P2P网络中基于信任的风险计算方法

李 开 李瑞轩 章华娟 卢正鼎
(华中科技大学计算机科学与技术学院智能与分布计算实验室 武汉 430074)

摘 要 由于P2P网络的开放性和动态性,对等点信息交换不可避免地会给系统带来安全问题。提出了运用信任评价与传统的风险计算相结合的方法来评估对等点信息交换中的风险。风险度的计算来源于信任风险和后果风险。信任风险是对节点长期累积行为表现的评价,反映了信任和风险之间的关系;后果风险是对节点短期行为所导致后果的评价。仿真实验表明,运用基于信任的风险计算方法可以有效地评估对等点间信息交换的风险。

关键词 对等网,信任,风险度,风险评估
中图法分类号 TP309 **文献标识码** A

Risk Assessment Approach Based on Trust in P2P Network

LI Kai LI Rui-xuan ZHANG Hua-juan LU Zheng-ding
(Intelligent and Distributed Computing Laboratory, College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract As a result of P2P network being open and dynamic, it is inevitable that peers' information exchange brings security issues to systems. A trust based approach was introduced in risk assessment, and a risk assessment method was put forword by combining trust estimation with the traditional risk calculation to evaluate the risk of information exchange between peers. Risk value is derived from estimation of trust risk and result risk. Trust risk is estimated according to the long-term behavior of a node, and reflects the relationship between trust and risk. Result risk is estimated according to the short-term behavior of a node. Simulation results show that the risk assessment approach based on trust can effectively work in P2P network.

Keywords Peer-to-peer network, Trust, Risk, Risk assessment

1 引言

随着Internet的迅速发展,P2P网络被越来越多的分布式系统所采用。在P2P网络中,各节点是对等的,每个节点既是资源提供者,也是资源消费者。P2P网络具有负载均衡、信息资源丰富等优点,但P2P网络的开放性和动态性也带来了许多安全问题[1]。各节点是不同种类的和未知的,有些节点能诚实提供有效服务,而有些节点则存在恶意欺骗性,降低了P2P网络服务的可靠性。在分散式的P2P网络中,由于没有中央节点对恶意节点的行为进行监控和惩罚,一些传统的安全技术(如服务节点需要访问授权,或消费节点需要服务认证)虽然在一定程度上能够避免与恶意节点进行信息交换,但不能阻止恶意节点提供不可靠服务[2]。风险评估是解决信息系统安全问题的有效方法[3]。通过对P2P网络进行充分有效的风险分析和计算,评估风险可能带来的安全威胁和影响程度,并采取相应措施对风险进行控制和处理,便能大幅提高P2P网络的安全防御水平。

信任和风险之间存在密切联系[2,4]。将信任机制引入到风险计算不失为一种有效方法。基本思想是:首先对现有信任模型进行改进得到一个信任计算方法,用来计算服务节点的信任值;然后,一方面根据信任和风险的函数关系计算得到信任风险,另一方面利用风险概率和风险影响的函数关系计算得到后果风险;最后,由信任风险和后果风险共同构成最终风险计算。

2 信任计算

信任值的计算采用基于评价反馈的全局信任模型。在对服务节点进行信任评估时,需要综合考虑其他与之进行过信息交换的消费节点对其所作的评价和该节点自身的信任值。在一次新的信息交换中,对服务节点 Ps 信任值的计算来源于两部分:一部分称为信任评价 T_{Ev},它是所有与节点 Ps 发生过交易的消费节点的信任值与这些消费节点对 Ps 的评价值

到稿日期:2009-11-30 返修日期:2010-01-25 本文受国家自然科学基金项目(60873225,60773191,70771043),国家高技术研究发展计划(863计划)项目(2007AA01Z403),软件工程国家重点实验室开放基金项目(SKLSE20080718),华中科技大学自主创新基金项目(01-09-210014)资助。

李 开(1968-),男,讲师,主要研究方向为分布式系统安全,E-mail:kli@mail.hust.edu.cn;李瑞轩(1974-),男,博士,副教授,主要研究方向为分布式计算、分布式系统安全;章华娟(1985-),女,硕士生,主要研究方向为P2P网络安全;卢正鼎(1944-),男,教授,博士生导师,主要研究方向为分布式计算、软件集成环境、信息安全等。

乘积之和的平均值；另一部分是服务节点 Ps 自身的信任值 T_{OLD}。

在一次交易完成以后，消费节点根据本次服务质量公平地给出服务节点所提供服务的质量的评价值。Peer 的历史交易记录是计算 Trust 的重要依据。如果只是单纯地用 0 表示对服务不满意或 1 表示对服务满意，就不能准确细化地评价服务质量。根据服务节点所提供的服务质量，把服务分成 4 种类别，如表 1 所列。我们把服务质量形式化定义为一个集合：$SQ=\{G,L,N,W\}$，则表 1 对应的 $SQ=\{1,0.5,0,-1\}$。集合 SQ 各元素的数值可以根据不同资源共享系统的需求具体设置。

表 1　4 种服务质量的评价值

服务质量	评价	服务描述
Good	1	服务节点提供了高质量服务，交易非常顺利。
Low Grade	0.5	服务节点提供的正确服务，但是服务有些延迟或降低。
No Response	0	服务节点拒绝合理的服务请求响应。
Worst	−1	服务节点提供错误信息，甚至提供恶意的文件下载。

P2P 是一个高度动态和不确定的网络环境，而 Peer 自身也处于动态变化中。曾经能够提供诚实优质服务的“好节点”，可能随着网络环境的改变或主观原因，已经退化成“坏节点”。过于久远的历史纪录对当前 Trust 的计算参考意义不大。为了解决时间对信任评价值的计算所带来的影响，需增加考虑评价值的时间衰减因子 δ。距离当前信息交互时间最近的交易评价参考价值更大，对应的权重较高；时间较远的交易评价参考价值较小，对应的权重也较低。

因此，当消费节点 Pr 广播服务请求时，为了便于在历史数据库中进行查询，应该给出历史交易事件发生的时间段 $[t_{开始},t_{结束}]=\{t_1,t_2,\cdots,t_L\}$，$t_k<t_{k+1}$，且 $1<k<L$，t_L 表示最近的时间。在获得了它所感兴趣的服务节点的历史交易数据后，Pr 还应在计算新的信任值前对交易评价的权重进行赋值 $\delta=\{\delta_k,1<k<l\}$，$\delta_k<\delta_{k+1}$。

在一次信息交互中消费节点为 Pr，服务节点为 Ps，假定 $E_{j\to s}^{(k)}$ 表示在时间段 k 节点 Pj 对服务节点 Ps 的评价，n 是 Pr 所获得的历史交易数据的总个数，A 是信任评价的权重，A 的取值区间是 $[0,1]$，并且假定节点的新信任值 T_{new}、原信任值 T_{OLD} 和信任评价 T_{Eu} 的取值区间均为 $[-1,1]$，则 Pr 对 Ps 的信任计算公式如下：

$$T_{new}=A\frac{\sum_{j\neq r}(T_j\times\delta_k\times E_{j\to s}^{(k)})+\sum_{j=r}E_{j\to s}^{(k)}}{n}+(1-A)T_{OLD} \quad (1)$$

从式(1)中可以得出：

$$T_{Eu}=\frac{\sum_{j\neq r}(T_j\times\delta_k\times E_{j\to s}^{(k)})+\sum_{j=r}E_{j\to s}^{(k)}}{n}$$

信任评价 T_{Eu} 综合考虑了间接信任和直接信任两个方面，间接信任是来自其他节点的推荐评价，直接信任是来自消费节点与服务节点的直接交互历史经验。间接信任要综合评价节点的信任值和评价值的时间衰减效应，而直接信任是完全采纳评价值，因为消费节点 Pr 有理由相信它的直接交易经验具有更高的参考价值。

在计算间接信任时，为了便于对评价值的权重进行赋值，下面给出式(1)中时间段 t_k 对应的权重值 δ_k 的生成公式。

$$\delta_k=e^{\frac{-u}{k}},u\in\{1,2,3,\cdots\} \quad (2)$$

式中，$1<k<L$。

根据式(2)，只要给出参数 u，则对应的权重 δ_k 便可计算出来。因为 δ_k 是单调递增的函数，所以 $\delta_k<\delta_{k+1}$，这就满足了最近时间的交易评价对应的权重更高。假设 $L=25$，相应的 δ_k 的函数曲线如图 1 所示。图 1 表明，参数 u 越大，函数计算得到的 δ_k 值就越小。从图 1 中可以看到：$u=1$ 时函数曲线位于最上方，则在 k 值相等的情况下，对应的 δ_k 比 u 的任何其他取值都要大；u 的取值越大，在同一 k 值时计算得到的 δ_k 就越小。

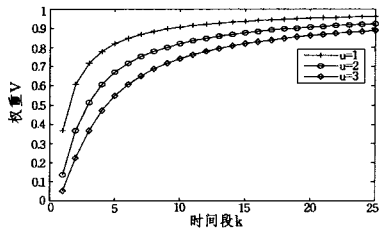

图 1　δ_k 的函数曲线

3　基于信任的风险计算

为了将风险进行量化，本文用风险度来表示一次交易事件中风险值的大小。风险度的定义如下。

定义 1　风险度 R 是在 P2P 网络中任意两个节点进行一次信息交换时存在的各种潜在风险对交易成功所产生威胁力的大小。

风险度的计算来源于两部分：信任风险 R_t 和后果风险 R_i，R_t 和 R_i 的权重分别为 W_{Rt} 和 W_{Ri}。信任风险根据信任和风险的密切关系来定量风险，是对节点长期累积的行为表现的评价。后果风险则根据传统的风险函数定义来定量风险，是对节点短期行为带来的后果的评价。下面分别介绍信任风险和后果风险的计算方法。

信任风险是信任关系规定的交易过程中，交易的一方不能履行服务承诺而给另一方造成损失的可能性。信任风险根据信任和风险的密切关系来定量风险，是交互一方从负面的角度考虑对另一方的信任程度，借助交互双方的信任值反映出交互事件存在的风险。信任直接影响交互双方对风险的接纳。在人际网络中的普遍规律是个体之间信任程度越高，往往他们之间交往所存在的风险就越小。参考这种规律，P2P 系统中节点的信任和风险有这样的反比关系：信任越高，风险就越低；反之，信任越低，风险就越高。本文中，近似地认为，信任值×信任风险值≈1。

在一次信息交互事件中，根据基于评价的信任计算得到节点的信任值为 T_{new}，则信任风险 R_t 的计算公式为：

$$R_t=\begin{cases}1-T_S, & 0\leqslant T_S\leqslant 1\\ 1, & -1\leqslant T_S<0\end{cases} \quad (3)$$

后果风险的计算理论依据是风险的定义。现实生活中风险的定义有很多种，一般情况，风险是风险事件发生的概率和风险事件发生的影响后果两者之间的函数[5]。可得，后果风险是交易事件失败的风险概率(P)和交易事件失败给消费节点带来的风险影响(M)之间的乘积。在一次交易事件当中，消费节点根据发生风险事件造成的实时损失的严重性以及交易数据的价值合理地对 M 进行赋值，因为节点自身对风险事件发生带来的实时损失最了解。M 的范围是 0 到 1，其中 0 表示风险事件发生带来的风险影响最小，1 表示风险事件发

生带来的风险影响最大。

在一次信息交互事件中，服务节点历史交易记录中交易成功的次数为 *success*，交易失败的次数为 *fail*，风险事件发生给消费节点带来的风险影响为 M，则后果风险 R_i 的计算公式为：

$$Ri=M\times P=M\times\frac{fail}{success+fail} \tag{4}$$

综上所述，可得如下关于风险度的计算公式。

消费节点为 Pr，服务节点为 Ps，一次新的信息交换存在的风险度 R 的计算公式如下：

$$R=F(R_t,R_i)=\begin{cases}(R_t,R_i)\times(W,1-W)^T,0<W<1\\R_t,W=0\\R_i,W=1\end{cases} \tag{5}$$

式中，R_t 是信任风险值，R_i 是后果风险值，它们对应的权重分别是 W 和 $1-W$。R，R_t 和 R_i 值的范围都是从 0 到 1。

4 实验与分析

为了验证基于信任机制的 P2P 节点信息交换的风险计算方法，进行了一些仿真实验。仿真实验的硬件环境是 Pentium4 2.0G，512MB，代码使用 Java 编写，调试工具用的是 JBuilder 2005。在仿真实验中，对网络规模和提供的服务进行了限制。设定实验中的节点是 1000 个，提供的服务是文件下载服务。为简单起见，实验中每个节点在一个时间里要么是服务节点要么是消费节点，不能同时担当起两种角色。仿真实验中一共有 200 个文件服务，均匀地分布在 1000 个节点中。每个节点保存了两个记录表。一个是节点记录表，它记录了下载过该节点文件的消费节点对其所作的评价值、评价时间序号 k 和评价节点的信任值。另一个是文件记录表，它记录了该节点所能提供的文件服务。实验中当节点对所选中的节点完成访问时，需要对服务节点的服务质量进行评价，生成的评价及相关信息要更新到服务节点的记录表中。当节点发起请求服务时，默认所有满足服务条件的节点都会发出信任评估响应。

仿真实验中把节点分成 3 种类型：Ⅰ类节点始终提供正确优质的文件下载服务；Ⅱ类节点有时候提供正确的服务，有时候提供错误的文件下载；Ⅲ类节点始终提供错误的文件下载服务。仿真实验中，假定 1000 个节点中有 80% 的Ⅰ类节点，10% 的Ⅱ类节点，10% 的Ⅲ类节点。

4.1 信任计算的仿真实验

(1)信任计算模型具有对善意节点的激励以及对恶意节点的惩罚功能。因为 $T_{new}=AT_{Eu}+(1-A)T_{old}=A(T_{Eu}-T_{old})+T_{old}$，当 $T_{Eu}>T_{old}$ 时，$T_{new}>T_{old}$，则节点信任值得到了提高。这就说明了两点：随着连续提供正确服务的次数的增加，Good peers 的信任值将会稳步增加；而随着连续提供错误服务的次数的增加，Worst peers 的信任值将会不断下降。假设节点刚加入 P2P 网络，交易历史为空白时，信任值为 0。我们从 3 类节点中各抽取了一个节点，当参数 $A=0.5$，时间衰减因子计算参数 $u=3$，$L=25$ 时，它们信任值的抽样值如图 2 所示。

从图 2 中可以看到：Ⅰ类节点随着提供正确服务次数的增加，信任值不断上升，最终将逼近 1；Ⅱ类节点的信任值有波动，但整体趋势是缓慢的上升；Ⅲ类节点随着提供错误的文件下载服务次数的增加，信任值将不断下降，最终将逼近 −1。本实验中用 1 表示信任值最高，−1 表示信任值的最低值。图中的数据可以说明上述理论分析与实验结果相吻合。

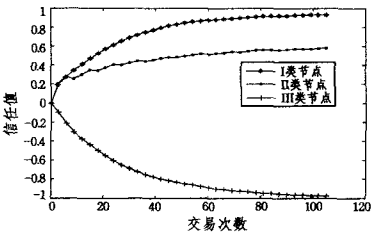

图 2 3 类节点的信任值情况

(2)实验还对恶意节点伪装成好的对等节点这种情况进行了仿真。假定恶意节点在积累到一定程度的信任值时就开始进行破坏，当参数 A 设置不同值时，这类节点的信任取样值如图 3 所示。图中的数据表明：恶意节点起初伪装成善意节点，骗取了节点对它的信任，信任值不断上升；恶意节点一旦开始其恶意行为，它的信任值会很快降低。

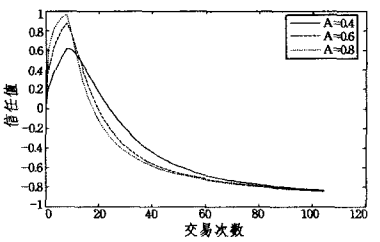

图 3 恶意节点伪装情况下的信任值

图 3 还表明参数 A 的取值在 0.6 上下比较合适，因为参数 A 取值太大时(如 A 的取值在 0.8 以上)，会使得信任值过度受信任评价的影响，甚至出现少量的评价记录便可以影响信任值的增减的情况，这将纵容节点的作弊行为，可能导致恶意节点只是提供了数次正确服务信任值就快速增加，或者善意节点不幸被被恶意评价了数次以后信任值就急剧下降。这种情况往往与节点的真实行为不相符合。因此 A 的值要设置得适中，才能使得信任值稳健真实地增减。

4.2 风险计算的仿真实验

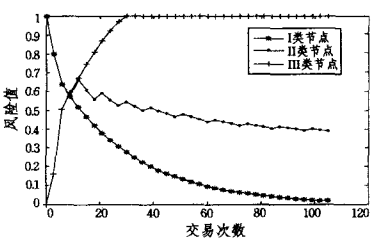

图 4 3 类节点的风险值情况

(1)在 3 种类型的节点中分别选取一个节点，当 $W=0.8$，且风险影响 $M=1$ 时，它们的风险值变化情况如图 4 所示。从图 4 可以得到：(a) Ⅰ类节点的风险初始值为 1，当它连续提高正确优质的文件下载时，交易事件的风险值将不断降低，大概在连续不断提供了 20 次服务后，就属于低风险值；(b) Ⅱ类节点的风险初始值为 1，与这类节点进行交易的风险值是波动的，整体看来风险值的趋势是很缓慢的下降，大约将稳定在 0.3～0.4；(c)为了方便实验，把Ⅲ类节点的风险初始值设

(下转第 122 页)

Networks Special Issue on Network Security, November/December 1999

[9] Capkun S, Nuttyan L, Hubaux J-P. Self-organized public-key Management for mobile ad hoc networks[J]. IEEE Transactions on mobile computing, 2003, 2(1)

[10] Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks[C]// Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio, TX, January 2002

[11] Hu Y-C, Perrig A, Johnson D B. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks[C]// Proceedings of the MobiCom 2002. Atlanta, Georgia, USA, September 2002

[12] Sanzgiri K, Dahill B, Levine B N, et al. A Secure Routing Protocol for Ad Hoc Networks[C]// Proceedings of 2002 IEEE International Conference on Network Protocols(ICNP). November 2002

[13] Hu Y-C, Johnson D B, Perrig A. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks[C]// Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications(WMCSA 2002). IEEE, Calicoon, NY, June 2002: 3-13

[14] Zhang Yongguang, Lee W. Intrusion Detection in Wireless Ad-Hoc Networks[C]// Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000). Boston, MA, August 2000

[15] Zhang Yongguang, Lee W. Intrusion Detection Techniques for Mobile Wireless Networks[J]. Mobile Networks and Applications, 2003

[16] Kachirski O, Guha R. Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks[C]// IEEE Workshop on Knowledge Media Networking(KMN'02)

[17] Puttini R S, Percher J-M, Mé L, et al. A Modular Architecture for Distributed IDS in MANET[C]// Proceedings of the 2003 International Conference on Computational Science and Its Applications(ICCSA 2003). LNCS 2668. San Diego, USA, Springer Verlag, 2003

[18] Huang Yi-an, Lee W. A Cooperative Intrusion Detection System for Ad Hoc Networks[C]// 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN '03). Fairfax, VA, USA, October 2003

[19] Sun B, Wu K, Pooch U W. Routing Anomaly Detection in Mobile Ad Hoc Networks[C]// Proceedings of 12th International Conference on Computer Communications and Networks (ICCCN 03). Dallas, Texas, October 2003: 25-31

[20] Albers P, Camp O, Percher J-M, et al. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches[C]// Proceedings of the First International Workshop on Wireless Information Systems(WIS-2002). Apr. 2002

[21] Bhargava S, Agrawal D P. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks[C]// Vehicular Technology Conference. vol. 4, 2001: 2143-2147

[22] Wang Weichao, Lu Yi, Bhargava B K. On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol[C]// Proceedings of 10th IEEE International Conference on Telecommunication(ICT). 2003

[23] Subhadrabandhu D, Sarkar S, Anjum F. A Framework for Misuse Detection in Ad Hoc Networks—Part I[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 274-289

[24] Johnson D B, Maltz D A, Hu Y-C. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09. txt, 15 April 2003[OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

(上接第 104 页)

置为 0，随着它不断提供错误服务，与之进行交易的风险值急剧上升，在第 30 次时，风险值就上升到 1。因此，基于信任的风险计算算法能够较准确地区分节点的善恶，并且对节点能够赏罚分明。

(2)节点请求下载服务时，对发出服务响应的服务节点进行风险评估，选择风险值最低的节点进行文件下载。如果风险评估模型评估后所选中的节点恰好是 Good peers，则风险评估是成功的；反之，如果经风险评估模型评估后所选中的节点恰好是 Worst peers，则风险评估失败。W 和 M 在 3 种不同的取值情况时，基于信任的 P2P 网络节点信息交换的风险评估成功率如图 5 所示。实验结果表明 W 和 M 取值比较大时更有利于提高风险评估的准确性。信任风险的权重 W 设置为大于 0.5 即可，而风险影响 M 设置为接近或等于 1 能更好地保证对节点信息交换的风险评估质量。实验得到的数据表明，在 P2P 网络中对节点的信息交换运用基于信任的风险评估方法能够较成功地评估节点，从而验证了该模型的可行性。

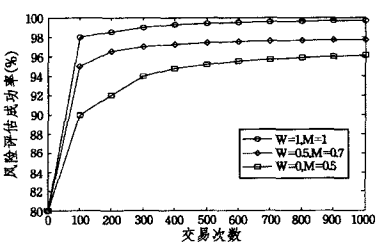

图 5 3 种参数情况下的风险评估成功率

结束语 由于 P2P 网络的开放性和动态性，节点间信息交换所存在的潜在风险是不确定的，对信息交换进行风险评估是解决安全问题的有效途径。本文提出从 P2P 网络的信任模型着手，利用信任和风险之间的内在联系同时结合传统的风险计算函数，得到一个新的风险计算方法。通过实验验证了该方法的有效性和可行性。在下一步工作中，将进一步探讨和改进基于信任的 P2P 网络风险评估模型。

参 考 文 献

[1] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks[C]// Proceedings of the Third International Conference on Peer-to-Peer Computing(P2P'03). IEEE, 2003: 150-157

[2] Wang Y, Lin F. Trust and Risk Evaluation of Transactions with Different Amounts in Peer-to-Peer E-commerce Environments [C]// Proceedings of IEEE International Conference on e-Business Engineering(ICEBE'06). IEEE, 2006: 102-109

[3] Asnar Y, Zannone N. Perceived risk assessment[C]// Proceedings of the 4th ACM workshop on Quality of protection(QoP'08). ACM, 2008: 59-63

[4] Josang A, Presti S. Analysing the relationship between risk and trust[C]// Proceedings of Second International Conference on Trust Management (iTrust 2004). Oxford, UK, March 2004: 120-134

[5] Singh A, Lilja D. Improving risk assessment methodology: a statistical design of experiments approach[C]// Proceedings of the 2nd International Conference on Security of Information and Networks(SIN'09). ACM, 2009: 21-29