

## 网络安全风险评估的云决策

陈亮<sup>1\*</sup>, 潘惠勇<sup>2</sup>

(1. 河南工业大学 信息科学与工程学院, 郑州 450001; 2. 中原工学院 计算机学院, 郑州 450007)

(\* 通信作者电子邮箱 13633855397@163.com)

**摘要:** 为了更合理地评估网络安全风险, 利用云模型集成随机性和模糊性的优点, 提出一种基于云模型的网络安全风险评估和决策方法。首先, 通过采样系统正常状态信息, 构造标准概念云; 在进行风险评估时, 采样处于风险状态时的信息, 计算其云数字特征; 然后利用改进的基于云滴距离的云相似度算法, 计算与标准概念云的相似度, 相似度最大的即为最终输出结果。最后, 通过 Kddcup99 数据集进行模拟攻击及性能采样仿真实验。结果表明, 该方法最大限度地保留了风险评估过程中固有的不确定性和模糊性, 提高了评估结果的可信性。

**关键词:** 网络安全; 风险评估; 云模型; 模糊性; 随机性

**中图分类号:** TP393.08; TP181 **文献标志码:** A

### Cloud-model based decision-making for network risk assessment

CHEN Liang<sup>1\*</sup>, PAN Hui-yong<sup>2</sup>

(1. College of Information Science and Engineering, Henan University of Technology, Zhengzhou Henan 450001, China;

2. School of Computer Science, Zhongyuan University of Technology, Zhengzhou Henan 450007, China)

**Abstract:** In order to assess the risk of network security more reasonably, a cloud-model based method for network risk assessment was proposed. It took advantage of cloud model featuring perfect combination of randomness and fuzziness. Firstly, standard clouds were constructed by sampling normal system status. When making risk assessments, the current risk state was sampled to calculate the cloud characteristics, then the cloud similarity algorithm based on the distance measurement of cloud droplets was used to calculate the similarity between them, and the biggest similarity was the final output. Finally, Kddcup99 data set was used to do simulated attack and performance sampling test. The experimental results show that the proposed method retains the maximum uncertainty of network intrusion assessment and improves the credibility of the results.

**Key words:** network security; risk assessment; cloud model; fuzziness; randomness

## 0 引言

目前, 网络安全事件层出不穷。但所有的网络安全防御措施都无法保证网络的绝对安全。因此, 对网络所面临的安全风险进行实时感知和分析评估(如危险程度大小)就非常重要。目前, 静态的网络风险评估模型<sup>[1]</sup>可以对网络长期所处的风险状态进行粗略评估, 但无法实时检测网络正在遭受的攻击, 缺少自适应性。动态网络风险评估方面, 文献[2]提出了基于主机的实时风险评估; 文献[3]提出了使用网络节点关联性的分析方法; 文献[4]提出了基于隐马尔可夫模型(Hidden Markov Model, HMM)的实时网络安全风险量化方法; 文献[5]提出了基于人工免疫的风险检测和评估方法; 文献[6]使用云模型对内部威胁进行感知; 文献[7-11]分别使用层次分析法、信息熵、核函数、粗糙集、概率风险分析法、模糊集合分析法等智能方法对网络风险进行评估; 文献[12]通过云控制器和规则实现了网络风险的分析和评估。

由于网络入侵具有随机性, 而对网络风险的评估一般用自然语言来描述(如危险、安全), 具有一定的模糊性, 并且随机性和模糊性之间具有一定的关联。此外, 网络风险程度是定性概念, 而引起网络风险变化的各个参数的值是定量的。典型的网络风险评估方法中, 多是单一地从定性(定量)角度去分析<sup>[1-5]</sup>, 或者分别从随机性和模糊性的角度去分析网络风

险<sup>[7-11]</sup>, 因此, 评估的结果还不够客观。基于此, 本文利用云模型有效集成了模糊性和随机性的特点, 提出一种基于云模型的网络风险评估方法。用云模型从多角度将网络入侵的定性、定量特征融合分析并进行决策, 同时兼顾网络风险的模糊性和随机性的特点, 提高了入侵风险评估的准确性和客观性。

## 1 理论基础和设计思想

### 1.1 云模型的基本概念

云模型能够实现用语言值表示的某个定性概念与其定量(数值)表示之间的不确定转换。它主要反映知识中概念的两种不确定性: 模糊性和随机性以及二者之间的关联性<sup>[13]</sup>。

云模型中云由许许多多云滴组成, 云的整体形状反映了定性概念的重要特性。云用期望值  $Ex$ 、熵  $En$ 、超熵  $He$  三个数值特征来表示, 记作  $C(Ex, En, He)$ , 即云的向量特征。它们反映了定性知识的定量特性: 期望  $Ex$  反映了相应的定性知识的信息中心值; 熵  $En$  是定性概念随机性的度量, 反映了能够代表这个定性概念的云滴的离散程度; 超熵  $He$  是熵  $En$  的熵, 反映了云的离散程度。超熵的大小间接地反映了云的厚度, 即确定度的不确定性,  $He$  越小, 说明随机性越小。经统计分析, 对于论域  $U$  中定性概念  $C$  有贡献的云滴(占 99.74%)主要落在区间  $[Ex - 3En, Ex + 3En]$ , 因此这个区间以外的云滴对定性概念的贡献可以忽略<sup>[13]</sup>。

收稿日期: 2011-08-08; 修回日期: 2011-09-26。 基金项目: 郑州市科技发展计划项目(2010GYXM374)。

作者简介: 陈亮(1978-), 男, 河南开封人, 讲师, 主要研究方向: 人工智能、网络安全; 潘惠勇(1977-), 男, 河南南阳人, 讲师, 主要研究方向: 软件工程、网络安全。

## 1.2 设计思想

在网络中,当主机遭受到入侵攻击时,其主要性能指标(如CPU占用率、内存占用率)必然会发生异常变化,同时,这些变化的幅度也决定了网络风险大小。因此,可以根据系统主要指标的变化来确定网络面临的风险程度。网络入侵的发生具有很大的随机性,而对网络入侵风险的评估多采用自然语言来描述,这导致风险评估结果又具有一定的模糊性;同时,在遭受到入侵时候,各参数之间的变化是相互关联的(比如,CPU占用率的提高往往跟内存占用率有关系)。因此,必须实现定量定性之间的转换,以及考虑模糊性和随机性的关联,才能更准确地评估风险。云模型把定性概念的模糊性和随机性及二者的关联性有效集成在一起,构成定性和定量相互间的转换。因此,可以采用云模型描述多个系统参数及其变化之间的关联性,从而对网络风险进行评估决策。

本文方法的基本任务为:根据系统当前性能指标的状态值,依据设计的云决策发生器,输出系统的危险级别。具体思想和实现过程如下:1)确定出能够影响系统性能的主要指标并形式化;2)设置系统的状态为(不正常,不太正常,基本正常,正常),相应的风险评估结果为(高,较高,较低,低),对相应危险级别的系统资源变量进行采样,利用逆向正态云算法计算相应级别的标准概念云;3)定量输入处理,根据云相似度算法,对于某一时刻的输入,输出系统的危险程度(高,较高,较低,低)。

## 2 关键技术与实现

**定义1** 风险评估模型为  $W = (F, V, E)$ , 其中,  $F, V, E$  分别代表因素集、权重集、评价集。因素集  $F = (F_1, F_2, \dots, F_n)$  分别代表影响网络风险评估值的  $n$  个因素,如CPU占用率、内存占用率、进程响应时间等;权重集  $V = (V_1, V_2, \dots, V_n)$  代表各因素所占的权重,且  $V_1 + V_2 + \dots + V_n = 1, V_i > 0 (1 \leq i \leq n)$ ; 风险结果评判集设为  $E = (\text{高}, \text{较高}, \text{较低}, \text{低})$ 。

**定义2** 系统变量云。定义系统变量云为:  $Cloud = (S, T, En, Ex, He)$ , 其中  $S$  代表需要采样的系统资源集合(包括内存占有率、CPU占有率、进程响应时间等),  $T$  为采样时间间隔。

### 2.1 云发生器的构造

云发生器的构造需要先验知识。虽然网络入侵的出现具有不确定性和难以预知性,但正常状态(安全状态)是确定的,同时某些已知入侵发生时系统的状态也是可得的。因此,可以得到正常状态下的数字特征,从而得到标准概念云。

#### 1) 标准概念云的生成。

在网络正常运行情况下,采用滑动窗口的方式<sup>[6]</sup>对系统参数进行连续采样,获取正常状态样本点,将样本点的各维(即各系统参数)规格化到  $[0, 1]$  内(这里尽可能多地进行采样,以便使结果更加准确)。由于网络风险评估中,只能得到采样到的一组数据值,而很难获得确定度,所以,本文采用未知确定度的逆向云发生器算法<sup>[12-13]</sup>,用此算法求出此云的数字特征,然后采用正向云生成算法,得到该正常概念云。

#### 2) 其他状态的概念云生成关键技术。

对于其他概念云的生成,本文采用实际数据采集与估算相结合的方法。理想情况下,“正常”概念云与“不正常”概念云有交集,说明两个概念可覆盖整个状态空间。但实际上对网络系统而言,不适宜直接划分为“正常”与“不正常”两个状

态。因此,在本文中,对两概念云之间未覆盖的区域进一步划分,生成四概念云(正常,基本正常,不太正常,不正常)以更好地满足定性描述网络风险的需要。

将正常云的重心  $Ex_z$  和  $Ex_F$  之间的区域平分为两部分,分别设为基本正常和不太正常概念云。根据云滴对概念的贡献,论域中对概念有贡献的云滴,主要落在区间  $[Ex - 3En, Ex + 3En]$ <sup>[13]</sup>。本文中,基于黄金分割率的云生产方法,相邻云的熵和超熵,预设较小者是较大者的 0.618 倍,估算出  $Ex_{z1}$ (较正常)和  $Ex_{F1}$ (较不正常)。最后,生成四尺度的概念云(不正常,不太正常,基本正常,正常),将其投影到一维平面上,如图1所示。

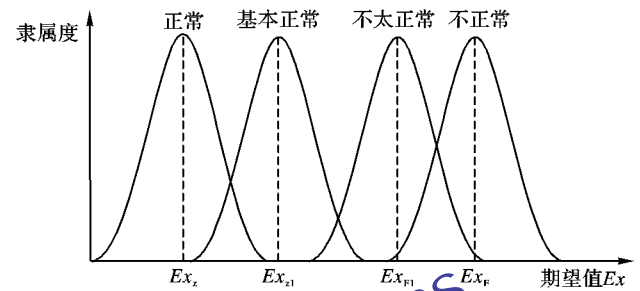


图1 四概念云在内存上的投影示意图

### 3) 综合评价云的生成。

其他各系统参数的概念云的生成类似,将其综合可以得到综合评估。权重的设置方法为对每个因素都分配相应的云权重(用云来描述权重)<sup>[14]</sup>,让云权重参与综合评判,最终通过云计算得到基于云滴分布的综合评价结果,改善了直接对期望值上界溢出进行修正而导致的不科学性函数。

### 2.2 网络入侵风险的评估和决策过程

本文方法的主要目的在于:根据当前系统变量值,直接感知出系统的安全风险,以正确评估风险。根据实际采集到的样本值,计算此时的  $C(Ex, En, He)$  和云模型,然后根据下面的云相似度算法(算法1),计算此云与已知概念云的相似度,相似度最高的即作为输出。算法1通过产生一定数量的云滴,基于云滴之间的距离来度量云的相似度。

#### 算法1 两个云相似度度量算法。

输入:  $C_0$  的数字特征  $C_0(Ex, En, He)$ ,  $C_1$  的数字特征  $C_1(Ex, En, He)$ , 产生的云滴数  $n$ ;

输出: 两个云的相似度量值  $s$ 。

具体步骤如下:

- 1) 使用正向云生成算法依次生成云  $C_0$  和  $C_1$  的  $n$  个云滴,保存云滴的横坐标,并分别记为:  $drop_0(n) = (x_0(1), x_0(2), \dots, x_0(k), \dots, x_0(n))$ ,  $drop_1(n) = (x_1(1), x_1(2), \dots, x_1(k), \dots, x_1(n)) (1 \leq k \leq n)$ 。
- 2)  $sort(drop_0(n)), sort(drop_1(n))$ , 对云滴按横坐标从小到大进行排序。
- 3) 分别筛选出落在  $[Ex - 3En, Ex + 3En]$  范围内的云滴;
- 4) 经过筛选后,  $drop_0(n) \rightarrow drop_0'(n_0)$ ,  $drop_1(n) \rightarrow drop_1'(n_1)$ , 分别得到  $n_0$  和  $n_1$  个云滴。
- 5) 设  $l = \min(n_0, n_1)$ , 假设  $n_0 < n_1$ , 则云滴  $drop_1'$  有  $C_{n_1}^{n_0}$  个组合  $drop_{1k}' (k \in (1, 2, \dots, C_{n_1}^{n_0}))$ ; 如果  $n_0 > n_1$ , 计算类似。
- 6) 依次计算云滴  $drop_0'$  和云滴  $drop_1'$  距离  $dis(k) = (x_{(0)k} - x_{(1)k})^2 (k \in (1, 2, \dots, C_{n_1}^{n_0}))$ 。

7) 定义二者之间的距离  $d = \text{Sqrt} \left( \sum \text{dis}(k) / C_{n_1}^0 \right) / l_0$ 。

8) 定义二者之间的相似度  $s_1 = 1/d$ , 距离越小, 相似度越大。

同样, 用算法 1 可以得到算出其他 3 个标准评估云  $C_2, C_3, C_4$  所对应的相似度  $s_2, s_3, s_4$ , 比较  $s_1, s_2, s_3, s_4$ , 选出最大的  $s_i (1 \leq i \leq 4)$  所对应的云  $C_i (1 \leq i \leq 4)$  就是与  $C_0$  最相似的云, 也即输出结果。

表 1 为本文提出的云相似度度量方法与基于属性相似度的云模型算法<sup>[14]</sup>度量结果的比较。

表 1 云相似度算法比较

云特征 $C(Ex, En, He)$	风险评估结果	
	文献[14]方法	本文方法
$C(3, 2.0, 0.6)$	低	低
$C(10, 3.8, 1.3)$	较低	较低
$C(38, 4.1, 1.2)$	较高	较高
$C(50, 2.0, 0.4)$	高	高

从表 1 可以看出, 两种相似性度量方法均可以正确度量两个云之间的相似度, 进而得到正确的评估结果。与基于属性相似度的云模型算法<sup>[14]</sup>相比, 本文方法是基于云滴之间的距离来计算的, 避免了属性权值等复杂计算, 算法更加简单。本文算法在度量云模型之间相似性方面的优点表现为: 它不仅考虑了云模型中所产生云滴之间的局部相似性, 还考虑了云模型整体形状之间的全局相似性, 使得该算法具有良好的泛化推广性能。

### 3 系统仿真实验

#### 3.1 仿真过程与结果

在 Windows 环境下, 用 VC 语言对算法进行了验证, 数据集为美国林肯实验室 Kddcup99 数据。具体步骤简述如下: 1) 用不含任何攻击流量的训练数据作为系统正常状态, 从  $t$  时刻开始, 以周期  $T$ , 分别对 CPU 占用率和内存占用率进行 20 次采样, 利用逆向云生成算法计算出其数字特征  $C_{\text{good}} = C(10, 2.2, 0.5)$ , 得到系统正常状态云。2) 分别进行 PROBE (端口扫描) 攻击、R2L (远程登录) 攻击、DoS (拒绝服务) 攻击, 作为系统基本正常、不太正常、不正常状态的采样环境, 得到  $C_{\text{comm}} = C(20, 2.8, 1.3)$ ,  $C_{\text{worse}} = C(35, 4.1, 1.2)$ ,  $C_{\text{bad}} = (50, 3.0, 0.4)$ 。这样就得到 (正常, 基本正常, 不太正常, 不正常) 状态云集合, 相应的风险评估结果为 (低, 较低, 较高, 高)。3) 进行随机网络攻击, 并采样系统当前的内存占用率和 CPU 占用率作为输入参数进行计算, 得到此时的云特征参数  $C(Ex, En, He)$ 。4) 利用云相似度算法, 计算此时的云与标准概念云的相似度, 相似度最大的为输出结果。5) 重复进行实验多次, 测试系统的性能。

表 2 为部分系统采样值及网络风险决策结果。

表 2 网络安全风险决策结果

系统参数平均采样值		云特征	网络风险
CPU 占用率/%	内存占用率/%	$C(Ex, En, He)$	决策结果
3.0	6.0	$C(3, 2.1, 0.5)$	低
8.4	12.6	$C(11, 3.6, 1.2)$	较低
40.5	36.0	$C(36, 4.2, 1.3)$	较高
52.0	53.5	$C(51, 2.0, 0.5)$	高

从表 2 可以看出, 本方法可以给出正确的评价和决策结果。同时, 从云的数字特征  $C(Ex, En, He)$  可以看出, 风险较

低、较高状态的熵  $En$  和超熵  $He$  相对较大。熵  $En$  较大表明了此定性概念随机性较大, 比较离散, 网络处于此状态具有较大的风险; 超熵  $He$  较大, 说明此时评估结果的不确定性较大。这恰好与现实生活一致: 对网络处于安全、不安全状态的认识和评估, 不同人评估结果差异较小; 而对网络处于较安全、较不安全状态时, 不同人评估结果差异性较大, 也就是说, 结果认定不同的可能性较大。因此, 基于云模型的网络风险评估不仅给出了正确的评估结果, 而且保留了评估过程中的不确定性, 结果具有更好的可理解性。

#### 3.2 相关算法比较分析

本文主要是利用云模型把模糊性与随机性完美结合的优点, 将其引入到网络风险评估中。因此, 主要与基于模糊思想与随机性思想进行风险评估的相关典型算法进行比较。与基于概率的评估方法<sup>[8]</sup>相比, 虽然概率评估方法保留了评估结果的不确定性, 但对评价集合的概率密度函数有严格要求, 而且没有考虑模糊性。与基于模糊思想 (型 1 模糊集) 的评估方法<sup>[7]</sup>相比, 模糊评估方法要求给出确定的隶属度函数, 一旦定义了隶属度, 实际上进入了精确数学, 此后的推理、计算毫无模糊性可言, 因此, 对于相同的输入, 总会得到相同的结果, 不符合人们对自然语言中概念理解的不确定性。型 2 模糊集<sup>[15]</sup>改进了型 1 模糊系统在处理不确定性方面的不足, 进一步给出模糊集合中隶属度值的模糊程度, 处理实际对象的不确定性。型 2 模糊集给出了隶属度函数的隶属度, 使描述的集合模糊性增强, 进一步刻画了模糊现象, 其评估过程与型 1 模糊集相似, 计算较为复杂, 运算量较大<sup>[15]</sup>。云模型方法既反映了性能采样样本出现的随机性, 又反映了隶属程度的不确定性, 揭示了模糊性和随机性之间的关联性, 最大限度地保留了评估过程中固有的不确定性, 并且对语言值的描述采用期望、熵、超熵表示, 具有相同的形态和更好的可理解性, 提高了评估结果的可信度, 推理结果更加合理而且贴近实际。表 3 给出了相关算法的比较分析。

表 3 相关网络风险评估算法比较

算法	模糊性	随机性	量化方法	计算量
模糊集法	✓	×	隶属度	一般
概率方法	×	✓	概率密度函数	一般
型 2 模糊集	✓	✓	隶属度 (次隶属度)	较大
本文算法	✓	✓	云数字特征	一般

注: ✓ 和 × 分别表示是否考虑模糊性与随机性。

### 4 结语

本文提出了一种基于云模型的网络入侵风险评估和决策方法, 设计了一种改进云相似度计算方法, 并验证了其有效性。如何更合理及更准确地采样影响系统的性能参数, 以使评价结果更科学可信, 是下一步研究的方向。

#### 参考文献:

- [1] VISINTINE V. An introduction to information risk assessment [J]. SANS Institute Journal, 2003, 8(5): 101 - 118.
- [2] CHU C K, CHU M. An integrated framework for the assessment of network operations, reliability, and security [J]. Bell Labs Technical Journal, 2004, 8(4): 133 - 152.
- [3] 张永铮, 方滨兴, 迟悦, 等. 网络风险评估中网络节点关联性的研究 [J]. 计算机学报, 2007, 30(2): 234 - 240.

(下转第 479 页)



表4 滚动指纹与指纹数字签名的安全性比较

手指	滚动指纹数字签名			指纹数字签名		
	平均比对相似度	误识率/%	安全性	平均比对相似度	误识率/%	安全性
左手1	2200	0.04	高	567	0.07	相对较低
左手2	1359	0.02		478	0.06	
左手3	1459	0.03		456	0.10	
左手4	1289	0.03		466	0.10	
左手5	1100	0.03		412	0.10	
右手1	2124	0.02		589	0.03	
右手2	1452	0.02		484	0.03	
右手3	1489	0.03		478	0.10	
右手4	1357	0.03		467	0.10	
右手5	1233	0.03		434	0.10	

#### 4 结语

电子商务过程安全性决定了电子商务的发展程度。本文通过结合滚动指纹认证与数字签名的方式很好地解决了信息安全性、保密性和完整性与交易者身份的真实性这两方面的安全问题。采用高精度、高效率的滚动指纹拼接算法以得到具有保障性的认证介质——滚动指纹,并与传统的数字签名整合确保电子商务过程的安全。本文系统一般应用于对电子商务交易信息以及交易者身份的安全认证过程中,相信在成熟的基于滚动指纹数字签名的安全认证体系建立以后,可以将其应用于网上付账等相关电子商务中。

#### 参考文献:

- [1] 马建林. 电子商务安全策略问题研究[J]. 中国科技信息, 2003, (17): 76, 104.
- [2] 刘继州. 信息安全技术在电子商务中的应用[J]. 商场现代化, 2007(16): 92-93.
- [3] 孙冬梅, 裴正定. 生物特征识别技术综述[J]. 电子学报, 2001, 29(Z1): 1744-1748.
- [4] 朱亚涛, 金花, 吕晶. 基于生物特征的身份识别技术[J]. 现代电子技术, 2005, 28(6): 6-7.
- [5] ZHANG LIN, CHEN ZHIXIN. Design and implementation of a E-commerce system based on PKI [C]// CCTAE: 2010 International Conference on Computer and Communication Technologies in Agriculture Engineering. Piscataway: IEEE, 2010: 4-7.
- [6] KUMAR P Y, GANESH T S. Integration of smart card and Gabor filter method based fingerprint matching for fast verification [C]// 2005 Annual IEEE INDICON. Piscataway: IEEE, 2005: 526-529.
- [7] SU M, BODDAERT X, INAL K. Numerical investigations of smart card module: Parametric analysis and design optimization [J]. IEEE Transactions on Device and Materials Reliability, 2008, 8(3): 464-470.
- [8] 邹华, 刘强, 郭成城, 等. 结合指纹识别和智能卡的安全电子商务系统[J]. 计算机工程, 2003, 29(1): 100-102.
- [9] 蒋艳凰, 白晓敏, 杨学军. 数字签名技术及其发展动态[J]. 计算机应用研究, 2000, 17(9): 1-3.
- [10] 毛幼菊, 陆音. 基于指纹识别和数字认证的网络商务系统[J]. 计算机工程, 2003, 29(10): 53-55, 64.
- [11] HONG LIN, WAN YIFEI, JAIN A. Fingerprint image enhancement: Algorithm and performance evaluation [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20(8): 777-789.
- [12] CHEN K, PANDIYAN P M, YAACOB S, et al. Fingerprint feature extraction based Discrete Cosine Transformation (DCT) [C]// ICOCI'06: International Conference on Computing & Informatics. Piscataway: IEEE, 2006: 1-5.
- [13] 张永良. 滑动指纹拼接与指纹匹配的算法研究[D]. 上海: 上海交通大学, 2006: 60-75.
- [14] 韩伟红, 黄子中, 王志英. 指纹自动识别系统中的预处理技术[J]. 计算机研究与发展, 1997, 34(12): 913-920.
- [15] KWON D, YUN I D, LEE S U. Rolled fingerprint construction using MRF-based nonrigid image registration[J]. Image Processing, 2010, 19(12): 3255-3270.
- [16] 段远翔. 结合方向图的指纹特征点提取基于覆盖技术的滚动指纹采集算法[J]. 今日科苑, 2010(8): 38.
- [17] 王朋, 张有光. 指纹图像帧序列拼接的波形匹配算法[J]. 计算机辅助设计与图形学学报, 2009, 21(10): 1467-1471.
- [18] ZHOU JIE, HE DI, RONG GANG. Effective algorithm for rolled fingerprint construction[J]. Electronics Letters, 2001, 37(8): 492-494.
- [19] 叶四民, 陈福祥. 指纹图像处理中的二值化技术[J]. 自动化与仪器仪表, 2001(2): 30-32.
- [10] 高会生, 郭爱玲. 组合核函数 SVM 在网络安全风险评估中的应用[J]. 计算机工程与应用, 2009, 18(4): 27-30.
- [11] 汤永利, 徐国爱, 钮心忻, 等. 基于信息熵的信息安全风险模型[J]. 北京邮电大学学报, 2008, 31(2): 50-53.
- [12] 杨柳, 吕英华. 基于云模型的网络风险评估技术研究[J]. 计算机仿真, 2010, 27(10): 95-98.
- [13] LI DEYI, LIU CHANGYU, GAN WENYAN. A new cognitive model: Cloud model[J]. International Journal of Intelligent Systems, 2009, 24(4): 357-375.
- [14] 张国英, 刘玉树. 基于属性相似度云模型分类器[J]. 北京理工大学学报, 2006, 25(6): 499-503.
- [15] WU D, MENDEL J M. A comparative study of ranking methods, similarity measures and uncertainty measures for interval type-2 fuzzy sets[J]. Information Sciences, 2009, 179(8): 1169-1192.

(上接第474页)

- [4] 李伟明, 雷杰, 董静, 等. 一种优化的实时网络安全风险量化方法[J]. 计算机学报, 2009, 32(4): 793-804.
- [5] LI TAO. An immunity based network security risk estimation [J]. Science in China Series F: Information Sciences, 2005, 48(5): 557-578.
- [6] 张红斌, 裴庆祺, 马建峰. 内部威胁云模型感知算法[J]. 计算机学报, 2009, 32(6): 784-791.
- [7] 赵冬梅, 马建峰, 王跃生. 信息系统的模糊风险评估模型[J]. 通信学报, 2007, 28(4): 51-56.
- [8] 李焕洲, 王祚学, 陈麟. 信息系统安全风险的概率描述及基本特征[J]. 四川大学学报: 自然科学版, 2008, 32(4): 87-90.
- [9] 李顺国, 李汇, 王学国. 基于粗糙集理论的信息化风险分析[J]. 武汉理工大学学报, 2009, 30(7): 67-71.