云计算环境下基于FANP的用户行为的可信评估与控制分析

吕艳霞[1] 田立勤[2,3] 孙珊珊[3]
(东北大学信息科学与工程学院 沈阳 110044)[1] (青海师范大学计算机学院 西宁 810008)[2]
(华北科技学院电子信息工程学院 北京 101601)[3]

摘 要 云计算环境下,开放的运行环境使其面临重大的安全挑战,仅仅提供用户身份认证的安全控制已经不能完全适应云计算等新型计算机网络的应用。结合动态的行为可信的安全措施,有效地确定不可信云终端用户并正确分析云用户的异常行为是在复杂动态环境下保证云安全的基础。采用基于三角模糊数的模糊网络分析法(FANP),通过使用模糊数来反映专家评判的模糊性,弱化了单纯使用ANP方法存在的主观性,并对网络用户行为各属性的权重进行了量化计算,使评判结果更加客观。评价结果为基于动态信任的安全控制提供了量化分析的基础,为服务提供者采取更加安全的策略来响应用户请求提供了量化依据。

关键词 模糊网络分析法,用户行为,可信评估,云计算
中图法分类号 TP393 **文献标识码** A

Trust Evaluation and Control Analysis of FANP-based User Behavior in Cloud Computing Environment

LV Yan-xia[1] TIAN Li-qin[2,3] SUN Shan-shan[3]
(College of Information Science and Engineering, Northeastern University, Shenyang 110044, China)[1]
(School of Computer Science and Technology, Qinghai Normal University, Xining 810008, China)[2]
(College of Electronic and Information Engineering, North China Institute of Science and Technology, Beijing 101601, China)[3]

Abstract The open environment in cloud computing is much more complex and unpredictable, and can not fully adapt to the new application of computer network such as cloud computing. Combining such security measures of dynamic user behavior trust, effectively confirming the untrusted cloud terminal users and correctly analyzing their abnormal behavior are the basis to ensure cloud security in complex and dynamic environment. This paper adopted the method of fuzzy analytic network process(FANP) based on triangular fuzzy numbers, which can reflect the fuzziness of expert evaluation through using fuzzy numbers, and weaken the subjectivity of simply using ANP. The paper also gave a quantization calculation to the weight of each attribute in order to make the evaluation results more objective. The evaluation results provide a quantitative analysis foundation for security control based on dynamic trust and provide the quantitative basis for service providers who adopt a more safe strategy in response to a user's requesting.

Keywords Fuzzy analytic network process, User behavior, Trust evaluation, Cloud computing

1 引言

随着云计算的飞速发展,人们在享受它带来的降低运营成本,改善运营效率等种种便利的同时,也面临着更为严峻的信息安全挑战。云系统中的海量重要用户数据对攻击者具有更大的诱惑力,同时云系统为用户提供的开放访问接口使云终端用户可以直接使用和操作云服务提供商的软件、操作系统,甚至是编程环境和网络基础设施,由此对云资源的影响和破坏远比目前利用因特网进行资源共享要严重得多。因此访问云资源的云终端用户身份是否真实、行为是否可信是保证云计算安全的重要内容。目前身份认证技术比较成熟,但身份认证并不能阻止身份认证失败或合法身份的恶意端用户对系统的破坏,因此对云终端用户行为进行有效分析控制是当前云计算应用中的一个研究重点。

用户行为可信是网络可信技术研究的主要内容之一[1]。文献[2]以可信网络中用户行为可信研究为核心,提出了面向可信网络的用户行为信任的评估、预测与控制架构,但文章是从宏观的角度对用户行为可信的整体架构、管理机制等方面进行研究。文献[3]建立可量化的信任证据与信任等级之间的对应关系,其与文献[4]都使用了贝叶斯网络对用户未来行为信任进行预测,但没有考虑到用户历史行为的评估。文献[5]提出了基于三角模糊数的模糊层次分析法(FAHP),其对网络用户行为各属性的权重进行量化计算,使评判结果更加客观,但是层次分析法(AHP)不能很好地反映用户行为各层

到稿日期:2012-03-20 返修日期:2012-09-18 本文受973计划专项(2011CB311809),国家自然科学基金项目(61163050),河北省自然科学基金项目(F2010001745),新世纪优秀人才支持计划(NCET-10-0101)资助。
吕艳霞(1982—),女,博士生,主要研究方向为计算机网络、可信网络;田立勤(1970—),男,博士,教授,主要研究方向为计算机网络、物联网、可信网络;孙珊珊(1984—),女,硕士生,主要研究方向为无线传感器网络信任管理。

次元素之间的相互作用和相互依存关系及反馈关系。文献[6,7]提出了一种基于动态博弈的用户行为模型，其通过不完全信息多阶段博弈来分析云终端用户的类型，快速甄别系统中潜在的不可信云终端用户，但主要考虑的是实时行为的分析。

本文借鉴上述相关研究成果提出采用基于三角模糊数的模糊网络分析法(FANP)，改进 FAHP 没有考虑到云端用户行为信任评估属性的内部循环相互支配的层次结构以及层次结构内部的依赖性和反馈性问题，用超矩阵的形式来定量地表示影响程度的大小，更能反映客观实际问题的复杂性，同时克服了单纯采用 ANP 方法的主观随意性，从而提高了用户行为信任评估的客观性和有效性。

2 基于 FANP 的云端用户行为信任的评估

这里的信任评估就是对云计算环境中的云端用户行为信任的评估，是一种动态的评估方法。所有云端用户的信任建立和更新都直接或间接地建立在各种行为证据的基础之上。用户行为证据是在用户和服务提供者交互过程中，服务提供者可直接根据软硬件检测获得的用来定量评估用户总体行为信任的基础数值，它具有客观性，本身不具有信任的主观特性。

2.1 建立模型

本文建立的用户行为信任评估的模型如图 1 所示，ANP 将系统的元素分为两个部分，即控制层和网络层[8]。第一部分是控制层，包括问题的目标和进行的决策准则，即图 1 的第 1 层。在控制层中，所有的决策准则都被认为是彼此独立的，且只受目标元素的支配。我们可以依据传统的 AHP 方法来获得各个准则的权重。ANP 的控制层中可以没有决策准则，但至少应有一个目标。本文建立的模型中控制层只有一个目标，即用户行为信任评估。第二部分是网络层，即图 1 的第 2～4 层，在元素组(如性能属性 P1，安全属性 P2)之间以及各子元素之间的关系都不是相互独立的，相互之间存有依存关系和反馈关系，如性能属性中的用户的平均吞吐量与安全属性中的用户存取文件的平均次数之间具有相互依赖关系，用户存取文件的平均次数越多，用户的平均吞吐量就会越大，这种不同属性的证据之间的相互依存关系形成了一个网络结构。

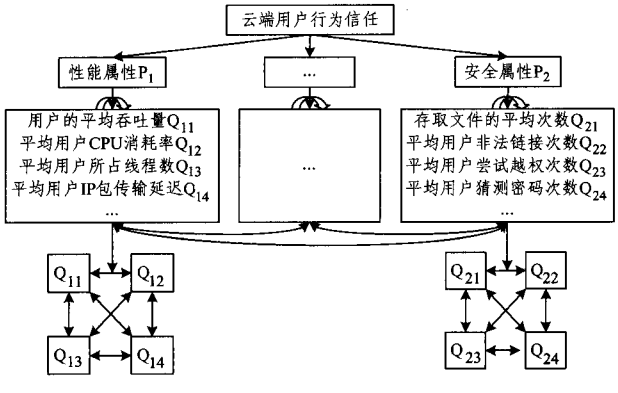

图 1 云端用户行为信任评估的 ANP 模型

2.2 构造模糊判断矩阵

为分析各元素的相对重要性，必须在云端用户行为信任评估的目标下对网络层中的各元素进行两两比较，列出两两判断矩阵。在 ANP 方法中，矩阵中的数据结合具体情况，可以通过专家打分得到，采用 Saaty 提出的 1～9 标度法来标度，如表 1 所列。每一个判断矩阵都应经过一致性检验，也就是逻辑的一致性，即若 $A>B, B>C$，则必有 $A>C$。而 FANP 采用三角模糊数取代 ANP 方法的 1～9 Saaty 标度，建立模糊判断矩阵。这样可以有效地解决 ANP 方法的主观随意性，提高用户行为信任评估的客观性和有效性。

表 1 判断矩阵标度

标度	含义
1	两个元素相比，同样重要
3	两个元素相比，前者比后者稍重要
5	两个元素相比，前者比后者明显重要
7	两个元素相比，前者比后者强烈重要
9	两个元素相比，前者比后者极端重要
2,4,6,8	上述相邻判断的中间值
倒数	两个元素相比，后者比前者的重要性标度

定义 1 若模糊数 $M=(l,m,u)$，其中 $0<l\leqslant m\leqslant u$，称 M 为三角模糊数，其隶属函数可表示为[9]：

$$\mu_M(x)\begin{cases}\dfrac{x-l}{m-l}, & l\leqslant x\leqslant m\\ \dfrac{x-u}{m-u}, & m\leqslant x\leqslant u\\ 0, & \text{其他}\end{cases} \tag{1}$$

式中，l 和 u 分别为 M 的上界和下界，m 为中值。

设 $M_1=(l_1,m_1,u_1)$，$M_2=(l_2,m_2,u_2)$，则有如下的运算法则：

(1) $M_1\oplus M_2=(l_1,m_1,u_1)\oplus(l_2,m_2,u_2)=(l_1+l_2,m_1+m_2,u_1+u_2)$

(2) $M_1\otimes M_2=(l_1,m_1,u_1)\otimes(l_2,m_2,u_2)=(l_1l_2,m_1m_2,u_1u_2)$

(3) $1/M_1=(l_1,m_1,u_1)^{-1}\approx(1/u_1,1/m_1,1/l_1)$

模糊判断矩阵中的数据结合具体情况，采用模糊语意变量来描述成对比较时的相对重要度，同样这里也需要进行一致性检验。实际应用中，出现不满足一致性的要求时，项目相关人员和专家必须重新给出判断信息，直到满足为止。

设 ANP 中目标层的元素为 $O_1,O_2\cdots,O_n$，网络层中元素组为 $P_1,P_2,\cdots,P_N$。在其元素组 P_i 中有元素 $Q_{i1},Q_{i2},\cdots,Q_{im_i}(i=1,\cdots,N)$，以控制层 O_s 为准则，以 P_j 中元素 Q_{jl} 为次准则，按照元素组 P_i 中元素对 Q_{jl} 的影响力大小进行间接优势度比较，构造模糊判断矩阵。在传统的 ANP 方法中，得到判断矩阵之后，就要进行相对权重的计算，在这里要得到相对权重，首先要使用式(2)计算矩阵中每个元素与其他元素相比较的综合程度值，记为 I_i：

$$I_i=\sum_{j=1}^{m}M_{P_i}^{j}\otimes\Big[\sum_{i=1}^{n}\sum_{j=1}^{m}M_{P_i}^{j}\Big]^{-1} \tag{2}$$

式中，M_{P_i} 为模糊判断矩阵中的模糊数，I_i 为三角模糊数，m 为矩阵列的数目，n 为矩阵行的数目。在得到 n 个三角模糊数后，就要计算每个三角模糊数大于其他模糊数的可能性程度，其可由式(3)计算：

$$V(M_1,M_2)=\begin{cases}1, & m_1\geqslant m_2\\ \dfrac{l_2-u_1}{(m_1-u_1)-(m_2-l_2)}, & m_1<m_2,u_1\geqslant l_2\\ 0, & \text{其他}\end{cases} \tag{3}$$

$V(M_1,M_2)$表示M_1大于M_2的可能性程度。每个三角模糊数大于其他模糊数的可能性程度的最小值即为该元素重要于其他元素的可能性程度，记为$d(A_i)$。可得到$w'=[d(A_1),d(A_2),\cdots,d(A_n)]^T$。经过归一化后就可以得到权重向量$w=[d'(A_1),d'(A_2),\cdots,d'(A_n)]^T$。

2.3 建立超矩阵

按照上述方法，计算其他的判断矩阵，并记为w_{ij}：

$$w_{ij}=\begin{pmatrix} w_{i1}^{(j1)} & \cdots & w_{i1}^{(jn_j)} \\ \vdots & \ddots & \vdots \\ w_{in_i} & \cdots & w_{in_i}^{(jn_j)} \end{pmatrix}$$

式中，n_j为第j个元素组含有元素的个数，w_{ij}的列向量就是元素组P_i中的元素对P_j中的元素$Q_{j1},Q_{j2},\cdots,Q_{jn_j}$($j=1,\cdots,N$)的影响程度排序向量。若元素组$P_j$中的元素不受$P_i$中元素的影响，则$w_{ij}=0$，可得超矩阵：

$$W=\begin{pmatrix} w_{11} & \cdots & w_{1N} \\ \vdots & \ddots & \vdots \\ w_{N1} & \cdots & w_{NN} \end{pmatrix}$$

由超矩阵的构成可以看出，超矩阵由子块w_{ij}组成。虽然超矩阵的各个子块都是归一化的，但是整个超矩阵并不是归一化的，因此要在准则O_s下对不同元素组的重要性进行比较，可以得到一个加权矩阵：

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix}$$

式中，列向量是各元素组对元素组P_j的重要性进行比较，得到的一个归一化的排序向量。

把加权矩阵A每一个元素乘以初始超矩阵的相应元素块，即$\overline{w_{ij}}=a_{ij}w_{ij}$，就得到加权超矩阵，将其记为$W'$。$W'$为加权超矩阵，其列的和为1，称为列随机矩阵。

2.4 计算极限相对排序向量

一个随机矩阵的任意次幂都是一个随机矩阵。加权超矩阵W'表示任何元素组中的任何一个元素对另一个元素组的任何一个元素的直接影响程度的偏好度量。$(W')^2$是其二次间接影响的程度的偏好度量。依次类推，$(W')^k$即是k次间接影响的偏好度量。当$k\to\infty$时，就得到了决策者的综合偏好度量。在加权随机矩阵的幂运算过程中，如果幂收敛，那么可以把这个收敛的结果作为综合权重。如果出现周期性，可以取平均作为综合权重。

2.5 实例分析

(1) 构造模糊判断矩阵

在信任评估值最大化的准则下，以性能为次准则，将性能与安全进行比较，列出两两比较矩阵，如表2所列。表2中的数据使用三角模糊数来描述相对重要性。

表2 在准则O下各元素组对P_1的重要性比较

	性能(P1)	安全(P2)
性能(P1)	(1,1,1)	(1,2,3)
安全(P2)	(1/3,1/2,1)	(1,1,1)

据式(2)计算综合重要程度值：

$S_{P1}=(0.33,0.67,1.2)$；$S_{P2}=(0.22,0.33,0.6)$

由式(3)计算出各元素组重要于其他元素组的可能性程度。

$d(S_{P1})=1.0$；$d(S_{P2})=0$

经过归一化后，得到权重向量为$W_{P1}=(1.0,0.0)^T$。

同样也可以建立在信任评估值最大、安全准则下的元素层的模糊判断矩阵。得到权重向量$W_{P2}=(0.5,0.5)^T$。由此可以得到一个加权矩阵：

$$A=\begin{pmatrix} 1.0 & 0.5 \\ 0.0 & 0.5 \end{pmatrix}$$

在本文所建立的模型中，网络层中有两个元素集，即性能属性集和安全属性集。分别以信任评估值最大为准则，元素集中的元素为次准则，建立两两比较矩阵，如在位置变化次数(Q_{24})一定的准则下，性能属性集内的元素间的两两比较矩阵如表3所列。所得的相对权重即为超矩阵的子块。

表3 位置变化次数(Q_{24})的准则下性能属性集内的两两比较矩阵

Q_{24}	Q_{11}	Q_{12}	Q_{13}	Q_{14}
Q_{11}	(1,1,1)	(1/3.2/5,1/2)	(1.2,4)	(1/2,2/3,1)
Q_{12}	(2,5/2,3)	(1,1,1)	(1/6,1/4,1/2)	(1/4,1/3,1/2)
Q_{13}	(1/4,1/2,1)	(2,4,6)	(1,1,1)	(1/5,1/3,1)
Q_{14}	(1,3/2,2)	(2,3,4)	(1,3,5)	(1,1,1)

得到归一化的权重向量为$W=(0.20656,0.16930,0.27633,0.34782)^T$。

(2) 建立ANP结构的超矩阵

用同样的方法求出其他的矩阵，并得到相应的相对权重。得到所有的相对权重就可以构造ANP矩阵，即本文应用中由相互作用元素的16个两两比较的相对权重组成的超矩阵，如表4所列。

表4 超矩阵

	Q_{11}	Q_{12}	Q_{13}	Q_{14}	Q_{21}	Q_{22}	Q_{23}	Q_{24}
Q_{11}	0.40116	0.27891	0.30074	0.27122	0.25873	0.36115	0.39109	0.20656
Q_{12}	0.20012	0.22102	0.28929	0.25895	0.21932	0.20016	0.02603	0.16930
Q_{13}	0.17023	0.28001	0.24063	0.27041	0.19786	0.15071	0.21012	0.27633
Q_{14}	0.22849	0.22006	0.16934	0.19942	0.32409	0.28798	0.37276	0.34782
Q_{21}	0.37252	0.23112	0.12526	0.28025	0.26115	0.22405	0.15787	0.21338
Q_{22}	0.10333	0.34248	0.31225	0.14779	0.39322	0.32547	0.28773	0.24313
Q_{23}	0.26560	0.16654	0.31267	0.18038	0.25251	0.18193	0.24082	0.28574
Q_{24}	0.25855	0.25986	0.24982	0.39158	0.09311	0.26855	0.31358	0.25775

超矩阵中的每一个子块都是归一化的，但是超矩阵本身并不是归一化的。因此，要对超矩阵的元素加权，得到一个加权超矩阵。之后，就是ANP的核心工作，即解超矩阵，加权矩阵自相乘，直到得到一个积收敛、长期稳定的极限矩阵为止，如表5所列。

表5 极限超矩阵

	Q_{11}	Q_{12}	Q_{13}	Q_{14}	Q_{21}	Q_{22}	Q_{23}	Q_{24}
Q_{11}	0.14614	0.14614	0.14614	0.14614	0.14614	0.14614	0.14614	0.14614
Q_{12}	0.08643	0.08643	0.08643	0.08643	0.08643	0.08643	0.08643	0.08643
Q_{13}	0.12865	0.12865	0.12865	0.12865	0.12865	0.12865	0.12865	0.12865
Q_{14}	0.12504	0.12504	0.12504	0.12504	0.12504	0.12504	0.12504	0.12504
Q_{21}	0.10877	0.10877	0.10877	0.10877	0.10877	0.10877	0.10877	0.10877
Q_{22}	0.13099	0.13099	0.13099	0.13099	0.13099	0.13099	0.13099	0.13099
Q_{23}	0.12293	0.12293	0.12293	0.12293	0.12293	0.12293	0.12293	0.12293
Q_{24}	0.15105	0.15105	0.15105	0.15105	0.15105	0.15105	0.15105	0.15105

这是一个非常复杂的计算过程，手工运算几乎不可能完成。可以利用MATLAB，Super Decision等工具软件来求解，这里使用AHP/ANP方法的专用工具Super Decision，得到

的极限超矩阵各行的非零值均相同。各行对应的值为各元素相对于目标的稳定的权重。取极限超矩阵任一列得到最后的排序向量。

(3) 用户行为信任值的计算

在进行用户行为的信任度计算时，各特性权重的确立发生在计算之前。假设已经获得了各元素的评估值(节点行为证据的量化值)，可以利用各元素的评估值和各元素的权重来评估节点的信任值。设元素的评估值向量为 $A=(a_1,a_2,\cdots,a_n)$，元素的权重向量为 $W=(w_1,w_2,\cdots,w_n)$，则计算节点的信任值有式(4)适用：

$$A*W=(a_1a_2\cdots a_n)(w_1w_2\cdots w_n)^{\mathrm{T}}=\sum_{i}^{n}a_iw_i \tag{4}$$

到此就完成了基于 FANP 的用户行为的信任评估。

基于 FANP 的用户信任评估模型通过递阶层次结构模型对用户信任进行逐层分解，把用户信任这一笼统的、抽象的概念分解成了直观的、具体的指标。通过建立用户信任评估公式实现用户证据和用户属性的"有机"组合。模型中恰当地运用了 FANP 方法，解决了评估中需要的用户行为信任证据和属性的具体权重分配问题，体现了用户信任评估的主观性和评估内容的客观性。评估模型和评估公式的建立及其与 FANP 方法的结合使模型具有很好的实用性和可扩展性，并体现了信任本身的特性。

3 基于用户行为信任的云计算控制策略

定义 2 信任等级 $R=\{R_1,R_2,\cdots,R_n\}$，若信任值 $e\in[r_m,r_{m+1}]$，则称 e 落在信任等级 R_m 内，其中 r_m、r_{m+1} 是信任等级 R_m 的下限值和上限值。又设用户行为的信任值 $e\in[lr,ur]$ 是一连续随机变量，其概率分布函数为 $f(e)$，则 r_m 满足条件 $lr=r_1<r_2<\cdots<r_m<\cdots<r_n=ur$，且

$$P(r_m<e<r_{m+1})=\int_{r_m}^{r_{m+1}}f(e)\mathrm{d}e=TP_m \tag{5}$$

$$(0<TP_m<1,m\in\mathbf{N},1\leqslant m\leqslant n)$$

式中，TP_m 称为该信任等级的阈值。

设信任划分为 $R=$｛很不信任，不信任，较信任，信任，很信任｝等 5 个等级，函数 $f(e)$ 不是本文讨论的重点，假设 $f(e)$ 函数曲线如图 2 所示，则 R 的区间可按图选取，选取 $TP=\{5\%,15\%,60\%,15\%,5\%\}$，即较信任用户行为应该为大多数(80%)，而不信任或很信任的行为只是很少一部分。

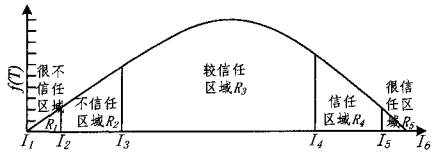

图 2 信任等级划分

如果 $e\in[r_m,r_{m+1}]$，$m=0,1,2,3,4,5$，则用户行为的信任等级为 R_m。如图 2 所示，如果 $R_m=R_1$，说明用户行为的信任等级为很不信任，针对处于这一信任等级的用户，云服务提供商可以采取拒绝为用户提供服务的策略来防止非法用户滥用或破坏云服务提供商的资源并对其做出惩罚，比如列入黑名单等；如果 $R_m=R_2$，说明用户行为的信任等级为不信任，针对处于这一信任等级的用户，云服务提供商可以采取限制用户访问的策略，比如只给用户很低的权限，只能做有限的不会对云服务提供商的安全造成影响的操作，并对用户提出警告以免其继续采取不信任的行为而降到很不信任的等级。因此，划分信任等级的目的是希望针对不同的用户信任值采用不同的措施，来保证用户接入网络的安全。e 值反馈给用户，能够指导用户采取更为信任的行为，以提高用户使用终端的安全意识。图 3 显示了整个评估过程的控制流程图。

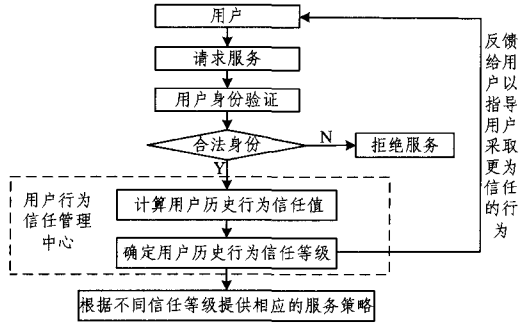

图 3 控制流程图

结束语 面对云计算开放的运行环境，有效地对云终端用户行为进行评估，是在复杂动态环境下保证云安全的基础，也是解决可信网络中用户端可信的基础。通过用户行为的可信评估，结合实时行为可信的监控能够对未来用户行为可信进行预测，从而为云计算环境的安全提供保证，为主动安全机制的实现奠定基础。用户行为的评估是可信网络中的重要内容，本文提出的基于三角模糊数的模糊网络分析法用于对用户行为各属性和因素权重进行量化分析，使权重结果更加精确和客观，体现了影响用户行为信任的各层影响因素之间的相互作用和相互依存关系，同时也减少了个人主观对评价结果的影响，较好地保证了评价结果的准确性，不仅为云服务提供者采用何种策略响应云端用户行为请求提供了科学的量化依据，也为用户改进自身行为提供了指导。但是基于 FANP 的用户行为的信任评估还有一些地方需要更进一步地研究：(1)信任值的扩展，将其他成熟的系统中获得的用户行为信任值扩展到当前系统，并结合当前系统中的用户行为共同获得更精确的用户行为信任值，这尤其适用于一个系统初期用户行为信任值的建立；(2)优化节点评估值计算算法，降低计算信任值的时间复杂度，在云计算环境下，用户规模和行为证据量庞大的情况下显得尤为重要；(3)利用随机 Petri 网的理论分析工具对评估系统的性能进行等价分析，从而为改进系统性能提供依据。

参 考 文 献

[1] Lin Chuang, Wang Yuan-zhuo, Tian Li-qin. evelopment of Trustworthy Network and Facing Scientific Challenges [J]. DZTE Communications, 2008, 14(1): 13-16

[2] Lin Chuang, Tian Li-qin, Wang Yuan-zhuo. Research on User Behavior Trust in Trustworthy Network [J]. Journal of Computer Research and Development, 2008, 45(12): 2033-2043

[3] Zhao Jie, Xiao Nan-feng, Zhong Jun-rui. Behaviour Trust Control Based on Bayesian Networks and User Behavior Log Mining [J]. Journal of South China University of Technology: Natural Science Edition, 2009, 37(5): 94-100

(下转第 138 页)

$$PK=q^{SK_0 2T+1} \bmod p \tag{17}$$

公开大素数 p,q 和计算得到的用户 A 的公钥 PK 和 T。

用户根据所设定的时间段不断对私钥进行变换,得到新的私钥,再将旧的私钥进行删除。

设 j 为时间段,则私钥的更新方法如下所示:

如果 $j=T+1$,则 SK_j 为空,即用户私钥的有效期已到。

如果 $1\leqslant j<T+1$,则用式(18)计算下个时间段的用户私钥:

$$SK_{j+1}=SK_j^2 \bmod p-1 \tag{18}$$

4 算法仿真

在相同的安全强度下,算法采用密钥长度越小,其安全性能越高。本文在同样的网络中对 RSA 算法、原有 ECC 算法和改进 ECC 算法进行安全性能测试,其实验结果如图 1 所示。

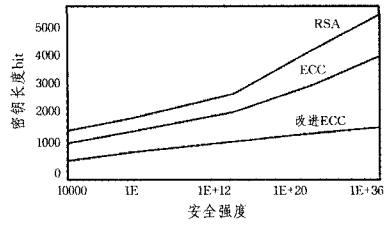

图 1 安全性能比较统计

从图 1 可以看出,经过本文改进后的 ECC 算法的抗网络攻击性能比其他算法更为优秀,且为了提高其安全性能而增加密钥长度的增长幅度比 RSA 算法和 DSA 算法小很多,具体比较如表 1 所列。

表 1 相同安全强度下模长比较

攻破时间	RSA 密钥长度	ECC 密钥长度	改进 ECC 密钥长度
104	512	106	96
108	768	132	118
1011	1024	160	124
1020	2048	210	156
1078	21000	600	418

从表 1 可以看出,在相同安全强度下改进 ECC 算法的密钥尺寸相对较小,说明其占用空间也小,这就意味着其防网络攻击能力更强。所有这些优势,使得改进 ECC 算法的安全性能比之以前的 RSA 算法和一般 ECC 算法来得更强。

从图 2 可以看出,在相同的网络中,分别采用 RSA 算法、ECC 算法和改进 ECC 算法进行加密,并使用穷举密码破解法对其进行解密操作,对改进 ECC 算法加密的信息进行解密的时间远大于 RSA 算法和 ECC 算法。综上所述,本文提出的改进 ECC 算法大大提高了网络信息的安全性能,达到了安全高效的目的。

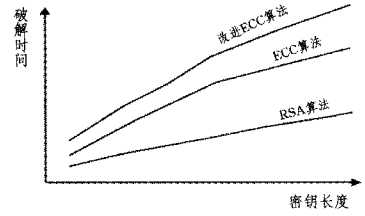

图 2 3 种算法破解时间比较

结束语 本文针对目前网络信息安全现状,提出了一种基于网络信息安全的改进 ECC 算法。该算法基于原有的 ECC 算法,对其进行点积运算的优化和平方剩余判定的优化,以提高原有 ECC 算法的安全性能。实验证明,改进 ECC 算法比普遍使用的 RSA 算法和原有的 ECC 算法安全性能更高。

参 考 文 献

[1] 赵龙,韩文报,杨宏志. 基于 SIMD 指令的 ECC 攻击算法研究[J]. 计算机研究与发展,2012,49(7):1553-1559

[2] 徐劲松,王志新,严迎建. ECC 专用指令处理器软硬件协同设计[J]. 计算机工程与设计,2012,33(3):916-920

[3] 尤马彦,凌捷,郝彦军. 基于 Elman 神经网络的网络安全态势预测方法[J]. 计算机科学,2012,39(6):61-63

[4] 罗利民,周震. 基于 IPV6 的网络安全入侵检测技术研究[J]. 科技通报,2012,28(4):114-115

[5] 陈亮,潘惠勇. 网络安全风险评估的云决策[J]. 计算机应用,2012,32(2):472-474

[6] 贺志强,楼芳,李亮. 基于攻击距离的攻击图优化方法[J]. 计算机工程与科学,2012,34(2):9-12

[7] 王庚,张景辉,吴娜. 网络安全态势预测方法的应用研究[J]. 计算机仿真,2012,29(2):98-101

[8] 查东辉. 网络蠕虫传播模型的分析与仿真研究[J]. 计算机仿真,2012,29(2):124-127

[9] 张栋毅. 校园网络安全分析与安全体系方案设计[J]. 计算机应用,2011,31(2):116-118

[10] 李志刚. 网络通信中加密算法优化仿真研究[J]. 计算机仿真,2011,28(12):130-133

[11] 熊万安,许春香. 一种新的基于 ECC 的 Ad hoc 组密钥协商协议[J]. 重庆邮电大学学报:自然科学版,2011,23(1):101-106

(上接第 135 页)

[4] Tian Li-qin, Lin Chuang, Sun Jin-xia. A kind of prediction method of user behavior for future trustworthy network [C]// Proc. of ICCT 06. Beijing: IEEE Press, 2006: 199-202

[5] Guo Shu-kai, Tian Li-qin, Shen Xue-li. Research on FAHP method in user behaviour trust computation[J]. Computer Engineering and Applications, 2011, 47(12): 59-61

[6] Tian Li-qin, Lin Chuang. A Kind of Game-Theoretic Control Mechanism of User Behavior Trust Based on Prediction in Trustworthy Network [J]. Chinese Journal of Computers, 2007, 30(11): 1930-1938

[7] Chen Ya-rui, Tian Li-qin, Yang Yang. Model and Analysis of User Behavior Based on Dynamic Game Theory in Cloud Computing[J]. Acta Electronica Sinica, 2011, 39(8): 1818-1822

[8] Saaty T L. Decisions with the Analytic Network Process(ANP) [C]// ISAHP'96 CANADA. University of Pittsburgh., USA, 1996

[9] Van Laarhoven P J M, Pedrycz W A. fuzzy extension of Statty's Priority theory[J]. Fuzzy Sets and Systems, 1983, 11: 229-241