P2P 网络中基于动态贝叶斯网络可信度量模型①

郭 磊, 杨 升, 肖钟捷, 程泽伟

(武夷学院 数学与计算机学院, 武夷山 354300)

摘 要: 本文针对 P2P 网络中节点匿名、动态导致安全性下降, 现有信任度模型计算动态性不足等问题, 提出了基于动态贝叶斯网络的可信度量计算模型, 模型依据历史交互记录数据, 从直接信任度与推荐信任度两个方面进行信任度量计算, 并考虑到时效性与恶意节点等问题, 引入时效因子与惩罚因子. 最后通过仿真实验验证了模型的有效性与可行性.

关键词: 动态贝叶斯网络; 信任; 可信度量; P2P

Trusted Measurement Model Based on Dynamic Bayesian Network in P2P Networks

GUO Lei, YANG Sheng, XIAO Zhong-Jie, CHENG Ze-Wei

(Department of Mathematics and Computer Science, Wuyi University, Wuyishan 354300, China)

Abstract: Inspired by the deficiency of anonymous nodes, the descent of safety caused by the dynamics and the computation insufficiency of current trustworthiness mode, the paper proposes a computing mode of trust evaluation based on the dynamic Bayesian network. The mode calculates the trustworthiness from the direct trust and commendation one according to the historical interaction data. Time-effect factor and penalty factor are introduced in the paper to solve the problems of timeliness and malicious node. The efficiency and practicability of the mode are proved by the simulation experiment.

Key words: dynamic Bayesian network; trust; trust evaluation; P2P

1 引言

由于 P2P 技术具有开发性、分布式等特点, 能极大提高网络资源共享利用率, 它已经成为 Internet 不可分割的一部分, 它的应用也在快速发展, 研究表明, 目前 P2P 网络的应用已经在 Internet 的通信总量中占较大比重. 但它的分布式管理模式弱化了对中央节点的依赖性, 将资源与责任分布在网络的分散节点, 使得它更容易被恶意节点攻击, 安全问题严重阻碍了 P2P 网络的发展, 同时, 分布式也为认证服务的提供带来了很多困难, 传统的安全管理模式主要采用集中式授权的模式, 对 P2P 网络显的无能为力.

在 P2P 网络中, 节点之间的资源共享与协同都涉及到实体之间的交互, 为提高交互安全性, 有关学者结合社会学中的人际关系信任理论, 提出基于信誉的安全控制模型. 模型首先需对节点之间提供可信度评估, 通常与可信度评估较高的节点交互具有更高的安全性与可靠性. 因此, 在 P2P 网络中提供一种可信度量模型, 为节点提供可靠的、客观的信任评价变得尤为重要.

目前, 已有大量的学者针对可信度量评估方法进行分析与建模. 1994 年 MARSH[1]首次提出了可信度量数学模型, 1997 年 ABDULRAHMAN[2]等人提出了推荐机制解决上下文的可信管理概念, 目前信任度量模型主要包含有基于模糊理论[3]、基于信息熵理论[4]、基于证据和概率统计理论[5]等. A.Josang[6]与 L.Mui[7]在他们的信任模型中使用了贝叶斯估计理论, A.Josang 在他的模型中提出了基于 Beta 分布函数描述二项事件后验概率的思想, 给出了一个基于肯定事件数与否定事

① 基金项目:福建省自然科学基金项目(2015J01668);福建省教育厅 A 类重点项目(JA14309);福建省大学生创新项目(201510397040)
收稿时间:2015-08-25;收到修改稿时间:2015-10-26 [doi: 10.15888/j.cnki.csa.005142]

件数的概率确定性密度函数, 并以此计算某个事件可信度. L.Mui 在他的文章中同样使用了这个方法, 但他们均未对信任度进行分级, 即未对直接信任值与推荐信任值进行区分. 文献[8]提出了一种基于 Kalman 方法的简化模型, 模型基于贝叶斯网络, 并引入了衰减机制, 但模型对时间连续性上存在不足, 难以适应复杂网络环境. 文献[9]提出了一种在分布式 P2P 环境中的具有激励效果的可信管理模型, 但改模型忽略了时间与动态环境的因素. 文献[10]提出了一种基于概率统计方法的 P2P 网络信任评价模型, 该模型依据经验和反馈信息, 利用概率统计方法计算节点直接信任值和间接信任值, 以此获得最终信任值, 但该模型未考虑恶意结点的影响; 文献[11]提出了一种基于 Kalman 方法的简化模型, 模型基于贝叶斯网络, 并引入了衰减机制, 但模型对时间连续性上存在不足, 难以适应复杂网络环境. 文献[12-14]都是基于概率理论建立模型的.

以上研究对可信度量模型的发展具有较大的推动作用, 但在 P2P 网络存在大量节点的情况, 对可行度量的动态适应与时效等问题仍存在不足, 主要体现为:

(1)仅对实体的交互动态性进行研究, 忽略了随上下文变化的动态适应性与交互时效性, 算法收敛速度慢.

(2)模型包含大量主观假设, 与现实应用不符, 使模型的准确性与科学性受到影响.

(3)对网络中存在的恶意节点考虑不足, 模型安全性不足.

针对以上问题, 结合动态贝叶斯网络动态适应能力强, 对先验证据反应速度快, 收敛性强等特点, 本文提出了一种 P2P 网络中基于动态贝叶斯网络可信度量模型. 本模型采用基于动态贝叶斯网络的方法, 该方法能表达随机变量随时间演变的过程, 同时考虑了网络行为的随机性和随机变量间的相互依赖、相互印象的关系, 能够体现随机和模糊的特性的同时, 提高可信度的准确性.

2　动态贝叶斯网络可信度量模型

目前可信度量建模常用的方法可以分为三种: 基于概率统计理论、基于多属性决策理论和基于模糊集合理论[15]. 这三种方法各有优缺点, 基于概率统计的方法在获取大量历史记录的基础上, 采用统计的方法对其进行分析, 并用概率算法来描述可信度, 该方法有较好的数学基础, 目前发展比较成熟, 但其依赖于历史记录, 在模型前期需依赖专家系统, 此外, 该方法无法消除恶意推荐所带来的影响. 基于多属性决策理论综合考虑的上下文信息及决策过程关注的属性, 以此决定可信度, 该方法无法体现可信度的模糊特性与不确定性. 基于模糊集合理论通过模糊集合理论对可信度进行描述和扩展, 但该方法无法描述可信度量过程的随机性的问题.

动态贝叶斯网络是建立在贝叶斯定理与贝叶斯公式的基础上, 将时序信息与传统贝叶斯网络结合, 以此来反应时间对事件概率的影响. 动态贝叶斯网络根据采集到的样本信息更新网络结构、条件概率与经验分布, 通过网络拓扑反应变量间依存关系随时间变化的情况, 而且可以改变拓扑结构或改变变量来反应变量间的各种关联关系, 具有较好的扩展性与灵活性. 此外, 动态贝叶斯网络推理过程具有较强的连续性, 采用概率方法对可信度进行度量, 使其具有时间衰减特性, 更加符合客观世界的推理过程.

2.1 主体信任度计算模型

主体信任度计算模型主要包含策略库、基础数据库、可信预处理模块、可信度量分析模块、可信度量决策模块与可信度量管理模块, 其结构图如图 1 所示.

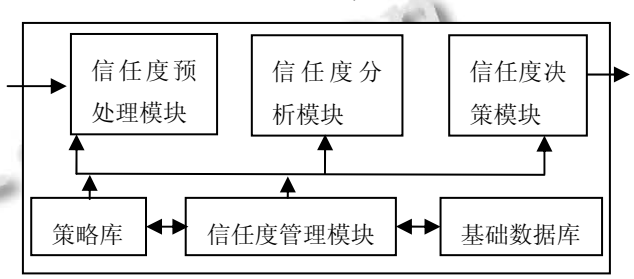

图 1　主体信任度计算模

① 信任度预处理模块: 用于主体基础数据采集、特征析取、规范化、数据关联、等级划分和交互信息预处理等.

② 信任度分析模块: 为本模型核心模块, 主要用于直接可信度计算、间接可信度计算和综合可信度计算等, 是本模型对主体可信度判定的唯一依据.

③ 信任度决策模块: 主要用于相关节点可信列表维护、隔离度量阈值以下实体等功能.

④ 策略库: 用于存储与更新可信度量的先验知

识和策略.

⑤ 基础数据库: 是可信度量计算的基础, 由于存储经过预处理的有效数据.

本文所关注的信任度量包括直接信任度、间接信任度和综合可信度 3 个方面, 综合信任度为最终用户信任度, 用于后期的交互排序等.

2.2 直接信任度计算

定义 1. 设 $P(H, t)$为 t 时间发生历史交互的上下文条件, 其中 t 为发生交互时间, H 为历史交互记录.

定义 2. 设对任意实体 x_i, y_i, 称 $DB_n(x_i,y_i,p(h,t),t)$ 为实体 x_i 对 y_i 在 t 时刻上下文交互条件 $p(h,t)$下的直接可信度量, 令

$$DB_n(x_i,y_i,p(h,t),t)=\begin{cases}(d_1,d_2,d_3\dots d_n),t=0\\ DB_n(x_i,\ y_i,p(h,t-1),t-1)\cdot\alpha(t),\Delta p=\emptyset\\ DB(x_i,y_i,p(h,t),t)\cdot\beta,\ \text{其他}\end{cases}$$

其中 $\Delta p=p(h,t)-p(h,t-1)$, 表示下一时刻上下文交互条件变化情况,$\alpha(t)$为时效因子,反应信任度随历史交互时间而衰减速率, 其值为:

$$\alpha(t)=\left(1-\frac{\Delta t}{t-t_0}\right)\cdot\omega$$

其中, t 为当前时刻, Δt 为两次计算的时间差. ω 为信任衰减调节因子, $\omega\in(0,1)$, ω 越小, 则可信度衰减越快, 反之衰减越慢.

β 为处罚因子, $\beta\in(0,1)$, 其值为

$$\beta=\begin{cases}1,\ \Delta DB\geq 0\\ 0<\beta<1,\ \Delta DB<0\end{cases}$$

其中, $\Delta DB=DB(t)-DB(t-1)$, 该因子主要针对网络中出现的恶意节点进行恶意推荐, 恶意欺骗时进行的信任度处罚, 快速下降恶意节点信任值, β 值越大, 信任度下降越快, 反之越慢.

在以上定义中, 模型将实体的直接信任度的初始值根据专家意见及主体等级进行初始赋值, 当然, 此处也可采用等概率均分. 在需进行主体交互时, 将当前主体交互记录与前一时刻主体交互记录对比, 若无上下文交互历史记录, 则依据间隔时间进行信任度衰减, 若存在上下文交互历史记录, 则重新对信任度进行计算, 若在历史交互中发现某主体存在恶意行为, 则迅速降低其信任度, 减少其对今后交互的影响.

2.3 推荐信任度计算

对于主体而言, 由于它对目标结点的信任判断可能存在交互数不足或欺骗等原因, 导致判断的局限性与片面性, 为更客观的进行信任度评价, 需引入第三方评价, 这个就是推荐信任度.

定义 3. 设对任意实体 x_i, y_i, 称 $SB_n((x_iy_i, p(h,t) ,t)$ 为实体 x_i 对 y_i 在时刻 t 上下文交互 $p(h,t)$下的推荐信任度,令

$$SB_n(x_iy_i,p(h,t),t)=\begin{cases}(s_1,s_2,s_3\dots s_n),t=0\\ SB_n(x_i,\ y_i,p(h,t-1),t-1)\cdot\alpha(t),\Delta p=\emptyset\\ \beta\cdot\frac{\sum_{o\in x}DB_n(x_i,\ y_kp(\Delta t-1),t-1)\times MB_n(x_k,\ y_lp(\Delta t-1),t-1)}{\sum_{o\in x}DB_n(x_i,\ y_lp(\Delta t-1),t-1)},\ \text{其他}\end{cases}$$

式中 O 表示所有与目标实体有交互的实体集合, $\alpha(t)$, ΔC, β 的算式及意义同上式. 模型初始化时, 将所有实体推荐信任度等概率均分, 此处同样可以根据需要进行单独赋值. 若产生交互时与前一个时刻相比, 有信任度推荐, 则可根据交互上下文记录, 进行推荐信任度计算, 若无推荐, 则推荐信任度随时间衰减.

2.4 综合信任度计算

实体的综合信任度是以自身交互经验为基础, 综合其他相关结点的推荐信任度而得出的对某个结点的最终信任度量.

定义 4. 设对任意实体 x_i, y_i, 称 $MB_n((x_iy_i ,p(h,t) ,t)$ 为实体 x_i 对 y_i 在时刻 t 上下文交互 $p(h,t)$下的综合可信度, 令

$$MB_n((x_iy_i ,p(h,t) ,t)=\begin{cases}SB_n(x_i,\ y_lp(\Delta t),t),\ p(h,t)=\emptyset\\ DB_n(x_i,\ y_kp(\Delta t),t),\ p(h,t)=P(H,t)\\ MB_n(x_i,\ y_kp(\Delta t-1),t-1),\ \Delta p=\emptyset\\ \beta[\theta\cdot DB_n(x_i,\ y_kp(\Delta t),t)+(1-\theta)\cdot SB_n(x_i,\ y_lp(\Delta t),t)],\ \text{其他}\end{cases}$$

式中 θ 为权重调节因子, 反应直接信任度与间接信任度的权重关系, 其式为:

$$\theta=\frac{H+h}{2H}$$

H 为有效的交互历史记录, h 为 x_i 与 y_i 之间的历史交互记录. θ 的取值区间一般设在(0.5,1), 这样可以让综合可信度的值偏向于直接信任度, 在前期交互记录数量足够的情况下, 可不考虑推荐信任度, 这也符合人类认知习惯.

在本模型中, 通过采用动态贝叶斯网络对交互过程进行不断的迭代, 对综合可信度进行动态更新, 经

过一定次数的交互后, 综合可信度将逐渐趋向与一个较稳定的值, 而该信任度则可作为访问控制过程实体权限管理的主要判断因素, 同时更新结果也不断对后续计算产生直接影响, 对主体间的动态交互过程有较高的灵敏性与准确性. 当有效历史交互记录增加, 通过动态贝叶斯网络的推理方式, 被评估对象的综合可信度量不断提高并趋于稳定, 这也符合人类的社会行为.

3 仿真实验

3.1 实验设置

本文通过实验对模型算法进行可行性与有效性验证. 在一个小型的 P2P 网络环境中, 实验初始设置邻接交互节点 10 个, 交互记录分为高(H),中(M), 底(L)三个级别, 实验仿真过程采用迭代 10 次, 并采用 Matlab2010b 对算法进行仿真实验.

对实验节点设置了行为变量, 变量可根据实际网络进行设定, 本实验设定了综合信任度(MB), 认证(T1)、交互记录(T2)、安全记录(T3)、交互失败率(T4)五个变量. 其相互依赖关系如图 2.

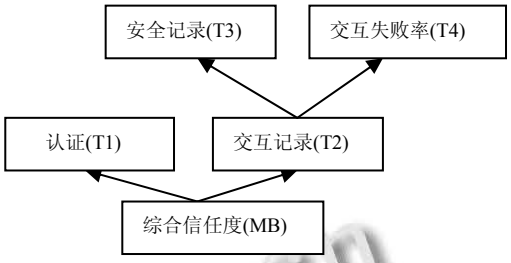

图 2　变量关系依赖图

在模型初始过程中, 利用了专家经验对各变量之间的依赖关系进行了条件概率值得设定, 这个设定会有一定的主观性, 但随着交互次数的增加, 交互记录得到不断的补充与更新, 则条件概率值会不断的调整, 从而更接近真实情况. 本实验对变量依赖条件概率值设定如表 1.

表 1　初始状态各变量依赖条件概率分布

P(A/B)	P(A=H/B=H)	P(A=H/B=M)	P(A=H/B=L)	P(A=M/B=H)	P(A=M/B=M)	P(A=M/B=L)	P(A=L/B=H)	P(A=L/B=M)	P(A=L/B=L)
P(T1/MB)	0.9	0.5	0.05	0.1	0.5	0.4	0.05	0.1	0.55
P(T2/MB)	0.85	0.45	0.15	0.1	0.55	0.35	0.05	0.15	0.6
P(T3/T2)	0.8	0.45	0.1	0.15	0.4	0.3	0.05	0.1	0.55
P(T4/T2)	0.9	0.55	0.1	0.05	0.45	0.25	0.05	0.05	0.5

3.2 实验分析

为了验证模型的有效性与动态自适应性, 实验分别采用了三组的<ω,β>的值进行了对比, 取值分别为<0.6,0.25>、<1,1>、<0.6,0.3>, 其中用三角形连接线表示<1, 1>的值, 用方形连接线表示<0.6,0.25>的值, 用菱形连接线<0.6, 0.3>的值. 交互记录共计 10 个步长, 等级依次为 *H*、*H*、*L*、*H*、*M*、*M*、*H*、*H*、*Φ*、*Φ*, 实验仿真结果如图 3 所示.

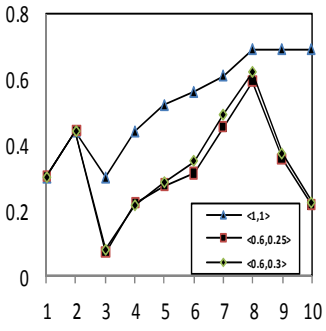

图 3　仿真数据图

实验结果显示, 当<ω,β>的值为<1, 1>时, 表示时效因子与处罚因子均无效. 在 T=1,2 两个时刻, 由于信任等级较高, 故信任度量快速上升, T=3 时刻, 由于被出现的 L 影响, 信任度量急剧下滑, 在惩罚因子的影响下, 方向曲线与菱形曲线下滑的更加明显, 在 T=4 到 T=8 期间, 信任度量随着等级为 H 和 M 的交互记录影响, 三条曲线均不同程度上升, 信任值不断提搞, 在 T=9,10 时, 由于无交互记录影响, 故三角形曲线保持不变, 而菱形与方形曲线随时间影响衰减. 从实验中可发现, 随着交互次数增加, 节点的可信度量也越来越接近真实值, 同时这也符合人类的认知习惯.

4 结束语

随着 P2P 网络应用的不断增强, P2P 网络的安全性一直为业界所关注. 本文针对目前可信度量模型动态自适应能力较差的问题, 提出了基于动态贝叶斯网络的可信度量访问控制模型, 模型首先提出了基于贝叶斯网络的信任度量的动态调整算法, 充分考虑每次交

互记录对可信度量的影响, 并从直接信任度与推荐信任度两个方面对主体信任度量进行动态调整; 其次, 模型充分考虑历史交互记录时效性, 引入了时效因子, 能够较准确、客观的反应相关主体信任度的动态变化情况; 最后, 考虑节点恶意推荐等问题, 引入惩罚因子, 让模型具有更好地顽健性. 仿真实验表面本模型针对 P2P 网络动态不确定的特点, 具有持续的可信度量计算能力, 并具有较好的动态调整能力, 能够为基于可信度量的可信管理、可信授权和可信连接等提供较好的后台支持. 与现有模型相比, 本模型具有动态适应能力强, 收敛速度快, 对恶意结点反应灵敏等特点. 后续作者将对模型进行进一步完善, 在本模型基础上对可信管理与决策展开研究.

参考文献

1 Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. Proc. of the 17th Symposium on Security and Privacy Oakland. Oakland, CA. 1996. 164−173.

2 Abdul-Rahman A, Hailes S. Using recommendationgs for managing trust in distrubuted systems. Proc. of IEEE Malaysia International Conference on Communication. Kuala Lumpur, Malaysia. 1977. 1−7.

3 Bhavna G, Harmeet K, Namita, Bedi P. Trust based access control for grid resources. International Conference on Communication Systems and Network Technologies. Jammu, India, 2011. 678−682.

4 Sun Y, Yu W, Han Z. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, 2006, 249(2): 305−319.

5 Feng RJ, XuXF, Zhou X. A trust evaluation a algorithm for wireless sensor networks based on node behaviors and D-S evidence theory. Sensors, 2011, 11: 1345−1360.

6 Josang A. A logic for uncertain probabilities. International Journal of Uncertainty Fuzzinessand Knowledge-Based Systems. 2001, 930: 279−311.

7 Mui L, Mohtashemi M, Halberstadt A. A computational model of trust and reputation. Proc. of the 35th Hawaii International Conference on System Sciences. 2002. 188−199.

8 Melaye D, Demazeau Y. Bayesian dynamic trust mode. LNCS3690. Berlin: Springer-Verlag,Germany, 2005: 480−489.

9 胡建理,周斌,吴泉源.P2P 网络中具有激励机制的动态 P2P 信任管理研究.通信学报,2011,32(5):22−32.

10 王小峰.信任管理的策略表示与量化模型研究[学位论文]. 长沙:国防科技大学,2009.

11 Melaye D, Demazeau Y. Bayesian dynamic trust mode. LNCS3690. Berlin: Springer-Verlag, Germany, 2005: 480−489.

12 Xiong L, Liu L. Peer trust: Supporting reputation-based trust for P2P electronic communities. IEEE Trans. Knowl. Data Eng., 2004, 16(7): 843−857.

13 Liu G, Wang Y, Orgun MA, Lim EP. A heuristic algorithm for trust-oriented service provider selection in complex social networks. Proc. of the 2010 IEEE International Conference on Services Computing, SCC i10, IEEE computer Society, Washington, DC, USA, 2010. 130−137.

14 Gyarmati L, Anh TT. Measuring user behavior in online social networks. Network, IEEE, 2010, 24(5): 26−31.

15 Li JX, Liu XD, Liu L, et al. HiTrust: Building cross-organizational trust relationship based on a hybrid negotiation tree. Journal of Telecommunication Systems, 2013, 52(2): 1353−1365.