基于 D-S 证据理论的多维度信任评估方法

吴旭 王杨 袁耀

（西安邮电大学计算机科学与技术系 西安 710121）

摘 要 针对当前云环境下信任评估存在的多维属性和不确定性问题，提出一个基于 D-S 证据理论的多维度信任评估方法，来评估云服务商的信任值。实体间的信任关系用信任、不信任和不确定来表示，依据与云服务商相关的属性证据进行直接信任度计算；并根据第三方用户的推荐计算间接信任度；最后综合直接信任和推荐信任得到云服务商的综合信任值。实验分析表明，该信任模型能够较为准确的对云服务商做出信任评估，从而有效的防止恶意攻击行为；同时将 D-S 证据理论引入到实体的直接信任度评估中，较好的解决了证据不确定性的问题。

关键词 云计算；多维属性证据；D-S 证据理论；信任评估

Multi - Dimensional Trust Evaluation Method Based on D - S Evidence Theory

WU Xu，WANG Yang，YUAN Yao

(Department of Computer Sience & Technology, Xi’an University of Post & Telecommunications, Xi’an 710121, China)

Abstract A multi-dimensional trust evaluation method based on D-S evidence theory is proposed to evaluate the trust value of cloud service provider in view of the multi-dimensional attributes and uncertainties of trust assessment in the current cloud environment. The trust relationship between entities is divided into trust, distrust, and uncertain, and the trustworthiness is calculated based on the attribute evidence associated with the cloud service provider. According to the recommendations of third-party entities to calculate indirect trust, and finally integrated direct trust and recommended trust to assess the entity's comprehensive trust. The analysis of experiment shows that the trust model can be more accurate to make a trust evaluation, so as to effectively prevent malicious attacks; At the same time, the D-S evidence theory is introduced into the direct trust evaluation of the entity, which solves the problem of uncertainty.

Key Words cloud computing; multi-dimensional attribute evidence; D-S evidence theory; trust evaluation

1 引言

随着云计算的快速发展，用户对云计算的安全、性能、可靠性持怀疑态度。要想消除用户在选择云服务时产生的顾虑和担忧，就需要采取有效的机制和手段管理云中用户和云服务商的信任关系[8,10]。

信任涉及许多因素，如假设，期望，行为，风险等。因此，可信度具有多维属性[12]。研究适用于云计算环境的信任关系建模和评估方法，是动态信任管理必须解决的核心问题[2-5]。

文献 2 从云服务的操作性能、QoS、安全隐私等方面考虑，将云服务的适用性、可扩展性、可持续性、可靠性等属性作为信任维度建立属性选择空间，并提出一种用于各信念度属性的证据推理算法，融合多个等级的评价。文献 8 在信任证据模型中引入滑动窗口来评估用户和云服务商的信任关系，但却不能有效的反映云服务商的服务行为变化。

由于 D-S 证据理论具有处理“不精确”和“不确定”的能力，因此，现有的信任模型大多采用 D-S 证据理论来融合多维信任证据[7,11]。但是，当前国内外学者提出的信

任证据模型仍然存在着不足：(1) 由于各证据的不确定性，不一定具有相同的重要程度，所以在实际应用中不能将多维证据直接利用 D-S 合成规则进行合成。(2)评估云服务商的信任度通常只考虑基本信任函数$m(T)$或信任函数$Bel(T)$，而忽略了不确定部分的基本信任函数值。

针对以上问题，提出一个新的多维度信任评估方法来评估云服务商的信任值。在该方法中，用信任、不信任和不确定性这三者来表示实体间的信任关系，依据云服务商相关的属性证据进行直接信任度计算，并引入证据权重和归一化算法得到更为真实直观的直接信任值；根据第三方用户的推荐计算间接信任度；最后以实体间的交互次数为权重综合直接信任和推荐信任得到实体的综合信任值。实验分析表明，该信任模型能够较为准确的对实体做出信任评估，同时将 D-S 证据理论引入到实体的直接信任度评估中，较好的解决了证据不确定性的问题。

2 改进的 D-S 证据理论

2.1 D-S 证据理论的基本原理

D-S 证据理论由 Dempster 于 1967 年提出，其学生 Shafer 在 1976 年将其进一步推广。D-S 证据理论的数学模型要先定义识别框架，然后确定证据对每个命题的支持程度，再利用证据合成公式算出对所有命题的支持度。

在 D-S 证据理论中，用识别框架 Θ 表示所研究对象的全集，Θ 中的元素之间相互排斥且为离散值。基于识别框架 Θ 的所有子集的集合称为 Θ 的幂集，记作2^{θ}。

定义 1 概率分配函数m：若存在函数$m: 2^{\Theta} \longrightarrow [0,1]$，且满足：

$$\begin{cases} m(\emptyset) = 0 \\ \sum_{A \subseteq \Theta} m(A) = 1 \end{cases} \quad (1)$$

则称$m(A)$称为A的基本概率分配函数，函数$m(A)$ 反映了证据体对事件 A 的相信程度。

定义 2 信任函数Bel：设函数$Bel: 2^{\Theta} \longrightarrow [0,1]$，且

$$Bel(A) = \sum_{B \subseteq A} m(B) \quad (2)$$

Bel又称为下限函数，$Bel(A)$表明对事件A的真实信任度。

定义 3 似然函数Pl：设函数$Pl: 2^{\Theta} \longrightarrow [0,1]$，且

$$Pl(A) = 1 - Bel(\neg A) \quad (3)$$

$Pl(A)$又称为上限函数，表明对事件A的非假信任度。

根据以上相关定义，Dempster 合成规则如下：

定义 4 合成规则：对于$\forall A \subseteq 2^{\Theta}$，识别框架上的有限个 mass 函数$m_1$，$m_2$，$\cdots m_{\mathrm{n}}$的合成规则为：

$$m(A) = m_1 \oplus m_2 \oplus \ldots \oplus m_{\mathrm{n}} = K^{-1} \times \sum_{A_1 \cap A_2 \cap \ldots \cap A_{\mathrm{n}} = A} m_1(A_1) \cdot m_2(A_2) \ldots m_{\mathrm{n}}(A_{\mathrm{n}}) \quad (4)$$

其中，$\mathrm{K} = 1 - \sum_{A_1 \cap A_2 \cap \ldots \cap A_{\mathrm{n}} = \emptyset} m_1(A_1) \cdot m_2(A_2) \ldots m_{\mathrm{n}}(A_{\mathrm{n}})$

K 称为归一化因子，1-K 则为矛盾因子，反映证据间的冲突程度，矛盾因子 K 与两条证据之间的冲突程度有关，当 K 的值越接近 1 时，证据体之间的冲突程度越大，融合结果越不准确；当 K 的值越接近 0，证据体之间的冲突程度越小，融合结果越准确；当 K=1 时，证据体之间相互矛盾，不能对其进行有效融合。

2.2 改进的 D-S 证据理论

由于云环境中信任具有不确定性，而实际应用中参与合成的证据的重要性一般是不同的，但是 D-S 证据理论并没有区分原始证据的重要性，所以会产生证据间的冲突 K。针对证据合成过程中的证据冲突问题，引入证据权的概念，本文提出证据的“有效性”来表示证据的重要性并作为证据权重对已有的基本可信度分配函数进行修正。证据有效性越高，则代表证据对于信任结果越重要，反之，则越不重要。

2.2.1 证据的重要性权重

综上，本文分析证据的“可信度”和“确定性”，来定义证据的有效性，继而判断证据的重要性。

定义 5 假定识别框架 Θ 下的信任证据 E_1和E_2，$A \subseteq \{\emptyset,\{T\},\{-T\},\{T,-T\}\}$ E_1和E_2 的证据距离即为m_1，m_2的距离，计算方式如下：

$$d(m_1,m_2)=\sqrt{\frac{1}{2}(M_1-M_2)^T D(M_1-M_2)} \tag{5}$$

式中$M_1=[\boldsymbol{m_{11}},\ \boldsymbol{m_{12}},\ \boldsymbol{m_{13}}]^T$，$M_2=[\boldsymbol{m_{21}},\ \boldsymbol{m_{22}},\ \boldsymbol{m_{23}}]^T$。$D=D_{ij}$为一个 $i\times j$的矩阵，其中，$D_{ij}=\frac{|A_i\cap A_j|}{|A_i\cup A_j|}$ 。

定义 6 设$m_1,m_2,\dots,m_{\mathrm{n}}$为同一识别框架下的 n 个证据，证据$m_i$被其他证据的支持程度为：

$$\mathrm{s}(m_i)=\sum_{j=1;j\neq i}^{n} sim(m_i,m_j) \tag{6}$$

其中$sim(m_i,m_j)$为证据m_i与m_j的相似度，且满足$sim(m_i,m_j)=1-d(m_i,m_j)$。

定义 7 将所得到的$\mathrm{s}(m_i)$进行排序，可以得到$\mathrm{s}(m_f)$：

$$\mathrm{s}(m_f)=\max_{1\le i\le n}\{\mathrm{s}(m_i)\} \tag{7}$$

根据信任证据权重的评定原则和证据距离的度量方法，已知被支持程度最高的信任证据m_f，以m_f的$\mathrm{s}(m_f)$为基数，则证据m_j的相对可信度如下：

$$\mathrm{s}(m_j)=\left[1-d\left(m_f,m_j\right)\right]\mathrm{s}(m_f)$$
$$0\le d\left(m_f,m_j\right)\le 1 \tag{8}$$

由信息熵理论，定义证据的确定性。

定义 8 $m(A)$为识别框架下任意证据E的基本可信度函数，$|\Theta|=I$，证据E提供的信息的相对确定性为：

$$Su(E)=1-\frac{V(E)}{|V(E)|} \tag{9}$$

上式中，$V(E)$为信任证据E所包含信息不确定性的信息熵。信息熵具体的计算公式为：

$$V(E)=-\rho\sum_{i=1}^{2^I} m(A_i)\ln(m(A_i)) \tag{10}$$

$$|V(E)|=-\rho\sum_{i=1}^{2^I}\left(\frac{1}{2^I}\ln\frac{1}{2^I}\right)_i=-\rho\ln\frac{1}{2^I} \tag{11}$$

上式中ρ为熵值系数且满足$\rho>0$。

综上可得证据的有效性，即识别框架下证据的重要性权重：

$$U(m_j)=\ \mathrm{s}(m_j)e^{-Su(E_j)},j=1,2,\dots,n \tag{12}$$

信任证据有效性$U(m_j)$是由信任证据的可信度和确定性共同决定，并且满足$0\le U(m_j)\le 1$。

由上述分析，本文依据信任证据重要性加权的方法对原来的基本概率分配进行改进，即可以得到新的概率分配函数(BPA)：

$$m_i'(A)=\begin{cases} U(m_i)\cdot m_i(A)\ , & A\neq\Theta \\ 1-\sum_{B\subseteq\Theta}U(m_i)\cdot m_i(B)\ , & A=\Theta \end{cases} \tag{13}$$

修改后的 D-S 证据理论合成规则对证据的重要性进行了区分，可以有效的缓解证据合成时由于证据重要性不同而引起的冲突。

3 信任模型

3.1 信任模型框架

云计算环境中的实体身份很多，本文主要评估云服务商(SP)和用户(SU)之间的信任关系，用户根据关于云服务商的直接信任度和推荐实体(SR)的间接信任度来计算云服务商的综合信任值。信任模型如图 1 所示。

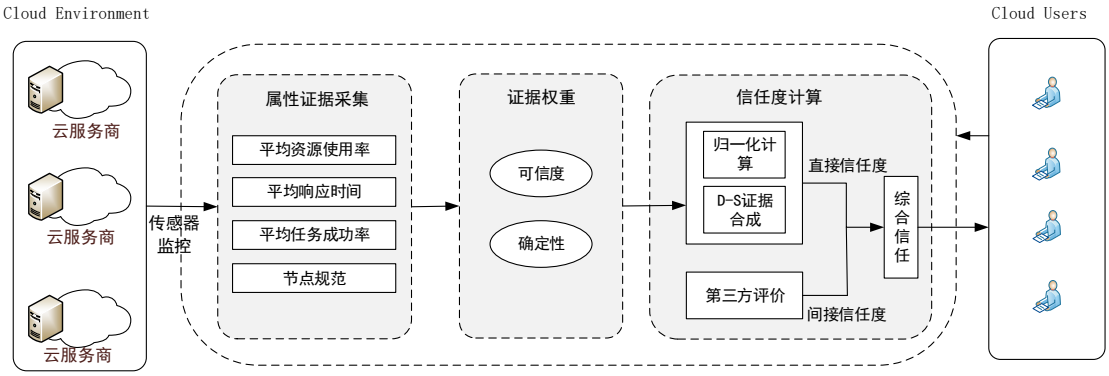

图 1 信任模型框架

如图 1，由于云服务商和用户间的信任关系具有模糊性和不确定性问题，而 D-S 证据理论能够很好的处理这种不确定性，因而提出基于 D-S 证据理论的多维度信任评估方法来计算实体间的直接信任度，用信任，不信任和不确定组成的三元组表示实体间的信任关系；该方法从保证 QoS 的角度来计算云服务商SP的直接信任度，主要关注其所提供云服务的四种可信属性，其中包括节点规范，平均资源使用率，平均响应时间，平均任务成功率。节点规范和平均资源使用率都包括四个可信赖的证据：CPU 频率，内存大小，硬盘容量，网络带宽。我们利用以下两种类型的软件传感器并采用基于推送的方法来获取这些 QoS 指标：(1)监控传感器负责收集计算资源的直接性能指标。例如 CPU 频率，内存大小，硬盘容量，网络带宽，扫描敏感端口次数等。(2)计算传感器负责收集和计算需要实时计算和统计的间接 QoS 指标。例如 CPU 利用率，内存利用率，硬盘利用率，带宽利用率，平均响应时间和平均任务成功率。

依据采集的属性证据对云服务商进行基本概率分配(BPA)；并根据重要性权重对原始的 BPA 函数进行加权修正；最后利用 D-S 证据合成规则融合信任证据；再对信任关系三元组进行归一化计算，得到更贴近真实值的直接信任度；接下来根据其他用户的推荐信任计算出间接信任度即可综合得到云服务商的综合信任值，为用户的下一步交互活动提供依据。

3.2 多维度信任评估方法

3.2.1 直接信任

直接信任值用$D(SR,SP)$表示，它反映了云服务商最直接的信任度，用户根据与云服务提供商的直接交易等因素来判断是否可信。本文中的直接信任值计算考虑了影响信任的多维属性证据。

在本文的信任模型中，将 Θ 定义为$\{T,-T\}$，实体间的关系分为信任$\{T\}$、不信任$\{-T\}$、不确定$\{T,-T\}$，从这三个方面对直接信任度进行评估，其步骤如下：

(1) 首先依据证据采集阶段采集的属性证据：节点规范$(\boldsymbol{E_1})$，平均资源使用情况$(\boldsymbol{E_2})$，平均响应时间$(\boldsymbol{E_3})$，平均任务成功率$(\boldsymbol{E_4})$，对实体进行基本概率分配，如表 1 所示。

信任结果	$\boldsymbol{E_1}$	$\boldsymbol{E_2}$	$\boldsymbol{E_3}$	$\boldsymbol{E_4}$
$\{\boldsymbol{T}\}$	$\boldsymbol{m_{11}}$	$\boldsymbol{m_{21}}$	$\boldsymbol{m_{31}}$	$\boldsymbol{m_{41}}$
$\{-\boldsymbol{T}\}$	$\boldsymbol{m_{12}}$	$\boldsymbol{m_{22}}$	$\boldsymbol{m_{32}}$	$\boldsymbol{m_{42}}$
$\{\boldsymbol{T},-\boldsymbol{T}\}$	$\boldsymbol{m_{13}}$	$\boldsymbol{m_{23}}$	$\boldsymbol{m_{33}}$	$\boldsymbol{m_{43}}$

表 1 基本概率分配表

识别框架 Θ 下的 4 个信任证据$\{E_1,E_2,E_3,E_4\}$对应的基本概率分配函数分别为m_1，m_2，m_3，m_4。

(2) 基于各证据对应的基本概率分配，运用公式(5)~(12)计算证据的重要性权重$U(m_j)(j=1,2,3,4)$；

(3) 将重要性权重代入公式(13)即可得到修正后的BPA函数，即$\{m_i'(T)，m_i'(-T)，m_i'(T,-T)\}(i=1,2,3,4)$；

(4) 最后根据公式2对属性证据进行合成，从而得到表示云服务商直接信任的信任三元组$\{m(\{-T\})，m(\{-T\})，m(\{T,-T\})\}$。

(5) 利用基于类概率函数的归一化方法计算直接信任值。

由上文所得的信任函数$Bel(A)$和似然函数$Pl(A)$来定义信任的类概率函数，作为信任的非精确性度量。根据可信和不可信事件发生的概率拆分不确定事件的基本可信度，并分配给可信和不可信两种事件，该方法综合考虑了信任关系的可信部分、不可信部分和不确定部分。

定义9 SU和SP之间的直接信任度$D(SU,SP)$计算如下：

$$D(SU,SP)=Bel(T)+\frac{P_1}{P_1+P_2}\times[Pl(T)-Bel(T)] \quad (14)$$

$$P_1=\frac{1-b}{1-b+a} \quad (15)$$

其中，P_1、P_2分别为可信和不可信事件发生的概率，且满足$P_1+P_2=1$，a、b分别是可信和不可信门限值。

该改进方法可以有效地处理证据合成产生的冲突问题，提高了证据冲突时合成结果的可靠性和合理性，可以准确地评估用户间的信任关系；既考虑了信任关系三元组中的每种事件，还能更直观，更贴近信任的真实性。

3.2.2 间接信任

对于云环境中的一些用户，可能没有足够的交互信息来进行直接可信度的评估。因此，用户需要来自其信任的第三方用户的推荐建议。有了这些建议，可以计算云服务商SP的可信度。

定义10 推荐信任　用户SU根据第三方用户SR提供的对实体SP的评价而做出的信任判断。推荐信任也称为间接信任。

用户SU收集其他用户对云服务商SP的评价并且融合这些评价生成推荐信任值。在完成与SP的交易之后，用户将提供它对SP的评价作为其他用户在未来交易中的参考。

$R(SU，SP)$为用户SU对云服务商SP的间接信任度，第三方推荐实体的集合为$RU=\{SR_1，SR_2，\cdots，SR_m\}$，则间接信任度计算方法如下：

$$R(SU，SP)\begin{cases}\frac{\delta}{\gamma+\delta}\sum_{j=1}^{m}D(SC_j，SP)，& m\neq 0\\ 0，& m=0\end{cases} \quad (16)$$

其中，$\frac{\delta}{\gamma+\delta}$表示关于$SP$的反馈可信度，其中$\gamma+\delta=m$，且$\delta$表示所有推荐者中针对云服务商$SP$的积极评分(>0.5)的个数，当$\delta=0$时，即对SP的积极评分个数为0时，我们认为针对服务提供商的推荐信任为0；γ则表示其中的消极评分(<0.5)的个数。推荐信任计算方法是一种轻量级的方法，其中涉及简单的算术运算和技术操作，减轻了系统的运行负载和简化评估方法的复杂度。

3.2.3 综合信任度评估

本文中用户SU对云服务商SP的综合信任度由直接信任度和推荐信任度综合得出，合理分配两者的权重也是综合信任度计算准确性的关键。

因此，综合信任度定义如下：

定义11 设T(SU,SP)表示用户SU对SP的综合信任度：

$$T(SU,SP)=\alpha D(SU,SP)+\beta R(SU,SP) \quad (17)$$

其中α、β分别表示直接信任$D(SU,SP)$和间接信任$R(SU，SP)$的权重，α、β∈[0,1]且α+β=1。

α、β值计算方法如下：

$$\alpha=\frac{n_1^{\frac{3}{2}}}{n_1^{\frac{3}{2}}+n_2}，\ \beta=\frac{n_2}{n_1^{\frac{3}{2}}+n_2} \quad (18)$$

其中，n_1代表用户SU与SP的直接交互次数，n_2代表推荐实体SR对实体SP的推荐次数。

本文提出的信任评估方法很好地解决

了信任的不确定性和模糊性问题。

4. 仿真实验

本节通过仿真实验来考察信任模型信任评估的准确性和抵抗恶意攻击的能力。我们将基于两种不同的指标，即云服务商的信任值和模型的服务失败率来评估本文信任模型的表现。为了方便比较，同时实现了基于贝叶斯的信任模型和 YuBin 信任模型。

实验设计模拟恶意实体在两种行为策略模式下的有效性：(1) 实体先建立信任，然后开始提供恶意服务，称之为静态行为策略模式；(2) 实体在诚实和欺骗行为之间振荡，称之为动态行为策略模式。

三种信任模型的实验场景：系统中有 100 个云服务商，用户将在每个周期中发送四个服务请求；参数设置：$a = 0.65, b = 0.8$。

4.1 信任值的变化分析

我们模拟上述两种行为策略模式下恶意实体的综合信任值。对于动态行为策略模式，该实体在每个周期内改变其行为 3 次。在每个周期中完成所有交互之后，选择和恶意实体有交互经验的诚实实体作为评估实体来计算恶意实体的信任值。信任值变化如图 2、图 3 所示。

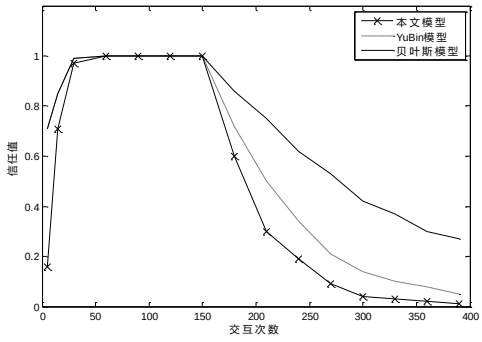

图 2 静态行为策略模式下的信任值变化

静态行为策略模式下恶意实体的信任值变化如图 2 所示。当恶意实体经过一段时间的信任积累后进行恶意欺骗，三种模型的信任值都呈下降趋势。但是与 YuBin 模型和贝叶斯模型相比，我们提出的信任模型可以快速反应实体行为的变化，如果实体的服务资源是恶意的将会很快被发现，但不能通过在短时间内表现良好来提高其信任值。

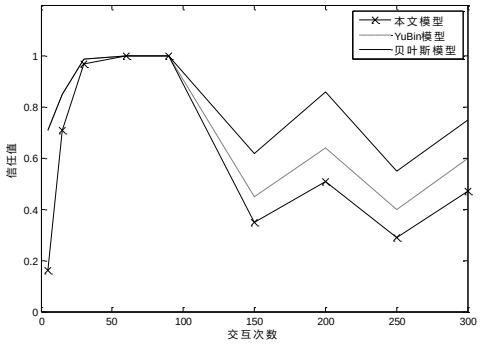

图 3 动态行为策略模式下的信任值变化

动态行为策略模式下恶意实体的信任值变化如图 3 所示。贝叶斯模型对实体服务行为的变化不是很敏感。相比之下，YuBin 模型和我们的信任模型可以快速反应实体服务的变化，但是 YuBin 模型在信任度的下降和提高方面都很敏感。本文模型能够有效地处理实体行为的动态变化。

4.2 抵抗恶意攻击能力分析

服务失败率是指实体获得的恶意服务数量与其获得的所有服务数量的比例。

分析三种信任模型的服务失败率，来比较模型的抗恶意攻击能力。同样，在每个周期中的所有交互完成之后，我们计算信任模型的服务失败率。其中，静态或动态行为策略模式下的恶意实体所占比例为 20%，三种信任模型的服务失败率变化如图 4、5 所示。

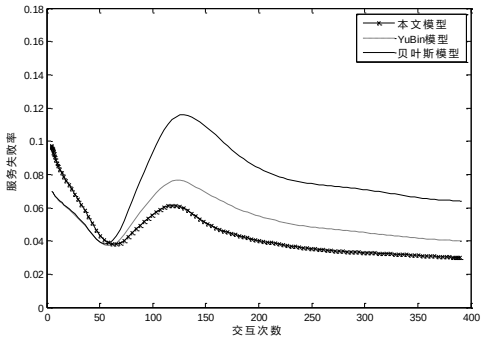

图 4 静态行为策略模式下服务失败率变化

考察静态行为策略模式下的恶意实体，三种模型的服务失败率变化如图 4 所示。这些恶意实体在前期交互建立了声誉，并在随后的交互中对其声誉进行损耗。随着交互次

数的增加，可以逐步识别出恶意实体，因此服务失败率也相应的减小。贝叶斯模型中的信任变化相对快速提升和缓慢下降，不能很好的检测恶意实体的不良行为，因此声誉值会很快的下降，则服务失败率最大。YuBin 模型的信任度提高相对缓慢，因此 YuBin 模型的服务失败率相对较小。本文信任模型对实体行为的变化很敏感，能够快速检测出具有恶意行为的实体并做出一定的惩罚，所以我们的模型的服务失败率是最小的。

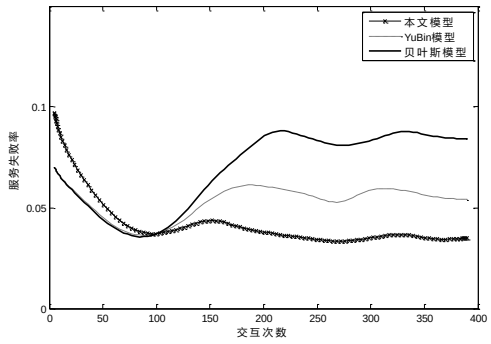

图 5 动态行为策略模式下服务失败率变化

考察动态行为策略模式下的恶意实体，三种模型的服务失败率变化如图 5 所示。贝叶斯模型不能准确有效的检测出恶意实体的不良行为，因此它的服务失败率波动最大，YuBin 模型和本文的模型对实体的恶意服务行为较为敏感，因此可以有效地发现恶意实体的恶意行为，服务失败率的波动相对较小。与 YuBin 模型相比，我们的模型能够有效地处理实体行为的动态变化，因此服务失败率最小，波动越来越小。

5 结语

本文提出了应用于云环境下的基于 D-S 证据理论的多维度信任评估模型，从信任、不信任和不确定三个方面对云服务商的直接信任度进行评估，很好地解决了云计算环境中信任的不确定性和模糊性问题；对传统的证据理论进行改进，并引入归一化算法，得到更为直观真实的直接信任值，同时也给出了简化的间接信任度和综合信任度计算方法，减轻系统负载。仿真实验结果表明，该信任模型能够较为准确有效的对云服务商的信任度做出评估。下一步的研究重点是改善现有的信任模型，扩充证据的维度以及第三方反馈的有效性，并将模型实际应用到云环境中实现其真正的价值。

参考文献

[1] 刘义春, 梁英宏. 基于上下文因素的 P2P 动态信任模型[J]. 通信学报, 2016, 37(8):34-45.

[2] FAN W, YANG S, PERROS H, et al. A multi-dimensional trust-awarecloud service selection mechanism based on evidential reasoning approach[J]. International Journal of Automation and Computing, 2015,12(2): 208-219.

[3] Ding Y, Liu F, Tang B. Context-sensitive trust computing in distributed environments[J]. Knowledge-Based Systems, 2012, 28(2):105-114.

[4] Fan W J, Yang S L, Perros H, et al. A Multi-dimensional Trust-aware Cloud Service Selection Mechanism Based on Evidential Reasoning Approach[J]. International Journal of Automation and Computing, 2015, 12(2):208-219.

[5] Yang B, Yamamoto R, Tanaka Y. Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs[C]// International Conference on Advanced Communication Technology. IEEE, 2013:223-232.

[6] 赵秋月, 左万利, 田中生,等. 一种基于改进 D-S 证据理论的信任关系强度评估方法研究[J]. 计算机学报, 2014(4):873-883.

[7] Li X, Zhou F, Yang X. A multi-dimensional trust evaluation model for large-scale P2P computing[M]. Academic Press, Inc. 2011.

[8] Choulakian V, Simonetti B, Gia T P. Some new aspects of taxicab correspondence analysis[J].Statistical Methods & Applications, 2014, 23(3):401-416.

[9] Jiang W, Li Q, Chen W. A Multi-dimensional Evidence-based Trust Evaluation Model and Algorithm[J]. International Journal of Security & Its Applications, 2015, 9(5):123-132.

[10] Wu X, Zhang R, Zeng B, et al. A Trust Evaluation Model for Cloud Computing[J]. Procedia Computer Science, 2013, 17:1170-1177.

[11] 费翔, 周健. 一种处理冲突证据的 D-S 证据权重计算方法[J]. 计算机工程, 2016, 42(2):142-145.

[12] 丁海洋, 李席广, 拱长青. 云计算环境下的信任评估模型[J]. 计算机工程与设计, 2016, 37(8):2007-2010.

作者简介：吴旭，女，博士，副教授，研究方向：可信计算、 普适计算、云计算和信任管理等.

王杨，女，硕士研究生，研究方向：云计算和信任管理.

袁耀，男，硕士研究生，研究方向：云计算和信任管理.

作者联系方式

通信地址：陕西省西安市雁塔区长安南路 563 号西安邮电大学

邮政编码：710061
联系电话：15229252819
电子邮件：wyfairy93@163.com