P2P 网络的信任评估安全模型研究

张祖昶,王 诚
(南京邮电大学 通信与信息工程学院,江苏 南京 210003)

摘 要:文中针对当前 P2P 网络安全的需要,提出了一种信任评估网络安全模型,给出了新的信任评估计算方法和仿真实验。文中提出的信任评估模型是属于对等信任模型,该模型适合 P2P 网络的分布式结构,也适应于 P2P 网络对节点保持对等、独立、自由和异构的要求。实验结果表明,在 P2P 网络中建立起对等的信任评估模型,其效果是明显的。P2P 网络中的节点能通过模型算法来判断来访节点的情况,通过对来访者真实情况的甄别和判断,能拒绝恶意节点的入侵,有效地抑制了网络中恶意节点的攻击成功次数。

关键词:对等网络;安全模型;防御;攻击
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2014)01-0163-04
doi:10.3969/j.issn.1673-629X.2014.01.042

Research of a Safe Model of Trust Evaluation for P2P Network

ZHANG Zu-chang, WANG Cheng
(College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: According to the requirement of P2P network security, propose a network security model based on the trust evaluation for P2P network, give a new calculation method of the trust evaluation, and the model's simulation experiment. In this paper, the proposed trust evaluation model is a peer-to-peer trust model. The model is suitable for the distributed structure of the P2P network, but also adapts to the requirements of maintaining equal, independent, free and heterogeneous for the nodes. The experimental results show that, to build up trust evaluation model of peers in P2P network, the effect is obvious. A node in the P2P network can determine the visiting nodes by the model algorithm, screen and judge the visitor, reject the invasion of malicious nodes, effectively restraining the number of success attack of malicious nodes.

Key words: peer-to-peer; safe model; defense; attack

0 引 言

随着 P2P 技术的快速发展和不断完善,P2P(Peer-to-Peer)网络的应用领域越来越广。P2P 网络提供了一种开放的、自由进行文件交换和资源共享的环境,广泛用于文件共享、分布式计算、协同工作、即时通信、电子商务等领域,使互联网的存储模式由中心化模式向泛边缘化模式发展[1-9]。P2P 网络有很多优点,但是也存在着很多问题。在 P2P 网络中,各个节点是对等、自由和独立的;网络节点的来源很多而且不确定,节点可以很随意和自由的进出,网络中缺乏强制措施,造成很多天然的安全隐患出现。由于节点行为的匿名性、自主性和异构性,使得节点间的信任关系难以建立,这严重制约了 P2P 网络的进一步应用和发展。因此,如何建立一种有效的信任机制来解决 P2P 网络的安全问题已经成为当前研究的重点。

1 相关工作

对于 P2P 网络而言,已经有很多人员或机构在从事这方面的安全研究,并取得了大量成果。

一般情况下,P2P 网络是采用分布式结构。这种结构比较灵活,而且具有丰富的可扩展性,但是这种结构也带来了巨大的安全风险。首先,这种结构一般是没有中心节点的,因此很难提供身份验证、授权、数据信息的安全传输、数字签名、加密等机制。其次,P2P 网络还面临许多安全威胁,如网络信息与知识产权的保护、路由保护、存取保护和网络病毒防御等问题。

收稿日期:2013-04-02 **修回日期**:2013-07-08 **网络出版时间**:2013-11-12
基金项目:江苏省青年基金项目-基础研究计划(自然科学基金)(BK2012434)
作者简介:张祖昶(1978-),男,广西来宾人,工程师,研究方向为信息技术与决策支持系统;王 诚,副教授,研究方向为信息技术与决策支持。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20131112.1634.017.html

对于这些网络安全问题,目前主要从四个方面进行解决:P2P 内容安全、P2P 网络安全、P2P 节点自身安全和 P2P 中对等节点之间的通信安全;相关的主要技术包括:诚信机制、数字版权保护机制、防火墙和防病毒软件等[10-13]。其中,诚信机制是使用最广泛、最频繁和最有效的一种方法。对于 P2P 网络,如何在网络节点之间建立起信任关系是最为关键的问题。

目前,P2P 网络的信任模型主要分为两类:集中式管理模型和对等信任模型。对于集中式管理,主要是借鉴传统网络管理的模式,希望将传统有效的方法应用到 P2P 网络中去。但是 P2P 网络与传统网络有很大的区别,因此该方法虽然能产生局部的有效性,但是从全局来看,它大大地限制了 P2P 网络的其他优点。而对于对等信任模型,虽然在如何建立节点之间信任关系上存在困难,但是它比较适合 P2P 网络的特点,有利于 P2P 网络的更进一步演变和发展,因此,一直是 P2P 网络研究的主要方向,也是信任模型研究的重点和难点。文中提出的基于信任评估的 P2P 网络安全模型研究,就是属于对等信任模型。

2 信任评估模型

在 P2P 网络中,各节点之间互为对等、独立、异构,因此,P2P 网络存在着很多不定的因素和巨大的安全风险,如何消除这些潜在的安全因素和防止节点之间恶意的访问一直是 P2P 网络研究的热点和重点。文中希望建立起一种有效的 P2P 网络安全模型,有助于 P2P 网络的更进一步完善和发展。

2.1 模型相关定义

对于 P2P 网络而言,节点之间的访问行为都可以抽象为某种交易行为,而这种交易行为与人类社会中的个体交易行为很类似。因此,可以将人类社会的交易评估机制引入到 P2P 网络中,使之成为解决 P2P 网络安全问题的一种手段。在人类社会的交易评估机制中,对某个体的信任评估一般由直接信任评估和间接(或推荐)信任评估组成。因此,文中在此相应地给出在 P2P 网络中信任评估的相关定义。

定义 1:令 $\Omega=\{r_1,r_2,\cdots,r_n\}$ 是含节点数为 n 的 P2P 网络节点集合,N 为集合 Ω 中任意两个不同节点 r_i 和 r_j 之间交易的次数,$f(x)$ 为时间衰减函数,其中 $x\in[0,N]$。

定义 2:对于 $\forall r_i\in\Omega$, $\forall r_j\in\Omega$,且 $r_i\neq r_j$,令 $T(r_i,r_j)_D$ 为节点 r_i 对节点 r_j 的第 $N+1$ 次直接信任估值,则有

$$T(r_i,r_j)_D=\frac{\sum_{0\leqslant x\leqslant N}\alpha\cdot f(x)\cdot T(r_i,r_j)_{D_x}}{N},\alpha>0 \tag{1}$$

定义 3:对于 $\forall r_i\in\Omega$, $\forall r_j\in\Omega$,且 $r_i\neq r_j$,令 $T(r_i,r_j)_R$ 为节点 r_i 对节点 r_j 的第 $N+1$ 次推荐信任估值,则有

$$T(r_i,r_j)_R=\frac{\sum_{0\leqslant x\leqslant N}\beta\cdot f(x)\cdot T(r_i,r_j)_{R_x}}{N},\beta>0 \tag{2}$$

定义 4:对于 $\forall r_i\in\Omega$, $\forall r_j\in\Omega$,且 $r_i\neq r_j$,令 $T(r_i,r_j)$ 为节点 r_i 对节点 r_j 的第 $N+1$ 次信任估值,则有

$$T(r_i,r_j)=\lambda\cdot T(r_i,r_j)_D+\mu\cdot\sum_{\substack{\forall i,j,k\in\langle 0,n\rangle,\\ i\neq j,i\neq k,j\neq k,\\ 0\leqslant x\leqslant N}}(T(r_i,r_k)_{D_x}\cdot T(r_k,r_j)_{R_x}) \tag{3}$$

其中 $\lambda+\mu=1$,且 $\lambda>0,\mu>0$。

在 P2P 网络的节点信任评估计算式中,文中引入了信任度随时间衰减的思想,通过时间衰减函数 $f(x)$ 使节点的信任评估机制更能准确地反映节点当前真实的情况。如果去除时间衰减函数,节点间的信任值则一直停留在节点最后一次交易后的情况。而真实的情况是,节点由于受各种因素的影响,它的相关条件和状况是随时改变的,这将决定节点下次交易时的诚信度。更糟糕的情况是,某些节点由于自身的原因,被其他恶意节点所利用,使其从事非法的访问行为,如果其他正常的节点不能早一些了解这种情况,那么其他正常的节点将会为此遭受损失。因此,时间衰减函数在节点的信任评估机制中是必不可少的,而且时间衰减函数应具有缩减远离当前交易的信任估值,保持临近当前交易的信任估值的特性。

文中定义的衰减函数定义如下:

定义 5:令时间衰减函数为:

$$f(x)=\kappa\cdot e^{-x},\kappa>0 \tag{4}$$

满足条件的时间衰减函数很多。文中在此选择了一个衰减率适中的衰减函数作为节点信任评估值的调节方法,使之更能适应一般的 P2P 网络情况。

节点的信任评估值 $T(r_i,r_j)$ 由直接信任评估 $T(r_i,r_j)_D$ 和间接信任评估 $T(r_i,r_j)_R$ 组成。在引入时间衰减函数后,直接信任评估 $T(r_i,r_j)_D$ 和间接信任评估 $T(r_i,r_j)_R$ 更能动态地改变,使得节点的信任评估值 $T(r_i,r_j)$ 更好地体现当前的交易状况。在组成节点的信任评估值 $T(r_i,r_j)$ 过程中,文中在对各个推荐节点给出的间接信任评估 $T(r_i,r_j)_R$ 加入交易节点对它们的直接信任评估值,使得值得信赖的推荐节点给出间接信任评估 $T(r_i,r_j)_R$ 拥有更大的影响力,让诚信节点的诚信充分发挥作用,激发各个节点恪守诚信的动力,从而使得整个网络形成一套良好的交易机制。

2.2 节点去伪

在人类社会中,恶意个体往往通过欺骗、强迫或伪造信息等不法手段来欺骗交易对方。在这些手段中,伪造信息是最普遍,也是最隐蔽和高明的一种欺骗手

段。在交易过程中要完全去除这些伪造信息是相当困难的。在 P2P 网络中,也有类似的情况出现。如何去除网络中的伪节点是 P2P 网络安全问题中的另一个难点。对于这个难题,文中依据节点交易行为的历史是关联的,通过将节点交易评估过程和评估值保存下来,从这些节点交易行为的历史中找出伪节点,使得交易评估值能真实地体现来访节点的情况。

定义 6:令矩阵 $\boldsymbol{S}$ 为 P2P 网络节点间历史推荐评估转换而来的 $n\times n$ 信任矩阵,n 是节点总数,S_{ij} 为信任矩阵 $\boldsymbol{S}$ 中任意一个元素,满足以下条件:$s_{ij}=\begin{cases}T(r_i,r_j)_R, i\neq j\\ 1, i=j\end{cases}$,则 $\boldsymbol{S}=\begin{pmatrix}s_{11} & \cdots & s_{1n}\\ \vdots & \ddots & \vdots\\ s_{n1} & \cdots & s_{nn}\end{pmatrix}$。

在此基础上,则可以使用相关性计算方法计算节点 r_i 与节点 r_j 之间的相关性。文中采用相关相似性来计算节点 r_i 与节点 r_j 之间的相关程度,典型的计算相关相似性的方法是 PCC(Pearson Correlation Coefficient)。

定义 7:对于 $\forall\ r_i\in\Omega$, $\forall\ r_j\in\Omega$,设 $M=\{r_1,r_2,\cdots,r_p\}$ 为节点 r_i 与节点 r_j 共同访问过的节点集合,且对于节点集合 M 有 $p<n$,$M\subseteq\Omega$ 约束条件,$\boldsymbol{S}^i$ 和 $\boldsymbol{S}^j$ 分别表示节点 r_i 与节点 r_j 对节点集合 M 的信任矩阵,$\overline{R_i}$ 和 $\overline{R_j}$ 分别表示节点 r_i 与节点 r_j 对节点集合 M 的所有节点评价的平均值,则节点集合 Ω 的节点间相关性计算公式为:

$$\mathrm{sim}(i,j)=\left|\frac{\sum\limits_{\substack{r_i\in\Omega,r_i\in\Omega,r_e\in M,\\ r_i\notin M,r_j\notin M,r_i\neq r_j}}(s_{ie}^i-\overline{R_i})\cdot(s_{je}^j-\overline{R_j})}{\sqrt{\sum\limits_{\substack{r_i\in\Omega,r_i\in\Omega,r_e\in M,\\ r_i\notin M,r_j\notin M,r_i\neq r_j}}(s_{ie}^i-\overline{R_i})^2}\cdot\sqrt{\sum\limits_{\substack{r_i\in\Omega,r_i\in\Omega,r_e\in M,\\ r_i\notin M,r_j\notin M,r_i\neq r_j}}(s_{je}^j-\overline{R_j})^2}}\right| \tag{5}$$

$\mathrm{sim}(i,j)$ 取值范围在[0,1]之间。$\mathrm{sim}(i,j)$ 的值越大,表示节点 r_i 与节点 r_j 之间的相关性越大。通过对节点的历史交易行为进行相关性计算,根据 $\mathrm{sim}(i,j)$ 的值,交易节点将能有效地去除一些伪造的推荐节点,从而保证了节点间信任评估值的准确性。

3　实验数据及分析

文中的信任评估模型适用于一般的 P2P 网络,特别是为了防止出现大量伪节点,模型通过计算节点之间的相关性来滤除这些伪节点。文中的信任评估模型的思想是越熟悉的、越值得信赖的节点,其推荐的节点就越值得信任,这与人类社会中的交往行为类似。

为了验证文中的信任评估模型的正确性和有效性,进行了实验仿真。仿真环境是采用 20 台随机安装不同操作系统的 PC 机,互联组成 P2P 网;仿真程序采用 C 语言编写,通过网络访问模拟节点访问过程。在这 20 台 PC 机中,指定其中的 10 台 PC 机作为恶意节点或伪节点,随意地去攻击或欺骗其他节点。在实验中,节点之间的信任评估值 $T(r_i,r_j)$ 取值范围为[0,1],按照公式(3)来计算,通过对公式(3)中的权值 λ 和 μ 取不同值来进行多次仿真实验。在实验初始化时,每个节点的信任评估值 $T(r_i,r_j)$ 均为 0.5。在实验过程中,节点间访问的次数、性质、结果及直接评估和推荐评估都将被记录,当节点的信任评估值 $T(r_i,r_j)$ 小于 0.2 时将被禁止访问。文中在网络访问次数 h 取不同值时,通过比较网络防御成功率 ρ 来验证信任评估模型在网络中是否有效。其中,网络防御成功率 ρ 的含义是指网络节点之间判断出所有恶意攻击的次数 E 与网络节点之间所有访问次数 G 的比率,即 $\rho=E/G$。实验仿真的具体结果如表 1 至表 3 所示。

从表 1 可以总结出以下规律:不论权值 λ 和 μ 的取值如何变化,包含时间衰减函数的信任评估模型的防御成功率要高于没有包含时间衰减函数的信任评估模型;在权值 λ 和 μ 取值相近时,不论是包含时间衰减函数的信任评估模型,还是没有包含时间衰减函数的信任评估模型,网络的防御成功率都是比较高,处于一个峰值状态。

为了使信任评估模型的有效性能得到更充分的验证,文中还在访问次数 h 取 600 次和 900 次时,做了相同的数据抽取,具体实验数据见表 2、表 3。

从表 1,表 2 和表 3 可以得出如下结论:随着网络访问次数 h 的增大,虽然网络防御失败的次数有所增

表 1　实验仿真结果 1($h=300$)

防御结果 / 权值	包含时间衰减函数			不包含时间衰减函数		
	防御成功	防御失败	防御成功率/%	防御成功	防御失败	防御成功率/%
$\lambda=0.1,\mu=0.9$	234	66	78	214	86	71.33
$\lambda=0.3,\mu=0.7$	235	65	78.33	220	80	73.33
$\lambda=0.5,\mu=0.5$	238	62	79.33	226	74	75.33
$\lambda=0.7,\mu=0.3$	233	67	77.67	223	77	74.33
$\lambda=0.9,\mu=0.1$	231	69	77	217	83	72.33

表 2 实验仿真结果 2($h=600$)

防御结果 / 权值	包含时间衰减函数			不包含时间衰减函数		
	防御成功	防御失败	防御成功率/%	防御成功	防御失败	防御成功率/%
$\lambda=0.1,\mu=0.9$	470	130	78.33	448	152	74.67
$\lambda=0.3,\mu=0.7$	474	126	79	453	147	75.5
$\lambda=0.5,\mu=0.5$	488	112	81.33	471	129	78.5
$\lambda=0.7,\mu=0.3$	471	129	78.5	450	150	75
$\lambda=0.9,\mu=0.1$	466	134	77.67	442	158	73.67

表 3 实验仿真结果 3($h=900$)

防御结果 / 权值	包含时间衰减函数			不包含时间衰减函数		
	防御成功	防御失败	防御成功率/%	防御成功	防御失败	防御成功率/%
$\lambda=0.1,\mu=0.9$	731	169	81.22	699	201	77.67
$\lambda=0.3,\mu=0.7$	736	164	81.78	702	198	78
$\lambda=0.5,\mu=0.5$	753	147	83.67	713	187	79.22
$\lambda=0.7,\mu=0.3$	744	156	82.67	696	104	77.33
$\lambda=0.9,\mu=0.1$	732	168	81.33	689	111	76.56

加,但是网络的防御成功率 ρ 总的趋势是提高的,而且不论权值 λ 和 μ 的取值如何变化,包含时间衰减函数的信任评估模型的防御成功率要高于没有包含时间衰减函数的信任评估模型。这表明在信任评估模型中,考虑信任评估值的时间衰减因素对整个模型来说,从总体上来看,是有助于提高网络防御成功率的。不论是信任模型中的直接评估,还是间接评估,时间衰减因素的作用都是正向的。

综上所述,在 P2P 网络中建立起对等的信任评估模型,其效果是明显的。这使得网络中的节点能通过一定的算法来判断来访节点的情况,通过对来访者真实情况的甄别和判断,拒绝了恶意节点的入侵,能有效地抑制网络中恶意节点的攻击成功次数,保证网络中正常的信息交互的进行,因此此次实验也证明了在 P2P 网络中开展信任评估防御模型的正确性和必要性。实验仿真结果的曲线图如图 1 所示。

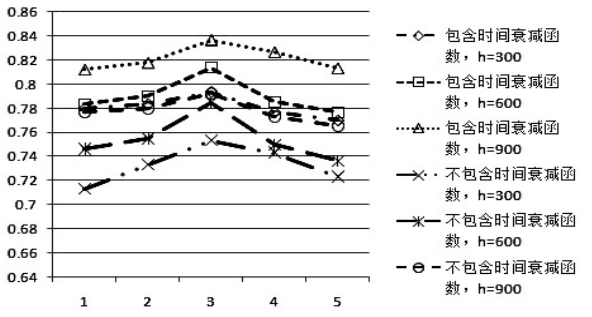

图 1 信任模型不同权值和访问次数下的防御成功率

4 实验结论

实验仿真结果表明,文中提出的信任评估模型在防止网络节点恶意攻击方面是有效的。在实验开始初期,由于缺乏对来访节点情况的了解,正常的节点被恶意攻陷的成功率比较高,但是当网络中各个节点持续互访一段时间后,节点与节点之间建立了一定的互知基础,信任评估模型开始表现出明显的效果,正常节点防御恶意节点的攻击能力大幅提高,而且在公式(3)中,权值 λ 和 μ 之间的比率越接近,节点对恶意节点的识别率就越高;去除伪节点后,参与推荐的节点越多识别率也越高。

这个实验结果与人类社会的实际经验相符:信任模型的评估需要通过节点自身直接评估和参考其他与来访节点交往过的节点的推荐意见来完成;越是值得信赖的节点,其推荐的信赖程度就越高。

5 结束语

一般情况下,由于 P2P 网络自身结构的原因,决定了 P2P 网络存在着很多不定的因素和巨大的安全风险。文中希望建立起一种有效的 P2P 网络安全模型,通过此模型来消除这些潜在的安全因素,防止节点之间的恶意访问。文中的 P2P 网络安全模型思想是越熟悉的、越值得信赖的节点,其推荐的节点就越值得信任。这与人类社会中的交往行为类似,具有一定的借鉴意义。

参考文献:

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

[2] 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). [s. l.]:ACM,2009:21-29.

(下转第 171 页)

了时空混沌系统轨道的随机性,即该时空混沌系统能够提供数量众多、非相关的、伪随机而同时具有确定性的混沌序列,且这种序列信号易于再生,仅需修改驱动系统的初始值和控制参数就可以产生大量的伪随机序列。新方案基于交叉耦合映像格子,采用 Logistic 混沌映射作为驱动序列、锯齿混沌映射作为局部状态演化方程,产生了拟平均分布的伪随机序列。该序列被应用于产生虚拟光学成像加解密系统中,对信息平面实行干扰,实现信息平面的安全加密。对系统密钥灵敏度的仿真结果和算法的时间复杂度的分析表明,该加密系统的密钥长度足够长,穷举密钥搜索是不可行的。

交叉耦合映像格子模型产生的每个格子的时间序列都是时空混沌的,可以利用该模型设计多路虚拟光学加密,对多个信息平面进行并行加密,实现对大批量数据和三维数据的快速加密,日后可从上述角度出发进一步展开研究。

参考文献:

[1] Peng X, Cui Z Y, Tan T N. Information encryption with virtual-optics imaging system[J]. Optics communications. 2002, 212(4-6): 235-245.

[2] Wang X G, Zhao D M J. Encryption of digital hologram based on phase-shifting interferometry and virtual optics[J]. Mod Opt, 2006, 53(11): 1561-1568.

[3] Wu Pan, Ling Qiao. An iterative optical image encryption based on double random phase[C]//Proc of 2010 international conference on computer application and system modeling. [s. l.]: [s. n.], 2010: 1480-1483.

[4] 秦　怡,张　帅,巩　琼,等. 基于干涉原理的虚拟光学加密系统[J]. 光学学报, 2012, 32(10): 72-77.

[5] 张　鹏,彭　翔. 基于公钥的虚拟光学信息安全系统[J]. 系统仿真学报, 2006, 18(1): 176-180.

[6] 于　斌,鹏　翔. 基于级联相位恢复算法的光学图像加密[J]. 光学学报, 2005, 25(7): 881-884.

[7] Liang Xiaoyong, Su Xianyu, Li Sikun, et al. Key rotation multiplexing for multiple-image optical encryption in the Fresnel domain[J]. Optical & laser technology, 2011, 43(4): 889-894.

[8] Niu C, Wang X, Mao X. Multiple-image hiding based on interference principle[J]. Opt quant electronum, 2012, 43: 91-99.

[9] Ge Xin, Liu Fenlin, Lu Bin, et al. An image encryption algorithm based on spatiotemporal chaos in DCT domain[C]// Proc of 2010 the 2nd IEEE international conference on information management and engineering (ICIME). [s. l.]: [s. n.], 2010: 267-270.

[10] Yin Ruming, Yuan Jian, Yang Qiuhua, et al. A stream cipher based on discretized spatiotemporal chaotic system[C]//Proc of 2009 1st international conference on information science and engineering (ICISE). [s. l.]: [s. n.], 2009: 1613-1616.

[11] Wang Yong, Luo Longyan, Xie Qing, et al. A fast stream cipher based on spatiotemporal chaos[C]//Proc of 2009 international symposium on information engineering and electronic commerce (IEEC). [s. l.]: [s. n.], 2009: 418-422.

[12] 张　鹏,彭　翔,牛憨笨. 一种虚拟光学数据加密的系统实现[J]. 电子学报, 2004, 32(10): 1585-1587.

[13] 刘建东,付秀丽. 基于耦合帐篷映射的时空混沌单向 Hash 函数构造[J]. 通信学报, 2007, 28(6): 30-38.

(上接第 166 页)

[3] Costa C, Soares V, Almeida J, et al. Fighting pollution dissemination in peer-to-peer networks[C]//Proc of ACM symposium on applied computing. Seoul: ACM Press, 2007: 1586-1590.

[4] Wang Xiaofeng. On the policy description and quantification model for trust management[D]. Changsha: National University of Defense Technology, 2009.

[5] Xiong Li, Liu Ling. Peer trust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE trans on knowledge and data engineering, 2004, 16(7): 843-857.

[6] Beth T, Borcherding M, Klein B. Valuation of trust in open network[C]//Proc of European symposium on research in security. [s. l.]: [s. n.], 1994.

[7] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks[C]//Proc of the 2nd Int'l workshop on agents and peer-to-peer computing. Berlin: Springer-Verlag, 2004: 23-34.

[8] 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型[J]. 计算机学报, 2006, 29(8): 1301-1307.

[9] Huang C L, Hu H P, Wang Z Y. Modeling time-related trust[C]//Proc of the 3rd international conference on grid and cooperative computing. Wuhan: [s. n.], 2004: 382-389.

[10] Wang Y, Lin F. Trust and risk evaluation of trans actions with different amounts in peer-to-peer e-commerce environments[C]//Proceedings of IEEE international conference on e business engineering (ICEBE'06). [s. l.]: IEEE, 2006: 102-109.

[11] 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.

[12] 韩正平,蔡凤娟,许榕生. 网络安全信息关联分析技术研究与应用[J]. 计算机应用研究, 2006, 23(10): 93-94.

[13] 李景涛,荆一楠,肖晓春,等. 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): 157-167.

P2P网络的信任评估安全模型研究

作者： 张祖昶， 王诚， ZHANG Zu-chang， WANG Cheng
作者单位： 南京邮电大学 通信与信息工程学院,江苏 南京,210003

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(1)