基于可信建模过程的信任模型评估算法

摘 要：目前缺少有效的评估方法对已存的信任模型进行分析和评估。为解决该问题，提出了一种新的基于可信建模过程的信任模型评估算法。将信任模型按照信任生命周期分解成信任产生、信任建模、信任计算、信任决策和信任传递五部分，对每个过程进行可信性分析，并用模糊理论量化评估值，用贝叶斯融合形成综合的评估结果。最后以分布式 WSN 信任模型为例，对所提算法进行了验证，同时给出了算法的有效性仿真，分析和实验结果表明所提算法是有效可行的。评估的结果为新的信任模型的提出提供了参考，也为实际应用中信任模型的最优化选择提供了理论依据。

关键词：信任；信任模型；模型评估；可信建模；模糊理论

中图分类号：TP311

A trust model evaluation algorithm based on trusted modeling process

Abstract: There are rare effective evaluation methods existed for analyzing and assessing the varied trust models. To solve this issue, a new trust model evaluation algorithm based on trusted modeling process was proposed. First, the evaluated trust model was divided into five trusted processes, including trust establishing, trust modeling, trust computing, trust decision-making and trust transmitting, according to trust lifecycle. Then each process is analyzed for reliability, simultaneously the fuzzy theory and Bayesian method were used for assessment and fuse to achieve the comprehensive quantitative evaluated results. Finally, the proposed method was validated in the form of example- the evaluation of distributed WSN trust models, and related simulations were performed. The analysis and simulation results show that the proposed algorithm is feasible and effective. The evaluated result provides a reference for the development of new trust models; also it laid a theoretical foundation for the optimal selection of trust models in the practical application.

Key words: trust; trust model; model evaluation; trusted modeling; fuzzy theory

1 引言

分布式网络的安全问题是近几年的研究热点[1]，信任管理技术作为“软安全”技术，相对传统的访问控制技术具有更好的灵活性和可扩展性。目前对信任管理研究的关键是在网络中建立可靠的信任模型。但是迄今为止尚没有关于信任的统一定义，作为信任关系的载体，信任模型的建立、度量和更新也缺乏可信的标准[2]。尽管如此，目前仍然可以从两个方面来向标准靠拢，一是根据不同的分布式网络安全需求建立相对标准的信任模型；二是针对不同的服务在已存在的信任模型中选择最优化的模型。而建立标准化模型的一个目的也是比较评估和指导改进不同的信任模型，所以不管是建立新模型还是优化选择已存在的模型，都涉及信任模型的评估，这正是本文的选题所在。

目前各种分布式场景下出现了大量的信任模型，如 P2P 的信任模型[3-4]、网格信任模型[5]、Ad hoc 信任模型[6]、WSN(Wireless Sensor Network)信任模型[7-10]和其他模型等。信任模型的进一步发展是基于分析和评估以往的模型的性能基础上的，同时需要评估标准的指导。然而目前对信任模型的评估的研究非常有限。Yang 等人借鉴软件工程开发的方法，为信任模型的评估建立了一个黑盒模型[11]。将信任模型当做一个黑盒子，比较模型的输入和输出，来评估模型的性能。这个评估系统存在的问题是衡量指标少，比较笼统。Wojcik 等人提出一组信任模型评估标准[12]，按照信任建立的过程分成四类：信任的表示、初始化信任值、更新信任值、信任的评估过程，每类有若干个影响因子。然而这些评估标准只是一个框架，没有具体的内容和系统。Karen 等人提出了一个代理推荐信任(ART)测试平台[13]。在该平台的实验场景中，研究者可以设置若干个实体，根据自身所用算法，参与评估交易，在一个时间段内观察参与实体的交易量和信任值的变化。然而本文只是一个实验平台，并没有做模型的比较。Schlosser 用仿真的方法对信誉系统进行评估和比较[14]。文中定义了一个形式化模型来规范不同模型的信誉值计算，给出的节点的分类和各个模型下各种节点的仿真曲线图。但是文中没有给出参数设置的依据和评估的标准，仅仅是仿真实验，缺乏理论分析，而且也只考虑了信誉系统的情况。文献[15]考虑了 WSN 融合到物联网中的情况，设定了一个场景：两个跨域陌生节点的信任建立和交互的情况，评估了各种 WSN 信任模型的性能和适用性，然而该评估方法还停留在分析阶段，没有具体的评估算法。总之，从国内外研究情况来看，信任模型的评估仍然是一个开放未解决的课题。

本文在充分调研信任模型的情况下，对信任模型的生命周期进行了分析和分解，将信任模型分解成信任产生、信任建模、信任计算、信任决策和信任传递五个部分来分析。对每部分进行分析和评估，综合出模型的评估结果。在分析过程中，从可信评估和量化评估两个方面考虑了模型的有效性和合理性，利用模糊理论和贝叶斯理论融合出量化结果。该评估结果为特定应用下的信任模型的最优化选择提供了可行的方法，也为信任和信任模型的标准化提出了一种思路。

本文的章节安排如下，第 2 节描述了信任模型的可信建模过程和评估指标，第 3 节给出了基于建模过程的可信性评估方法，第 4 节提出了一种量化评估的新算法。第 5 节给出了评估结果和系统实现，第 6 节给出了分布式 WSN 信任模型评估实例和仿真分析，最后一节总结了全文。

2 信任模型的可信建模过程和评估指标

2.1 信任的定义和信任建模过程

信任的概念来自于人类社会，计算机专家将之引入到网络安全中。目前一般认为信任是主体对客体特定行为的主观预期。信任在信任管理和模型中的表现主要是信任作为一种度量来控制访问用户的权限和刻画用户的信任程度来获取相应的服务机会。从分布式网络应用(WSN)来看，信任的作用主要体现在确定合作对象的不确定性；灵活性比较好，能够处理多变的网络和个性化的安全需求；信任关系能够异构跨域传递；与其它安全方式的兼容性[16]。实际上，在信任管理的提出之初，就认为网络安全需要附加可信的第三方来维持，信任机制就是可信的第三方机制。基于上述说明，我们给出分布式网络场景下的信任管理的定义：

定义 1：信任是考察的节点的身份和行为符合预期的一种概率度量。

定义 2：信任管理是一种第三方的服务机制，基于服务对象的信任状态来自组织一组合作对象，来完成一个决策服务。

信任管理的形式化定义为 $T=\{X, T_X, T_{tar}, T_{con}\}$，其作用是基于节点或子网络集合 X 的信任状态 T_X，自组织一组对象 $X_S \subset X$，在网络上下文控制 T_{con}(如能量、效率等)下，完成一个决策目标 T_{tar}(如数据感知、路由传递等)。

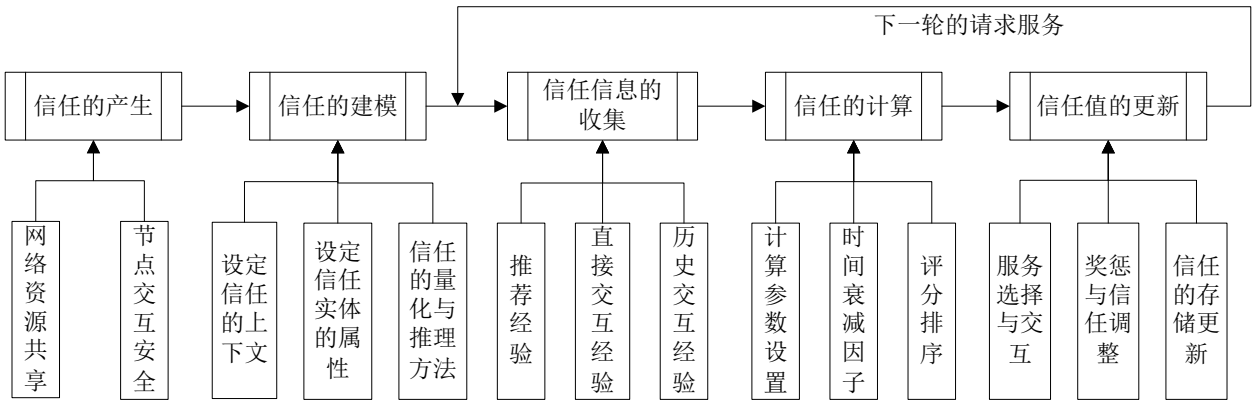


图 1 基于信任度的信任管理的建立过程

根据文献[3-10]特别是文献[4]的分析，可以提取出一个典型的基于信任度的不同场景下的信任管理系统的建立过程，如图 1 所示。其实现过程也就是信任模型的建立过程，信任模型作为信任的载体，是信任管理的关键和技术实现。

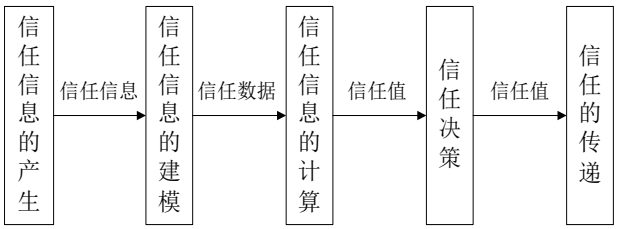


图 2 信任模型的生命周期流程

基于图 1 可以提取出一个典型的信任模型的生命周期，如图 2 所示。信任信息经过采集和挖掘产生信任数据，经过信任的建模、信任信息的收集和信任的计算、信任的更新和存储，产生决策信息，对管理对象辅助决策，然后传递到下一轮的信任周期，实际上信任的传递和决策并没有先后关系，传递可以在决策之前或之后进行。

2.2 信任模型的评估内容和指标

基于图 1 和图 2 的信任的流程和信任模型的生命周期，给出本文的信任模型的评估内容和指标。

评估内容是分布式的信任模型(以 WSN 场景为例)，对备选的经典模型，考察从信任的建立到信任的传递流程中每一阶段的可信性，并融合到综合量化评估中，从多粒度来考察信任评估结果，以此来判断该模型的性能优劣，从而为特定场景下的信任模型的优化选择提供参考。所涉及的评估指标为：

可信性：评估信任模型在每一个生命流程上的可信性。包括信任对象身份和行为表征的正确性和符合性，信任对象的动态描述的合理性和完备性。

合理性：信任建模数据的合理性，信任的建模主要采用基于数学基础的信任度的计算，其可信性需要考察对节点实际行为的合理性，比如是否符合人类社会交往行为的客观情况。

完备性：信任建模对某一个场景下标准信任概念的完备性。例如 WSN 信任模型需要考虑信任和信誉、多路信息收集、多维度，时衰，重要性等。

清晰性：描述信任模型的建模过程的语义的清晰易懂，无歧义。代表了语用层次的一个指标。

可用性：评估信任模型与具体应用场景(本文以 WSN 为例)的符合性。各种网络基于结构和功能的需要，对信任模型的机制运作提出了一定的要求。

可服务性：需要考察信任模型的服务效用，如服务效率、质量等。另外，用户的个性化需求也是需要考虑的，有的人看重信任计算效率，有人更重视信任决策正确性，反映在评估结果上是不同的。

3 基于信任模型的建模的可信性评估

3.1 可信计算的信任评估体系

可信计算中的可信的概念是参与计算的组件、操作或过程在任意的条件下是可预测的和能够抵抗一定的干扰的。可信计算联盟 TCG 的可信计算技术的思路是通过在硬件平台上引入可信平台模块 TPM 来提高计算机系统的安全性。在理论上讲，可信计算的执行需要确保可信的环境、可信的软件执行、可信的行为等；从应用范围来看，可信是一种层次式的递归结构，从终端、硬件平台、操作系统、应用软件、网络平台逐级扩展。如图 3 所示。

图 2 所示的信任生命周期与可信的扩展过程类似。本文将可信的概念应用于信任模型的评估中，对信任模型的每一个阶段的建模过程进行可信性评估，主要包括建模本身的完备性、合理性分析等。

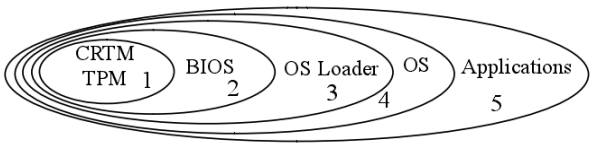


图 3 可信计算的可信根逐级扩展

3.2 建模的可信性评估

一般来说，一个基于信任度的信任模型会包括以下五个部分：信任的产生、信任的建模、信任的计算、基于信任的决策、信任的传递。一个信任模型的语义模型可由一个五元组表示：$T=(P, R, T_V, S, P_r)$，其中 P、R 和 T_V 分别代表服务提供者(Provider)、服务请求者(Requester)和服务对象信任度(Trust Value)，而 S 表示基于信任模型的具体服务，如判断节点的可信、协助路由传递等。P_r 则表示信任建模的过程，也即是信任模型的生命周期。

$$P_r = (TE, TM, TC, TD, TT) \quad (1)$$

其中，*TE, TM, TC, TD, TT* 分别表示信任的产生(Trust Establishment)、信任的建模(Trust Modeling)、信任的计算(Trust Calculating)、信任决策(Trust Decision)、信任的传递(Trust Transferring)。

对于 *TE* 的可信性的形式化定义如下：

定义 3：设立一组评估指标集合 $C=\{C_1, C_2, \ldots, C_n\}$，其中 n 为指标数。如果同时满足 $p(TE.\ C_1)\geq kh_1$, $p(TE.\ C_2)\geq kh_2$, …, $p(TE.\ C_n)\geq kh_n$，则 *TE* 可信，否则 *TE* 不可信。其中 $p(TE.\ C_i)$ ($i\in[1, n]$) 表示 *TE* 在第 i 个指标上的概率值，$kh_1, kh_2, \ldots, kh_n$ 分别表示相应的判断阈值，且 $kh_i\in[0, 1]$。

TE 在第 i 个指标上的概率值确定方式如下：先信任的产生 TE 阶段涉及的数据或概念是否满足第 i 个指标，其指标受制于经验值，经验概率的最高值取为 P_m，实际的相对概率为 P_a，则评估结果可定义为 $p(TE.\ C_i)= P_m\times P_a$。

根据 2.2 节的评估指标，对可信性的评估最常用的两个参数是完备性和合理性，特定应用场景下最完备的信任模型需要满足的特性可由相关文献给出，如文献[16]给出了 WSN 场景下的信任管理和模型应该满足的完备的基本特性，满足该系列特性的经验概率为 P_1(可取 1 或以下)，实际的模型的产生阶段的完备性用 P_2 表示，则该评估指标的结果为 $p(TE.\ C_1)= P_1\times P_2$。文献[4]给出了一个信任模型需满足的信任特性和社会网络特性，可以作为完整的合理性的表征。类似的结果也可以得到。

对于 *TM, TC, TD, TT* 的可信的分析，除了考察的对象和维度不同外，其处理过程与 *TE* 一致。

在上述的评估结束后，可得到各个阶段的评估结果，即可信性值，下面需要综合出整个信任模型建模过程的可信性及其范围。本文用确定性可信值(Deterministic Trusted Value, *DTV*) 来衡量最终融合的信任模型的表现。

确定性可信值*DTV*可从可信计算角度来分析得到，信任关系是有顺次性的，信任链是一级级扩展的，最后的信任值取决于最顶层的信任值，本文中是指信任的决策或信任的传递(决策和传递是平行交叉的关系)，*DTV*的定义如下：

$$DTV = T_{TE}\cdot T_{TM}\cdot T_{TC}\cdot T_{TD}\cdot T_{TT} \quad (2)$$

其中 $T_{TE}, T_{TM}, T_{TC}, T_{TD}, T_{TT}$ 分别标示了信任产生、建模、计算、传递、决策过程的可信性，是一个布尔变量，如满足定义 3 的情况时，$T_{TE}=1$，否则 $T_{TE}=0$。其他的变量 $T_{TM}, T_{TC}, T_{TD}, T_{TT}$ 通过相同的方法获取。由此可以看出，当且仅当信任模型的所有过程都为真时，$DTV=1$，该信任模型是可信的。当存在某个过程不为真时，$DTV=0$，需要对结果进一步分析，确定具体不可信的阶段，看是否与前述阶段关联，可以通过调整判断阈值，与关联的阶段联合重新评估，作为整体参与式(2)的计算。同时某个阶段不可信也反映了信任建模的薄弱环节，为模型的改进提供理论指导。

4 基于可信建模过程的模型量化评估

4.1 评估方法的选取

目前在其他领域(如安全系统风险评估)存在的评估方法有定性的评估方法，如 Delphi 方法、历史因素法等；定量的评估方法，如熵权系数法、聚类分析法、决策树等；定性和定量相结合的方法，如层次分析法、模糊综合评价法等。

信任的评估是一个复杂的过程，需要考虑的因素很多，有些评估要素是可以用量化的形式来表达，而对有些要素的量化又是很困难甚至是不可能的，在复杂的信息系统风险评估过程中，不能将定性分析和定量分析两种方法简单的割裂开来。而是应该将这两种方法融合起来，采用综合的评估方法。模糊综合评价法是建立在模糊数学理论基础上的一种预测和评价方法。它的特点在于其评价方式与人们的正常思维模式很接近，用程度语言描述对象。它特别适合于用来解决那些只能用模糊的、非定量的、难以明确定义的实际问题。由于信任建模的主观、模糊、类社会等特性，采用模糊理论分析和评估信任模型是合理的。

模糊综合评价法的基本原理：模糊综合评价是在考虑多种因素的影响下，运用模糊数学工具对某事物做出综合评价。设$U=\{u_1,\ u_2,\ \cdots,\ u_m\}$为刻划被评价对象的 m 种因素，$V=\{v_1,\ v_2,\ \cdots,\ v_n\}$为刻划每一因素所处状态的 n 种决断。这里存在着两类模糊集，以主观赋权为例，一类是标志因素集 U 中诸元在人们心目中的重要程度的量，表现为因素集 U 上的模糊权重向量$A=(a_1,\ a_2,\ \cdots,\ a_m)$；另一类是$U\times V$上的模糊关系，表现为$m\times n$模糊矩阵 R，这两类模糊集都是人们价值观念或偏好结构的反应。再对这两类集施加某种模糊运算，便得到 V 上的一个模糊子集$B=(b_1,\ b_2,\ \cdots,\ b_n)$。因此，模糊综合评价是指寻找模糊权重向量$A=(a_1,\ a_2,\ \cdots,\ a_m)\in F(U)$，以及一个从 U 到 V 的模糊变换 f，即对每一因素u_i，单独做出一个判断 $f(u_i)=(r_{i1},\ r_{i2},\ \cdots,\ r_{in},)\in F(V)$，$,i=1,2,\cdots,m$，据此构造模糊矩阵$R=[r_{ij}]_{m\times n}\in F(U\times V)$，其中$r_{ij}$表示因素$u_i$具有评语 v_j 的程度。进而求出模糊综合评价$B=(b_1,\ b_2,\ \cdots,\ b_n)\in F(V)$，其中$b_j$表示被评价对象具有评语$v_j$的程度，即$v_j$对模糊集 B 的隶属度。

模糊评价的几个步骤分别为确定各种集合(对象集、因素集、评语集)、建立评价因素的权重分配向量 A，通过隶属函数获得模糊综合评价矩阵 R，复合运算求得综合评价结果$B=A\times R$，计算每个评价对象的综合分值并进行排序。其中，模糊权重向量 A 的获取十分重要，直接涉及综合评价的正确性，本文中为了避免评估主观性过强，引入熵权系数法来修正主观确定的向量系数。

设对于评价因素的经验主观判定权值为W_i, 则修正后的综合权值为:

$$\sigma_i=\frac{H_iW_i}{\sum_{i=1}^{n}H_iW} \tag{3}$$

其中H_i为用熵权系数法得到的客观判定权重。熵权系数法是采用不确定性熵理论，通过统计专家的评判集W_i，利用熵理论处理数据集合，定量计算求得各因素权向量。具体过程可参见文献[17]。权重分配向量$A=(a_1,\ a_2,\ \ldots,a_m)$应该满足条件：

$\sum_{i=1}^{m}a_i=1,a_i\geq 0$。

4.2 信任模型的量化评估

对于一个待评估的信任模型，分解为 *TE, TM, TC, TD, TT* 五个部分。不失一般性，对于单个过程 *TX*，评估其性能涉及 *TX* 的数据集合(*DA*)和指标集合(*CA*)两部分。*DA* ={ DA_1 , DA_2 ,…, DA_s}，*CA* ={ CA_1 , CA_2 ,…, CA_t}，数据和指标的数目分为为 *s* 和 *t*。关于过程 *TX* 的形式化评估定义如下：

定义 4：$\forall DA_i\in DA$，并且有$DA_i.Imp\geq I,$，$I\in\{1,2,...,n\}$，如果对于 DA_i 的评价集合值$CA_{DA_i}=\{DA_i.CA_1,DA_i.CA_2,...,DA_i.CA_{t1}\}$ ($t1\leq t$) 均有效存在，则存在一个函数关系 f，使得$Q(DA_i)=f(p(DA_i.CA_1),p(DA_i.CA_2),...,p(DA_i.CA_{t1}))$成立，$Q(DA_i)$为数据 DA_i 的量化评价值。

其中$DA_i.Imp$为数据的重要性指标，分为 *n* 个级别。为了提高评估的效率，只有当数据项的重要程度满足某个级别 I 时，才需要评估其可信性。$DA_i.CA_i$ 为数据 DA_i 在 CA_i ($i\in[1,t1]$)上的评价值。$p(DA_i.CA_i)=p(DA_i\mid CA_i)$表示对应的模糊评价值的概率。

$DA_i.CA_i$ 可用模糊理论确定，对应上节的原理，设$U=\{u_1,u_2,...,u_m\}$为刻划被评价对象的 m 种因素 U，如合理性指标中，设置 *m*=3，表示{数据合理性，结构合理性，关联合理性}，即 *U*={*DR, CR, CN*}，$V=\{v_1,\ v_2,\ \cdots,\ v_n\}$为刻划每一因素所处状态的 *n* 种决断。本文设置 *n*=5，V 中的元素分别表示{不合理，最低合理性，一般合理，比较合理，非常合理}，即{NR, LR, GR, FR, VR}。设定一个从 U 到 V 的模糊变换 *f*(本文设置为梯形隶属函数)，对 U 中每个因素单独判断，构造一个模糊矩阵$R=[r_{ij}]_{m\times n}\in F(U\times V)$，其中$r_{ij}$表示因素 d_{ai} 具有评语v_j的程度。对于因素集 U 上的权重模糊向量$A=(a_1,\ a_2,\ \cdots,\ a_m)$，标识着因素集诸元在人们心目中的重要程度的量，可由前述的熵权系数法获得。最后通过 R 变换为决断集 V 上的模糊集$B_R=A\circ R$。$B_R=(b_{r1},\ b_{r2},\ \cdots,\ b_{rn})\in F(V)$，其中$b_{rj}$表示被评价对象 DA_i 具有评语v_j的程度，即v_j对模糊集 B 的隶属度。

数据项的概率定义为 $p(DA_i.CA_i)=\frac{\max(b_{rj})}{\sum_1^n b_{rj}}$，即最大隶属度相对总的隶属度的比值。

以合理性为例，取对于决断集最大隶属度为最可能的合理性。这与模糊理论中以最大隶属度优先的原则对评价对象做出一个最佳决断的思想是吻合的。

在得到数据项的各个评价概率 CA_{DA_i} 后，需要融合计算该数据项的具体评价值 $Q(D_{Ai})$，可用贝叶斯网络融合。贝叶斯网络是一个关系网络，使用静态的方法来表示不同的值的概率关系，它的理论基础是贝叶斯规则。

$$p(h|e)=\frac{p(e|h)\cdot p(h)}{p(e)} \tag{4}$$

$p(h)$ 是假设*h*的先验概率，$p(e)$ 是证据*e*的先验概率。$p(h|e)$ 是在给定*e*的条件下的*h*的概率，$p(e|h)$ 是在给定*h*的条件下*e*的概率。

本文以三个指标为例(实际上本文只考虑了三个评估指标：合理性、完备性、清晰性)，*h*设置为评价数据的评价指标*T*，证据*e*设置为子指标：*e*= (*R, C, A*)，分别表示合理性，完备性，清晰性。则式(4)可以写成式(5)。

$$p(T|R,C,A)=\frac{p(R,C,A|T)\cdot p(T)}{p(R,C,A)} \tag{5}$$

下面来求解公式(5)。考虑到三个子指标相互独立性，利用全概率公式和贝叶斯定理，可得到：

$$p(T|R,C,A)=\frac{p(T|R)\cdot p(T|C)\cdot p(T|A)}{p(T)\cdot p(T)} \tag{6}$$

其中 $p(T|R)$，$p(T|C)$，$p(T|A)$ 是贝叶斯网络中的各条边的概率，$p(T)$ 是数据指标的先验概率，一般设置为 1。将式(6)扩展到本文中的 t_1 个指标概率的情况，令 $T=DA_i$，$p_i=p(DA_i.CA_i)$，则可以推理出数据 DA_i 的的后验概率值。

$$p(DA_i|CA_1,CA_2,...,CA_{t1})=\frac{\prod_{k=1}^{t1}p(DA_i|CA_k)}{\prod_{k=1}^{t1-1}p(DA_k)} \tag{7}$$

其中 $p(DA_k)$ 为数据 DA_k 的先验概率，为了避免分子递减效果，本文设置 $p(DA_k)$ 为 0.8-1。根据贝叶斯网络模型，并不失一般性，令 $Q(DA_i)=p(DA_i|CA_1,CA_2,...,CA_{t1})$ 为数据 DA_i 的量化值。

对于单个过程 *TX*，数据 *DA* ={ DA_1 , DA_2 ,…, DA_s}，考虑到数据之间的不相关性，*TX* 的评估值也可用式(7)的贝叶斯网络继续融合，得到 $Q(TX)=\prod Q(DA_i)/P$，*P* 为 *s*-1 个 *TX* 的先验概率的乘积。

具体到信任模型的 *TE, TM, TC, TD, TT* 五个阶段，先看指标集合(*CA*)部分，根据数据的语言学范畴[18]，判断一个数据是否符合规则可以从数据的语义、语法和语用三个方面来评估，因此指标集合可以表示为 *CA*={G_a, S_i, A_i}。语义方面的具体指标包括合理性(Rationality)，源追溯性(Retrospective)等，语法的评估包括完备性(Completeness)、有效性(Effectiveness)等，语用的评估包括清晰性(Clarity)、一致性(Consistency)、可用性(Availability)等。

信任的产生阶段，选择合理性(Rationality)、完备性(Completeness)、清晰性(Clarity)。分别对应语义、语法和应用(语用)三个方面。CA_{TE} = {Rationality, Completeness, Clarity}。信任的建模、信任计算、信任决策、信任的传递部分的指标分为选择为 CA_{TM} = {Rationality, Completeness, Availability}，CA_{TC} = {Rationality, Completeness, Effectiveness}，CA_{TD} = {Rationality, Effectiveness, Consistency}，CA_{TT} = { Retrospective, Completeness, Consistency}。

数据集合(*DA*)部分，根据图 1 所示的信任建模的细节，进行数据的挖掘，形成各部分的数据集合。先从主观概念入手来描述数据，如 *TE* 阶段可考察信任的产生背景、概念、维度、初始化等，然后可用不同的维度和单位对数据进行表征，得到一组数据集合 $DA_{TE}=\{DA_{TE_1},DA_{TE_2},...,DA_{TE_{s1}}\}$，其中 *s*1 表示数字数。$DA_{TE}$ 可进一步按需用标准化的方法[21]转换为一个[0, 1]直接的数字，同理，*TM* 的数据集合主要考察第一手建模信息的收集、信任建模的方法、建模的目标等，$DA_{TM}=\{DA_{TM_1},DA_{TM_2},...,DA_{TM_{s2}}\}$，*TC* 的数据集合主要考察计算的时间复杂度、空间复杂度、计算的时效性，$DA_{TC}=\{DA_{TC_1},DA_{TC_2},...,DA_{TC_{s3}}\}$。*TD* 的数据集合主要考察信任的决策的表达方式、决策的效率、抗攻击、信任的更新，$DA_{TD}=\{DA_{TD_1},DA_{TD_2},...,DA_{TD_{s4}}\}$。*TT* 的数据集合主要考察传递的效率、多路径的传递、数据的损失度量，$DA_{TT}=\{DA_{TT_1},DA_{TT_2},...,DA_{TT_{s5}}\}$，*s*2, *s*3, *s*4, *s*5 分别表示相应的数目。

在上述的评估结束后，可得到各个阶段的评估结果第 3 节已经得出了确定性可信值 *DTV*，本节从

另外两个角度：概率评估值(Probabilistic Evaluation Value, *PEV*)，权重信念值(Weighted Belief Value, *WBV*)，来进一步衡量最终融合的信任模型的表现。

概率可信值*PEV*根据前面的各个部分的概率计算可信性值融合得到，定义如下：

$$PEV = \sum_{i=1}^{n} \frac{f(k_i) \cdot p_{T_i}}{\sum_{i=1}^{n} f(k_i)} \tag{8}$$

其中 p_{T_i} 表示前面求得的单个阶段的概率值 $Q(TX)$，n=5，k_i 表示对第i个过程的权重值。权重向量为$\{k_1, k_2, k_3, k_4, k_5\}$，跟前述一样，可以用熵权系数法来确定，各个阶段的熵是不确定性的表示。考虑到信任的五个阶段重要性差别不大。在重要性角度看，为了简化起见，可以设置各个向量相等。然而这五个阶段并不是完全独立的，存在耦合和顺次关系，权重向量需要进行相关联处理。例如信任的建模和信任的计算就具有一定的关联，k_2的熵越小，k_3对应也会越小，概率值 p_{T_2} 越大，则 p_{T_3} 越大。我们设置权重信念值 $WBV = \{f(k_1), f(k_2), f(k_3), f(k_4), f(k_5)\}$ 来更新权重向量。$f(k_i) = \alpha_i \cdot k_i, i \in [1,5]$，$\alpha_i$ 对应于每一个阶段的加权值，根据信念确定。如果我们确信某个过程与上面过程相关，我们可以调整α_i，使后续的权重降低，以免相关的几个高权重阶段湮没了其他阶段的影响；另一方面，根据2.2中的**可服务性**指标的概念，我们可以根据参与者的关注点来调整权重，如某个参与者更希望看到信任决策方面模型的性能，那更加会采信该阶段的概率值，因此可提高对应的α_i。

本文最终衡量信任模型是用三元组表示的：(*DTV, PEV, WBV*)，第一个参数是信任模型的定性衡量，第二个参数是信任模型的定量衡量，第三个可以表示约束条件或者上下文因素。我们可以根据*WBV*得到相对概率值，以供模型选择参考。

5 评估结果和系统框架

5.1 评估过程和结果概述

本文所提的信任模型评估的过程简述如下：

1) 对待评估的信任模型 *A*，从信任的产生(*TE*)、信任建模(*TM*)、信任的计算(*TC*)、信任决策(*TD*)和信任传递(*TT*)5 个方面，分析各部分的基本组成，根据图 1 提出各部分的评估数据(*DA*)，并给出评估指标(*CA*)。

2) 对各部分的数据对应的指标部分，用模糊理论和熵权系数法计算各个指标的可信度概率，用贝叶斯理论融合成单个过程 *TX* 的评估概率值。最后根据公式(8)计算待评估模型的评估概率值 *PEV*。

3）同时根据信任建模的可信性理论，得出单个过程的可信值，用计算(2)计算待评估的信任模型的可信性指标 *DTV*。

4）根据特定场景和个性化需求，给出各阶段的权重信念值和权重向量 *WBV*。综合得出待评估模型的评估结果 Evaluation(A)= (*DTV, PEV, WBV*)。

5) 对各种待评估模型在同一种场景下按照上述过程评估，得到一组结论集合，用 *DTV* 筛选可信模型，根据 *PEV* 得出模型优劣排序，最后根据可信阈值选择一组合适的信任模型和最佳的模型，用于执行任务。

本文所提信任模型评估的预期结果是能对待评估的模型进行定性和量化的评分，基于评分基础上选择相对最优的信任模型执行任务。

5.2 评估结果的一致性分析

由于评估过程中仍然存在主观因素，需要对结果的一致性进行分析。主要是决策结果的抖动问题，上述评估结果主要是根据 *PEV* 是对各个阶段可信性的线性加权求和，从而确定信任模型的量化值，排序得到最优选择模型。由于决策中如权重向量涉及主观判断，我们需要分析权重值的变化对排序结果的影响。

公式(8)是对单个信任模型的评估，采用了线性加权平均的方法，其中 p_{T_i} 是概率值，设 PEV_i 为第 i ($i \in [1, m]$，m 为模型数目)个待评估模型的量化决策值。

记 $hm = \min\{|PEV_i - PEV_j|\}$，其中 $i \neq j$, 且 $i, j = 1, 2, ..., m$。对于各个阶段的概率值 p_{T_i} 对应的权重 $k_j, j = 1, 2, ..., n$，如果存在一个微小的扰动 Δk_j，那么将引起评价值 PEV_i 有一个微小的扰动 ΔPEV_i。

于是有 $\Delta PEV_i = \sum_{i=1}^{n} \Delta k_i \cdot p_{T_i}$，从而有：

$$\begin{aligned} |\Delta PEV_i| &= \left| \sum_{i=1}^{n} \Delta k_i \cdot p_{T_i} \right| \le \sum_{i=1}^{n} |\Delta k_i| |p_{T_i}| \\ &\le \sum_{i=1}^{n} (\max |p_{T_i}|) \times |\Delta k_i| = n \|A\| \times \|\Delta k\| \end{aligned} \tag{9}$$

其中$\|A\|$为概率序列p_{T_i}的范数，定义为无穷范数。$\Delta k=\{\Delta k_1,\Delta k_2,...,\Delta k_n\}$。为保证决策集中的结果影响不大(即涉及的评估模型排序不变)，则有$|\Delta PEV_i-\Delta PEV_j|<hm$，从而有$|\Delta PEV_i|<hm/2$，所以只要$\|\Delta k\|<hm/2n\|A\|$时，就可以保证最终的决策在扰动过程中保持结果不变。同理，对于*WBV*中$f(k_i)=\alpha_i\cdot k_i, i\in[1,m]$，设$\alpha=\{\alpha_1,\alpha_2,...,\alpha_m\}$，$k=\{k_1,k_2,...,k_m\}$，其权重$\alpha_i$也是主观值，可以推测出当$\|\Delta\alpha\|<hm/2m\|k\|$时，主观性造成的抖动不改变决策的结果。

至于概率序列p_{T_i}，由前述定义可知，是由频率确定的，由概率论的知识可知，当频率大到一定程度时，概率值等价为频率值，所以p_{T_i}也是客观值。对于概率门限值T_{th}，其抖动直接影响到p_{T_i}的判断，进而*DTV*可能发生变动，T_{th}是由经验值确定的，这里不再叙述。

5.3 系统实现

图4给出了基于本文所提算法的信任模型评估系统的基本框架。

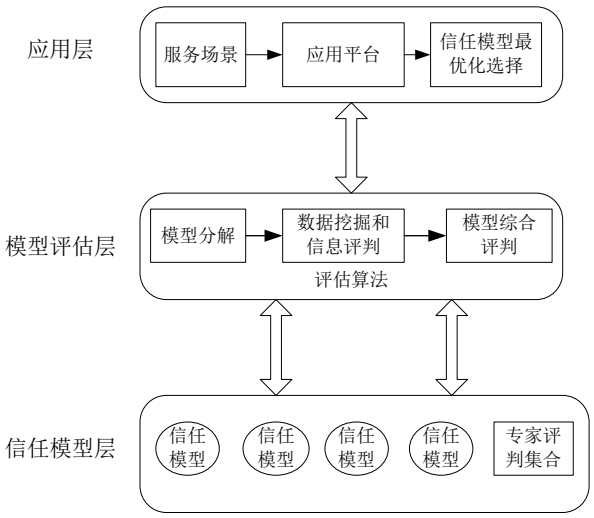


图4 信任模型评估系统框架

在图4中，最底层是信任模型库，收集了各种场景下各种测度的信任模型，第二层是模型评估层，顶层是应用层。

基于本文所提的评估算法融合到评估系统中，其评估过程如下：(1) 首先从信任模型层中提取待评估的信任模型，一般提取同一应用场景下的若干信任模型。(2) 利用本文的评估算法评估模型的性能，包括模型的分解、单个过程的数据挖掘和模糊评判、模型的综合评判，最后形成可信决策和量化值。(3) 根据形式化的服务场景提取供求信息，确定上下文约束条件*WBV*，调整决策量化值。(4) 通过应用平台(主要包括操作引擎和人机界面)选择最优化的信任模型，用于任务的执行。

6 评估实例和仿真验证

6.1 分布式WSN信任模型的评估

本文选择WSN作为一种特定的应用场景，评估几种典型的WSN信任模型，来验证所提算法的评估效果。选取了文献 HRMSN[7]、 BNWSN[8]、GTMS[9]、基于熵的Ad Hoc模型(EBM)[6]、RFSN[10]、EigenTrust[3] 6个最具代表性的信任模型，前4个分别从信任的维度、信任的方法、信任的粒度、网络的相似度来建模的方法，第5个模型是WSN经典的综合模型，第6个是通用的分布式信任模型。

针对可信性的获取，由合理性和完备性的概率加权得到，其中完备性权重取0.7，合理性取0.3。合理性用文献[4]中对于信任模型需满足的9个信任特性来衡量，完备性用文献[16]中给出的WSN场景下的信任管理和模型应该满足的完备的基本特性来衡量。文献[16]给出了一组适合WSN的信任管理系统完备的要素：考虑信任和信誉(Trust and reputation)、信任和基站(Trust and base station)、第一手信息收集(First hand information，信任计算信息)、第二手信息收集(Second hand information，推荐和合作信息)、初始信任值(Initial values)、信任的粒度(Granularity，指信任的多维性)、信任的更新和时衰(Updating and aging)、风险和重要性(Risk and importance)。表1给出了可信性指标*DTV*的评估结果。其中*Th*为每个阶段以及*DTV*的门限值。进一步分析其他指标，按照前述4.2量化评估的方法，得到各个模型在不同阶段的不同指标上的量化值，如表2所示。

表 1 可信性评估 *DTV*

	TE	*TM*	*TC*	*TD*	*TT*	*Th*	*DTV*
HRMSN	0.8	0.67	0.73	0.67	0.56	0.5	1
BNWSN	0.79	0.76	0.53	0.56	0.52	0.5	1
GTMS	0.63	0.53	0.64	0.63	0.83	0.5	1
EBM	0.43	0.5	0.65	0.58	0.88	0.5	0
RFSN	0.63	0.87	0.75	0.67	0.78	0.5	1
EigenTrust	0.33	0.39	0.5	0.53	0.5	0.5	0

表 2 信任量化评估

	TE			*TM*			*TC*			*TD*			*TT*		
评估模型	RA	CO	CL	RA	CO	AV	RA	CO	US	RA	EF	US	RS	CO	CS
HRMSN	0.8	1	0.67	0.67	0.78	0.9	1	0.78	0.67	0.6	1	0.78	0.78	0.5	0.3
BNWSN	1	0.86	0.89	1	0.78	1	0.75	0.56	0.67	0.7	0.71	0.55	0.89	0.4	0.3
GTMS	0.7	0.75	1	0.67	0.56	0.8	0.63	0.78	0.89	0.7	0.86	1	1	0.8	1
EBM	0.5	0.5	0.67	0.56	0.56	0.9	0.38	0.89	0.89	1	0.57	0.89	0.67	1	0.9
RFSN	0.7	0.75	0.67	0.89	1	0.9	0.5	1	1	0.6	1	0.67	0.55	0.9	0.4
EigenTrust	0.4	0.38	0.78	0.67	0.33	0.5	0.63	0.56	0.56	0.6	0.71	0.44	0.55	0.5	0.6

表2中的标号分别为合理性(RA)，完备性(CO)，清晰性(CL)，可用性(AV)，有效性(EF)，符合性(US)，一致性(CS)。表2中数据的获取方式：首先分析待评估模型，比如信任的建模，从合理性、完备性、可用性衡量每个过程的每个参数，其中合理性与完备性与*DTV*部分类似，可用性主要考察数据能否反映WSN的应用，如信任数据能处理节点的合作感知等。根据模糊理论，用五级评分法(优、良、中、次差、差)衡量指标的性能，给出备选模型的参考范围。

上述范围可以有效的衡量无量纲的值，比如完备性和合理性的单位就不同。为了进一步量化，取1-10之间的数字表示上述衡量值。由于本文的目的是模型的比较，没有绝对的标准模型，所以取相对值，对得到的数据进行标准化处理，得到[0,1]之前的数值。标准化的处理过程如下：类似表 2 构造一个 6*15 矩阵 R，元素 $r_{ij}\in R$，$r_{ij}^{'}=(r_{ij}-E(r_j))/S_j$，其中 $E(r_j)$ 为第 j 列元素的均值，S_j 为第 j 列元素的标准差，然后以极值标准化的方法：$r_{ij}^{''}=(r_{ij}^{'}-\min(r_{ij}^{'}))/\max(r_{ij}^{'})-\min(r_{ij}^{'})$，将矩阵中的数据转化为区间[0, 1]的数值，即为表 2 中的结果。根据贝叶斯理论计算式(7)，融合得到单个阶段的评估值。为简单起见，设置每个阶段的权重向量一致，$WBV=\{f(k_1),f(k_2),f(k_3),f(k_4),f(k_5)\}=\{1/5,1/5,1/5,1/5,1/5\}$，最终得到各个信任模型的相对评估值和可信值，如表 3 所示。

表 3 最终的评估结果

评估模型	评估值(*PTV*)	可信值(*DTV*)
HRMSN	0.586	1
BNWSN	0.652	1
GTMS	0.692	1
EBM	0.601	0
RFSN	0.54	1
EigenTrust	0.48	0

信任模型的最终评估结果是*(DTV, PEV, WBV)*，由表3可知，在本例的设置下，GTMS可信且概率值最大，是最优的WSN信任模型。

6.2 方案的有效性分析和仿真

6.2.1 对比方案的有效性分析

本文所提方案相对于文献[11][12][13][14][15]在评估的效果和性能上面有一定的提升。从评估方案的准确性、应用性、效率 3 个角度来分析。

在准确性方面，文献[11]通过提取行为特征和交互双方的信任历史序列作为考察对象，将信任模型输入黑盒，比较序列的输入输出，用敏感性和预测性来判断性能的好坏，其准备性依赖于信任和行为特征的初始化，未能全面反映信任模型的特点，准确性有待提高；文献[12]很全面的展示了信任的整个建立过程，但是没有具体的评估方案，相对于文献[11]，准确性较高；文献[13]用 ART 的方式模拟仿真信任模型的评分得失，只描述了推荐信任和可信评分的关系，准确性较低；文献[14]用形式化的方式描述了多个信誉系统，并模拟了攻击情况下信任的走势图，客观性得到一定的提高，该方案只考虑信誉系统，完整性不够；文献[15]分析了几种信任模型在物联网场景下的适用性，分析了几种特性，客观性和具体性有待提高。本文所提算法利用客观的模糊理论和贝叶斯理论来量化信任模型的评估值，对每个过程详细的评估，评估结果更客观、具体、全面，因此准确性较高。

在应用性角度，文献[11][12]以及本文算法都是通用的，对各种场景适用，文献[11]对于参数选取、特征提取缺乏一定的可信性分析，可用性分析不足；文献[12]适合用于风险评估的指导意见，实施的可用性和关联性需要进一步建模；文献[13]适用于评分和推荐的情况，其初衷并不是各种场景下的信任模型评估；对于文献[14]，前面已经分析，没有考虑非信誉模型的可用性，其仿真参数设置也是不明确的，可操作性不强；文献[15]只考察了 WSN

信任模型在单个物联网场景下的适用性；本文算法从信任模型的结构方面分析了其可信性，普适性较强，定量分析部分可操作性较强。

方案的效率考察在评估系统中，结果的获取时间以及资源的消耗情况。文献[11]根据设定的行为特征搜集信任双方的历史记录，涉及历史行为的迭代和信任的调整更新，时间复杂度在 O(n)左右，n 为需采集的行为数目；文献[12]不涉及系统的耗时，资源的消耗根据采用的算法不同而不同，是不确定的；文献[13]需要交互很多次才能统计得出模型的性能，时间和资源消耗较大；文献[14]在建模阶段效率高，仿真阶段以节点为粒度模拟了信誉系统的抗攻击情况，方案随节点增大而消耗增加；文献[15]评估几种典型的模型在 4 个参数上的表现，涉及计算和存储很小，效率高；本文算法单个阶段评估中采用模糊理论和贝叶斯模型，综合评估中加权计算，时间复杂度与文献[11]类似，在 O(n)左右，n 为考察的评估参数。

总结上述分析，用高、较高、中、较低、低 5 档表示方案的性能，上述结果可用表 4 所示。

表 4 方案的对比性能分析

	文献[11]	文献[12]	文献[13]	文献[14]	文献[15]	本文算法
准确性	中	较高	较低	较低	一般	高
应用性	较高	较高	较低	较低	较低	高
效率	较高	不详	低	一般	高	较高

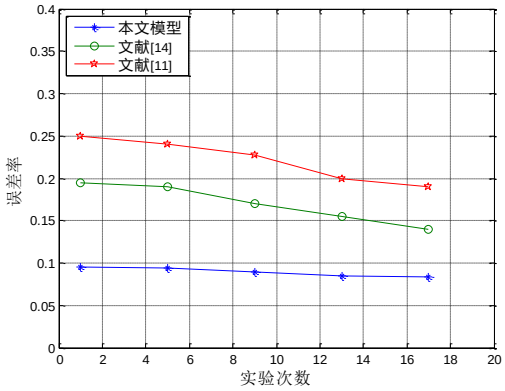
6.2.2 方案的仿真分析

本文从算法的准确性、稳定性、效率三个方面进行了仿真分析，其对比方案是文献[11]的 Yang 的方案和文献[14]的 Schlosser 方案，因为其他三个文献都是叙述的内容。

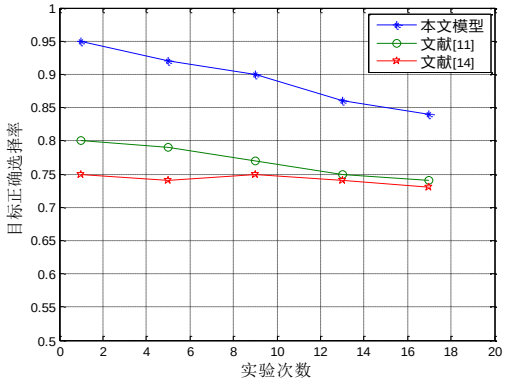
准确性仿真：反映为不同的实验次数下(x)模型评估的误差(y)，定义为 $\Delta F = |F_{Act} - F_{The}| \times 100\%$，其中 F_{Act} 为实际评估值(本文算法是 PEV 值)，F_{The} 是理论值，用文献[4]中的通用模型评估近似代替。实验次数设置为 20 次，参与的专家人数起始 10 人，按照次数人数依次增加 1。

稳定性仿真设置为随着实验次数的增加模型最优化选择的稳定性。以表 3 结果为基础，描述 GTMS 模型被选择的概率。效率设置为随着实验次数(对应不同的评估参数数目)的增加其资源消耗情况，主要是计算的耗时。仿真结果如图 5 所示。

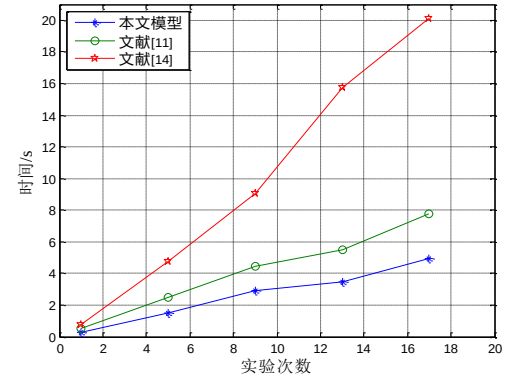
图 5(a)反映了所提算法的准确性，可以看出，本文算法相对文献[11][14]的算法误差更小，误差在



(a) 准确性仿真



(b) 稳定性仿真



(c) 效率仿真

图 5 仿真结果

10%之内，因为本文是基于多维细粒度的评估，与通用模型接近，文献[11][14]的参数设置较少。图 5(b)反映了所提算法的稳定性，在模型数目增加的情况下，本文算法显示了一定的抖动，这是由于主观误差引起的，当实验次数增加时，GTMS 选择的概率仍然在 80%以上。图 5(c)描述了算法效率，随着评估参数 n 的增加，计算耗时增加，本文算法和文献[11]算法呈近似线性增加，但文献[14]增加较快，实验结果与表 4 的分析一致。

7 总结

信任模型的评估是信任模型发展到一定阶段必须解决的问题，本文提出了一种基于可信建模过程的信任模型分析和评估方法，从可信性、概率评估值和信念权重向量三个角度衡量了信任模型，分析结果、WSN 实例和仿真实验表明所提算法是合理有效的，评估的结果为新的信任模型的提出提供了参考，也为实际应用中信任模型的最优化选择提供了理论依据。下一步的工作是对信任模型进行进一步的挖掘提取多维的数据，如属性、关联数据等。提出基于多维数据的融合和评估算法，进一步完善评估的理论。

参考文献

[1] 沈昌祥,张焕国,冯登国,曹珍富,黄继武.信息安全综述[J].中国科学:E辑:信息科学,2007,37(2):129-150.

[2] Félix G.M, Gregorio M. P. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems [J]. Computer Standards & Interfaces, 2010, 32(4): 185-196.

[3] Kamvar S.D., Schlosser M.T., Garcia-Molina H., The EigenTrust Algorithm for Reputation Management in P2P Networks [C], Proceedings of the 12th international conference on World Wide Web, ACM Press New York, NY, USA, 2003, pp. 640-651.

[4] 汪京培，孙斌，钮心忻，杨义先.基于参数建模的分布式信任模型[J].通信学报, 2013, 34(4):47-59.

[5] Goyal M.K., Gupta P., Aggarwal A.,*et al*. QoS based trust management model for Cloud IaaS [C], 2012 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), 2012, Page(s): 843-847.

[6] Sun Y L., Yu W, Han Z, Liu KJR. 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):305−317.

[7] Aivaloglou E, Gritzalis S. Hybrid trust and reputation management for sensor networks [J], Wireless Networks, 2010, 16(5): 1493-1510.

[8] Momani M, Challa S, Alhmouz R. Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks [J], Journal of Networks, 2010, 5(7): 815-822.

[9] Shaikh R. A, Jameel H, d'Auriol B J., *et al*. Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks[J], IEEE Transactions on Parallel and Distributed Systems, 2009, 20(11): 1698-1712.

[10] Ganeriwal, S., Balzano, L. K., & Srivastava. Reputation-based framework for high integrity sensor networks [J]. ACM Transactions on Sensor Networks, 2008, 4(3): 1-37.

[11] Yang M, Wang L N, Lei Y D. Research on Evaluation of Trust Model [C], 2008 International Conference on Computational Intelligence and Security, 2008, pp. 345-349.

[12] Wojcik, M., Venter, H.S., Eloff, J.H.P., Trust Model Evaluation Criteria: A Detailed Analysis of Trust Representation [C], Proceedings of SATNAC: South African Telecommunications Networks and Applications Conference, September 2006, Western Cape, South Africa.

[13] Fullam K. K., Klos T. B., Muller G., J. *et al*. A specification of the agent reputation and trust (ART) testbed: experimentation and competition for trust in agent societies[C]. In Proc. 4th International Joint Conference on Autonomous Agents and Multi-agent Systems, Pages 512–518, 2005.

[14] Schlosser A, Voss M, Lars Br¨uckner. Comparing and Evaluating Metrics for Reputation Systems by Simulation [C]. Proc. IAT Workshop on Reputation in Agent Societies, 2004.

[15] Wang J P, Sun B, Yang Y, Niu X X. WSN Trust Models Evaluation in the Context of the IoT [J]. Journal of Computational Information Systems, 2013, 9(8): 3109-3116.

[16] Lopez J, Roman R, Agudo I, *et al*.. Trust management systems for wireless sensor networks: Best practices [J], Computer Communications, 2010, 33(9): 1086-1093.

[17] 赵冬梅, 张玉清, 马建峰. 熵权系数法应用于网络安全的模糊风险评估[J]. 计算机工程，2004, 30(18): 21-23.

[18] 王勇，复杂仿真系统概念模型建立与评估方法研究[D]. 哈尔滨工业大学博士学位论文, 2010: 65-89.