一种多参量评估的云计算信任模型

王 君 刘文芬 郜 燕
(信息工程大学 郑州 450001)
(信息工程大学数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 针对云计算环境下服务商的信任问题,提出了一种新的云计算信任模型。模型旨在帮助用户从大量云服务商中选择最安全的资源,信任评估考虑了云服务过程中资源的可用性、可靠性、数据完整性、诚信度和周转效率 5 个参量,5 个参量利用主观评价和客观数据对服务商进行全面评估。模型还运用了贝叶斯统计、时间衰减函数等方法对海量数据进行动态分析,使得统计结果可以及时地反映服务质量。由于不同用户对每个参量的倚重程度不同,因此结合层次分析法中权重向量的构造方法对各信任分量的权值进行分配,以满足个体用户的特殊需求。仿真实验进一步验证了该模型能够抵御较复杂的策略攻击并且具有一定的实用性。

关键词 云计算,信任评估,服务商选择
中图法分类号 TP393 文献标识码 A

Trust Model of Cloud Computing Based on Multi-parameters Evaluation

WANG Jun LIU Wen-fen GAO Yan
(PLA Information Engineering University, Zhengzhou 450001, China)
(State Key Laboratory of Engineering Mathematics and Advanced Computing, Zhengzhou 450001, China)

Abstract A novel trust model was put forward to solve the trust problem of cloud resource providers. In order to help users select the safest resource in a large number of providers, trust evaluation considered five parameters in cloud service process: availability, reliability, data integrity, honesty and turnaround efficiency. These parameters make a comprehensive assessment on the resource providers with subjective evaluation and objective data. The model achieves dynamic analysis of massive data by using some methods, such as Bayesian statistics and time attenuation function, and the statistical result can reflect the quality of service in time. Due to the different degree of users relying on each parameter, the model distributes the weight value of trust factor combining the way of constructing weight vector in analytic hierarchy process (AHP) to meet the special need of individual users. The result of simulation experiment verifies the model can resist strategic attack with certain practicality.

Keywords Cloud computing, Trust evaluation, Selection of resource provider

1 引言

云计算是融合了虚拟化、Web2.0 等技术,由并行计算、网格计算、P2P 计算等发展而来的一种新的计算模式。云计算体现了“网络就是计算机”的理念,将大量的计算资源、存储资源和软件资源链接成巨大规模的共享虚拟资源池,凭借便利、经济、高可扩展性的特点在 IT 产业界得到了广泛的应用[1],Amazon、Google、IBM、Microsoft 等 IT 巨头已开始对外提供云计算服务。信任是云计算在商业领域应用的关键技术,也是其面临的巨大挑战:用户由于对云服务供应商缺乏足够了解而担忧交易过程中会存在欺诈行为。在提供服务之前,用户与供应商关于服务质量 QoS(Quality of Service)签署一份服务等级协议 SLA(Service Level Agreement),QoS 包含如下 5 个方面:周转时间、服务费用、安全等级、计算能力(处理器速度、内存大小和硬盘容量)、网络速度(带宽和缓冲时间)[2]。因此需要一套高效简洁的算法对所承诺服务质量的完成情况以及其他服务参量进行实时分析和评估,为用户的决策增加可靠的依据,还要求建立相应的信任管理系统来应用此模型。

2 相关工作

1996 年,Blaze 为解决网络服务的安全问题提出了信任管理的概念,信任模型的研究也逐渐成为信息安全领域中的热点。在计算机科学中,信任的定义可以如此表述:当实体 A 假定实体 B 严格地按 A 所期望的那样行动,则 A 信任 B[3],本文中信任度的取值范围为[0,1]上的连续值。最初的信任关系通过实体间的直接交互而来;信任也存在反馈关系,若两实体没有直接交互则只能通过其他实体提供的反馈信息来参

本文受国家 973 计划项目子课题(2012CB315905):可重构基础网络的安全和管控机理与结构资助。
王 君(1990—),男,硕士生,主要研究方向为概率论在网络安全中的应用;刘文芬(1965—),女,博士生导师,主要研究方向为概率统计理论及应用;郜 燕(1986—),女,博士生,主要研究方向为信息安全。

考,还要对反馈信息的可信度进行评估。文献[4]利用概率统计方法计算直接信任和推荐信任,通过区分直接经验的重要程度判断反馈信息的可信度从而提高了信任评估的有效性,抑制了复杂的协同作弊攻击。信任还具有动态性和衰减性,文献[5]在信任计算中通过近期信任、长期信任、累积滥用信任等参数提高了模型的动态适应能力;文献[6]将历史交互窗口引入到了信任评估中,提出了基于交互感知的动态自适应信任模型,这些方法都有效地提高了信任评估的准确性。在信任模型的量化研究中,国内外专家学者将诸多数学方法如贝叶斯统计推断[7]、主观逻辑理论[8]、熵理论[9]、模糊理论[10]等作为工具应用到不同的网络环境中。然而,不同的应用环境对信任评估提出了不同的需求,现有模型都是针对特定的应用背景提出来的,各环境的模型之间不具备通用性。

针对云计算环境下的服务商选择问题,文献[11]设计了一种基于信任生成树的云服务组织方法,形成提供相似服务功能的云服务集合,将恶意和虚假的服务排除在信任生成树之外;文献[12]建立了对服务提供商和用户评价的双层激励机制,设计了一个共谋欺骗检测算法从而提高了评价的综合性;文献[13]提出了 QoS 偏好感知算法 QoPA 用来处理个体服务质量敏感的约束条件,并通过基于模糊综合评判的副本选择算法 FCE—RS 进行综合评价,最终得出 QoS 满意度最高的服务商。同时,一些云计算环境下的信任管理系统架构也相继提出[2,14,15]。本模型则是针对云资源服务的特点从一类新的角度对信任进行评估。

3 云计算信任模型

3.1 模型结构框架

本文提出的云计算信任模型如图 1 所示,由用户界面、云服务目录、中心系统、信任管理中心、监测系统、SLA 代理以及云服务提供商组成,其中云服务包括基础设施服务(Infrastructure as a Service,Iaas)、平台服务(Platform as a Service,Paas)和软件服务(Software as a Service,Saas)3 层。

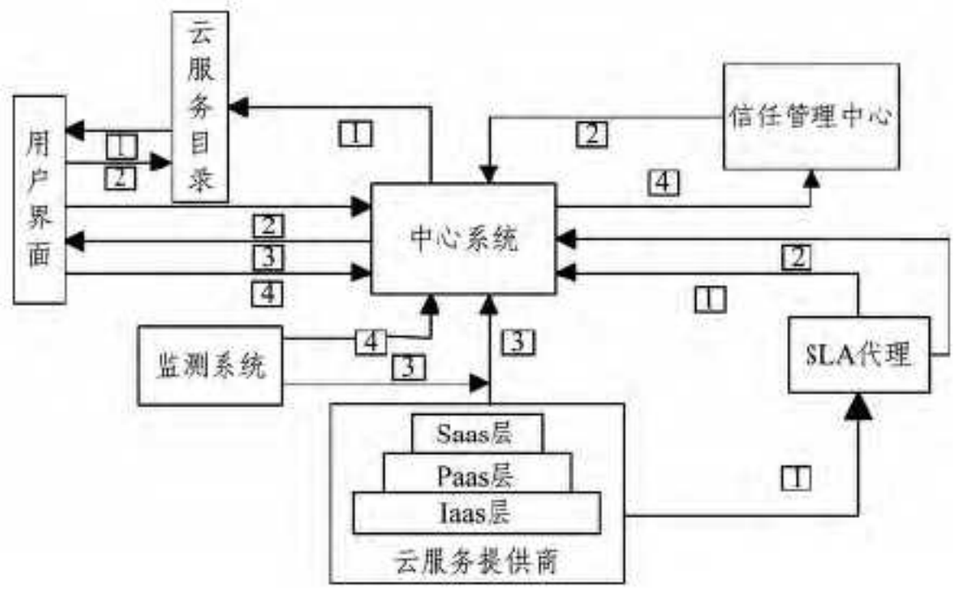

图 1 云计算信任模型

3.2 模型服务工作流程

1)处于各个层次的云服务商根据自身能力范围提交一份 QoS 列表,储存在 SLA 代理中,并通过中心系统显示到云服务目录里,通过用户界面可以浏览。

2)用户查看各服务商的 QoS 列表,向中心系统提交符合其需求的服务商名单。中心系统向信任管理中心收集名单内服务商的信任值反馈给用户,用户在其调配下与 SLA 代理就选定的服务商签订服务等级协议。

3)服务提供商开发出符合需求的云资源并且提供相应的使用环境交予用户,在交付过程中监测系统负责对可用性、可靠性、周转效率的数据进行实时整理。

4)用户在接收服务商提供的云资源后,对资源的数据完整性进行检测并根据 SLA 中所承诺服务水平的完成状况给出满意度评价,计算出诚信度的直接信任值。用户将这两部分数据交付信任管理中心,同时监测系统也将可用性、可靠性、周转效率的实时数据向上传递,由信任中心对各服务商的综合信任值进行动态更新。

4 模型相关计算方法

经过第 i 个时间段后,用户 U_a 对服务商 R_b 的总体信任用 $Trust^i_{total}(U_a,R_b)$ 表示:

$$Trust^i_{total}(U_a,R_b)=\omega_1\cdot Trust^i_{AV}(R_b)+\omega_2\cdot Trust^i_{RE}(R_b)+\omega_3\cdot Trust^i_{DI}(R_b)+\omega_4\cdot Trust^i_{HON}(U_a,R_b)+\omega_5\cdot Trust^i_{TE}(R_b) \quad (1)$$

其中,$Trust^i_{AV}(R_b)$、$Trust^i_{RE}(R_b)$、$Trust^i_{DI}(R_b)$、$Trust^i_{HON}(U_a,R_b)$、$Trust^i_{TE}(R_b)$ 分别为可用性、可靠性、数据完整性、诚信度、效率的信任分量。$W=[\omega_1,\omega_2,\omega_3,\omega_4,\omega_5]^T$ 为权重向量,$\omega_1+\omega_2+\omega_3+\omega_4+\omega_5=1$,用户更为看重的分量所占权值更大。

4.1 可用性(Availability)

可用性是指云服务商响应用户提出的服务请求的能力。云服务在发生故障后会转到线下进行系统修复,在此期间无法响应服务申请。设 θ 为某服务商在一段时间内接受用户提出的服务请求的概率,可运用贝叶斯统计对 θ 进行估计。

θ 的先验分布 $\pi_0(\theta)$ 反映了抽样前人们对于 θ 的认识,因此在没有任何监测记录的情况下可选取 θ 的先验分布为[0,1]上的均匀分布,即 $\theta\sim U(0,1)$。在云服务环境中,一般认为用户向服务商发出的服务请求是相互独立的,而且服务请求是否被接受也是相互独立的,因此在一个固定的时间段内服务请求被接受的次数可以用二项分布来刻画。设第 i 个时间段内服务商接受的总服务次数为随机变量 X_i,那么在第 i 个时段内所有用户发出的 N_i 次服务请求中被接受 A_i 次的概率为:

$$p(X_i=A_i\mid\theta)=C^{A_i}_{N_i}\theta^{A_i}(1-\theta)^{N_i-A_i} \quad (2)$$

根据 θ 的先验分布和第一个时间段内的监测记录可对 θ 的概率分布函数进行修正,得到 θ 的后验分布如下:

$$\begin{aligned}\pi_1(\theta)&=\pi(\theta\mid X_1=A_1)\\&=\frac{p(X_1=A_1\mid\theta)\cdot\pi_0(\theta)}{\int p(X_1=A_1\mid\theta)\cdot\pi_0(\theta)\mathrm{d}\theta}\\&=\frac{\Gamma(N_1+2)}{\Gamma(A_1+1)\cdot\Gamma(N_1-A_1+1)}\theta^{A_1}(1-\theta)^{N_1-A_1}\end{aligned} \quad (3)$$

所以经过第一个时间段后 θ 的后验分布为 Beta 分布,$\theta\sim Be(A_1+1,N_1-A_1+1)$。由贝叶斯统计可知,在事件发生概率的先验分布服从 Beta 分布,总体分布为二项分布时,后验分布与先验分布具有相同的函数形式[16]。因此可将修正过的后验分布作为下一时间段的先验分布,从而对 θ 的分布函数进行动态调整。设经过 $k-1$ 次分布调整后,$\theta\sim Be(\alpha,\beta)$:

$$\pi_{k-1}(\theta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\cdot\Gamma(\beta)}\theta^{\alpha-1}(1-\theta)^{\beta-1} \quad (4)$$

在第 k 个时间段的抽样调整后

$$\pi_k(\theta)=\pi(\theta\mid X_k=A_k)=\frac{p(X_k=A_k\mid\theta)\cdot\pi_{k-1}(\theta)}{\int p(X_k=A_k\mid\theta)\cdot\pi_{k-1}(\theta)\mathrm{d}\theta}=\frac{\Gamma(N_k+\alpha+\beta)}{\Gamma(A_k+\alpha)\cdot\Gamma(N_k-A_k+\beta)}\theta^{A_k+\alpha-1}(1-\theta)^{N_k-A_k+\beta-1}\tag{5}$$

即 $\theta\sim Be(A_k+\alpha,N_k-A_k+\beta)$，由数学归纳法可知经过第 i 个时间段后

$$\theta\sim Be(\sum_{l=1}^{i}A_l+1,\sum_{l=1}^{i}(N_l-A_l)+1)$$

服务商 R_b 的可用性用 θ 的期望表示为：

$$Trust_{AV}^{i}(R_b)=E(\theta)=\frac{\sum_{l=1}^{i}A_l+1}{\sum_{l=1}^{i}N_l+2}\tag{6}$$

4.2 可靠性(Reliability)

可靠性是指系统在规定的条件下和规定的时间内完成相应的功能的能力，用服务的成功率度量。用户在提交服务请求后接收到了服务商提供的云资源，可认为本次服务是成功的。可靠性同样可用贝叶斯统计进行评估，设第 i 个时间段服务商接受 A_i 次服务请求并成功完成了 C_i 次服务，则 R_b 的可靠性可表示为：

$$Trust_{RE}^{i}(R_b)=\frac{\sum_{l=1}^{i}C_l+1}{\sum_{l=1}^{i}A_l+2}\tag{7}$$

4.3 数据完整性(Data Integrity)

数据完整性是对云资源提出的安全性需求，要求数据在传输过程中不被未经授权者修改、破坏，用户可利用已有的技术如 hash 函数、数字签名等进行验证。设云服务商在第 i 个时间段内成功完成了 C_i 次，其中数据完整的服务次数为 D_i，由贝叶斯统计可得服务商 R_b 的数据完整性为：

$$Trust_{DI}^{i}(R_b)=\frac{\sum_{l=1}^{i}D_l+1}{\sum_{l=1}^{i}C_l+2}\tag{8}$$

4.4 诚信度(Honesty)

诚信度考量的是服务商关于 SLA 中所承诺的服务质量的履行情况，用户对其服务的 QoS 的评价基于用户自身体验。由于是主观评价，诚信度指标分为直接信任和间接信任两部分。

4.4.1 直接信任(Direct Trust)

定义　用户根据自身的交互情况计算出对服务商的信任值称为直接信任，在此根据满意度(degree of satisfaction)计算，引用文献[17]中提出的计算方法，随后的仿真实验可证明，该算法对策略型恶意攻击有着很好的抵御作用。

用户 U_a 对服务商 R_b 当次提供服务的满意度用数值来度量：

$$dos_{cur}(U_a,R_b)=\begin{cases}0, & \text{用户对服务非常不满意}\\ 1, & \text{用户对服务非常满意}\\ \in(0,1), & \text{其他}\end{cases}\tag{9}$$

$dos_i^{r-1}(U_a,R_b)$ 表示在第 i 个时间段内经过 $r-1$ 次交易后的满意度评价，$rd_i^r(U_a,R_b)$ 和 $ad_i^r(U_a,R_b)$ 为满意度当次偏差(recent deviation)和累积偏差(accumulated deviation)：

$$rd_i^r(U_a,R_b)=|dos_i^{r-1}(U_a,R_b)-dos_{cur}(U_a,R_b)|\tag{10}$$

$$ad_i^r(U_a,R_b)=\psi\times rd_i^r(U_a,R_b)+(1-\psi)\times ad_i^{r-1}(U_a,R_b)\tag{11}$$

$$c=0.25+\psi\times\frac{rd_i^r(U_a,R_b)}{1+ad_i^r(U_a,R_b)}\tag{12}$$

其中，$ad_0^0=0$，$ad_i^0=ad_{i-1}^{last}$，常数 ψ 用来控制 $re_i^r(U_a,R_b)$ 在累积值中的影响程度。满意度的计算公式如下：

$$dos_i^r(U_a,R_b)=dos_{cur}(U_a,R_b)\times c+dos_i^{r-1}(U_a,R_b)\times(1-c)\tag{13}$$

设定 $dos_0^0=0.6$，$dos_i^0=dos_{i-1}^{last}$，所以在经过第 i 个时间段后 U_a 对 R_b 的直接信任值用交易满意度表示为：

$$DT_i(U_a,R_b)=dos_i^{last}(U_a,R_b)\tag{14}$$

4.4.2 间接信任(Indirect Trust)

定义　通过第三方的推荐建立信任关系并获取的推荐信任值称为间接信任值。

用户将计算完成的直接信任值传递给中心系统，最终由信任管理中心进行汇总。在此提出过滤区间，首先引入峰度和偏度的概念。

峰度(kurtosis)是表征数据概率密度曲线在顶端处峰值高低的统计量，直观地反映了尾部的厚度。当数据的总体分布为正态分布时，峰度值为 3。数据分布较正态分布更陡峭时，峰度大于 3，两侧极端数据分布范围较广，这种分布称为粗尾的；峰度小于 3 时，数据分布更平坦，两侧极端数据较少，分布则称为细尾的。$User(R_b)$ 为所有接受过 R_b 服务的用户的集合，设 $|User(R_b)|=n$，即 $User(R_b)=\{U_{d_1},U_{d_2},\cdots,U_{d_n}\}$。

$$\overline{DT_i(R_b)}=\frac{1}{n}\sum_{l=1}^{n}DT_i(U_{d_l},R_b)\tag{15}$$

$$s=\sqrt{\frac{1}{n-1}\sum_{l=1}^{n}(DT_i(U_{d_l},R_b)-\overline{DT_i(R_b)})^2}\tag{16}$$

$$kur=\frac{n^2-2n+3}{(n-1)(n-2)(n-3)}\times\frac{\sum_{l=1}^{n}(DT_i(U_{d_l},R_b)-\overline{DT_i(R_b)})^4}{s^4}-\frac{3(2n-3)}{n(n-1)(n-2)(n-3)}\times\frac{[\sum_{l=1}^{n}(DT_i(U_{d_l},R_b)-\overline{DT_i(R_b)})^2]^2}{s^4}\tag{17}$$

其中，$\overline{DT_i(R_b)}$ 为数据均值，s 为标准差[18]。

偏度(skewness)则是用来表征数据对称性的指标，关于均值对称的数据偏度为 0，当极端数据或概率密度曲线的拖长尾巴偏向右侧时称为正向偏态，偏度为正，左侧数据更分散的数据偏度为负。

$$ske=\frac{n}{(n-1)(n-2)}\times\frac{\sum_{l=1}^{n}(DT_i(U_{d_l},R_b)-\overline{DT_i(R_b)})^3}{s^3}\tag{18}$$

当某一用户给出的评价与大众分歧较大时，可以认为其提供的信息参考价值不大，并且不排除恶意评价的可能性。因此本文选择去掉用户评价中的部分极端数值，这样既可以排除某些异常值的影响，也可以反映绝大多数用户的评价。

数据呈现正态分布时，$kur=3$，$ske=0$，将占总体比例为 δ 的边缘数据过滤，两端的过滤区间各占 $\frac{\delta}{2}$。当 $kur>3$ 时，两

侧的极端数据较之正态分布更多，增大过滤数据所占比例；$kur<3$ 时则减小过滤区间的总长度。当 $ske>0$ 时，右侧极端数据较多，应对过滤区间进行调整，延长上区间，缩短下区间；$ske<0$ 时则相反。即生成过滤上区间 $(filter_u,1)$ 和下区间 $(0,filter_d)$，两区间内的数据分别占总体比例的 $\frac{\delta+\zeta_1\times(kur-3)}{2}+\zeta_2\times ske$ 和 $\frac{\delta+\zeta_1\times(kur-3)}{2}-\zeta_2\times ske$，其中 ζ_1,ζ_2 为调节参数。评价可信度(Feedback Credibility)用来描述用户推荐信息的准确性：

$$FC_i(U_a,R_b)=\begin{cases}0, & DT_i(U_a,R_b)\geqslant filter_u\\ Decay(rec,i), & filter_d<DT_i(U_a,R_b)<filter_u\\ 0, & DT_i(U_a,R_b)\leqslant filter_d\end{cases}\tag{19}$$

由于信任具有时间相关性，历史证据对当前决策的重要程度会随着时间的流逝而逐渐降低，因此引入时间衰减函数 $Decay(rec,i)=e^{-\varphi(i-rec)}(i\geqslant rec)$，$U_a$ 对 R_b 最近一次评价在第 rec 个时间段。当所给评价处于过滤区间内时，不将其用于间接信任的计算中。

$$IT_i(U_a,R_b)=\frac{\sum\limits_{x\in User(R_b)\setminus\{U_a\}}FC_i(x,R_b)\times DT_i(x,R_b)}{\sum\limits_{x\in User(R_b)\setminus\{U_a\}}FC_i(x,R_b)}\tag{20}$$

4.4.3 诚信度信任计算

诚信度信任值由直接信任和间接信任两部分加权而成，其权值由用户根据交互情况自行给出。

$$Trust^i_{HON}(U_a,R_b)=\partial\times DT_i(U_a,R_b)+(1-\partial)\times IT_i(U_a,R_b)\tag{21}$$

4.5 效率(Turnaround Efficiency)

云计算平台上资源提供商完成用户的服务请求包括如下 3 个时段，如图 2 所示。

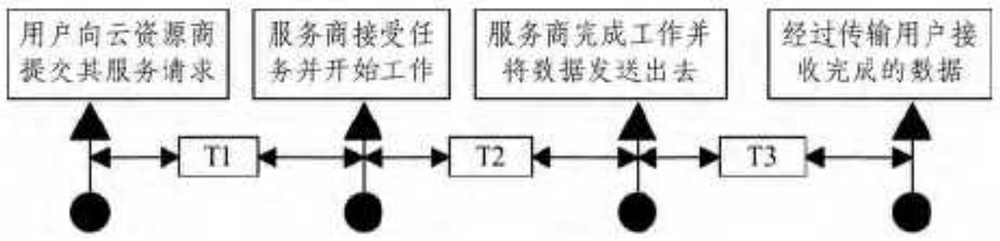

图 2 云服务数据传输过程

如图 2 所示，取 T_2 为服务提供商在 SLA 中承诺的周转时间，考虑到服务请求过程和数据传输所花费的时间，实际的周转时间为用户从提交服务请求到接收到已完成的数据这段时间，用 $T_{total}=T_1+T_2+T_3$ 表示。因此，每次云服务数据传输的周转效率可定义为 $\frac{T_2}{T_{total}}$，$E_k(TE)$ 表示第 k 个时间段 R_b 所有服务的周转效率的期望，关于效率的信任分量也使用了衰减函数用作各时段数据的权值分配。

$$Trust^i_{TE}(R_b)=\frac{\sum\limits_{l=1}^{i}Decay(l,i)\times E_l(TE)}{\sum\limits_{l=1}^{i}Decay(l,i)}\tag{22}$$

4.6 权值分配

权重向量 $W=[\omega_1,\omega_2,\omega_3,\omega_4,\omega_5]^T$ 的计算引入美国运筹学家 T. L. Satty 提出的层次分析法 AHP(Analytic Hierarchy Process)中影响因素权值分配的方法：首先运用九级标度法，根据用户偏好，通过两两比较的方法，构建正互反判断矩阵 $A=(a_{ij})_{5\times5}$，其中 $i,j=1,2,3,4,5$，分别对应可用性、可靠性、数据完整性、诚信、效率 5 个指标的信任分量。元素 a_{ij} 为在用户的主观判断下分量 i 与 j 相比的重要程度，取值标准如表 1 所列，由矩阵元素的正互反性可得 $a_{ii}=1$ 且 $a_{ij}=\frac{1}{a_{ji}}$。

表 1 九级标度法

重要性等级	a_{ij} 赋值
i,j 分量同等重要	1
i 分量比 j 分量稍重要	3
i 分量比 j 分量明显重要	5
i 分量比 j 分量强烈重要	7
i 分量比 j 分量极端重要	9
i 分量比 j 分量稍不重要	1/3
i 分量比 j 分量明显不重要	1/5
i 分量比 j 分量强烈不重要	1/7
i 分量比 j 分量极端不重要	1/9
处于上述相邻判断之间	2,4,6,8,1/2,1/4,1/6,1/8

$W=[\omega_1,\omega_2,\omega_3,\omega_4,\omega_5]^T$ 为判断矩阵 A 的最大特征值 λ_{max} 相应的特征向量，信任分量 i 所占权重 ω_i 可由计算矩阵各行元素的几何平均并进行归一化而得。

$$\omega_i=\frac{[\prod\limits_{j=1}^{5}a_{ij}]^{\frac{1}{5}}}{\sum\limits_{k=1}^{5}[\prod\limits_{j=1}^{5}a_{kj}]^{\frac{1}{5}}},\sum_{i=1}^{5}\omega_i=1\tag{23}$$

其中，

$$\lambda_{max}=\frac{1}{5}\cdot\sum_{i=1}^{5}\frac{\sum\limits_{j=1}^{5}a_{ij}\cdot\omega_j}{\omega_i}\tag{24}$$

由于是用户的主观判断，元素并不具有传递性，即不一定满足 $a_{ij}=a_{ik}\cdot a_{kj}$，因此要进一步对矩阵的一致性进行检测。

一致性指标(consistency index)：$CI=\frac{\lambda_{max}-n}{n-1}$，即判断矩阵最大特征根外其余特征根的负平均值，其中 n 为矩阵的阶数，此处 $n=5$。当矩阵具有完全一致性时，$a_{ij}=\frac{\omega_i}{\omega_j}$，$\lambda_{max}=n$，$CI=0$；当矩阵非完全一致时，$\lambda_{max}>n$，并且 λ_{max} 越大于 n，矩阵的一致性就越差。

一致性比例(consistency ratio)：$CR=\frac{CI}{RI}$，RI 为对正互反矩阵进行 1000 次计算得到的平均随机一致性指标(random index)，各阶矩阵的 RI 值层次分析法中均已给出，5 阶矩阵的 $RI=1.12$。

Satty 规定当 $CR<0.1$ 时，认为该判断矩阵的一致性可以接受，权重向量 $W=[\omega_1,\omega_2,\omega_3,\omega_4,\omega_5]^T$ 符合要求；若 $CR\geqslant0.1$，应该对判断矩阵进行修正，再进行一致性检测。

5 模型实验仿真

CloudSim 是一款由墨尔本大学开发的云仿真工具，通过将云基础设施实例化来对云服务过程进行建模和仿真。仿真实验在其提供的基于数据中心的虚拟云环境中初始化具有不同服务特性的云服务商，实验过程可以专注于研究信任模型设计的合理性，而不必关心底层基础设施的细节。本文以 CloudSim 为基础搭建实验平台模拟信任管理中心、用户、云服务提供商之间的交互行为，将交互后的数据输入 Matlab 中进行分析对比，从而验证模型对实体进行信任评估的准确性和安全性。

5.1 云服务商的选择

不同的用户对于各服务属性的需求不同，这里以实例验证模型的可行性。假定该用户对各属性的重视程度依次为：

可用性＜效率＜可靠性＜数据完整性＜诚信，以此为依据构造判断矩阵：

$$A=\begin{bmatrix}1 & 1/5 & 1/7 & 1/9 & 1/3\\ 5 & 1 & 1/3 & 1/5 & 3\\ 7 & 3 & 1 & 1/3 & 5\\ 9 & 5 & 3 & 1 & 7\\ 3 & 1/3 & 1/5 & 1/7 & 1\end{bmatrix}$$

计算得 $\lambda_{max}=5.2372, CI=0.0593, CR=0.0529<0.1$，矩阵满足一致性要求，得到权重向量 $W=[0.0329, 0.1296, 0.2638, 0.51, 0.0636]^T$。对模拟产生的 20 个云服务商进行综合评判，结果如图 3 所示，第 8 个服务商最符合用户的需求。由此可见，基于 AHP 的权值分配方法在一定程度上解决了不同用户的个性化需求问题。

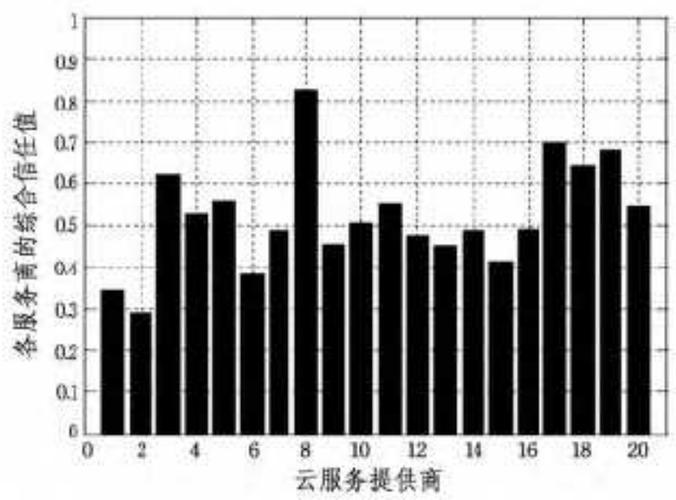

图 3　云服务商选择

5.2　时间衰减因子的影响

在云服务商的相关信任计算中，加入时间衰减因子对数据进行加权平均可以有效地反映出实体近期的交互行为。以模拟出的某一效率数据较不稳定的服务商为例，该实体在取样的 100 个时间段里数据波动较大。如图 4 所示，通过仿真实验可以看出，在加入时间衰减因子后距当前时间越近的数据所占权重越大，相比起算术平均的统计更能反映数据近期的变化趋势。在第 10 个时间段后数值略微下降，加权平均的数据要稍低于算术平均；而在第 40 个时间段后该服务商的数据则明显提高，加权平均的数据增长速率更快。通过仿真还可看出，当数据量越来越大后算术平均的统计变化幅度很小，而加入时间衰减因子的加权平均则可实时反映服务商的近期情况。

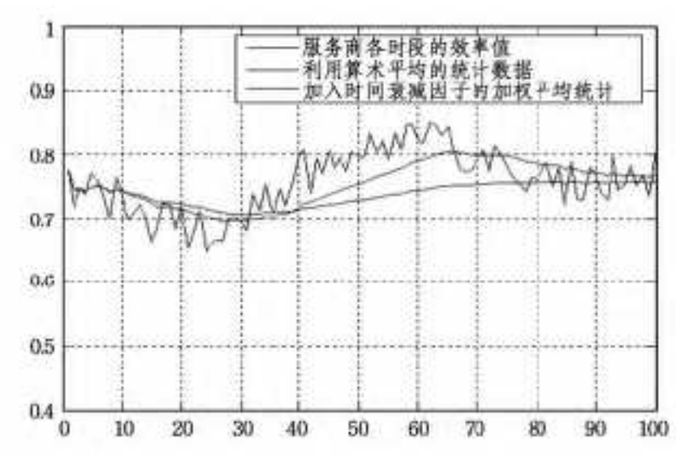

图 4　时间衰减因子的影响

5.3　针对策略型恶意攻击的抵御能力

云环境中，一些服务商为达到某些目的，会从可用性、可靠性、提供远低于 SLA 中承诺的服务水平等方面对用户进行恶意攻击。一些简单的恶意攻击应对起来较为容易，文中所讨论的是关于策略型恶意攻击的应对情况：此类服务商在前期会提供优质服务从而提高用户对其评价，在自身信任值升高后再进行恶意攻击。实验中设定有 1000 种服务，每种服务含有 100 个服务商，恶意服务商的比例为 10%，每轮从其中的 10 到 20 个服务商中选择综合信任值最高的进行交易并给出服务评价，若最终选择的是恶意服务商，则可认为对策略型恶意攻击的抵御失败，实验中用每轮恶意服务的通过率描述模型的安全性，交易初期设定服务商每个信任分量的值均为 0.6。本文是在文献[2]的 QoS 模型基础上用贝叶斯统计、时间衰减因子等数学方法进行了扩展，并且进一步提出了诚信度的信任评估参量，因此在安全性和评估的准确性上有了一定提高。在实验初期，由于交易次数不足，信任数据不充分，并且一些策略性恶意服务商还处于“潜伏”阶段，在前 50 轮交易过后，恶意服务通过率并没有明显下降，而随着交易的逐渐深入，其通过率呈现明显下滑趋势，在 500 次交易过后，通过率仅为 4.12%，如图 5 所示。

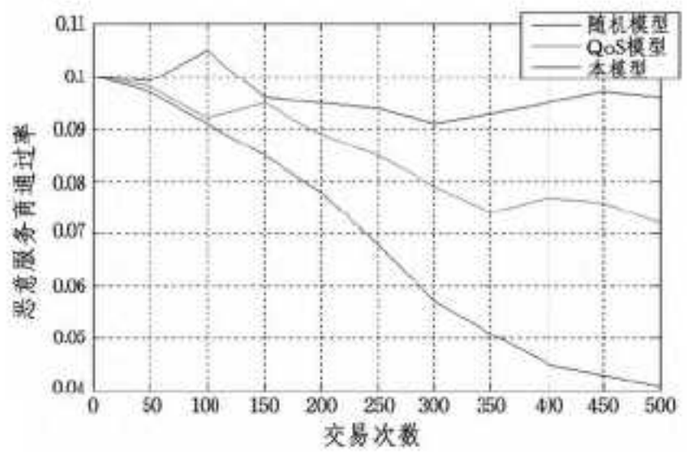

图 5　对策略型恶意攻击的抵制能力

结束语　云计算环境下，用户如何从海量的服务商中选择一个既可信又满足其个人需求的资源已成为当前研究的重要课题。本文所构建的模型为服务商的选择问题提供了一种全新的思路，模型中考虑了资源可用性、可靠性、数据完整性、诚信度和周转效率 5 个参量，运用了贝叶斯统计、时间衰减因子、权重向量分配等数学方法对大量数据进行整合，模型计算便利，具有较高实用性和安全性。但是云计算中一些其他参量如云资源利用率(Utilization of Resources)、服务商投资回报(Return on Investments)等在模型中没有考虑，我们将在下一步工作把这些因素考虑进来，对信任评估做进一步的完善。

参 考 文 献

[1] 冯登国，张敏，张妍. 云计算安全研究[J]. 软件学报，2011，22(1)：71-83

[2] Manuel P. A trust model of cloud computing based on Quality of Service[J]. Annals of Operations Research，2013，4

[3] 桂小林，李小勇. 信任管理与计算[M]. 西安：西安交通大学出版社，2011

[4] 吴鹏，吴国新，方群. 一种基于概率统计方法的 P2P 系统信任评价模型[J]. 计算机研究与发展，2008，45(3)：408-416

[5] 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

[6] 李峰，申利民，司亚利，等. 基于交互感知的动态自适应的信任评估模型[J]. 通信学报，2012，33(10)：60-70

[7] Boreale M，Celestini A. Asymptotic Risk Analysis for Trust and Reputation Systems[C] // Springer-Verlag Berlin Heidelberg 2013，SOFSEM 2013，LNCS 7741，2013. 169-181

[8] Jøsang A，Hayward R，Pope S. Trust network analysis with subjective logic[C] // Proceedings of the Australasian computer science conference (ACSC'06). Hobart，2006：139-161

[9] Sun Y L，Han Z，Yu W，et al. A trust evaluation framework in distributed networks：vulnerability analysis and defense against

attacks[C]//IEEE INFOCOM. Barcelona, Spain, 2006: 1-13
[10] Boukerche A, Ren Y. A trust-based security system for ubiquitous and pervasive computing environments[J]. Computer Communications, 2008, 31(18): 43-51
[11] 胡春华, 刘济波, 刘建勋. 云计算环境下基于信任演化及集合的服务选择[J]. 通信学报, 2011, 32(7): 71-79
[12] 谢晓兰, 刘亮, 赵鹏. 面向云计算基于双层激励和欺骗检测的信任模型[J]. 电子与信息学报, 2012, 34(4): 812-817
[13] 熊润群, 罗军舟, 宋爱波, 等. 云计算环境下 QoS 偏好感知的副本选择策略[J]. 通信学报, 2011, 32(7): 93-102
[14] Abbadi I M, Alawneh M. A framework for establishing trust in the cloud[J]. Computers and Electrical Engineering, 38(5), 1073-1087
[15] Noor T H, Sheng Q Z. Trust as a service: a framework for trust management in cloud environments[C]// Web information system engineering(WISE 2011). 2011, 6997: 314-321
[16] 茆诗松. 贝叶斯统计[M]. 北京: 中国统计出版社, 1999
[17] Das A, Islam M M. Dynamic Trust Model for Reliable Transactions inMulti-agent Systems[C]// Proceedings of the 13th International Conference on Advanced Communication Technology. Seoul, 2011: 1101-1106
[18] 数学手册[M]. 北京: 人民教育出版社, 1978

(上接第 314 页)

献, 因而使得许多的冗余节点处于工作状态。从图 8 可以看出, ACPUDC 协议的覆盖质量与 ELIQoS 的覆盖质量基本相同, 但由图 7 已经知道, 在相同覆盖质量要求下, ELIQoS 的工作节点数要略高于 ACPUDC 的工作节点数, 因此, 必然导致 ELIQoS 的网络能耗要高于 ACPUDC。

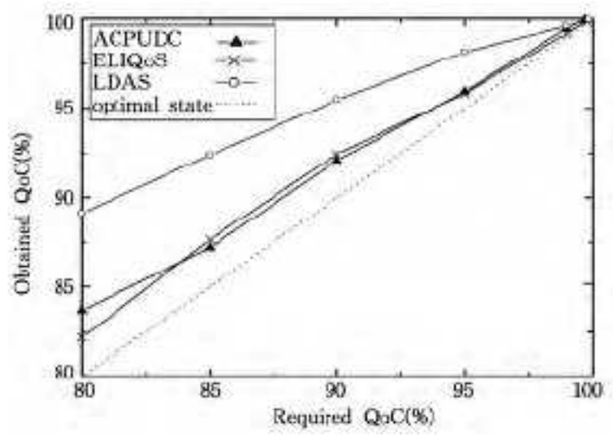

图 8 获得的覆盖质量比较

综合上面的比较结果可以得出, ACPUDC 采用数据冗余来判断冗余节点能够更精确地描述网络的覆盖能力, 同时, ACPUDC 能够选取最少的工作节点以保证网络的覆盖质量要求。

结束语 本文应用线性代数中的相关理论给出了节点间数据相关性的计算模型, 同时研究了网络连通性问题, 在此基础上提出了基于数据相关性的冗余节点判断准则, 并设计了一种高效节能的覆盖控制协议——ACPUDC。ACPUDC 协议选取最少的工作节点来保证网络覆盖质量和连通性, 同时采用基于剩余能量的退避机制来保证网络的整体能耗分布均衡, 从而实现了减少网络能量消耗、延长网络有效寿命的目的。

参 考 文 献

[1] Sun Ya-juan, Wang Huan-zhao, Zhang Ke-wang, et al. Associated Clustering Strategy for Wireless Sensor Network[J]. International Journal of Distributed Sensor Networks, 2014, 2014: 7
[2] Kondo S, Kanzaki A, Hara T, et al. Energy-Efficient Data Gathering Using Sleep Scheduling and Spatial Correlation Based on Data Distribution in Wireless Sensor Networks[C]// 2011 14th International Conference on Network-Based Information Systems (NBiS). 2011: 194-201
[3] Hongbo J, Shudong J, Chonggang W. Prediction or Not ? An Energy-Efficient Framework for Clustering-Based Data Collection in Wireless Sensor Networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22 (6): 1064-1071
[4] 徐立. 基于数据相关性的 WSN 分簇路由协议的研究[D]. 南京: 东南大学, 2010
[5] Tian D, Georganas N D. A coverage-preserving node scheduling scheme for large wireless sensor networks[C]// Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications. ACM: Atlanta, Georgia, USA, 2002: 32-41
[6] Kasbekar G S, Bejerano Y, Sarkar S. Lifetime and Coverage Guarantees Through Distributed Coordinate-Free Sensor Activation[J]. IEEE/ACM Transactions on Networking, 2011, 19 (2): 470-483
[7] W You-Chiun, T Yu-Chee. Distributed Deployment Schemes for Mobile Wireless Sensor Networks to Ensure Multilevel Coverage[J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19(9): 1280-1294
[8] Zhuang M, Lingguo C, Baihai Z, et al. Deployment patterns for k-coverage and l-connectivity in Wireless Sensor Networks [C]// IET International Conference on Wireless Sensor Network, (IET-WSN 2010). 2010: 73-77
[9] Yan J, Ling W, Ju-Yeon J, et al. EECCR: An Energy-Efficient m-Coverage and n-Connectivity Routing Algorithm Under Border Effects in Heterogeneous Sensor Networks[J]. IEEE Transactions on Vehicular Technology, 2009, 58 (3): 1429-1442
[10] YuanYuan L, Parker L E. A spatial-temporal imputation technique for classification with missing data in a wireless sensor network[C]// IEEE/RSJ International Conference on Intelligent Robots and Systems, 2008(IROS 2008). 2008: 3272-3279
[11] Changlei L, Guohong C. Spatial-Temporal Coverage Optimization in Wireless Sensor Networks[J]. IEEE Transactions on Mobile Computing, 2011, 10(4): 465-478
[12] 刘金旺, 李冬梅. 线性代数[M]. 天津: 天津大学出版社, 2010
[13] Wu K, Gao Y, Li F, et al. Lightweight Deployment-Aware Scheduling for Wireless Sensor Networks[J]. Mobile Networks and Applications, 2005, 10 (6): 837-852
[14] 毛莺池, 龚海刚, 刘明, 等. ELIQoS: 一种高效节能、与位置无关的传感器网络服务质量协议[J]. 计算机研究与发展, 2006, (06): 1019-1026