人类心理认知习惯与云模型相结合的P2P信任模型

陆玲玲 徐 建 张 宏

(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 为了解决P2P网络信任模型的计算复杂度以及信任的不确定问题,提出了一种适合于P2P网络的信任模型。该模型借鉴人类心理认知习惯中优先采纳直接经验进行判断的思想来评估节点信任度,进而降低模型的计算复杂度,同时减少获取虚假推荐信息的风险。在此基础上,应用传统云模型中表征不确定性的两个参数——熵和超熵,引入奖励因子和惩罚因子分别对善意节点实施奖励和对恶意节点实施惩罚。仿真实验表明,该模型能很好地抵御网络中策略型恶意节点的欺骗行为,有效辨识出以小概率作恶的复杂恶意节点。

关键词 P2P,云模型,信任,认知

中图法分类号 TP393 **文献标识码** A

Human Psychological Cognitive Habits and Cloud Model Based P2P Trust Model

LU Ling-ling XU Jian ZHANG Hong

(Institute of Computer Science & Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract To solve the problems of the computational complexity and uncertainty of trust in P2P trust model, this paper proposed a new trust model for P2P network. The proposed model evaluates the peer's trust degree from the idea that absolute priority is given to human's direct experience in human psychological cognitive habits to judge, which reduces the computational complexity and the risk of accepting false recommendation information. Further, two characteristic parameters of cloud model, entropy and hyper entropy, are used to introduce positive and negative reward factors to encourage good peers and punish malicious peers respectively. Experiments show that the proposed model can resist cheating behaviors of strategic malicious peers and also distinguish complex malicious peers which behave badly with small probabilities.

Keywords P2P, Cloud model, Trust, Cognition

1 引言

目前,P2P技术的应用日益广泛。P2P网络中每个节点的地位都是相等的,每个节点既充当服务器,为其他节点提供服务,也充当客户机,享用其他节点提供的服务。但由于网络中参与交易的节点大多为陌生节点,且存在大量具有不诚实及恶意行为的节点,使得P2P网络中存在诸如夸大、诋毁、协同作弊等安全问题。因此,亟需建立合理的信任模型来解决上述安全问题。

已有的P2P网络信任机制研究成果在理论或者实现方面尚存在一些问题。本文就目前存在的问题选取两点进行研究:

1) 计算复杂度问题。目前许多信任模型涉及到较为复杂的数学推导过程,算法的实现复杂度尚需进一步研究。

2) 信任的不确定性。不确定性是信任的一个重要属性,主要表现为模糊性和随机性,无法精确地加以描述,尤其对于陌生实体之间的信任关系,不确定性表现得更为明显。传统的信任模型没有很好地考虑到信任的不确定性。

从社会学角度来讲,信任是主体间的一种信念,是一个抽象的心理"认知"过程[1],涉及多种因子,包括假设、期望、行为和环境等。所谓认知,是指人们认识活动的过程,即个体对感觉信号接收、检测、转换、简约、合成、编码、储存、提取、重建、概念形成、判断和问题解决的信息加工处理过程。信任本身又是对主体特定上下文行为特征的主观判断,具有很强的主观性、模糊性和随机性,无法精确地加以描述,尤其对于陌生实体之间的信任关系,不确定性表现得更为明显。

在开放网络环境下的安全问题研究工作中,多位学者从不同的研究背景提出了各自的信任评估模型。文献[2]提出一个基于经验和概率统计解释的信任评估模型,该模型认为信任的不确定性和随机性是等同的概念,忽略了信任本身具有的模糊特性。文献[3]考察了主观信任的模糊性,运用模糊集理论对信任管理问题进行了建模,但该模型否定了信任的随机性,把模糊性作为信任的不确定性来研究。

文献[4,5]提出了基于云模型的信任评估模型,该模型较

到稿日期:2011-09-22 返修日期:2011-11-25 本文受高等学校博士学科点专项科研基金(20093219120024),南京理工大学自主科研专项计划资助项目(2011YBXM81),江苏省自然科学基金重点研究专项(BK2011023)资助。

陆玲玲(1987—),女,硕士生,主要研究方向为信息安全、可信计算,E-mail:lulinglingxg2008@163.com;徐 建(1979—),男,博士,副教授,主要研究方向为信息安全、可信计算;张 宏(1956—),男,教授,博士生导师,主要研究方向为无线网络与网络安全。

好地解决了信任的模糊性和随机性，但没有考虑网络中存在的各种恶意行为，并且计算的复杂度较大。

本文结合 P2P 应用环境，采用云模型理论，提出了一种符合人类社会关系网中人类心理认知习惯的信任模型；同时考虑信任的不确定性，引入了奖励因子和惩罚因子分别对善意节点进行奖励和对行为波动的节点进行惩罚，使得信任评价的结果更加客观和真实。

2 基于云模型和人类心理认知习惯的信任模型

云模型[6]是 20 世纪 90 年代初李德毅院士在传统模糊数学和概率统计的基础上提出的定性定量互换模型，主要反映人类知识中概念的两种不确定性：模糊性（边界的亦此亦彼性）和随机性，已经在智能控制、模糊评测、数据挖掘和知识发现中取得广泛的应用。云模型所表达的概念整体特性可以用云的 3 个数字特征来反映：期望 Ex 是云滴在论域空间分布的期望，是该概念的最典型量化样本；熵 En 代表定性概念的可度量粒度，熵越大，通常概念越宏观，也是定性概念不确定性的度量，由概念的随机性和模糊性共同决定；超熵 He 是熵的不确定性度量，即熵的熵，由熵的随机性和模糊性共同决定，反映代表定性概念值的样本出现的随机性，揭示模糊性和随机性的关联。

2.1 信任云

信任云是一种特殊的云模型，它根据信任关系及其描述方式的特点，把信任的表达用云模型的方式反映出来。

定义 1（信任云） 在 P2P 环境中，把信任空间 $TD=[0,1]$ 作为云的定量论域，C 是 TD 上的定性信任概念，$x\in TD$ 是定性概念 C 的一次定量信任评价，x 对 C 的确定度 $\mu(x)\in[0,1]$ 是有稳定倾向的随机数：$\mu: TD\rightarrow[0,1]$ $\forall x\in TD$ $x\rightarrow\mu(x)$，x 在论域 TD 上的分布称为信任云，记为云 $TC(x)$。每一个 x 称为一个云滴。用 3 个数字特征表示的信任概念的整体特征记作 $TC(Ex,En,He)$。

2.2 信任值的度量

信任评价模型通过计算节点的信任值来评价一个服务节点提供服务的能力。在 P2P 环境中，节点之间在每次交互之后会根据对方节点提供的服务质量给出一个评价，称之为满意度评价。满意度评价标准见表 1。

表 1 评分刻度表

评分值	评分刻度描述
0.0	最坏的交易质量，很不满意
0.25	交易失败，不满意
0.5	服务质量一般
0.75	成功的交易，满意
1.0	非常成功的交易，很满意

为了更好地对云模型进行阐述及更客观地描述信任问题，本文采用离散标度（0.0，0.25，0.5，0.75，1）来描述满意度高低，并且用自然语言对不同满意度进行描述。假设善意节点只提供满意度为 0.75 和 1.0 的服务，恶意节点不合作时提供满意度为 0.0 和 0.25 的服务，合作时提供 0.5 的服务。

服务节点的信任值通常由两部分组成：自身对服务节点的直接信任和来自推荐节点的推荐信任。直接信任指的是访问节点根据自身和服务节点的历史直接交互经验得到的对服务节点的服务能力的一种评价；推荐信任则来自某些曾和服务节点有交互经验的推荐节点。

定义 2（直接信任云） 假设节点 i 和节点 j 在近期时间区间 t 内发生的交互次数为 n，则根据交互满意度评价集合，由逆向云[6]生成算法，可以得到直接信任云的 3 个数字特征，记作 $TC_D^{ij}(Ex_D,En_D,He_D)$，简记为 $TC_D^{ij}(C_D)$。

定义 3（推荐信任云） 推荐信任来自于某些曾和服务节点有过交互经验的节点，当节点 i 想要获取节点 j 的推荐信任值时，节点 i 会根据节点 j 的推荐节点集合来获取近期内所有曾经与节点 j 有过交互历史经验的节点对节点 j 提供服务的评价值，将这些评价值作为逆向云生成算法的输入，即可得到推荐信任云的 3 个数字特征，记作 $TC_I^{ij}(Ex_I,En_I,He_I)$，简记为 $TC_I^{ij}(C_I)$。

在直接信任云和推荐信任云的基础上，借鉴人类社会关系网中人类的心理认知习惯，即人们优先相信自己的直接经验与判断，当已有的历史直接经验足以判断他人的信任程度时，就不再去询问第三方的推荐信息。扩展了文献[1]的信任模型，提出了一种新的综合信任云计算方法，如式(1)所示。

$$TC_{tol}^{ij}(C_{tol})=\begin{cases}TC_D^{ij}(C_D), & h\geqslant H\\ TC_I^{ij}(C_I), & h=0\\ \alpha\otimes TC_D^{ij}(C_D)\oplus(1-\alpha)\otimes TC_I^{ij}(C_I), & 0<h<H\end{cases}\tag{1}$$

当节点 i 和节点 j 在规定的时间区间 t 内交互的次数大于或等于给定的阈值 H 时，认为节点 i 根据自己已有的历史经验，完全能够判断节点 j，此时综合信任云退化为直接信任云，不用再计算推荐信任云，减少了计算的复杂度，同时降低了采纳虚假推荐的风险；当节点 i 和节点 j 的交互次数等于 0 时，节点 i 只能信任其他节点的推荐，此时综合信任云退化为推荐信任云，无需计算直接信任云，减少了计算的复杂度；当节点 i 和节点 j 的交互次数在 0 到 H 范围内的时候，综合信任云由直接信任云和推荐信任云共同决定。$\otimes$ 为逻辑乘算子，$\oplus$ 为逻辑加算子，α 表示节点自身对直接信任和推荐信任的侧重程度，其大小可以调节，其中：

$$Ex_{tol}=\alpha\cdot Ex_D+(1-\alpha)\cdot Ex_I$$

$$En_{tol}=\frac{En_I(Ex_D-Ex_{tol})+En_D(Ex_{tol}-Ex_I)}{Ex_D-Ex_I}$$

$$He_{tol}=\frac{He_I(Ex_D-Ex_{tol})+He_D(Ex_{tol}-Ex_I)}{Ex_D-Ex_I}$$

当 $Ex_D=Ex_I$ 时，定义 $Ex_{tol}=Ex_D$，$En_{tol}=\frac{En_D+En_I}{2}$，$He_{tol}=\frac{He_D+He_I}{2}$。

可以看出，综合信任云的期望、熵和超熵值由直接信任云和推荐信任云的期望、熵和超熵值线性内插得到。随着 α 的增大，综合信任云受推荐信任云的影响将会减小，受直接信任云的影响将会增大。具体算法见算法 1。

算法 1

```
ComputeTrustCloud(IDi,IDj)
Input:节点 i 的 id 号 IDi,节点 j 的 id 号 IDj
Output:节点 j 的综合信任云 TCtol ij(Ctol)
//获取与节点 j 的交互次数 h
h←GetTradeNum(IDj)
  //获取节点 i 本身对节点 j 各次交易提供服务的评价值列表
  dtlist←GetDirectTrustList(IDj)
    //获取推荐节点 k 对节点 j 提供服务的评价值列表,
      I(j)为节点 j 的推荐节点集合
  for k in I(j)
```

idtlist. add(GetInDirectTrustList(ID_j, ID_k))
end for
//根据式(1)计算节点 j 的综合信任云
if h=0
$TC_{tol}^{ij}(C_{tol})$←ComputeInDTCloud(idtlist)
elseif(0<h<H)
$TC_{tol}^{ij}(C_{tol})$←α⊗ComputeDTCloud(dtlist)⊕(1−α)⊗ComputeInDTCloud(idtlist)
else
$TC_{tol}^{ij}(C_{tol})$←ComputeDTCloud(dtlist)
end if

现在得到节点 i 对节点 j 的综合信任云为 $TC_{tol}^{ij}(Ex_{tol}, En_{tol}, He_{tol})$，根据云的 3 个特征参数的涵义以及正态云的统计分析[7]，记 $\Delta=\sqrt{En_{tol}^2+He_{tol}^2}$ 为不确定因子。在信任模型中，节点依据提供服务的节点的信任值来选择服务节点。善意节点提供服务质量为 0.75 和 1 的服务，信任值(期望)比较高，不确定因子比较小，而且通过统计分析知善意节点的不确定因子不会高于某一正常数[8]，将其记为 θ，并称之为善意节点不确定因子阈值。一直作恶的节点其服务质量为 0 和 0.25，虽然行为较稳定，但一直提供质量较差的服务，因此信任值(期望)较低。行为波动节点视情况以不同的概率提供可信服务，但是该类节点行为不稳定，因此不确定性较大。

为了区分善意节点和恶意节点，通过不确定因子对善意节点提供奖励，也即提高其信任值；对恶意节点的信任值进行“折中”处理来达到对节点摇摆行为惩罚的目的，见式(2)。

$$T(j)=\begin{cases}\lambda\times T(j)+(1-\lambda)\times(\theta-\Delta), & \Delta\geqslant\theta \text{ and } T(j)\geqslant 0.75 \quad (a)\\ T(j)+\rho\times(\theta-\Delta), & 0\leqslant\Delta<\theta \text{ and } T(j)\geqslant 0.75 \quad (b)\\ T(j), & T(j)<0.75 \quad (c)\end{cases} \tag{2}$$

式(2)中，式(a)用于计算节点在高不确定性状态下的信任值，其中 $\lambda\in[0,1]$ 为惩罚因子，λ 的取值可以根据系统对被评价节点提供的服务的肯定或否定进行变化，以修正对节点信任值的处罚力度。λ 越小，则不确定性对节点信任值的影响越大，节点的信任值对不确定性越敏感。式(b)用于计算节点在低不确定性状态下的信任值，当节点的不确定性低于设定的不确定因子阈值时，需要对节点进行奖励，提高节点的信任值，其中 $\rho\in[0,1]$ 为奖励因子，用于调整系统对节点信任值的奖励力度。另外 θ 的取值不能过大，可以通过大量实验对善意、恶意节点的不确定因子进行统计分析获得。具体算法见算法 2。

算法 2

ComputeTrust(ID_i, ID_j)
Input：节点 i 的 id 号 ID_i，节点 j 的 id 号 ID_j，
节点 i 计算得到的节点 j 的综合信任云 $TC_{tol}^{ij}(C_{tol})$
不确定阈值 θ，惩罚因子 λ、奖励因子 ρ
Output：节点 j 的信任值 T(j)
Δ←$\sqrt{En_{tol}^2+He_{tol}^2}$
T(j)←Ex_{tol}
if(T(j)≥0.75)
if(Δ≥θ)
T(j)←λ×T(j)+(1−λ)×(θ−Δ)
else
T(j)←T(j)+ρ×(θ−Δ)
end if
else
T(j)←T(j)
end if

3 实验

3.1 环境设置

本实验是对 Stanford 开发的 Query Cycle[9] 改进后进行仿真。构造了一个具有 100 个节点的 P2P 文件共享网络，文件目录种类 20 个，每个节点至少拥有 4 个文件类型，查询请求以类似 Gnutella 的方式进行广播，通过 *TTL* 的减少来控制传输，*TTL* 值为 5，模型的不确定阈值 θ 为 0.2873，惩罚因子 λ 为 0.5，奖励因子 ρ 为 0.5，交互次数阈值 H 为 10，直接信任和推荐信任的侧重程度 α 为 0.5。

为了对模型进行更好的阐述，本文定义了 3 种节点，即善意节点、复杂恶意节点和策略型恶意节点。

- 善意节点：以随机的概率提供 0.75 和 1 的服务。
- 复杂恶意节点：该类节点以 *mrate* 的概率作恶，其他情况提供好的服务。在作恶时，该类节点以随机的概率提供 0.0 和 0.25 的服务，其他情况以随机的概率提供 0.75 和 1 的服务。
- 策略型恶意节点：该类节点视情况以不同的概率提供可信服务，信任值大于或等于 T 时开始以随机概率提供服务质量较差的服务，当信任度低于该值时又以随机概率开始提供好的服务，从而使自己的信任度始终维持在系统规定的可信门限之内，企图不被信任系统觉察。

3.2 模型的安全性能测试

3.2.1 “奖励”性能测试

为了验证模型对于善意节点的善意行为能根据其不确定因子对其进行适当的奖励，本实验在网络中随机选择一个善意节点周期性计算另一个善意节点的信任值，结果如图 1 所示。

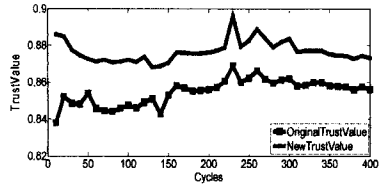

图 1 “奖励”性能测试的结果

由图 1 可以看出，善意节点的信任值通过式(2)的式(b)对节点进行“奖励”，使得善意节点的信任值得到提高，能够更好地与恶意节点区分。

3.2.2 抗“行为波动”性能测试

为了验证本模型抵御复杂恶意节点“行为波动”的有效性，在网络中随机选择一个善意节点周期性地计算复杂型恶意节点的信任值，分别对 *mrate* 为 0.1 和 0.05 的情况进行了测试，结果如图 2 所示。

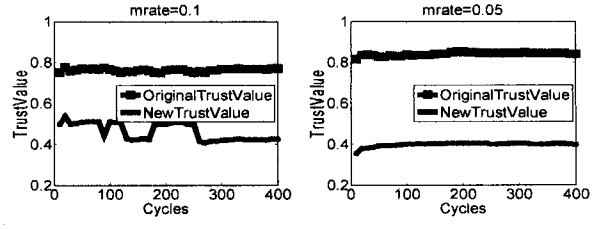

图 2 抗“行为波动”性能测试

由图 2 可以看出，经过“惩罚”的恶意节点信任值(New

TrustValue)远远低于恶意节点原始信任值(OriginalTrustValue);另外当 *mrate*=0.05 时,也即复杂恶意节点以很小的概率作恶时,恶意节点的信任值高于 0.8,甚至可能高于善意节点的信任值,模型也能够很快地识别出恶意节点作恶行为,对其信任值进行降低处理,从而保证善意节点在进行节点选择时,能够进行准确的选择。

3.3 成功交易率

成功交易率就是整个系统成功交易次数在所有交易次数中所占的比例,它直观地反映了信任模型的应用效果。

本组实验设置 3 种实验场景:1) 节点根据信任评价选择响应,考虑了节点的不确定因子,信任评价算法使用本文所述的信任模型,记为 Our-Model;2) 节点根据信任评价选择响应,但不考虑节点的不确定因子,记为 No-Uncertainty-Factor;3) 节点随机地选择响应节点下载,记为 No-Trust。

3.3.1 存在策略型节点情形交易的成功率

为了测试网络中存在善意节点和策略型节点时的成功交易率,分别对 T=0.8 和 T=0.85 进行了测试。在本实验中,善意节点的个数为 50,策略型节点的个数为 50,仿真了 3000 个周期,结果如图 3 所示。

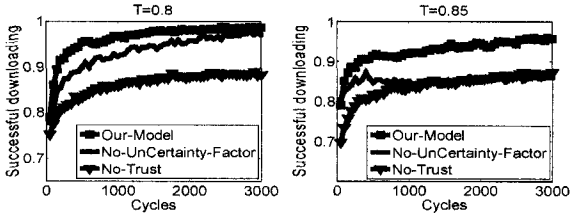

图 3 策略型节点存在时的交易成功率

由图 3 可以看出,当网络中存在大量策略型恶意节点时,Our-Model 能够很好地抵御策略型恶意节点的这种欺骗行为,整个网络的成功交易率高于 No-Uncertainty-Factor 模型和 No-Trust 模型。当 T=0.85,也即该恶意节点的信任值可能高于善意节点时可以看到,在没有考虑节点不确定因子的 No-Uncertainty-Factor 模型中虽然节点是根据信任评价进行选择的,但是其成功交易率比较低,而考虑了节点不确定因子的 Our-Model 的成功交易率还是维持在比较高的水平。

3.3.2 复杂恶意节点存在下交易成功率

为了测试网络中存在善意节点和复杂恶意节点时的成功交易率,分别对 *mrate* 取 0.1 和 0.05 进行了测试。本实验中善意节点的个数为 50,复杂恶意节点的个数为 50,仿真 3000 个周期,结果如图 4 所示。

由图 4 可以看出,当网络中存在复杂恶意节点时,Our-Model 能够很好地辨识出节点的动态行为,使得网络的整体成功交易率高于 No-Uncertainty-Factor 模型和 No-Trust 模型。当 *mrate* 取值 0.05 时,复杂恶意节点虽然以很小的概率作恶,但是也难以掩盖其作恶的本质。由于 Our-Model 引入了不确定因子,使得恶意节点一旦作恶,就能够通过不确定因子达到对恶意节点惩罚的目的,从而保证了网络的整体成功交易率。

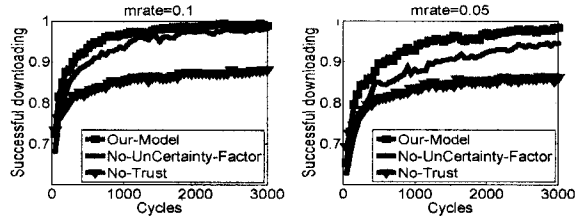

图 4 复杂恶意节点存在时的交易成功率

结束语 本文在传统的云模型的基础上提出了一种符合人类社会关系网中人类心理认知习惯的信任模型。在该模型中,人类认知习惯的引入较好地解决了信任模型中的计算复杂度问题。同时利用云模型,较好地解决了信任的不确定性问题。分析和仿真表明,该模型可以有效抵御网络中恶意节点的欺骗行为和波动行为,提高了 P2P 网络的安全性。如何引入激励机制是以后工作的重点。

参 考 文 献

[1] 李小勇,桂小林. 动态信任预测的认知模型[J]. 软件学报,2010(1):164-176

[2] Beth T,Boreherding M,Klein B. Valuation of Trust in open network[A]// Proceedings of the European Symposium on Research in Computer Security (ESORICS)[C]. New York: Springer-Verlag,1994:3-18

[3] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报,2003,14(8):1401-1408

[4] 张光卫,康建初,孟祥怡,等. 基于云模型的主观信任表示研究[J]. 计算机科学,2006,33(11):158-161

[5] 路峰,吴慧中. 基于云模型的信任评估研究[J]. 中国工程科学,2008,10(10):84-90

[6] 李德毅,杜鹢. 不确定性人工智能[M]. 北京:国防工业出版社,2005

[7] 刘常昱,李德毅,杜鹢,等. 正态云模型的统计分析[J]. 信息与控制,2005,34(2):236-239

[8] 孙秋景,曾凡平. 一种信誉机制与云模型相结合的 P2P 环境信任模型[J]. 小型微型计算机系统,2010(7):1328-1332

[9] QueryCycleSimulator[EB/OL]. http://p2p.stanford.edu/www/demos.htm,2004

(上接第 19 页)

[43] Castells P,Fernández M,Vallet D. An Adaptation of the Vector-Space Model for Ontology-Based Information Retrieval[J]. IEEE Transactions on Knowledge and Data Engineering,2007,19(2):261-272

[44] Bimrah K K,Mouratidis H,Preston D. Information Systems Development:A Trust Ontology[C]// Lecture Notes in Computer Science(LNCS). 2007,4805:25-26

[45] Bimrah K K,Mouratidis H,Preston D. Trust Ontology for Information Systems Development [C]// Information Systems Development:Challenges in Practice,Theory,and Education,2009(2):767-779

[46] Hoo K. How much is enough? a risk-management approach to computer security[EB/OL]. Consortium for Research on Information Security and Policy (CRISP). http://iis-db.stanford.edu/pubs/11900/soohoo.pdf. 2000

[47] Thomas C J. Just What Is an Ontology, Anyway [J]. IEEE Computer Society,2009,11(5):22-27

[48] Gao J B,Zhang B W,Chen X H. A logic analysis of ontology-based Classified Protection Standard[C]// International Conference on Computer and Network Technology (ICCNT). 2011(5):337-341