doi:10.3969/j.issn.1000-436x.2013.04.006

基于参数建模的分布式信任模型

汪京培[1,2]，孙斌[1,2]，钮心忻[1,2]，杨义先[1,2]
(1. 北京邮电大学 信息安全中心，北京 100876；2. 北京邮电大学 灾备技术国家工程实验室，北京 100876)

摘 要：从信任的定义和信任模型的功能特性出发，提取了 9 个功能参数：灵活性、主观性、模糊性、时间衰减性、传递性、抗攻击性、奖惩机制、敏感性和可扩展性。在对这 9 个参数建模的基础上提出了一种分布式信任模型。分析结果表明所提信任模型满足提取参数的功能要求，具有一定的通用性。仿真结果表明所提的信任模型是合理有效的，相对于其他相关模型表现较为优越。

关键词：网络安全；信任；信任模型；功能参数；参数建模
中图分类号：TP311 **文献标识码**：A **文章编号**：1000-436X(2013)04-0047-13

Distributed trust model based on parameter modeling

WANG Jing-pei[1,2], SUN Bin[1,2], NIU Xin-xin[1,2], YANG Yi-xian[1,2]
(1.Information Security Research Center, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. National Engineering Laboratory Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing 100876, China)

Abstract: A distributed trust model based on parameter modeling was posed. Nine functional parameters were extracted after investigating the trust mechanism and current trust models. These parameters included flexibility, subjectivity, fuzziness, time decay property, transitivity, anti-attacks property, rewards & punishment property, sensitivity and scalability. Each parameter was modeled and integrated to form a comprehensive trust model. Analytical results indicate that the proposed trust model satisfies all the nine functional parameters and thus has fair universality Experimental results show that the proposed trust model is reasonable and effective. Comparisons with previous algorithms indicate that the performance of the proposed trust model has been improved.

Key words: network security; trust; trust model; functional parameter; parameter modeling

1 引言

网络安全是近几年的研究热点，信任管理技术作为“软安全”技术，能够从语义层次上对合作对象的行为进行建模来避免交互风险和辅助决策，相对传统的安全技术(如访问控制技术、加密技术、安全路由)具有更好的灵活性[1]。然而信任是一个主观和抽象的概念，对它的定义、度量和更新缺乏可信的标准，所以迄今为止尚没有关于信任的统一定义。目前对信任管理研究的关键是建立可靠的信任模型。自从 M.Blaze 提出 PolicyMaker[2]信任模型之后，国内外学者对信任管理的研究迅速开展起来，出现了大量的信任模型。

目前出现的各种信任模型各有侧重点，都只是部分解决了信任问题。EigenTrust 模型[3]将信任理解为对实体未来行为的期望，它是一种全分布式的算法，该模型具有较好的传递性，但是基于成功失败交易次数的关系来计算信任的方式对节点的行为刻画不够敏感。Sun 等人提出了一种基于熵理论的信任模型[4]，信任被定义为建立在 2 个实体间对特殊行为执行的不确定性关系，该模型敏感性比较好，但需要多层多级计算信任，扩展性不足。

收稿日期：2012-07-02；**修回日期**：2012-11-29
基金项目：国家重点基础研究发展计划（“973”计划）基金资助项目(2007CB310704)；国家自然科学基金资助项目(61161140320, 61121061)
Foundation Items: The National Basic Research Program of China (973 Program)(2007CB310704); The National Natural Science Foundation of China (61161140320, 61121061)

Almenarez 等认为信任是实体对另一个实体的信念，他们提出的 PTM(pervasive trust management)[5]模型侧重于实现敏感性和动态性，但是奖惩能力明显不足。eBay[6]等电子商务应用领域的基于全局信誉的信任模型具有较好的奖惩机制，缺点在于抗攻击能力和可扩展性较差。为了提高模型的可扩展性，Gao 提出基于行为的分层网格信任模型[7]，通过层次化的节点管理网格域内域外的推荐值计算，该模型的缺点是抗攻击性能不好。Selcuk 模型实现了时间衰减性[8]，而且抗攻击效果较好，但灵活性和传递性明显不足。

另外一方面，各种模型在处理信任问题的方法上不尽相同。Yao Wang 提出的 Bayesian 网络模型[9]采用概率论的方式衡量信任值及其变化，还有采用三元组向量来描述信任的模型[10]，采用数学量化的方法来描述信任，信任的主观性体现不充分。Azzedin[11]把信任分级别来度量，每个级别赋予不同数值。一定程度上反映了信任者的主观性，但计算复杂，降低了系统可扩展性。目前还出现了基于模糊理论[12]和基于云理论[13]的信任模型，将实体之间信任程度的描述和不确定性描述统一起来。然而这些算法的计算复杂度较高，抗攻击能力仍然不够。

总之，现有的信任模型各有侧重点，对信任的定义和描述方法各不相同，在功能特性上存在顾此失彼的现象，因此有必要探索更通用的信任模型，来解决分布式网络中的安全问题。首先，本文对信任定义为：主体对客体提供服务的能力的主观预期和动态认知过程。其内涵包括在特定的上下文中，对服务提供者完成任务的可靠信念和风险评估。从该定义和信任模型功能特性出发，提取了 9 个功能参数，在此基础上提出了一种基于参数建模的信任模型，该模型实现了所提参数功能要求，具有一定的通用性。

2 参数提取

为了探索通用的信任模型，首先必须明确信任模型应该具备哪些功能特性。本文提取 9 个功能参数如下。

1) 灵活性。传统的访问控制是根据控制列表判断访问权限。信任机制使得信任关系动态调整，节点可以定义个性化的信任策略得到动态的服务，不同的服务信任值可以不同，授权策略可以不同。

2) 主观性。信任是评价方对评价对象的一种主观判断。即便对于相同评价对象相同的行为，不同的评价者由于判断标准不同，都有可能给出不同的判断。信任模型应该能够反映信任主体的主观差异。

3) 模糊性。在现实生活中，信任具有不确定、不准确和不清楚的自然属性。信任模型必须能够反映信任的这些属性。另外，目前的信任模型绝大多数是基于数值计算推理的，所以必须考虑模糊关系的合理量化。

4) 时间衰减性。信任的改变与时间密切相关，通常情况下，随着时间的推移，信任值会逐渐下降，最为直接的表现是：越久远的信任评价，其说服力越差。

5) 传递性。信任模型应具有传递性，即使这种传递可能是不完全的。传递性使得 2 个陌生节点之间能够建立信任关系，特别是在跨异构域的情况下，需要信任链传递信任信息。推荐是比较典型的信任传播方式，是信任传递性的一种体现。

6) 抗攻击性。能抵抗各种有意无意的攻击。信息网络中存在不诚实反馈、冒名、诋毁以及联合欺诈等恶意行为。信任模型必须能识别和抵抗这些攻击。

7) 奖励和惩罚机制。信任模型要能够提供适当的激励机制，鼓励良好的节点提供更好的服务。同时要具有惩罚算法，对于恶意节点要能够及时地惩罚，降低信任值或禁止参与交易。

8) 敏感性。反映网络或节点变化引起信任关系变动的速度。节点可以随时加入和离开网络，某些节点故障可能会影响整个网络的运行。信任模型应该具有识别功能，按照网络的不同敏感性的需求及时调整信任关系。

9) 可扩展性。反映了网络规模、服务资源等扩充与信任服务节点的负载变化的关系。节点负载主要包括计算复杂度、空间复杂度和查询机制。当网络扩展时，具有稳定或较低负载的信任模型具有较好的可扩展性。

3 基于功能参数建模的信任模型

3.1 信任模型的框架和工作流程

一个理想的信任模型应该包含上述 9 个功能参数所描述的功能，本文首次尝试将上述 9 个参数建模并隐含到一个大的信任模型框架中。本文提出的信任模型的框架和工作流程如图 1 所示。按照信任管理的生命周期分为信任的产生、信任的建模、信任信息的收集、信任的计算、实体的交互与信任的更新 6 个部分。

3.2 信任模型的功能建模和协议的实现

3.2.1 信任的产生

信任是在网络资源共享和节点交互安全需求

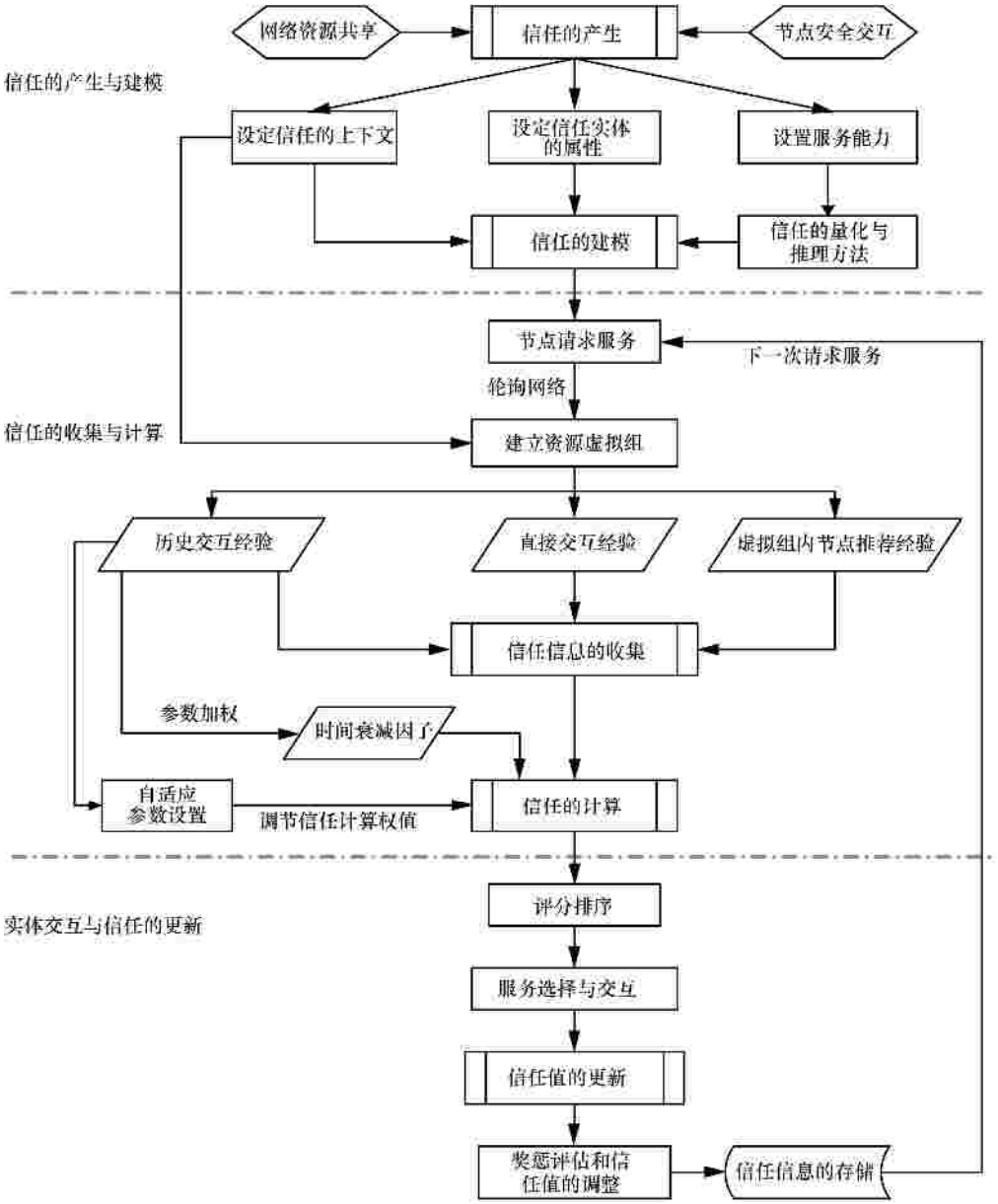


图 1　信任模型的框架和工作流程

的背景下产生的，它是解决交互安全问题的一个有效的机制。信任的形成是主体的行为，信任的基本信息可以用一个协议字段表示，主体对自身设置的信任协议字段如表 1 所示。

表 1　　信任协议字段设置

节点身份	时间	初始信任值	资源列表	资源访问阈值	服务能力
Identity	Time	T_0	$R_1, R_2, \cdots, R_n$	$T_1, T_2, \cdots, T_n$	SC

节点身份：由于信任借鉴了人类社会的相互关系，信任的主体是有身份标识的。节点身份(Identity)可以表示为 $Identity=h(KEY)\|\|Sig_X(S_K(ID))$，$ID$ 是实体身份，S 是置乱算法，K 是置乱密钥，$Sig_X()$是数字签名，X 是用户私钥，KEY 是实体服务关键词，$h()$是散列函数，关键词的散列得到对象标识符 KeyId，用于 DHT(distributed hash table，分布式散列表)机制中的服务搜索，标识符是公开的，“||”是连接绑定符，使标识身份和真实身份相对应。签名可实现认证，置乱保证了实体匿名性。至于在分布式匿名条件下的合法身份验证，可以通过简单的零知识证明方式[14]来完成。

时间：节点的加入时间，可用作节点交互的历史经验和时间衰减的时间起点。

初始信任值：节点加入网络时分配的信任值，

一般不超过最高信任值的一半，信任值过高容易导致恶意节点攻击，过低会使得有些节点没有表现机会。

资源列表：单个节点的共享资源可能不止一个，用 $R_1, R_2, \cdots, R_n$ 表示。

资源访问阈值：与资源列表对应的资源访问阈值，用 $T_1, T_2, \cdots, T_n$ 表示，通过这些阈值设置访问权限，如某 T_h=1，信任值在 0~1 之间的节点请求访问是不被响应的。

服务能力 SC：每个节点的服务能力是有限的，每个节点应该标注服务能力，如带宽、速度限额等。

3.2.2 信任的主观建模

信任具有主观性，需要反映服务请求者的兴趣和要求。不同的上下文，不同的兴趣需求，对应的信任值是不同的。本文建立 3 层结构来描述信任 Trust=A·Aspect·Attribute，其中，A 为节点，Aspect 可以理解为场景，Attribute 是服务属性，即信任是主体在特定的上下文中对客体提供服务的主观评判值。通过分析各种分布式场景，属性可以概括为 4 种：服务质量(SQ)、交互数量(TQ)、响应处理时间(PT)、费用及其他(CM)。不同的需求者可以通过调节各个属性权重来计算直接交互信任值。

$$DT = a \cdot SQ + b \cdot TQ + c \cdot PT + d \cdot CM \qquad (1)$$

其中，a, b, c, d 为属性权重，且 $a+b+c+d=1$。属性权重由服务请求者根据个人兴趣和要求来确定，不关心的属性权重可以设置为 0。这里假设每次交互只在一个场景下进行，所以式(1)不需要考虑上下文。但是在推荐信任的计算上，需要同时考虑上下文。为了控制搜索复杂度，可以设立虚拟组，比如按照专家组设定推荐范围。由于在信任建立时设置有资源列表，搜索节点的资源列表即可确定该节点是否进入相应的虚拟组。

节点对属性的判断具有一定的模糊性，为便于推理和计算，信任需要量化成数值形式。具体量化值可以根据节点在交易后对属性评分确定，评分的值域范围从 0 到 5，分别表示严重不信任、不信任、最低信任、一般信任、比较信任、完全信任。例如对于即时通信上下文中的传输速度，该属性的评分的设置如图 2 所示。

其他属性也可以按照上述例子设置评分，总共需要设置 4 张表。对各个属性评分之后，就可以综合推理出本次交互的直接信任值，为了简便同时保持一定的精确性，本文就用式(1)来完成综合推理过程。

考察指标	即时通信中的传输速度	
服务能力 SC	标称的传输速度是 1Mbit/s，可用带宽 2Mbit/s	
评分细则	Very Fast (小于等于 1Mbit/s)	5
	Fast (512kbit/s~1Mbit/s)	4
	General (128~512kbit/s)	3
	Slow (64~128kbit/s)	2
	Very Slow (1~64kbit/s)	1
	Malicious (小于 1kbit/s)	0

图 2 信任属性评分实例

3.2.3 信任信息的收集

在本文的信任框架下，当节点 i 发起服务请求时，它首先轮询网络，查找和搜集含有所需服务资源的节点，进而建立一个虚拟的以所需服务资源为分类对象的网络节点子集。设整个分布式网络节点集合为 G，含有所需服务的资源 R_i 的网络节点集合为 G_{R_i}，其中，$G_{R_i} \subset G$，$R_i \in \{R_1, R_2, \cdots, R_n\}$，$R_1, R_2, \cdots, R_n$ 是表 1 中定义的节点资源列表。在集合 G_{R_i} 中收集信任信息，包含直接信任值、推荐信任值和历史交互信任值的收集。

设集合 G_{R_i} 中的节点有 m 个，当节点 i 收集节点 j 的信任信息时，首先考察它们之间的直接交互经验，$DT_{ij} = \{DT_{ij}^1, DT_{ij}^2, \cdots, DT_{ij}^n\}$，其中，$n$ 表示直接交互次数。间接推荐的情况下，最多有 m-2 个推荐节点，其经验序列为 $RT_{ij} = \{RT_{1j}, RT_{2j}, \cdots, RT_{(i-1)j}, RT_{(i+1)j}, \cdots, RT_{(m-2)j}\}$，其中，$RT_{kj} = \{RT_{kj}^1, RT_{kj}^2, \cdots, RT_{kj}^l\}$，$k \in \{1, 2, \cdots, m-2\}$，$k \neq i$，$l$ 为 k 和 j 的交互次数。若 2 个节点之间没有交互历史，则 RT_{kj}=0。

历史交互经验信息主要收集统计以下几组数据。

1) 一定观察时间 $t_{\text{ref}} = t_n - t_0$ 内(t_n 为起点时间，t_0 为当前时间，下同)，2 个节点交互的总次数 N，节点持续提供满意服务的次数 N_{suc}。假设满意阈值为 Th_{suc}，则评分信任值大于 Th_{suc} 的服务为满意服务，如果 N_{suc} 足够大，说明该节点在某一段时间表现良好。

2) 节点评价的差别信任度。将观察时间 $t_{\text{ref}} = t_n - t_0$ 平均分成长度为 t_m 的时间段，在一个时间段内节点 i 的信任值序列 $T_i^{t_x}, T_i^{t_{x+1}}, \cdots, T_i^{t_{x+p}}$，其差别信任度衡量如下

$$Dif = \frac{\sum_{q=x}^{x+p} | T_i^{t_{q+1}} - T_i^{t_q} |}{p} \qquad (2)$$

差别信任度衡量了一个时间段 t_m 内信任评价的稳定性，设置门限值 Th_{Dif}，若差别信任值低于这个门限值，则表明该段时间节点一直表现比较稳定。

3) 节点评价相似度。用源节点和目标节点对评价节点的信任评价相似值来表示，计算如下

$$Sim = 1 - \sqrt{\frac{\sum_{n}(u_i - v_i)^2}{25n}} \tag{3}$$

其中，i 为评价节点标号，$u_i, v_i \in [0,5]$ 分别是源节点和目标节点对节点 i 的评价信任值，n 为源节点数目，25 是归一化参数。信任相似值越小，相似度越低。

4）节点的活跃度。用于评价节点在观察时间内的活跃水平，计算如下

$$Act_j = \frac{\sum req_j}{\sum req_{G_{R_i}}} \tag{4}$$

其中，req_j 表示节点 j 在过去一段时间 t_{ref} 内发出的交易请求，$req_{G_{R_i}}$ 表示在过去一段时间集合 G_{R_i} 中节点总的交易请求值。

5）节点的欢迎度。用于评价节点在一段观察时间 t_{ref} 内的受欢迎程度，计算如下

$$Pop_i = \frac{\sum tra_i}{\sum tra_{G_{R_i}}} \tag{5}$$

其中，tra_i 和 $tra_{G_{R_i}}$ 分别表示在观察时间内集合 G_{R_i} 中与节点 i 交互次数和与集合 G_{R_i} 中所有节点交互总数。

3.2.4　信任的计算

节点 i 对节点 j 的信任值的计算框架如下

$$T_{ij} = a \cdot DT_{ij} + b \cdot RT_{ij} + RW \tag{6}$$

其中，a 和 b 分别是直接信任值和推荐信任值的权重，且 $a + b = 1$，RW 是奖励信任值。

直接信任值序列为 $DT_{ij} = \{DT_{ij}^1, DT_{ij}^2, \mathrm{L}, DT_{ij}^n\}$，直接信任值计算如下

$$DT_{ij} = \sum_{t_k=1}^{n} \frac{d(s,t_k) \cdot DT_{ij}^{t_k}}{\sum_{t_k=1}^{n} d(s,t_k)} \tag{7}$$

其中，$d(s,t_k)$ 是衰减函数，定义如下

$$d(s,t_k) = \mathrm{e}^{-s \cdot L(t_k)} \tag{8}$$

其中，s 是衰减速率，$0 < s \leq 1$，衰减速率为 100% 时，s=1；衰减速率为 1%时，s=0.01。t_k 对应于直接信任序列中的 n 次交易时间点，$L(t_k)$表示每次交易相对于当前时间 t_0 的时间距离，本文中设置参考时间为 3 个月 90 天，每月 30 天，$L(t_k)$按照距离当前时间的月数更新并取整，即 $L(t_k) = round((t_k - t_0)/30)$，$round()$是取整函数。最小距离是 0/30，最大距离是 90/30，大于 90 天的交易按照第 90 天的时间计算衰减。需要注意的是衰减函数的 2 个因素 s 和 $L(t_k)$相互独立，共同调整衰减程度。

关于推荐信任值的计算，前面已给出了推荐信任值序列 $RT_{ij} = \{RT_{1j}, RT_{2j}, \mathrm{L}, RT_{(i-1)j}, RT_{(i+1)j}, \mathrm{L}, RT_{(m-2)j}\}$，对于该序列中每一个元素 $RT_{kj} = \{RT_{kj}^1, RT_{kj}^2, \mathrm{L}, RT_{kj}^l\}$，其本质上是节点 k 和节点 j 的直接信任值，也按照式(7)来计算。设 $G_{R_i}(j)$ 为集合 G_{R_i} 中不包含节点 i 和 j 的节点，则推荐信任序列的合成计算公式为

$$RT_{ij} = \frac{\sum_{k \in G_{R_i}(j)} R_{ik} \cdot RT_{kj}}{\sum_{k \in G_{R_i}(j)} R_{ik}} \tag{9}$$

其中，R_{ik} 为节点 i 对推荐节点 k 的信任度，$0 \leq R_{ik} \leq 1$。由于本模型中的节点都是匿名的，不存在朋友节点，推荐节点彼此都是平等的，唯一不同的是各个节点的主观性不同会导致其推荐值趋同于各个节点的属性评分，节点 i 对节点 k 的推荐值的采信程度可通过评判这 2 个节点相对目标节点的属性评分相似程度来确定。设 j 为目标节点，节点 i 对节点 j 属性评分权重形式化为 $\boldsymbol{X}=\{x_1, x_2, x_3, x_4\}=\{a_{ij}, b_{ij}, c_{ij}, d_{ij}\}$，节点 k 对节点 j 主观评分权重分别为 $\boldsymbol{Y}=\{y_1, y_2, y_3, y_4\}=\{a_{kj}, b_{kj}, c_{kj}, d_{kj}\}$。则属性评分相似度可用相关系数表示。

$$R_{ik} = \frac{l_{XY}}{\sqrt{l_{XX}\, l_{YY}}} = \frac{\sum_{i=1}^{4}(x_i - \overline{p}_{ij})(y_i - \overline{q}_{kj})}{\sqrt{\sum_{i=1}^{4}(x_i - \overline{p}_{ij})^2}\sqrt{\sum_{i=1}^{4}(y_i - \overline{q}_{kj})^2}} \tag{10}$$

其中，$\overline{p}_{ij} = (a_{ij} + b_{ij} + c_{ij} + d_{ij})/4$，$\overline{q}_{kj} = (a_{kj} + b_{kj} + c_{kj} + d_{kj})/4$ 为向量数学期望。相关系数越大，表示属性评分权重越相近，即节点 i 和节点 k 共同关注度越接近，R_{ik} 越大，则推荐值 RT_{kj} 越容易被采纳(见式(9))。现实的反例可解释：只关注物品质量的推荐信任值对于只关心物品价格的人来说可能不被采信。

直接信任值和推荐信任值的权重 a 和 b 反映

了服务请求者对直接信任和推荐信任采信的比重。规定 $a=a(t)/(a(t)+b(t))$，$b=b(t)/(a(t)+b(t))$，$a+b=1$，$a(t)$ 表示节点 i 和节点 j 直接交互的次数，可以统计得到。在考察的时间内，当直接交互达到一定的次数 Th_n 时，可以认为交互双方完全建立了信任关系，这时可设置 $a=1$，只考虑直接信任，这与人类的心理认知习惯是相符的[15]。$b(t)$ 由式(4)定义的节点活跃值 Act_j 确定。

RW 奖励信任值由节点持续好评、节点欢迎度来确定。这 2 个参数都与时间段相关，一定观察时间 t_{ref} 内，奖励值为 $RW=\frac{1}{4}\left[\left(\frac{N_{\text{suc}}}{N}+Pop_i\right)\cdot \mathrm{e}^{-s\cdot L(t_k)}\right]$，即奖励值控制在 0.5 以下，同时也随时间衰减，且满足加入奖励之后总的 T_{ij} 小于信任评分最大值 5。

3.2.5 实体交互与信任的更新

对集合 G_{R_i} 中所有节点的信任值计算之后，形成一个 m 个元素的信任值列表。对这些信任值进行排序，选择信任值高的节点(一般选相对信任最高的节点)进行交互。被选节点出于数据隐私保护，还需要考察服务请求者的信任状态来决定是否提供服务和数据。服务请求者最近更新的信任值可通过其对象标识符按照 DHT 所指的节点提取，其信任值 T 要满足 $T\geq T_i$ 才能访问所选节点的资源，其中，T_i 是表 1 中定义的对应资源 R_i 的被选节点的资源访问阈值。如果请求节点的信任值低，则只能选择访问阈值较低的节点交互。

交互完成之后，服务请求者和服务提供者按照式(1)相互评分，评分之后的结果按照 DHT 方式存储到选定的节点上。

信任值更新后，还需要对信任节点进行奖惩评估，在信任计算框架中，已经实现了奖励机制，在这里主要阐述的是针对惩罚的发现和实施机制。惩罚主要考察不提供反馈、虚假反馈、策略攻击和安全事件 4 种。

不提供反馈的情况：如果服务请求节点在规定的时间内不提供反馈信息，则降低服务请求节点的信任值，降低幅度为 $T_{\text{no\_rep}}$。

虚假反馈：服务请求节点提供不符合客观事实的信任反馈值。按照式(3)计算各个节点的相似度来判断节点反馈的可信度。其中，u_i 设置为服务提供者对目标节点 j 的反馈信任值，v_i 设置为其他多个节点对目标节点 j 的反馈值。当相似度低于一定门限值(比如 0.5)时，认为存在虚假反馈。此时纠正反馈值 $u_i=\sum v_i/n$，同时降低提供虚假反馈节点的信任值，降低幅度为 $T_{\text{fal\_rep}}$。

策略性动态改变行为：节点实施摇摆行为攻击(on-off 攻击)。考察节点 i 的信任值序列，按照式(2)计算差别信任度。若差别信任值高于设置的门限值 Th_{Dif}，则表明该段时间节点表现不稳定。计算差别信任值 $\Delta T_i^q=T_i^{t_{q+1}}-T_i^{t_q}$，$q\in[1,p]$ 且 $q\in Z$。若 $\Delta T_i^q>0$，则调整 $T_i^{t_{q+1}}=T_i^{t_q}+\frac{1}{r_1}\cdot\Delta T_i^q$；若 $\Delta T_i^q<0$，则 $T_i^{t_{q+1}}=T_i^{t_q}+r_2\cdot\Delta T_i^q$，其中，$r_1$、$r_2$ 控制惩罚的力度。

安全事件：如果节点被攻陷或者提供特别恶意的服务(如病毒等)。服务请求者(源节点)将该节点的信任值设置到不信任临界点(全网节点的最小的资源访问阈值)以下，并通报全网，同时启动系统修复软件(如杀毒软件)的运行。信任值经过奖惩评估和信任值调整之后，按照 DHT 方式将评价节点信任值存储到对象标识符对应的若干节点上，用于下一轮服务请求。

4 信任模型参数功能分析

上述建立的信任模型满足第 2 节讨论的 9 个功能参数要求。下面将从这 9 个参数角度出发，全面分析所提的信任模型的功能特性。

4.1 灵活性

传统的访问控制主要是对节点的身份进行控制，信任机制提供了包括身份、行为和个性化的授权策略等多维的决策对象，节点可以定义个性化的信任策略得到动态的服务。

本文所提信任模型在信任的产生阶段，每个节点保存如表 1 所示的协议字段来引入信任机制。节点身份字段是 $Identity=h(KEY)\|Sig_X(S_K(ID))$，对身份 ID(类似于现实中人的身份证)进行置乱是为了保持节点的匿名性，只有节点自己拥有置乱密钥，匿名性的作用后面详细分析。数字签名是为了认证用户，当提供虚假服务和重复登记攻击时可以追踪实体的真实身份。通过绑定标识身份和真实身份来表示节点身份，标识身份对外公开交互，真实身份按需验证，身份标识比较灵活。

本文使用 6 级评分制（0~5 分别表示极其不信任到极其信任的过程），初始信任值设置在 1.5~2.5 之间比较合理。信任阈值设置是针对节点崩溃和病

毒攻击等安全事件的，安全事件导致惩罚机制的启动，信任值被降到阈值以下。表 1 中的资源列表、访问控制阈值和服务能力都可以由节点根据自身情况设置，根据服务请求者的信任值动态调整访问权限和资源的分配，非常灵活。

另一方面，本模型使用自适应算法计算信任值，式(6)中设置了直接信任值和推荐信任值的权重 a 和 b ，a 值依据直接交互次数确定，b 值与推荐节点活跃度相关。相对于采用固定权重的模型，进一步提高了灵活性。

4.2　主观性

信任模型需要反映服务请求者的兴趣和要求。本模型的主观性反映在信任建模阶段。考虑到信任的上下文和属性，建立 3 层结构：A，Aspect，Attribute，Aspect 可以理解为场景或主体的多项能力，如服务 1、服务 2 等上下文。因为不同的上下文，不同的兴趣需求，信任是不同的。例如同一个节点可能具有文件共享、即时通信、电子商务等不同的上下文，在每一种上下文下，有的服务请求节点可能关注传输速度，有的更看重交易质量，有的则重点考察交易费用等。

信任属性主要归纳考虑了服务质量、交易数量、响应处理时间、费用及其他 4 个属性。不同的节点可以根据自身的兴趣和要求调节各个属性权重，按照式(1)来计算本地信任值。推荐时搜索相似兴趣一组节点，为了控制搜索复杂度，按照服务上下文形成虚拟组来设定推荐范围。例如涉及资源共享应用时，在轮询网络时，只收集存在该项资源相关的节点作为推荐范围。这样就可以对比评判不同兴趣爱好节点推荐采信程度。

4.3　模糊性

模糊性是评价者对评价对象信任状态的主观不确定、不清楚和不准确的属性，一个实体对其他对象的评价经常是“我很信任他”或“我有些不信任他”。在模糊理论中，往往通过隶属度函数和设置的推理规则来归类量化这些模糊评价。类似地，本文所提模型采用属性评分，主观推理的方式来解决类似的模糊问题。模糊性体现在节点对属性的判断上，属性的好坏程度都具有一定的主观不确定性。为便于推理和计算，属性需要量化成数值形式。具体量化值可以根据节点在交易后对属性评分确定，评分的值域范围从 0~5，分别表示严重不信任、不信任、最低信任、一般信任、比较信任、完全信任。评分规则由服务请求节点根据不同的属性设置。本模型对照节点的服务能力设置评分规则，如图 2 所示，按照属性数目需要设置 4 张表，这样形成的评分非常精确。节点在请求服务时，在请求服务标注协议中可自主设置属性权重。对各个属性评分之后，就可以综合推理出本次交互的直接信任值，为了简便，本文就用式(1)来完成综合推理过程。

4.4　时间衰减性

时间衰减主要考虑 2 个方面，一是信任评价随着时间推移，其准确性和有效性越低，如 3 年前建立的信任值肯定没有 3 天前交互的信任值可信。二是不能完全否定过去的交易历史，否则最近一次交易失败会抹除以前交互成功建立的信任值，一般在信任模型中通过调节历史和当前的信任权值实现时间的衰减性。

本文的信任模型的时间衰减特性反映在信任值的计算之中，通过引入时间衰减函数 $d(s,t_k)=\mathrm{e}^{-s\cdot L(t_k)}$ 来加权信任值。衰减函数通过 s 和 t_k 2 个参数调节衰减的程度，以此达到信任值随着时间衰减但过去交易经验不能完全抹除的折中。引入衰减速率是因为考虑到节点交易的重要性不同。如果交互历史中有重要的交易，比如电子商务中，有一笔很大的交易金额成功或失败，其信誉对后续交易产生的影响比多次小额交易的信誉的影响要大，这时应该降低衰减速率，提高重要交易的参考比重。另外，也有可能存在交易的不对称集中，比如在一个很小的时间段内，交易数量特别多，除了按照 t_k 衰减外，还可以根据个人需要调整衰减速率 s，使该段时间内的信任值对当前信任值有更合理的参考意义。这种调整具有一定的自适应性，符合人类社会的交易习惯。

时间跨度参数 t_k 随着时间的流逝，其值持续增加，时间越久远，其信任值衰减越大。衰减前后的值表示为 $T_{\mathrm{new}}=T_{\mathrm{old}}\cdot\mathrm{e}^{-s\cdot L(t_k)}$，当 t_k=0 时，$T_{\mathrm{new}}=T_{\mathrm{old}}$；当 t=8 时，T_{new}=0。时间设置的上限可以根据不同的交互环境的时效要求，本文信任模型设置的失效是 3 个月，大于 3 个月的评价按照 3 个月计算，即 $L_{\min}$=0/30，$L_{\max}$=90/30。当 s=1，$L_{\max}$=3 时为最大衰减，T_{new} ；$0.05\cdot T_{\mathrm{old}}$，最大衰减将近达到 95%。

4.5　传递性

传递性对于信任来说很重要，它在已知节点和未知节点之间架起了一座桥梁，使得 2 个陌生节点之间能够建立信任关系。推荐比较典型的信任传播方式，是信任传递性的一种体现。本文信任模型在

计算没有直接交互经验节点的信任值时，通过中间若干个节点提供目标节点的信任信息，然后通过源节点对推荐节点的信任度加权得到目标节点信任值。对于本文模型，网络中传递的其实是信任的属性评分，对这些评分还需要询问者实时调整，调整的方法是用式(10)描述的相关系数加权作为对属性评分的采信度。

信任模型应具有传递性，然而这种传递可能是不完全的。也就是说，若 A 信任 B，且 B 又信任 C，则不一定得出 A 信任 C 的结论。究其原因，一是信任具有不同的上下文特性，比如 B 是一名好医生但不是一名好厨师。A 信任 B 的医疗技术，B 信任 C 的厨艺，但是 A 不一定信任 C 的厨艺。二是可能存在竞争关系，A 和 C 是竞争关系，A 出于利益考虑很可能就不会相信 B 的推荐，虽然 B 相信 C。比如 A、B、C 分别表示移动、电信和联通，移动和电信之间的互信，电信和联通之间的互信就不一定能够推出移动和联通之间的互信。

本文的信任模型具有完全传递性。针对上述原因，本文模型通过以下 2 个方法解决了不完全传递性。

1) 将参与传递信任的节点范围控制在任务需求的上下文之内。如前述主观性中信任协议中设置了资源列表，每个资源代表不同的上下文服务，在轮询网络时，选择包含服务请求者的请求资源的节点作为交互节点范围，构成虚拟组网络参加信任的计算和信任的推荐。

2) 保持节点的匿名性。在信任建立阶段，表 1 所示的协议字段中，节点的身份是匿名的，一个目的即是为了克服信任的不完全传递性，身份 ID 通过置乱密钥 K 来保密节点身份。资源请求者只需知道哪些用户是合法的，而不需要知道具体的身份，节点彼此都是平等的。至于合法性证明，可以用零知识证明的知识解决。匿名性可以消除竞争关系带来的不完全传递性，这在网络中存在敏感节点时尤为重要。

4.6 抗攻击性

信任模型中讨论的攻击性主要是一些恶意的策略式的行为攻击。比如不诚实反馈、冒名、诋毁以及联合欺诈和对于节点本身的恶意行为。本文模型抗攻击性的主要思想是在交易之后，评估攻击性行为的存在，结合奖惩机制调整信任值，使得恶意节点的交易机会减少，请求节点更多地寻求信任值高的节点交互，使得良好节点的成功交易率保持一定水平，从而屏蔽和抵抗攻击。抗攻击性的评估主要涉及检测攻击的精确性和抵抗攻击的机制。本文主要评估以下的攻击行为：1) 不提供反馈的情况。可直接从服务对象的行为进程中发现该行为，然后转入惩罚阶段。由于惩罚幅度小，又存在时间衰减加权，这种情况对信任值改变并不大。2) 虚假反馈，含有诋毁和抬高信任值行为，可通过全局的评价相似度来衡量差异，因为不可能所有节点提供的反馈都是不合理的，网络建立之初必定会有一些预信任节点和一些诚实节点。当评价相似度差别较大时，即低于一定门限值(比如 0.5)时，可认为提供的反馈不可信。这时一方面纠正反馈值，控制虚假反馈的传递，另一方面转入惩罚阶段。3) 共谋攻击，由于本模型的节点都是匿名的，而且其信任值都是通过 DHT 模型随机分配到其他节点上的，很难形成共谋的节点集合。即使存在使用对象标识符行为的共谋集合，也能够通过上述的虚假反馈识别出来。4) 策略性改变行为攻击。本模型对这种攻击有一定的容忍度，评估这类攻击需要给定一个独立的观察时间段 t_m，里面有 p 个信任值，按照式(2)计算差别信任度。差别信任度大于选择的阈值，则认定存在不稳定信任，这时转入惩罚阶段。阈值的选择可以根据该段时间的信任值的数学特征(如均值和方差)来选定，也可以根据实验调整。5) 安全事件，节点提供特别恶意的服务，立刻启动最大幅度惩罚，并通报全网，其他节点可避开与其交互，从而控制攻击的蔓延，保持全网的稳定性。

4.7 奖惩机制

本文信任模型的奖惩机制是通过信任值的调整实现的。奖励效果体现在信任的计算阶段，RW 奖励信任值由节点持续好评、节点欢迎度来确定。奖励强度用式 $RW=\frac{1}{4}\left[\left(\frac{N_{\mathrm{suc}}}{N}+Pop_i\right)\cdot \mathrm{e}^{-s\cdot L(t_k)}\right]$ 计算，系数 $\frac{1}{4}$ 的设置是考虑到量化评分时，等级度量是 1，奖励值应该控制在 0.5 以下，才不影响直接信任值和推荐信任值加权计算后的评分等级的效果。实验中也确定了系数在 $\frac{1}{4}\sim\frac{1}{2}$ 比较合适。

惩罚机制是随着抗攻击性进行的，当检测出攻击后，就开始惩罚。惩罚的方式是降低信任值，使节点失去和其他节点交互的机会。一方面不同的攻击对应不同的调整幅度，上述各种攻击的程度依次

加强，其信任降低幅度也依次加强，比如 $T_{\text{fal\_rep}}>T_{\text{no\_rep}}$，安全事件下信任值降幅最大，可以直降到临界信任值以下，由于本文模型的信任机制在临界点以下信任值的节点请求服务是拒绝的，所以也保证了其他节点免受攻击。另一方面，节点的惩罚机制要符合人类社会的一种习惯，即信任增加是缓慢的，信任下降是很快的，恶意行为的节点需要更长时间的成功交互才能恢复到原来信任值。在策略攻击的惩罚计算中，当差别信任值 $\Delta T_i^q>0$ 时，调整方式为 $T_i^{t_{q+1}}=T_i^{t_q}+\frac{1}{r_1}\cdot\Delta T_i^q$；若差别信任值 $\Delta T_i^q<0$，则 $T_i^{t_{q+1}}=T_i^{t_q}+r_2\cdot\Delta T_i^q$，其中，$r_1$ 和 r_2 控制惩罚的力度，r_1 一般取 2~3，r_2 一般取 3~5。即发生策略攻击时，减小信任值增加的幅度，加大信任值下降的幅度，从而实现了较好的惩罚效果。

4.8　敏感性

敏感性反映的是网络环境的变化引起研究对象变化的速度问题。本文所提信任模型的敏感性主要是网络行为变化引起信任变化的程度和调整信任关系的及时性。主要反映在以下几个方面。

1) 信任模型采用 DHT 方式存储节点信息，当节点加入和离开时，只需要调整其后续节点分配的关键字，所需的时间主要是例行检测时间，反应调整的时间可以忽略不计。

2) 交易评分后，立即开始信任值奖惩的评估，一旦发现攻击行为，立即调整信任值，信任关系变化非常及时。特别是对于出现重大安全事件时，快速的反映机制是很重要的。奖惩机制实现了信任值随着恶意行为的出现(特别是安全事件如病毒攻击时)快速下降，也反映出对恶意节点的敏感性较好。

3) 在时间衰减性建模中，设置了衰减因子 s，配合时间因子 t_k，用于调整信任值的计算。s 越小，信任值衰减越小，该机制类似于可伸缩的时间轴。引入 s 可以调整出现某次重要交易时或某段时间密集的交易的敏感性和整个信任关系的变化程度。

4.9　可扩展性

可扩展性反映了网络规模、服务资源等扩充与信任服务节点的负载变化以及网络性能的关系。节点应具有较好的可扩展性，在网络扩展时，能够与尽可能多的节点建立信任和提供服务。本文的信任模型的可扩展性主要体现在稳定的负载和防止网络堵塞 2 个方面。

负载主要包括 3 个方面：计算复杂度、空间复杂度和搜索传输机制。本文引用 DHT 机制中的 Chord 算法作为分布式查找算法，给定一个关键字(通常是节点 IP 地址)，通过 SHA-1 散列算法得到对象标识符 KeyId，Chord 可以有效地把该标识符映射到网络中某个节点上，形成一个环形的逻辑坐标空间。DHT 的最大的优点在于每一次查询请求的复杂度只有 log$N$，N 为网络大小，相对洪泛机制的复杂度 N 大大降低。本文算法在轮询网络时要搜索整个网络 N-1 个点，形成大小为 m 的资源虚拟组后，计算、存储、搜索的范围都在虚拟组内。直接信任度、间接信任度、奖惩评估信息搜索都能在复杂度 log$m$ 内得到响应。本文模型只是在计算推荐信任值和评价相似度时，计算复杂度达到 $O(m)$，其他的计算复杂度可以忽略不计。每个节点只存储信任协议字段、按照散列表映射的若干个节点的直接信任值的交互历史记录以及一些参数，因此存储资源较小。计算复杂度和空间复杂度都很低。

另外，信任模型使用服务能力 SC 作为评分精确化的参考，形成的信任值与服务能力相关。服务请求者可以按需选择具有较高信任值的不同服务能力的节点交互，这样可以合理分配资源。因为如果按照绝对服务能力设置信任值和服务选择时，那些服务能力强大的节点将不堪重负，而服务能力较弱的节点将没有表现机会，这样网络的堵塞和拒绝服务情况会很严重，网络扩张时可扩展性会很差。根据本文的思路，一个服务能力只有 2Mbit/s 带宽的节点持续提供 1Mbit/s 带宽服务比服务能力 100Mbit/s，但只提供 10Mbit/s 服务的节点信任值可能要高。对于 1Mbit/s 带宽的用户，以上 2 种网络服务都会有被选中的机会。所以用服务能力相对值评价节点得分，能够均衡负载，这也是提高可扩展性的一个方面。

5　信任模型的仿真分析

本文在 MATLAB 7.0 的环境下对所提的信任模型进行了仿真实验，主要验证了所提模型的合理性和有效性，以及相对于其他经典模型的优越性。

5.1　信任模型仿真结果

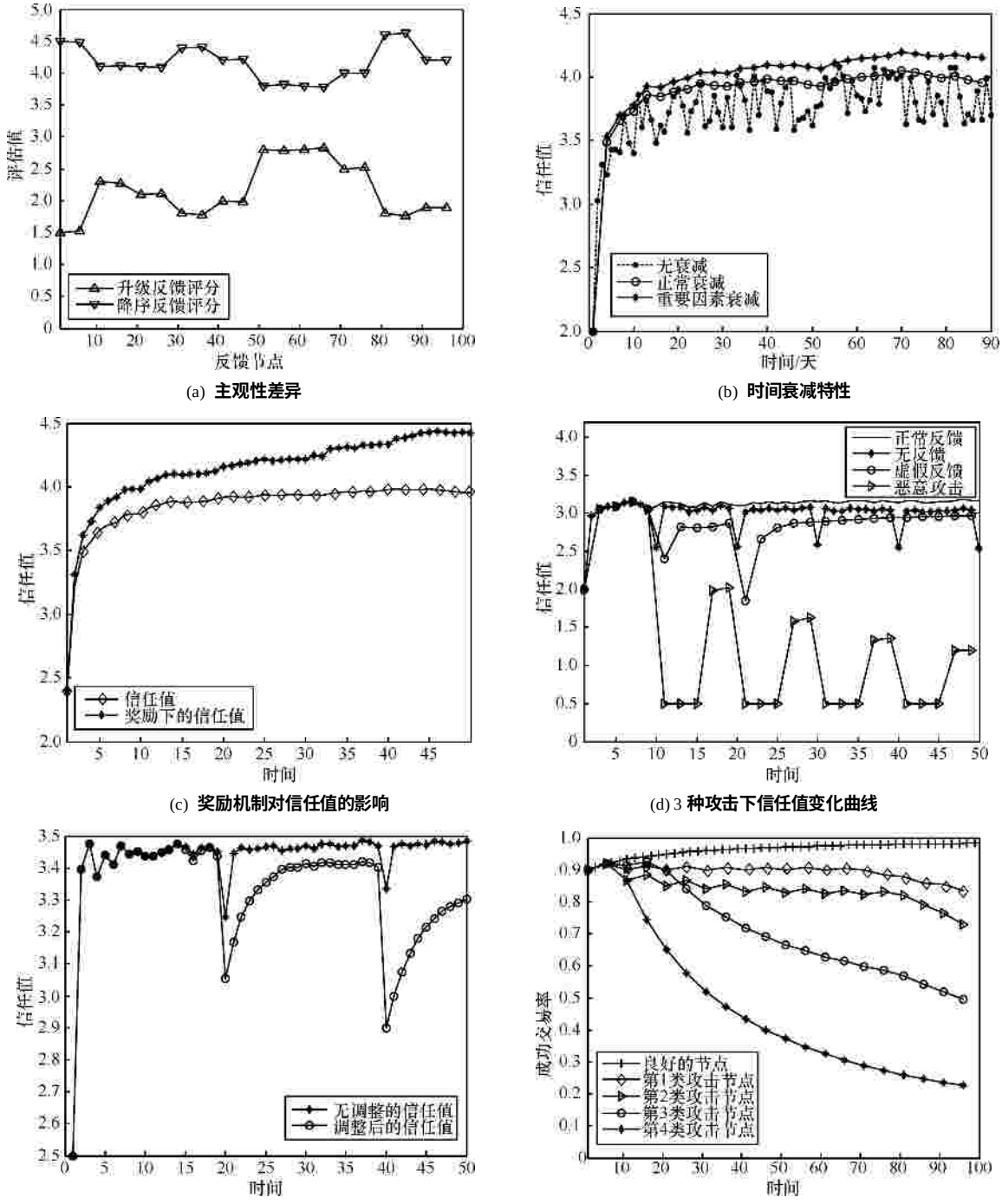
在实验中选择 100 个节点参与计算，仿真结果如图 3 所示。图 3(a)描述了不同的服务请求者(x 轴)的不同主观性引起的信任值(y 轴)的变化，需要注意的是，主观特性与反馈评分和属性权重均有关。图中给出了 4 个属性反馈评分分别为 2、3、4、5(升序)；5、4、3、2(降序)这 2 种典型情况下的信任值变化曲

线。由图可知，不同的服务请求者(对应不同的属性权重)对相同反馈评分值的信任值反映是不同的。

图 3(b)描述了本文模型的时间衰减特性。没有衰减时计算出的信任值是随机序列。当衰减系数设置为 s=1,$L(t_k)\in$[0/30,90/30]时，随着好评的增加，信任值上升并趋于稳定。当存在重要交易时且好评时，设置 s=0.1，衰减变慢，信任值适量上浮。

图 3(c)描述了奖励机制对信任值的影响，由于节点的持续好评，奖励值也逐渐增加，造成总的信任值适量上浮，上浮的最大值接近 0.5。

图 3(d)描述了不提供反馈、虚假反馈、安全事件 3 种攻击下攻击节点的信任值变化曲线。图中给出了正常反馈和这 3 种攻击下攻击节点的信任值变化对比。由图可知，不反馈的节点每隔 10 次交易



(a) 主观性差异　(b) 时间衰减特性

(c) 奖励机制对信任值的影响　(d) 3 种攻击下信任值变化曲线

(e) 策略攻击下信任值的变化　(f) 各种情况下节点成功交易率的变化

图 3　仿真实验结果

进行 1 次不反馈攻击，虽然信任值变化较小，但仍然相对正常反馈信任值的距离逐渐加大。虚假反馈的节点在第 10 次和第 20 次交易时产生攻击行为，后面提供较好的反馈，但直到第 50 次交易时信任值才恢复到第 9 次交易时的水平，说明攻击下信任值下降快但恢复起来慢。遇到安全事件时，信任值立刻降至阈值(设为 1)以下，而且必须要有一个缓冲时间(比如查杀病毒的时间)才能重新获得交易权限，但这时的信任值在初始值范围，当后续交易仍然出现恶意攻击时，其信任值会不断降低，从而参加交易的机会更少。对于策略攻击的情况，节点开始通过持续好评获得足够高的信任值，然后以 20 为周期进行恶意攻击。图 3(e)显示了该节点的信任值和经过本文算法调整后的信任值曲线。调整后的效果是攻击发生时信任值的增加是缓慢的，下降则是迅速的，每攻击一次，节点需要花费更多的努力才有可能回到原来的信任值，这与人类社会的感知模型是相符的。以上信任值变化过程反映了本文模型具有较好的惩罚机制和检测攻击的敏感性。

图 3(f)仿真出了该模型在以上 4 类攻击情况下的节点成功交易率的变化。攻击频率都按照第一类攻击节点的行为每 10 次交易攻击一次。初始状态没有攻击，所有节点都能正常参与交易，成功率为 0.9，良好节点的成功交易机会稳步上升，逐渐接近于 1。4 类恶意节点的交易成功率呈下降趋势。其中第 1 类节点信任值降低较小，交易成功率下降缓慢。第 2 类节点攻击时，由于存在纠错机制，其成功交易率呈波浪形缓慢下降，第 3 类节点使用策略攻击，惩罚效果较明显，其交易率下降较大。第 4 类节点攻击惩罚机制最严重，成功交互率下降最多。该结果证明了良好节点的成功交易率几乎不受影响，恶意的节点能够得到完全或部分的屏蔽。表明所提模型抗攻击性比较好，奖惩机制合理。

以上仿真验证了所提模型的主观性、时间衰减性、奖惩特性、敏感性和抗攻击性。灵活性和模糊性不便仿真，分析即可。传递性和可扩展性将在下面的对比仿真中一并给出。

5.2　信任模型对比分析

为了验证本文信任模型的优越性，对所提的信任模型与部分经典的信任模型进行了比较分析。首先本文所提的信任模型具有较全面的参数特性，相对于其他模型对信任的反映更全面，表 2 列出了调研的比较典型的信任模型参数分布。其中“v”表示相关的信任模型具有对应的功能参数。

其次，结合表 2 和信任模型的优势特性，对于同一种功能参数，不同的信任模型也有程度上的差异，图 4 给出了本文所提信任模型与部分经典模型在相同参数下的对比仿真效果。

表 2　本文模型和几个典型模型的参数分布比较

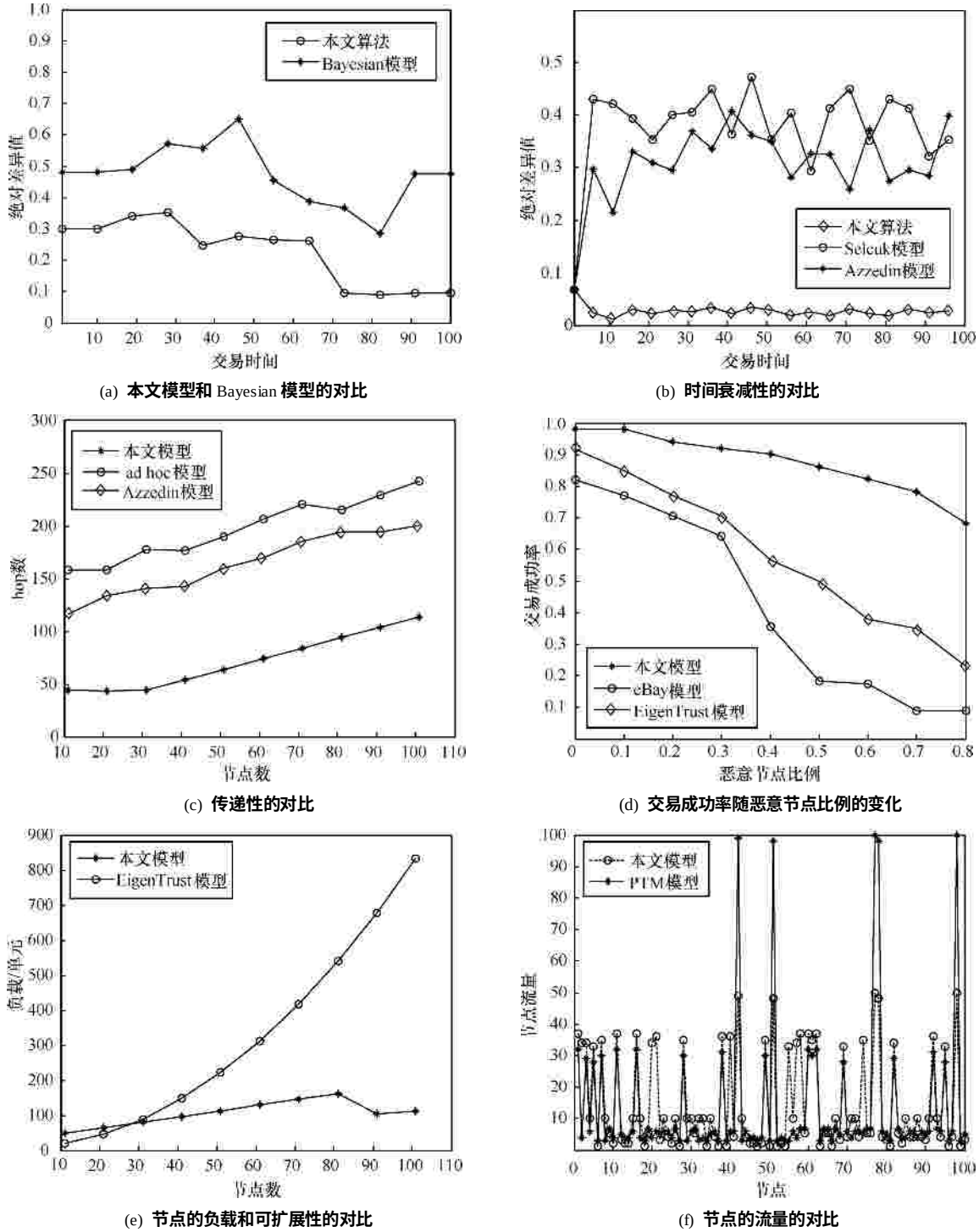
模型	参数								
	灵活性	主观性	模糊性	时衰特性	传递性	抗攻击性	奖惩机制	敏感性	可扩展性
Bayesian	v	v			v				
Selcuk	v			v		v	v	v	v
Azzedin			v	v	v				
eBay		v				v	v		
EigenTrust	v				v	v	v		v
Ad Hoc		v	v		v	v			
PTM	v		v		v			v	v
本文	v	v	v	v	v	v	v	v	v

主观性参数上经典的模型是 Bayesian 模型，在属性反馈评分均是 1、2、3、4 的情况下，用信任模型计算的信任值和真实值之间的归一化绝对差来衡量信任模型的效果，真实值代表现实交易中的信任关系，可以通过一批咨询者询问得到。图 4(a)描述了本文模型和 Bayesian 模型的对比效果，可以看出，本文模型的误差较小。

图 4(b)描述了本文模型相对于 Selcuk 模型(交易减半衰减)和 Azzedin 模型(按固定权重衰减)在时间衰减性参数上的表现，本文模型误差小而且变化平缓。

图 4(c)描述了本文模型的传递性，用一定的网络规模下源节点到目标节点的跳数来衡量，可达表示可传递，跳数少表示传递效率高。本文模型相对于多级多路径传递的 ad hoc 模型到达目标的跳数要少，传递效率较高。Azzedin 模型类似于本文的多跳机制，但由于存在不完全传递，竞争节点拒绝服务时需绕道传递，且本文模型在虚拟组内传递，故传递效率比本文模型要低。

图 4(d)从恶意节点比例和交易成功率角度反映出了本文所提信任模型相对于 eBay 模型和 EigenTrust 模型在抗攻击性上的表现。eBay 模型通过查看评分高低避免和恶意商家交易，EigenTrust 模型通过一定概率选择预置的可信节点交易来屏蔽部分恶意节点。图中 4 类恶意节点按照相同比例配置，可以看出，本文模型随着恶意节点的增加，成功交易率下降较慢。



(a) 本文模型和 Bayesian 模型的对比

(b) 时间衰减性的对比

(c) 传递性的对比

(d) 交易成功率随恶意节点比例的变化

(e) 节点的负载和可扩展性的对比

(f) 节点的流量的对比

图 4 对比实验结果

图 4(e)描述了节点的负载随着网络规模的变化。对比模型是同样采用 DHT 方式搜索和存储信任值的 EigenTrust 模型。当网络规模较小时，本文算法由于要存储额外的协议字段和信任值序列，负载相对较大。但随着网络规模的增大，EigenTrust 模型多级迭代计算推荐值，负载增加更快。当直接交互达到一定次数时，本文算法只考虑直接交互经验，虽然网络继续扩张，负载却会有一定的下降，图 4(e)也模拟示意了该种情况。

图 4(f)模拟出了节点的流量对比。横坐标表示 100 个节点，纵坐标用节点的交易请求的次数来近似表示每个节点上的流量。从图中可以看出，PTM 模型

(与本文模型类似选择最高信任值的节点参与交易)的流量集中在少数几个节点处，而本文模型的流量比较分散，本文按照相对服务能力计算信任值使多个节点都获得一定的交易机会，这样不至于造成大部分流量挤向几个服务能力强大的节点而造成网络的堵塞和拒绝服务攻击。从图 4(e)和图 4(f)可以看出，本文算法具有较低的负载，能达到负载的均衡，所以可扩展性较好。

总之，本文所提信任模型具有较完善的功能特性，具有较好的合理性和有效性，相对于其他相关模型，本文所提模型表现较为优越。

6　结束语

本文总结了目前存在的各种信任模型的优缺点，并从信任的定义和信任模型的一般功能特性出发，提取了 9 个功能参数，并提出了一种基于参数建模的信任模型，该信任模型按照信任管理的生命流程逐个实现了所提取的参数功能要求，分析和仿真结果表明所提信任模型是合理和有效的，相对于其他相关模型表现较为优越，该模型在分布式场景下具有一定的通用性。下一步工作一方面是进一步细化分类信任的功能特性，使之理论上更符合人类社会网络特征，并在具体的分布式场景加以改进应用。另一方面提取信任模型评估参数，利用该通用模型对现存模型进行对比评估，以解决服务模型的相对最优化选择问题。

参考文献：

[1] CHANG K D, CHEN J L. A survey of trust management in WSNs, Internet of things and future internet[J]. KSII Transactions on Internet and Information Systems, 2012, 6(1): 5-23.

[2] BLAZE M, FEIGENBAUM J, LACY J. Decentralized trust management[A]. Proceedings of the 17th Symposium on Security and Privacy[C]. IEEE Computer Society Press, Oakland, 1996. 164-173.

[3] KAMVAR S D, SCHLOSSER M T, GARCIA-MOLINA H. The eigentrust algorithm for reputation management in P2P networks[A]. Proceedings of the 12th International Conference on World Wide Web, ACM[C]. Press New York, NY, USA, 2003. 640-651.

[4] SUN Y, YU W, HAN Z, LIU K J R. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. IEEE Journal on Selected Areas in Communications, Selected Areas in Communications, 2006, 24(2): 305-319.

[5] ALMENAREZ F, MARIN A, CAMPO C, *et al*. A pervasive trust management model for dynamic open environments[A]. Proceedings of the First Workshop on Pervasive Security and Trust　MobiQuitous[C]. 2004.

[6] RESNICK P, ZECKHAUSER R. Trust among strangers in internet transactions: empirical analysis of ebay's reputation system[A]. The Economics of the Internet and E-Commerce Advanced in Applied Microeconomics[C]. 2002. 127-157.

[7] GAO Y, ZHAN J. A layered trust model based on behavior in service grid[A]. 2nd International Conference on Advanced Computer Control (ICACC)[C]. Shenyang, China, 2010. 511-515.

[8] SELCUK A, UZUN E, PARIENTE M. A reputation-based trust management system for P2P networks[J]. International Journal of Network Security, 2008, 6(3):235-245.

[9] WANG Y, VASSILEVA J. Bayesian network-based trust model in peer-to-peer networks[A]. Proceedings of IEEE/WIC International Conference on Web Intelligence[C]. Halifax, Canada, IEEE, 2　3.372-378.

[10] AARTHI N, VIJAY V. Dynamic trust enhanced security model for trusted platform based services[J]. Future Generation Computer Systems, 2011, 27(5): 564-573.

[11] AZZEDIN F, MAHESWARAN M. Evolving and managing trust in grid computing systems[A]. IEEE Canadian Conference on Electrical and Computer Engineering(CCECE'02)[C]. 2002. 1424-1429.

[12] AYMAN T, AYMAN K, ALI C, *et al*. Fuzzy reputation-based trust model[J]. Applied Soft Computing, 2011, 11(1): 345-355.

[13] MURALIDHARAN S P, KUMAR V V. A novel reputation management system for volunteer clouds[A]. 2012 International Conference on Computer Communication and Informatics (ICCCI)[C]. Coimbatore, 2012. 1-5.

[14] 谷利泽，郑世慧，杨义先.现代密码学教程[M].北京:北京邮电大学出版社,2009.
GU L Z, ZHENG S H, YANG Y X. Modern Cryptography Tutorial[M]. Beijing: Beijing University of Posts and Teleco　munications Press, 2009.

[15] LI X, ZHOU F, YANG X. A multi-dimensional trust evaluation model for large-scale P2P computing [J]. Journal of Parallel and Distr　uted Computing, 2011, 71(6): 837-847.

作者简介：

汪京培（1983-），男，湖北咸宁人，北京邮电大学博士生，主要研究方向为网络安全和信任管理。

孙斌（1967-），女，山东龙口人，北京邮电大学副教授，主要研究方向为计算机网络与网络安全。

钮心忻（1963-），女，浙江湖州人，博士，北京邮电大学教授、博士生导师，主要研究方向为信息安全、信息隐藏与数字水印技术、数字内容安全、软件无线电等。

杨义先（1961-），男，四川盐亭人，博士，北京邮电大学教授、博士生导师，主要研究方向为信息安全、网络安全、编码密码学、数字信号处理、视经网络等。