面向云计算基于双层激励和欺骗检测的信任模型

谢晓兰*①② 刘 亮① 赵 鹏①
①(桂林理工大学信息科学与工程学院 桂林 541004)
②(广西空间信息与测绘重点实验室 桂林 541004)

摘 要：针对云计算环境下存在的信任问题，该文提出基于双层激励和欺骗检测的信任模型(CCIDTM)。该模型提出了一组云计算服务属性评价指标，引入了信任度随时间衰减的动态信任机制，建立了对服务提供商服务行为和用户评价行为的双层激励机制，提出了一个共谋欺骗检测算法，提高了模型的动态适应性和评价的综合性。实验结果表明，与已有信任模型相比，该模型评估的结果更接近服务提供商的真实服务行为，能够有效地抵抗各种恶意行为的攻击，表现出良好的鲁棒性。

关键词：云计算信任；双层激励；欺骗检测；信任模型
中图分类号：TP311 **文献标识码**： A **文章编号**：1009-5896(2012)04-0812-06
DOI: 10.3724/SP.J.1146.2011.00787

Trust Model Based on Double Incentive and Deception Detection for Cloud Computing

Xie Xiao-lan①② Liu Liang① Zhao Peng①
①(*Institute of Information Science and Engineering*, *Guilin University of Technology*, *Guilin* 541004, *China*)
②(*Guangxi Key Laboratory of Spatial Information and Geomatics*, *Guilin* 541004, *China*)

Abstract: Considering at the trust problem existing in cloud computing environment, a double incentive based on trust and deception detection model CCIDTM (Cloud Computing Incentive and Detection Trust Model) is proposed. The model proposes a set of cloud computing services property evaluation, introducing a dynamic mechanism of trust decaying over time, establishing a double incentive mechanism about service behavior of service providers as well as users' evaluate behavior. An algorithm of conspiracy to deceive group testing which improves the model of dynamic adaptation and evaluation of comprehensive is also proposed. Experiment results show that the model results of the assessment service providers closed to the true service behavior. Thus it can effectively resist the attacks of malicious behavior, showing a good robustness compared with the existing trust model.

Key words: Cloud computing trust; Double incentive; Deception detection; Trust model

1 引言

随着互联网的发展和网络经济的繁荣，Web2.0 的到来，并行计算、网格计算、P2P 计算的发展和融合，一种新的计算模式——云计算应运而生。不少公司和企业想到使用云计算来实现以较低成本和较高性能解决海量信息存储和大规模计算问题的愿望。在云计算环境里，由于虚拟化技术的使用，用户担心有的服务提供商受商业利益的驱使在服务交易过程中存在欺骗行为，而云计算中心又没有信任认证的相关服务，导致一些用户上当受骗，从而引发信任危机。

文献[1]中把受保护对象为服务提供商，潜在的恶意攻击来自用户的安全机制称为“硬安全”，把身份验证和访问控制归为硬安全的范畴；把受保护对象为用户，潜在的恶意攻击来自服务提供商的信任安全机制称为“软安全”，把包含信任和信誉评估归为“软安全”的范畴。云计算的硬安全已经被大规模应用的云计算先驱 Google 和 Amazon 所证明，在此背景下云计算的软安全，成了用户关注的焦点，因此研究一个面向云计算的信任模型既有一定的理论意义，又具有一定的实际价值。

关于信任模型的研究，国内外许多专家学者针对特定研究领域，采用不同的方法和工具，提出了一些信任模型。文献[2]提出了一个基于贝叶斯网络的信任模型，文献[3]提出了一个基于全局信任信息的信任模型 EigenRep，文献[4]提出了一个基于模糊

2011-07-29 收到，2011-12-26 改回
广西空间信息与测绘重点实验室建设基金(1103108-25)，国家自然科学基金(41071294)和桂林理工大学博士基金资助课题
*通信作者：谢晓兰 xie_xiao_lan@foxmail.com

逻辑的信任模型，文献[5]提出了一个基于权重的动态信任模型等等。

但已有信任模型仍然存在一些问题：(1)信任度计算的因素考虑不全。没有考虑交易时间、交易次数、交易背景以及历史信任等因素。(2)没有对服务提供商服务行为和用户评价行为建立激励机制。有的信任模型对推荐信任度不同的用户评价不加区别地计入信任度计算，导致模型难以识别恶意评价。

针对上述文献中所存在的不足，本文提出了一组云计算服务属性评价指标，引入了信任度随时间衰减的动态信任机制[6]，建立了对服务提供商服务行为和用户评价行为的双层激励机制，提出了一个共谋欺骗检测算法，提高了模型的动态适应性和评价的综合性。结果表明，该模型评估的结果更接近服务提供商的真实服务行为，能够有效地抵抗各种恶意行为的攻击，表现出良好的鲁棒性。

2　基于双层激励和欺骗检测的信任模型 CCIDTM(Cloud Computing Incentive and Detection Trust Model)

2.1 模型的定义及相关表示

信任到目前还没有形成统一的定义，目前最常用的是 ITU-T 标准的 x.509 规范：实体 A 认定实体 B 将严格按实体 A 期望的方式行动，则实体 A 信任实体 B。根据对其的理解，本文对信任定义如下：

定义 1　信任：在给定背景和时段中，信任实体对被信任实体某一服务属性在诚信性、安全性、可靠性等方面的主观肯定。信任也称为可信。

定义 2　面向云计算的动态信任模型用五元组表示 CCIDTM(A,W,T,V,F)，其中 A 表示服务属性集合，W 表示服务属性权重，T 表示交易时间，V 表示交易额，F 为交易次数。

定义 3　直接信任度：实体 i 根据与实体 j 的直接交易情况对其的信任度，用 $\mathrm{DT}_{i,j}$ 表示。

定义 4　推荐信任度：实体 i 对实体 j 所作服务评价的信任度，用 $\mathrm{RT}_{i,j}$ 表示。

定义 5　信誉度：所有与实体 j 进行交易的实体 j_r 对实体 j 直接信任度的聚合，用 R_j 表示。

定义 6　综合信任度：实体 i 综合对实体 j 的直接信任度和实体 j 本身的信誉度而得出的信任度，用 $\mathrm{CT}_{i,j}$ 表示。

2.2 模型的设计

根据模型的定义，将模型划分为 5 个子模块：服务评价计算、直接信任度计算、推荐信任度计算、信誉度计算以及综合信任度。

2.2.1 服务评价计算子模块设计　考虑到服务请求的多样性，选取服务属性评价指标为：服务效率、可靠性、安全性、可维护性、服务等级协议(SLA)、满意度。

引入服务属性权重因子来衡量服务属性相对服务评价的重要程度[7]。设第 l 种服务属性的权重因子为 W_l，满足条件：$0 \le W_l \le 1, \sum_{l=1}^{n} W_l = 1$。这里采用模糊数学的方法来确定服务属性的权重。

基于模糊逻辑的服务属性权重确定方法如下：

(1)建立服务属性集 $A=(A_1,A_2,\cdots,A_n)$，服务属性的 6 个评价指标分别为：服务效率、可靠性、安全性、可维护性、服务等级协议、满意度。

(2)建立服务属性等级集 $D=(D_1,D_2,\cdots,D_m)$，服务等级分别为：优秀、良好、中等、一般、较差、差。

(3)对服务属性根据服务属性等级进行模糊评判，得到模糊评判矩阵 $\boldsymbol{E}=(E_{ij})_{n\times m}$，综合评判结果集 $C=W\circ E=(C_1,C_2,\cdots,C_n)$，服务属性权重备选集 $\beta=(\beta_1,\beta_2,\cdots,\beta_n)$，求出 $\sim C_l=\beta_l\circ R$，按式(1)计算。

$$\sigma(\sim C_l,C)=\frac{\sum_{k=1}^{n}(\sim C_l(x_k)\wedge C(x_k))}{\sum_{k=1}^{n}(\sim C_l(x_k)\vee C(x_k))} \tag{1}$$

(4)最佳权重分配方案为 $\sigma(\sim C_l,\ C)=\max\limits_{1\le j\le m}\{\sigma(\sim C_j,C)\}$，得出最佳服务属性权重集 β_l，这里取 $W=\beta_l=(W_1,W_2,\cdots,W_n)$。服务评价的计算方法如下：

$$\mathrm{SE}_k=\sum_{l=1}^{n} W_l^k A_l^k \tag{2}$$

2.2.2 直接信任度计算子模块设计　根据距离当前时刻越近的服务评价越能反映近期服务行为，引入时间衰减因子的概念。

定义 7　时间衰减因子：用户实体 i 与服务提供实体 j 当前交易周期(第 $s+1$ 个周期)进行第 l 次交易位于第 k 个时段相对于当前时段(第 r 个时段)的衰减程度，用 TD_r^l 表示。

时间衰减因子的计算方法如下：

$$\mathrm{TD}_l^{s+1}=1-\rho^{(r-k)/\eta} \tag{3}$$

$\rho(0\le\rho\le1)$ 为衰减速率因子，η 为调节因子，随时段大小进行调节。

设当前交易周期第 l 次交易的交易额为 $v_{i,j,l}^{s+1}$，进行 $f_{i,j,l}^{s+1}$ 次交易，当前直接信任度为 $dt_{i,j,f_{i,j}^{s+1}}^{s+1}$，其计算方法如下：

$$dt_{i,j,f_{i,j}^{s+1}}^{s+1}=\varphi(f_{i,j}^{s+1})\sum_{l=1}^{f_{i,j}^{s+1}}\mathrm{TD}_{i,j,l}^{s+1}\mathrm{SE}_{i,j,l}^{s+1}\psi(v_{i,j,l}^{s+1}) \tag{4}$$

$\varphi(f_{i,j}^{s+1})=\sqrt{\dfrac{f_{i,j}^{s+1}}{f_{i,j}^{s+1}+1}}$ 为交易次数因子，反映当前交易周期交易次数越多，做出的服务评价越准确。$\psi(v_{i,j,l}^{s+1})=\exp\left(-\dfrac{1}{v_{i,j,l}^{s+1}}\right)$ 为交易额因子，反映交易额越大用户实体 i 就越有理由信任服务提供实体 j。

当前交易周期累计直接信任度 $\mathrm{DT}_{i,j}^{s+1}$ 的计算方法如下：

$$\mathrm{DT}_{i,j}^{s+1}=\begin{cases}(1-\mu)dt_{i,j,f_{i,j}^{s+1}}^{s+1}, & s=0\\ \mu\mathrm{DT}_{i,j}^{s}+(1-\mu)dt_{i,j,f_{i,j}^{s+1}}^{s+1}+\delta_{i,j}^{s+1}, & s>0\end{cases}\tag{5}$$

$\delta_{i,j}^{s+1}$ 为奖惩因子，其计算方法如下：

$$\delta_{i,j}^{s+1}=\begin{cases}\varphi(f_{i,j}^{s+1})(\overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}}), \overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}}<0\\ \varphi^2(f_{i,j}^{s+1})(\overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}}), \overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}}\ge 0\end{cases}\tag{6}$$

当 $\overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}}<0$ 时，表明当前交易周期服务质量下降了，作为惩罚用户实体 i 对服务提供实体 j 的当前直接信任度减小一个较大的值 $\varphi(f_{i,j}^{s+1})\cdot(\overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}})$。反之表明，当前交易周期的服务质量提高了，作为奖励用户实体 i 对服务提供实体 j 的当前直接信任度增大一个较小的值 $\varphi^2(f_{i,j}^{s+1})(\overline{\mathrm{SE}_{i,j}^{s+1}}-\overline{\mathrm{SE}_{i,j}^{s}})$，这样可以有效地激励服务提供实体提高服务质量。

μ 为历史遗忘因子，其计算方法如下：

$$\mu=\begin{cases}1-\alpha, & \mathrm{DT}_{i,j}^{s}<\varepsilon\\ 1-\beta, & \mathrm{DT}_{i,j}^{s}\ge\varepsilon\text{且}v_{i,j}^{s+1}<\xi\\ 1-\gamma, & \mathrm{DT}_{i,j}^{s}\ge\varepsilon\text{且}v_{i,j}^{s+1}\ge\xi\end{cases}\tag{7}$$

其中 $0<\alpha<\beta<\gamma<1$，ε 为初始直接信任度阈值，ξ 为当前交易周期交易额阈值。

2.2.3 推荐信任度计算子模块设计 用户在进行服务评价时更愿意相信那些与他们具有相同交易对象并且持相同或相近评价用户所给的服务评价，引入评价相似度的概念[8]。

定义 8 评价相似度：用户实体 i 和 j 针对共同的服务提供实体集 $p_1,p_2,\cdots,p_m$ 所作服务评价的相似程度，用 $S_{i,j}$ 表示。

设当前交易周期与用户实体 i 和 j 的评价相似度为 $S_{i,j}^{s+1}$，其计算方法如下：

$$S_{i,j}^{s+1}=1-\sqrt{\sum_{l=1}^{m}\left(\overline{\mathrm{SE}_{i,p_l}^{s+1}}-\overline{\mathrm{SE}_{j,p_l}^{s+1}}\right)^2}\Big/m\tag{8}$$

$\overline{\mathrm{SE}_{i,p_l}^{s+1}}$ 和 $\overline{\mathrm{SE}_{j,p_l}^{s+1}}$ 分别表示用户实体 i 和 j 对服务提供实体 p_l 的累计平均服务评价。

用户实体 i 对 j 的推荐信任度 $\mathrm{RT}_{i,j}^{s+1}$ 可以通过其评价相似度得到，其计算方法如下：

$$\mathrm{RT}_{i,j}^{s+1}=S_{i,j}^{s+1}+\sigma_{i,j}^{s+1}\tag{9}$$

$\sigma_{i,j}^{s+1}$ 为奖罚因子，其计算方法如下：

$$\sigma_{i,j}^{s+1}=\begin{cases}\dfrac{1-S_{i,j}^{s+1}}{2}\times\dfrac{\theta-(1-S_{i,j}^{s+1})}{\theta}, & 0<\theta<S_{i,j}^{s+1}\le 1\\ -\dfrac{S_{i,j}^{s+1}}{2}\times\dfrac{(1-S_{i,j}^{s+1})-\theta}{1-S_{i,j}^{s+1}}, & 0<S_{i,j}^{s+1}<\theta<1\end{cases}\tag{10}$$

设当前交易周期与用户实体 j 存在推荐信任关系的用户实体集为 $u_1,u_2,\cdots,u_n$，则实体 j 的综合推荐信任度为 RT_{j}^{s+1}，其计算方法如下：

$$\mathrm{RT}_{j}^{s+1}=\psi(n)\sum_{l=1}^{n}\mathrm{RT}_{u_l,j}^{s+1}\Big/n\tag{11}$$

$\psi(n)=e^{-1/n}$，用来调节推荐实体数量对推荐信任度的影响。

2.2.4 信誉度计算子模块设计 设当前交易周期与服务提供实体 j 有交易行为的用户实体集 $j_1,j_2,\cdots,j_n$，则服务提供实体 j 的信誉度为 r_j^{s+1}，其计算方法如下：

$$r_j^{s+1}=\varphi(n,F_j^{s+1})\sum_{l=1}^{n}\mathrm{RT}_{j_l}^{s+1}\mathrm{DT}_{j_l,j}^{s+1}\psi(v_{j_l,j}^{s+1})\Big/n\tag{12}$$

$\varphi(n,F_j^{s+1})=\exp\left(-1/(n\times F_j^{s+1})\right)$ 为交易规模因子，反映与服务提供实体 j 交易的用户实体数量越多且交易次数越多，其信誉度就越有说服力。

$\psi(v_{j_l,j}^{s+1})=\exp\left(-\dfrac{1}{v_{j_l,j}^{s+1}}\right)$ 为交易额因子，反映与服务提供实体 j 进行交易的交易额越大，实体 i 就越有理由信任服务提供实体 j。

当前交易周期累计信誉度 R_j^{s+1} 的计算方法如下：

$$R_j^{s+1}=\begin{cases}(1-\mu)R_j^{s+1}, & s=0\\ \mu R_{i,j}^{s}+(1-\mu)r_j^{s+1}, & s>0\end{cases}\tag{13}$$

μ' 为历史遗忘因子，其计算方法如下：

$$\mu'=\begin{cases}1-\alpha', & R_{i,j}^{s}<\varepsilon'\\ 1-\beta', & R_{i,j}^{s}\ge\varepsilon'\text{且}v_j^{s+1}<\xi'\\ 1-\gamma', & R_{i,j}^{s}\ge\varepsilon'\text{且 }v_j^{s+1}\ge\xi'\end{cases}\tag{14}$$

其中 $0<\alpha'<\beta'<\gamma'<1$，$\varepsilon'$ 为初始信誉度阈值，ξ' 为当前交易周期交易额阈值。

2.2.5 综合推荐信任度计算子模块设计 设当前交易周期用户实体 i 对服务提供实体 j 的累计直接信任度为 $\mathrm{DT}_{i,j}^{s+1}$，累计信誉度为 R_j^{s+1}，则综合信任度 $\mathrm{CT}_{i,j}^{s+1}$，其计算方法如下：

$$\mathrm{CT}_{i,j}^{s+1}=\lambda_{s+1}\mathrm{DT}_{i,j}^{s+1}+(1-\lambda_{s+1})R_j^{s+1}\tag{15}$$

λ_{s+1} 为自信因子，其计算方法如下：

$$\lambda_{s+1}=\begin{cases}\lambda_s-\alpha'', & \left|R_j^{s+1}-\mathrm{CT}_{i,j}^{s}\right|<\Delta\\ \lambda_s-\beta'', & \left|R_j^{s+1}-\mathrm{CT}_{i,j}^{s}\right|>\Delta(\mathrm{Honest})\\ \lambda_s-\gamma'', & \left|R_j^{s+1}-\mathrm{CT}_{i,j}^{s}\right|>\Delta(\mathrm{Fraud})\end{cases}\quad(16)$$

在用户实体 i 与服务提供实体 j 没有进行服务交易前，$\lambda_0=0$。$0<\alpha''<\beta''<\gamma''<1$，$\alpha''$，$\beta''$ 为自信因子减小的辐度，γ'' 为自信因子增加的辐度，Δ 为信誉度波动阈值。

当 $|R_{i,j}^{s+1}-\mathrm{CT}_{i,j}^{s}|>\Delta$ 时，反映当前交易周期服务提供实体 j 的信誉度表现出较大辐度的变化，需要进行共谋欺骗检测，经过检测如果这种变化不是由共谋欺骗行为引起的，那么用户实体 i 应该较大辐度地减小自信因子的值。反之，用户实体 i 应该较大辐度地提高自信因子的值。

根据共谋团体在进行服务评价时存在很大相似性的特点，于是设计了基于相似评价的共谋欺骗检测算法[9]，具体步骤如下：

(1)初始化评价类。为每一个用户实体设立标志变量，用于区分是否进行归类。创建第 1 个评价类，将第 1 个用户实体添加到该类中。

(2)进行归类操作。如果标志变量flag(l)=1，说明已归类；如果标志变量flag(l)=0，说明尚未归类，先将标志变量flag(l)置为1，然后按照从小到大的顺序与已分类的用户实体依次比较，如果 $S(l,k)$ 大于评价相似度阈值 ∂，则认为用户实体 l 的评价和该类相似，将其添加到该类中。反之，则认为用户实体 l 的评价和该类的第 k 个用户实体不相似，继续比较第 $k+1$ 个用户实体。如果与该类用户实体的评价相似度都小于相似度阈值 ∂，则与下一个评价类的用户实体评价相似度进行比较，如果与已有评价类的所有用户实体的评价相似度都小于相似度阈值 ∂，则创建一个新的评价类，并将其添加到该类中。

(3)共谋欺骗团体的判定。如果某个评价类的用户实体个数大于类规模阈值 ∂，则认为该评价类为一个共谋欺骗团体。

根据上文的分析和设计，共谋欺骗检测的算法实现如表 1 所示。

表1 共谋欺骗检测算法的实现

```
Algorithm 2.2.5: Conspiracy_Fraud_Detection Algorithm
Algorithm: Conspiracy_Fraud_Detection (S(i, j), Fraud)
Input: i, j, S(i, j), n
Output: Fraud
begin
for i ← 1 to n //为每一个用户实体建立 1 个标志变量，并对其初始化
    flag(l) ← 0
endfor
    Creat new class //建立第 1 个评价类
    flag(1) ← 1
    Subclass_account ← 1
    Insert(1 , Class(Subclass_account)) //将第 1 个用户实体插入到该类中
    Number(Subclass_account) ← 1 //该类的数量增加 1
for l ← 2 to n
  if(flag(l) == 0) //如果第 l 个用户实体还没有归类，则将标志变量置为 1
    then flag(1) ← 1
    for j ← 1 to Subclass_account
      for k ← 1 to Number(Subclass_account)
      if(S(l, k) > ∂)
        then Insert (l, Class(Subclass_account))
        Num(Subclass_account) ← Num(Subclass_account) + 1
      endif
  endfor
  Subclass_account ← Subclass_account + 1
  Number(Subclass_account) ← 1
  Insert (l, Class(Subclass_account))
endfor
for j ← 1 to Subclass_account
      if Number(Subclass_account) > Δ′
        then Fraud ← Fraud + 1
endfor
Return Fraud
end
```

2.3 模型的基本框架

本文参照面向服务的体系结构(SOA)架构模式提出一种面向云计算的信任评估模型。该模型包括 3 个角色：用户实体、服务提供实体、服务注册中心，同时增加信任评估的机构——云计算信任评估中心 CCTEE，模型的基本框架如图 1 所示[10]。

具体描述如下：

(1)在服务注册中心注册的每一个服务提供实

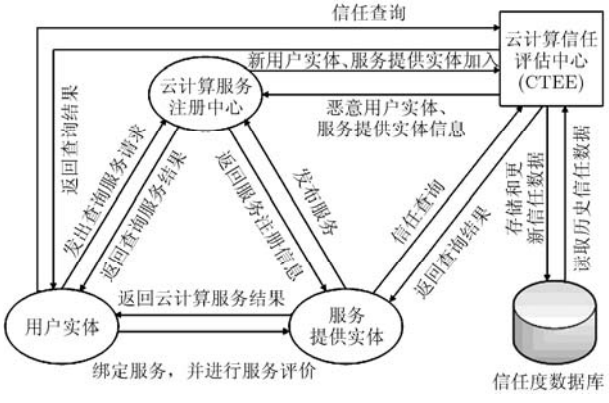

图 1 面向云计算的信任评估模型 CCETrust 的基本框架

体节点，注册中心都会分配一个初始直接信任度，该直接信任度在每次交易完成后实现更新。

(2)用户实体在提出服务请求前，信任评估中心提供服务提供实体的信誉度、用户实体对其的直接信任度及该服务提供实体的交易情况，如果综合信任度大于信任度阈值，才接受用户实体对服务提供实体提出的服务请求。

(3)每次交易完成后，用户实体给出相应的服务评价，云计算信任评估中心根据信任度计算公式更新对该服务提供实体的直接信任度、信誉度。

(4)如果用户实体对已经使用过的服务，可以根据其直接信任度和该服务提供实体的信誉度来计算服务提供实体的综合信任度。

3 实验仿真与分析

为了验证模型的有效性，本文采用 Stanford 大学开发的 Query Cycle Simulator 构建仿真实验平台，在此平台上进行仿真实验。仿真实验设置实体总数为 1000 个，下载文件为 10000 个，查询周期为 100。为了检测模型的有效性，在此环境下选取实体总数 10%到 50%的诽谤恶意实体和共谋欺骗攻击实体分别作为攻击者用以和 EigenTrust 模型作对比。EigenTrust 模型[11]是由 Stanford 大学针对 P2P 网络下的信任问题，提出的一种管理信誉度的算法。

如图 2 所示，EigenTrust 和 CCIDTM 模型的文件下载服务(STR)在诽谤恶意实体(DM)比例较小时，相差不大，但随着诽谤恶意实体(DM)比例地扩大，CCIDTM 模型显示较大的优势，这是因为 CCIDTM 模型引入了服务评价相似度的概念，对于服务评价相似度低于给定阈值的实体节点所给评价其推荐信任度本来较低还要接受降低地惩罚，使得 CCIDTM 模型能有效地抵抗诽谤恶意实体(DM)的攻击，即使在恶意实体节点比例达到 0.5 时，也能具有较高的 STR。对诽谤恶意实体攻击起到了一定地遏制作用，显示出模型的健壮性。

如图 3 所示，EigenTrust 和 CCIDTM 模型在共谋恶意实体(CM)的攻击下的文件下载服务 STR 的对比图。在 CCIDTM 模型中，虽然共谋恶意实体(CM)节点相互夸大该团体内部实体节点的评价，但是少量的夸大评价对实体节点的信誉度影响较小，因为信誉度的计算不仅和评价有关还与交易的次数有关，少量的夸大评价对实体节点的信誉度影响较小，同时共谋欺骗检测算法也可以将共谋团体检测出来，提高了实体节点的辨别能力，从而可以保持较高的 STR。EigenTrust 模型因为无法正确区分共谋恶意实体(CM)，导致 STR 的下降。

4 结束语

本文所提出的动态信任模型是面向云计算环境的，同时也广泛适用于各种分布式环境。该信任模型综合考虑了直接信任和推荐信任两种信任关系，提出了一组云计算服务属性评价指标，进行了模块的划分，对各个模块进行了详细的设计，通过引入一系列影响因子，使得所做出的评价更加科学合理。仿真实验结果表明，该模型相比其他信任评估模型能更加准确地评估实体的信任度，能有效地抵抗各种恶意攻击行为，显示出较强的健壮性。

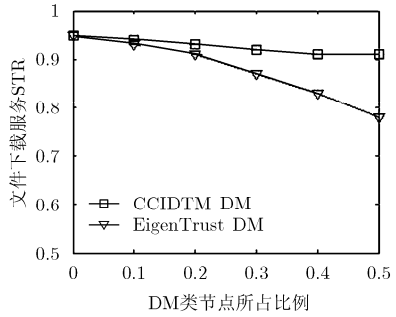

图 2 DM 类节点攻击下的文件下载服务 STR

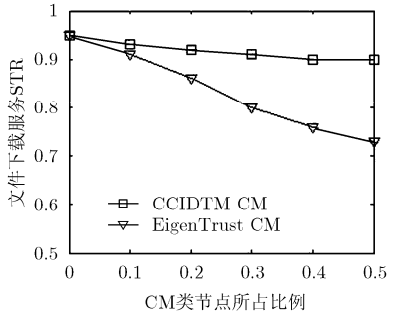

图 3 CM 类节点攻击下的文件下载服务 STR

参 考 文 献

[1] 马杰. 网络安全威胁态势评估与分析方法研究[D]. [博士论文], 华中科技大学, 2007.
Ma Jie. Research on network security threat situation assessment and analysis [D]. [Ph.D. dissertation], Huazhong University of Science and Technology, 2007.

[2] Wang Y and Vassileva J. Trust and reputation model in peer-to-peer networks[C]. Proceedings of the 3rd International Conference on Peer-to-Peer Computing, Washington, DC, USA, 2003: 150–157.

[3] Kamvar S D, Sehlosser M T, and Molina H G. The eigentrust algorithm for reputation management in P2P networks[C]. Proceedings of the 12th International Conference on World Wide Web ACM, Budapest: ACM Press, 2003: 640–651.

[4] 唐文, 胡建斌, 陈钟. 基于模糊逻辑的主观信任管理模型研究[J]. 计算机研究与发展, 2005, 42(10): 1654–1659.
Tang Wen, Hu Jian-bin, and Chen Zhong. Research on a fuzzy logic-based subjective trust management model [J]. *Journal of Computer Research and Development*, 2005, 42(10): 1654–1659.

[5] 王涛春, 罗永龙, 左开中, 等. P2P 网络中基于权重的动态信任模型[J]. 计算机应用研究, 2011, 28(1): 300–303.
Wang Tao-chun, Luo Yong-long, Zuo Kai-zhong, et al.. Dynamic trust model based on trade weight for P2P network [J]. *Application Research of Computers*, 2011, 28(1): 300–303.

[6] 常俊胜, 王怀民, 尹刚. DyTrust: 一种 P2P 系统中基于时间的动态信任模型[J]. 计算机学报, 2006, 29(8): 1301–1307.
Chang Jun-sheng, Wang Huai-min, and Yin Gang. DyTrust: a time-frame based dynamic trust model for P2P systems [J]. *Chinese Journal of Computers*, 2006, 29(8): 1301–1307.

[7] 李景涛, 荆一楠, 肖晓春, 等. 基于相似度加权推荐的 P2P 环境下的信任模型[J]. 软件学报, 2007, 18(1): 157–167.
Li Jing-tao, Jing Yi-nan, Xiao Xiao-chun, *et al.*. A trust model based on similarity-weighted recommendation for P2P environments [J]. *Journal of Software*, 2007, 18(1): 157–167.

[8] 詹涛, 周兴社, 杨刚. 基于相似度的分布式信任模型[J]. 西北工业大学学报, 2010, 28(1): 67–71.
Zhan Tao, Zhou Xing-she, and Yang Gang. An effective similarity based trustModel in open distributed system [J]. *Journal of Northwestern Polytechnical University*, 2010, 28(1): 67–71.

[9] 王进, 孙怀江. 一种用于信任管理的新主观逻辑[J]. 计算机研究与发展, 2010, 47(1): 140–146.
Wang Jin and Sun Huai-jiang. A novel subjective logic for trust management [J]. *Journal of Computer Research and Development*, 2010, 47(1): 140–146.

[10] 李明楚, 杨彬, 钟炜, 等. 基于反馈机制的网格动态授权新模型[J]. 计算机学报, 2009, 32(11): 2187–2199.
Li Ming-chu, Yang Bin, Zhong Wei, *et al.*. Grid dynamic authorization model based on feedback mechanism[J]. *Chinese Journal of Computers*, 2009, 32(11): 2187–2199.

[11] Stanford University. EigenTrust Algorithm. http://p2p.stanford. edu/www/projects.htm, 2010.

谢晓兰：　女，1974 年生，博士，副教授，硕士生导师，研究方向为网格计算、云计算.

刘　亮：　男，1982 年生，硕士，研究方向为云计算、计算机网络.

赵　鹏：　男，1986 年生，硕士，研究方向为网格计算、云计算.