

# 一种具有分类决策属性的信任模型

李 坤, 姜 浩

(东南大学 计算机科学与工程学院, 江苏 南京 211189)

**摘 要:**如何安全、有效地选择信任度满足要求的服务提供者是目前信任研究领域的热点问题。文中提出了一种多属性决策的层次化信任模型,将决策属性分为定量属性和定性属性,有利于属性的分类度量、属性的系统化分析和信任等级的设定,同时给出了对具有不同信任等级的属性进行融合的方法。用置信区间来表示定性属性,可以很好地表达主观不确定性和风险意识。利用推荐者的推荐信息可以快速建立实体间的信任关系,针对网络中存在的恶意实体的推荐,列举了检验推荐信息可信度的方法并分析了各自的优缺点。介绍了几种典型的信任模型并提出了建立信任模型的关键。

**关键词:**信任模型;属性分类;推荐信任

**中图分类号:**TP393.0

**文献标识码:**A

**文章编号:**1673-629X(2010)03-0036-04

## A Trust Model with Classified Decision Attributes

LI Kun, JIANG Hao

(School of Computer Science & Engineering, Southeast University, Nanjing 211189, China)

**Abstract:**Currently, it is a hot issue in trust research area of how to select the trust-satisfied service providers safely and effectively. A hierarchical trust model was provided through dividing decision attributes into quantitative attributes and qualitative attributes. This was beneficial to the classified measurements of the attributes, systematic analysis of the attributes and the setting of the decision levels. Then, the method of combining different trust levels was explained. Using confidence interval to indicate qualitative attributes could express subjective uncertainty and risk consciousness better. The trust relationships between entities could be established quickly by using the recommendations from recommenders. For the existing malicious recommendations, inspecting methods were listed accompanying with the respective advantages and disadvantages. At last, several typical trust models were introduced and the key issues of how to establish trust models were proposed.

**Key words:**trust model; attributes classification; recommended trust

## 0 引 言

网络的大规模普及和新型业务的不断涌现,已经无人怀疑它无处不在的影响力。网络是一个虚拟的世界,人们探索了许多种不同的模式和工具进行信息的流通和资源的共享。实际上,网络行为的交互过程也都是现实生活的模拟,所以也同样需要相应的机制和手段来约束网络行为及其参与的实体。今日互联网的规模和复杂程度同设计之初相比有着天壤之别,如何构建一个安全、可信的网络环境,使得互联网向完美再迈进一步,已经成为研究人员和行业开发者共同努力的方向。

信任是个古老的概念,社会学、心理学、自然科学

都有相关的研究,它能让一个不确定的环境通过信息的交换演变成一个相对稳定的、广泛的信息网络。与信任相关联的另一个词是信誉。信任主要来自于相互交往的经历和相应的制度,而信誉既是信任长时间的累积,又是信任的一个重要来源。“我信任你是因为你有良好的信誉”这句话可以很好地表达两者的差异。在计算机科学领域,这两个概念被模糊化了,文中不加以区分,统一称之为信任,并采用 Tyrone Grandison 和 Morris Sloman 在文献[1]中对信任的定义:在指定的环境中,对一个实体能够可信地、安全地、可靠地实施行为的一种坚定的信念(假设可信性包含了可靠性和时效性)。

将信任的理念融合到网络的应用当中,可以帮助实体建立起对其它实体的信心,从而创造一个稳定的环境以推动虚拟状态下事物的交互,同时降低与之相关的风险。信任信息的维护过程可以分为信任信息输入、信任信息处理和信任等级或策略输出三个部分<sup>[2]</sup>。

收稿日期:2009-06-05;修回日期:2009-10-17

作者简介:李 坤(1984-),女,山东日照人,硕士研究生,CCF 会员,研究方向为信任管理;姜 浩,副教授,研究方向为工作流应用研究。

文中提出了一种利用多属性进行决策的信任模型,并将属性划分为定量属性和定性属性两种类别,综合体现了信任的主客观结合性、动态性、衰减性以及多样性的特点。

1 模型描述

1.1 信任分层结构

在一个分布式的网络环境中,假设一个实体可以扮演的角色有三种:服务提供者、服务请求者和推荐者。简单起见,假设某一时刻,一个实体只能扮演一种角色。本例中,将实体的服务提供能力作为信任的度量标准,并从实体的性能、安全、可靠性三个方面评估实体信任值。可以根据具体的网络环境增减属性的个数。采用文献[3]的分层方法,方便逐个分析,同时,下层的每个属性改变,不会影响到整体的分析架构。如图1所示。

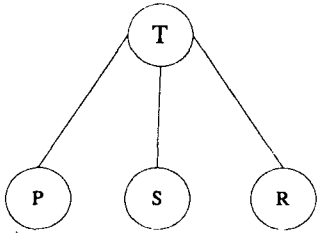


图1 信任的层次关系

本例中选取实体的“性能”(P)、“安全”(S)、“可靠性”(R)作为计算“综合信任值”(T)的三个属性。每一个属性可以分为不同的等级,如表1所示。其中,前一个等级优于后一个等级。例如在“性能”方面位于 $P_1$ 级比位于 $P_2$ 级“性能”要好。

表1 “综合信任值”及各属性分级列表

T	T <sub>1</sub>		T <sub>2</sub>		T <sub>3</sub>
P	P <sub>1</sub>	P <sub>2</sub>	P <sub>3</sub>	P <sub>4</sub>	
S	S <sub>1</sub>	S <sub>2</sub>	S <sub>3</sub>		
R	R <sub>1</sub>	R <sub>2</sub>	R <sub>3</sub>		

服务提供者的不同属性都可能影响一个服务请求者作最后的决策。在这些属性中,有些对“综合信任值”的贡献较大,有些也许没有影响。所以如何筛选出对某个特定网络影响比较大的因素,需要对用户及网络的行为进行事先分析。同时,不同的属性可能有不同的评价等级,例如本例中将“性能”分为4级,“安全”分为3级。并且有些属性是可以严格量化的,也就是定量属性,能用具体的测量数字表示出来,有些属性则只能进行定性分析。如果以下载速度来衡量“性能”属性的话,可以用具体的数字来区分不同的等级。但是实体的“安全”和“可靠性”则要靠用户的感知来分级。如上表,将“综合信任值”(T)、“安全”(S)、“可靠性”(R)分

为三个等级{高,中,低},将“性能”(P)分为四个等级{5M/s,1M/s,500kB/s,100kB/s,50kB/s}。

1.2 信任值的更新

网络中的每个实体都会为其它实体维护一张诸如表1那样的信任列表。当服务提供者完成服务请求者所请求的服务后,服务请求者根据其表现对服务提供者进行各个属性的评价。

1) “性能”属性(定量属性):

设服务请求者所接受服务的平均下载速度为 $P_i$ ,服务请求者对服务提供者的本次服务“性能”属性的评价为 $P'_i(i = 1, 2, 3, 4)$ ,即四个等级的数值,计算方法如下:

a) 若 $P_i \geq P_1$ ,则 $P'_1 = 1, P'_2, P'_3, P'_4 = 0$ ;

b) 若 $P_{n+1} < P_i \leq P_n (n = 1, 2, 3)$ ,那么 $P_i$ 对各个等级的贡献为:

$$P'_n = \frac{P_n - P_i}{P_n - P_{n+1}}, P'_{n+1} = \frac{P_i - P_{n+1}}{P_n - P_{n+1}}, \text{其它等级为}$$

0;

c) 若 $P_i < P_4$ ,则 $P'_4 = 1$ ,其它等级为0;

且以上各式满足:  $\sum_{n=1}^4 P'_n = 1$ 。

2) “安全”、“可靠性”属性(定性属性):

由于定性的属性靠服务请求者的感知来进行对各个等级的分配,可以选用置信区间来表达服务请求者这种不确定的主观决策。例如“安全”表达如下:  $\{(S'_n : 0.2), (S'_{n+1} : 0.6)\}$  且  $\sum_{n=1}^3 S'_n \leq 1$ 。代表服务请求者感觉在“安全”属性方面很难用确切的“高”、“中”、“低”来严格描述。那么就给 $S_n$ 等级分配0.2的概率, $S_{n+1}$ 分配0.6的概率。注意到 $0.2 + 0.6 < 1$ ,其中的差值代表了服务请求者主观上的不确定度,从另一方面也反映了服务请求者的风险意识[3]。

通过以上方法,对各个属性进行评价完毕后,可以得到这单独一次交互的评价值,如表2所示。

表2 一次交互后各属性评价值

P	P' <sub>1</sub>	P' <sub>2</sub>	P' <sub>3</sub>	P' <sub>4</sub>
S	S' <sub>1</sub>	S' <sub>2</sub>	S' <sub>3</sub>	
R	R' <sub>1</sub>	R' <sub>2</sub>	R' <sub>3</sub>	

1.3 信息的集成

对各个属性计算完毕之后,要进行信息的集成,以便确定本次交互的“综合信任值”(T)。通过建立权重矩阵来表示各属性的各个等级对“综合信任值”(T)的各个等级的贡献。如“性能”(P)属性各等级对“综合信任值”(T)的各等级的贡献大小可以表示为(注意在矩阵每项值的确定过程中只考虑P对T的影响,并不考虑S,R的影响):

$$T_p = \begin{bmatrix} T_{p1(\text{old})} \\ T_{p2(\text{old})} \\ T_{p3(\text{old})} \end{bmatrix} + \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix} \times \begin{bmatrix} P'_1 \\ P'_2 \\ P'_3 \\ P'_4 \end{bmatrix} \quad (1)$$

同理可建立  $T$  和  $S$ 、 $R$  的等价关系式(2)、(3):

$$T_S = \begin{bmatrix} T_{s1(\text{old})} \\ T_{s2(\text{old})} \\ T_{s3(\text{old})} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix} \times \begin{bmatrix} S'_1 \\ S'_2 \\ S'_3 \\ S'_4 \end{bmatrix} \quad (2)$$

$$T_R = \begin{bmatrix} T_{R1(\text{old})} \\ T_{R2(\text{old})} \\ T_{R3(\text{old})} \end{bmatrix} + \begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{bmatrix} \times \begin{bmatrix} R'_1 \\ R'_2 \\ R'_3 \\ R'_4 \end{bmatrix} \quad (3)$$

其中等式右边的常数项为表 1 中各项旧的历史记录,也就是此次交互发生之前的值。矩阵的系数为表 2 中的值。由于现实生活中,很多情形是可以忽略的,比如可以定义“性能”(P)很差( $P_4 = 1$ )对“综合信任值” $T_1$ 等级的贡献为 0,那么  $a_{34} = 0$ 。上述矩阵通常为稀疏矩阵,可以简化存储空间。

最后,权衡每个属性对“综合信任值”的影响,可以得到最后“综合信任值”(T)各个等级的数值:  $T = \omega_p \cdot T_p + \omega_s \cdot T_s + \omega_R \cdot T_R$ 。其中  $\omega_p, \omega_s, \omega_R$  为三个实数,分别为属性 P, S, R 的权重。计算完毕后,进行归一化处理,使得  $\sum_{n=1}^3 T_n = 1$ 。

将“综合信任值”分为不同的等级可以让服务请求者对服务提供者有更多不同类型的选择。通过调节  $\omega_p, \omega_s, \omega_R$  的值,体现了服务请求者对各个属性的不同的重视程度。假如不要求可靠性保证,则  $\omega_R = 0$ 。如果服务是按照“综合信任值”也就是提供服务能力收费的话,那么服务请求者可能会选择  $T_2$  值最高的实体,以减少成本,获得折中的服务。甚至可以同时在全网范围内设立对“综合信任值”进行统一的权重:  $\{v_1, v_2, v_3\}$ , 则实体的“综合信任值”就可以用一个具体的数值来表示:

$$|T| = v_1 \cdot T_1 + v_2 \cdot T_2 + v_3 \cdot T_3。$$

## 2 模型改进

### 2.1 信任的衰减

旧的交互记录并不总和现在的信任值相关,因为实体会随着时间改变它的行为。所以一个能体现时间上动态性的方法就是:相对于最近的交互记录,对历史久远的记录赋予较小的权重。信任有随时间衰减的性

质,类似于人有遗忘的特性。假如没有了这个特性,那么一旦建立起稳定的信任值后,最近的信任记录就很难影响到信任值的改变。带来的后果可能是实体依赖于历史的高信任值作背景,进行最近几次的规模较大的欺骗行为<sup>[4]</sup>。

本模型中,定义一个衰减因子向量  $\lambda = \{\lambda_1, \lambda_2, \lambda_3\}$ , 并且定义每隔一个时间段  $K$  对“综合信任值”进行衰减操作。则在一个新的时间段里,服务请求者接受完服务提供者的第一次服务后,“综合信任值”的各个等级更新为:  $T_{n(\text{old})}\lambda_n + T'_n, n=1,2,3$ 。最后进行归一化处理,使得和为 1。

这样做的好处有:

1) 信任值越高,衰减的越快:说明信任值越高建立起来越困难,需要更多诚实可靠的服务来维持。但是一次失败会对信任值产生很大影响,是对失败服务的惩罚。

2) 如果实体很长时间没有进行交互活动了,那么它的“综合信任值”会趋向于最低信任等级:  $T_3 \rightarrow 1$ 。那么这个实体会逐渐被淘汰,类似于加入了黑名单。

### 2.2 推荐信任值

由于客观世界的模糊性、不确定性和人们认识上的局限性,当请求服务的实体对服务提供者的信息掌握得不够完整,不能准确地判断服务提供者是否诚实可信,或者服务请求者是一个刚刚进入网络的新实体,这时候推荐者的推荐信息是一个快速建立信任关系的有效方法。

推荐信息的来源有与自己交互过的熟悉的实体,也有来自陌生实体的推荐。有信任值高的实体的推荐也有信任值低的实体的推荐。推荐信息的质量参差不齐,虚假的推荐信息可能会使整个网络建立错误的信任关系,让网络存在很多潜在的风险。通过增加文献[5]提及的以下两种主要错误推荐信息的鉴别,来进行模型的改进。

(1) 网络中存在一种恶意推荐者,为了利益,所发出的推荐信息总是对其它实体的诋毁;

(2) 实体之间的合谋:对合谋组内的实体给予好的评价,相互提升信任度,而对组外的实体进行恶意评价。

对推荐信息进行鉴定主要采用两种方法:

1) 建立分离的两个系统:分别对某个实体的提供服务能力进行评价和对由该实体发出的推荐信息的可信度进行评价。

2) 在一个系统中通过隐式的计算得出推荐信息的可信度:人们可能会很自然地想到,实体的“综合信任值”越高,其推荐信息就越可信。相反,“综合信任

值”越低,实体就越可能会撒谎。虽然说服务和推荐是两个分离的变量,推荐的好,不一定服务的质量就好。但是实际表明后一种情况往往成立,前一种却不然。原因是在一个网络环境中,存在很多实体,它们或是相互诽谤、诋毁,或是相互串谋,通过损害竞争对手的信任值来提升自己的相对信任值。

如果缺乏相应的检测方法,实体就没有了约束和动力去提供真实可靠的服务和推荐。

信任的生成算法主要涉及以下几个问题:

(1)信任的表述和度量;

(2)由经验推荐所引起的信任度推导和综合计算<sup>[6]</sup>。

PeerTrust 模型<sup>[7]</sup>提供了一个很好的方法来计算推荐信任度,但它计算复杂度偏大,只适用于小型网络,在大型网络中,计算的效率和成本都是一个问题。它的主要思想是:假如实体 A 要判断实体 B 的推荐信息是否可信,则可以通过比较实体 A 和实体 B 对共同交互过的实体的评价记录(评价相似性),来判断实体 B 诚实与否,当然前提是实体 A 认为自己的评价是客观正确的。

在本模型中,引用 PeerTrust 的思想进行相似性的计算,某实体请求网络中的其它实体对其目标实体进行推荐。那么只通过推荐者的推荐信息计算出来的“综合信任值”为:

$$T_r = \sum_{i=1}^N T_{p(i)} \frac{\text{sim}(r, p(i))}{\sum_{j=1}^N \text{sim}(r, p(j))} \quad (4)$$

其中,  $N$  为推荐者的总数,  $r$  代表请求推荐者,  $p(i)$  代表第  $i$  个推荐者,  $\text{sim}(r, p(i))$  表示请求推荐者和第  $i$  个推荐者的相似度,选用均方差的大小作为评判标准。  $T_{p(i)}$  表示第  $i$  个推荐者计算的关于目标实体  $d$  的“综合信任值”。

相似度的计算公式为:

$$\text{sim}(r, p(i)) = 1 - \sqrt{\frac{\sum_{x \in I(r, p(i))} \sum_{n=1}^3 (T_n(r, x) - T_n(p(i), x))^2}{|I(r, p(i))|}} \quad (5)$$

其中  $I(r, p(i))$  为请求推荐者  $r$  和第  $i$  个推荐者  $p(i)$  共同交互过的实体集,  $|I(r, p(i))|$  为集合中实体的个数,  $T_n(r, x)$  为请求推荐者  $r$  对实体  $x$  的“综合信任值”第  $n$  个等级的评价数值,本例中,已经假设了“综合信任值”分为 3 个等级,所以  $n=1, 2, 3$ 。

同时,可以利用相似度的原理检测网络中的欺骗实体。因为对于恶意欺骗者,请求推荐者  $r$  和第  $i$  个推荐者  $p(i)$  对于共同交互过的那些“综合信任值”高的实体的评价差异会很大。这种欺骗者总会给其它实体恶意的评价。

### 3 信任模型的相关研究与总结

1994 年 Marsh Stephen<sup>[8]</sup>从信任的概念出发,结合信任的主观性提出了信任度量的模型。自此以后,伴随着网络新型应用的出现,信任扮演着越来越重要的角色。许多研究机构和学者对信任模型进行了相关的探索研究。Audun Jøsang<sup>[9]</sup>基于信任度模型和主观逻辑,把信任抽象为二元事件的概率分布,其先验概率分布可用 Beta 密度函数表示,将信任值归结为后验概率分布的表达,并定义了信任的结合、折扣、遗忘等操作; PeerTrust 模型的信任计算综合了反馈内容反馈数量,反馈源可信度,事务上下文,社群环境五个信任变量,并同时分析了模型在 P2P 环境中抵抗特定攻击的能力;基于 Bayesian 模型的信任机制其理论基础是贝叶斯准则,利用大量的统计数据作为条件概率,推断在特定条件下实体信任的概率;此外还有 Ben - Jye Chang 在分布式移动 Ad Hoc 网络中基于马尔科夫链<sup>[10]</sup>的模型,将信任值作为状态,定义引起状态改变的事件类型,节点经过一系列的事件后,状态变迁符合非周期的时间连续的马尔科夫链的性质,并由此推断下一个状态,也就是下一个信任值。这些模型,从不同的网络环境和不同的网络应用出发,体现了信任在如今互联网中发挥的重大作用。

基础信息的采集是建立模型的基础,包括现在互联网用户行为的研究<sup>[11]</sup>。不论一个模型理论上有多么高效,假如变量设置的不合理,模型属性的选取、等级的设定、权值的定义不当,就会影响整个网络信任模型的操作。定义这些变量,关键在于对网络行为和用户行为信息的采集、分析和模式的提取。此外,设计一个模型的时候,还要考虑服务请求频度、服务动态频度(资源的稳定性)、社群动态频度等,反映了系统的繁忙、稳定程度<sup>[12]</sup>。这需要各学科的协同合作,加强基础理论的研究,对模型进行形式化分析,增加其实际的应用价值。

#### 参考文献:

- [1] Grandison T, Sloman M. A Survey of Trust in Internet Applications[J]. IEEE Communications Surveys & Tutorials, 2000, 3(4): 2-16.
- [2] 林 闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005, 28(5): 751-758.
- [3] 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.
- [4] 王晓玉, 晁钢令. 信任-风险关系研究的梳理与评价[J].

(下转第 43 页)

内部、外部信息分析,及时的向流程层提供客户关系管理方案和协作信息。流程层将做出的联合决策和企业间的业务流程及时传递给分析层,分析层更新信息,并将信息传递给企业内部各个子系统,执行流程层做出的联合决策和企业生产计划。分析层主要集成的子系统包括:供应链管理(SCM);客户关系管理(CRM);供应商管理(SRM);产品生命周期管理(PLM);员工周期管理(ELM)——集成一个员工从被雇佣到被解雇期间的所有相关信息;企业绩效管理(CPM)——提供一个基于整个供应链全局的绩效管理评价;财务管理(FM);工作流管理(WM);决策支持系统(DSS)。

●电子商务层:电子商务层主要包括四个部分:

\* B2C: B2C 的交易是指商业销售或者与企业或个人客户的电子媒介,通常是因特网。这确实需要一个广泛的基础设施,主要是在线订购设施和状态查询设施。

\* B2B: 企业对企业的电子商务,除了在线交易和产品展示, B2B 的业务更重要的意义在于,将企业内部网,通过 B2B 网站与客户紧密结合起来,通过网络的快速反应,为客户提供更好的服务,从而促进企业的业务发展。

\* B2E: 企业内部互联网为员工提供升级更新和进入企业网的个人入口。通过内部互联网,加强企业间员工的信息交流,组织文化建设共享,知识共享,协同合作等。

\* EAI: 提供一个平台,集成供应链上企业或者供应链外部企业。EAI 基于各种不同平台、用不同方案建立的异构应用集成在一起,通过建立底层结构,来联系横贯整个企业的异构系统、应用、数据源等,完成在企业内部的 ERP、CRM、SCM、数据库、数据仓库,以及其他重要的内部系统之间无缝地共享和交换数据的需要。

### 3 结束语

在经济全球化的商业环境下,市场上的竞争已经由单一企业之间的竞争逐步转化为由多个企业组成的供应链之间的竞争。文中基于新的市场需求分析,设计了企业间 ERP 的概念框架,对于解决供应链上成员之间的流程链集成和信息共享问题有重要意义。由于企业间 ERP 系统可以充分利用企业中在功能方面已经十分成熟的信息系统,不需要进行过多的业务流程重组,因此降低了实施成本,缩短了实施周期。文中所提及的企业间 ERP 系统模型只是企业间 ERP 系统研究的第一步,还需要对当前的研究加以延伸并对该系统的局限性进行讨论。

#### 参考文献:

- [1] McCaughey R E. Enterprise Resource Planning(ERP): Past, Present and Future[J]. International Journal of Enterprise Information Systems, 2007, 3(3): 23-35.
- [2] 孙长俊,周晓峰. 基于 Web Services 的企业应用集成模型[J]. 计算机技术与发展, 2006, 16(5): 209-210.
- [3] Christopher M. Logistics and Supply Chain Management - Strategies for Reducing Costs and Improving Services[M]. London: Pitman Publishing, 1998.
- [4] 余名高,贾秀峰,林坤江,等. 基于 Web 服务的企业应用集成[J]. 计算机技术与发展, 2007, 17(5): 55-58.
- [5] 罗 涛. ERP 原理设计实施[M]. 北京: 电子工业出版社, 2002.
- [6] 韦峻峰. 跨越异构平台[J]. 中国计算机用户, 2007(21): 54-55.
- [7] 姜 婷. 企业信息化中的新技术应用[J]. 安徽科技, 2002(12): 26-27.
- [8] Moller C. ERP II: a conceptual framework for next-generation enterprise systems[J]. Journal of Enterprise Information Management, 2005, 18(4): 483-497.

(上接第 39 页)

上海管理科学, 2008(1): 36-40.

- [5] Resnick P, Zeckhauser R. Reputation Systems[J]. Communication of ACM, 2000, 43(12): 45-48.
- [6] 郭 晶, 吴国新. P2P 网络环境下信任模型的研究与实现[J]. 计算机技术与发展, 2009, 19(3): 102-105.
- [7] Xiong L, Liu L. PeerTrust: Supporting Reputation-based Trust in Peer-to-Peer Communities[J]. IEEE Transactions on Data and Knowledge Engineering, Special Issue on Peer-to-Peer Based Data Management, 2004, 16(7): 843-857.
- [8] Marsh S P. Formalising Trust as a Computational Concept[D]. UK. University of Stirling, 1994.
- [9] Joang A. A Subjective Metric of Authentication[C]//In:

Quisquater, J. Proceedings of the ESORICS'98. Louvain-la-Neuve.: Springer Verlag, 1998: 329-344.

- [10] Chang Ben-Jye, Kuo Szu-Liang, Liang Ying-Hsin, et al. Markov Chain-based Trust Model for Analyzing Trust Value in Distributed Multicasting Mobile Ad Hoc Networks[C]//IEEE Asia-Pacific Services Computing Conference. [s.l.]: [s.n.], 2008: 156-161.
- [11] 冀铁果, 田立勤. 可信网络中一种基于 AHP 的用户行为评估方法[J]. 计算机工程与应用, 2007, 43(19): 123-126.
- [12] 李小勇, 桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报, 2009, 32(3): 405-416.