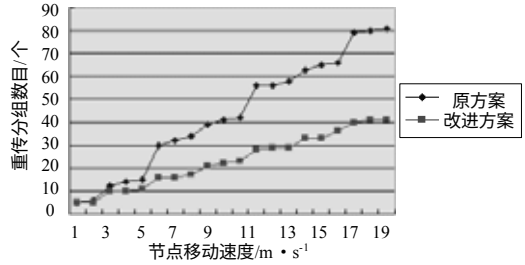


图 5 不同节点移动速度下 CN 重传分组数

4 结论

本文在一种分布式路由方案的基础上进行了以下改进：(1)在转向代理处为移动节点构造一个循环列表，按顺序存储数据分组，这样能够进一步解决转向代理重传数据分组时的乱序问题；(2)通过向前一个转向代理发送转发请求，转发原 RA 缓存中的数据分组到新链路，解决了转向代理切换时的分组集中丢失问题；(3)在 RA 处引入 Snoop 机制，对移动节点的应答及时响应，降低了通信对端的重传次数。本文利用 NS2.26 进行了仿真，仿真结果表明：本文方案减少了重传分组和乱序分组，进一步减少了远程信令流量和数据流量，提高了网络资源的利用率，有效地改善了移动 IP 的性能。

参考文献

1 Perkins C E. IP Mobility Support for IPv4[S]. IETF, RFC3344, 2002.

2 Johnson D, Perkins C, Arkko J. Mobility Support in IPv6[Z]. IETF, 2003.

3 Sun Xuejun, Li Shengli, Liu Tao, et al. A Distributed-agent Scheme in Mobile IP Networks[C]//Proc. of IEEE CCECE'04. 2004.

4 Blondia C, Van den Wijngaert N, Willems G. Performance Analysis of Optimized Smooth Handoff in Mobile IP[C]//Proceedings of the 5th ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems. 2002: 22-29.

5 Balakrishhan H, Seshan S, Katz R H. Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks[J]. ACM Wireless Networks, 1995, 1(4): 469-481.

6 Ding W, Jamalipour A. A New Explicit Loss Notification and Acknowledgement for Wireless TCP[C]//Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. 2001: 65-69.