第 42 卷 第 6A 期
2015 年 6 月
计 算 机 科 学
Computer Science
Vol. 42 No. 6A
June 2015

入侵检测系统的多层次混合评价方法研究

李云婷 夏仲平 熊 婧
(工业和信息化部电子第五研究所软件质量工程研究中心 广州 510610)

摘 要 随着入侵检测系统(IDS)的快速发展,基于各类技术产生的入侵检测系统层出不穷,而目前对于入侵检测系统的评估方法存在不够全面、主观性较强的问题,通过研究分析建立了一套符合目前主流 IDS 的评价指标体系,该体系中指标的选取依据一定的原则,具有广泛性和可信性。并引入层次分析法和变异系数法构建了多层次混合综合评价模型,最终实现了关于混合层次分析法和变异性系数法的混合综合评价算法。该评价方法综合了主观和客观评价法,能够较准确地完成评价 IDS 的任务。

关键词 入侵检测系统,指标体系,层次分析法,变异系数法,多层次混合综合评价模型
中图法分类号 TP301 文献标识码 A

Study on Evaluation Method of Multi-layer Hybrid Intrusion Detection System

LI Yun-ting XIA Zhong-ping XIONG Jing
(Software Quality Engineering Research Center, The 5th Electronics Research Institute of Ministry of Information Industry, Guangzhou 510610, China)

Abstract Increasing sophistication and diversification of network attacks challenge network security seriously. Evaluating intrusion detection system thoroughly and objectively has important implications with various technology-based intrusion detection systems continuously emerging. The evaluation methods most of which involve few evaluation metrics have their own weaknesses such as partial and subjective considerations. Aiming at these issues, a general evaluation system of intrusion detection systems was introduced which can be applied in typical intrusion detection systems, including universal and credible indexes chosen by specific principles. And throught the introduction of AHP and the variation coefficient method, hybrid AHP comprehensive evaluation model was constructed. Finally the algorithm of comprehensive evaluation of mixed layer analysis method and coefficient of variation method was realized. The comprehensive evaluation method of subjective and objective evaluation method can accurately complete the evaluation of the IDS task.

Keywords Intrusion detection system, Index system, AHP method, Variation coefficient method, Mixed AHP comprehensive evaluation model

1 引言

入侵检测系统起源于 1980 年的 James P. Anderson 的《计算机安全威胁监控与监视》,文章第一次详细阐述了入侵检测的概念。从 20 世纪 90 年代到现在,入侵检测系统的研发呈现出百家争鸣的繁荣局面,并在智能化和分布式两个方向取得了长足的进展。Nicholas、J. Puketza 等人在 1994 年率先进行入侵检测系统评估的研究,提出检测范围、检测系统开销及高负荷下的检测能力 3 项通用评估指标,并对 3 项指标进行了入侵鉴别测试、资源使用率测试、高负荷测试[1]。

IDS 的评价目前有采用模糊综合评价法、基于属性测度评价法等,它们基本都是主观赋权值的方法,缺乏客观性,影响 IDS 评价值的实际意义,从而导致评价值与实际产生偏差,用户采购的产品不符合需求;另外目前的评价指标体系缺乏与技术发展的关联性,随着技术的进一步成熟以及市场的需求,IDS 除了发展原来的产品特点,还进一步扩展出新的特征,因此评价指标必须涵盖这些新的指标。为此,本文试图建立一套新的综合评价指标体系,引入主观、客观评价法,建立多层次混合评价模型,通过使用层次分析法和变异系数法,实现目标系统综合评价指标赋权的合理化,尽可能地提高评价结果的可靠性和实用性。

2 评价指标体系

根据国标 GB/T 20275—2006 对入侵检测系统技术要求和测试评价方法,以及对软件的可靠性、易用性要求,建立包括功能、安全性、性能、可靠性、易用性 5 个质量属性的评价指标体系,为 IDS 的评价提供依据。

由于入侵检测系统的复杂性,导致评价指标也同样具有

本文受 2012"核高基"科技专项:基于国产 CPUOS 的办公信息系统应用方案评测及规范研究(2012ZX01045-006-003)资助。
李云婷(1982—),硕士生,主要研究方向为信息系统集成、软件评测与软件工程管理、实验室认可和项目管理,E-mail:lytpea@163.com;夏仲平(1984—),硕士生,助理工程师,主要研究方向为基础软件测试技术,E-mail:xiazp@ceprei.com;熊 婧(1985—),硕士生,工程师,主要研究方向为软件可靠性及安全性测评技术、软件可靠性工程技术与质量保证技术、基础软件测评技术,E-mail:xiongj@ceprei.com。

复杂性，本文对这 5 个质量属性的评价指标进行了筛选，筛选的原则如下：

1)尽量选取每个质量属性中的主要指标项。主要指标项是最能够体现该质量属性的特点以及能够对系统产生较为明显影响的指标项。

2)尽量选取能够区分入侵检测系统不同级别的指标项。该指标项能够较为明显地区分不同层次不同级别的入侵检测系统，为评价不同入侵检测系统提供有力的数据基础。

经过筛选后建立的入侵检测系统的综合评价指标体系如图 1 所示。

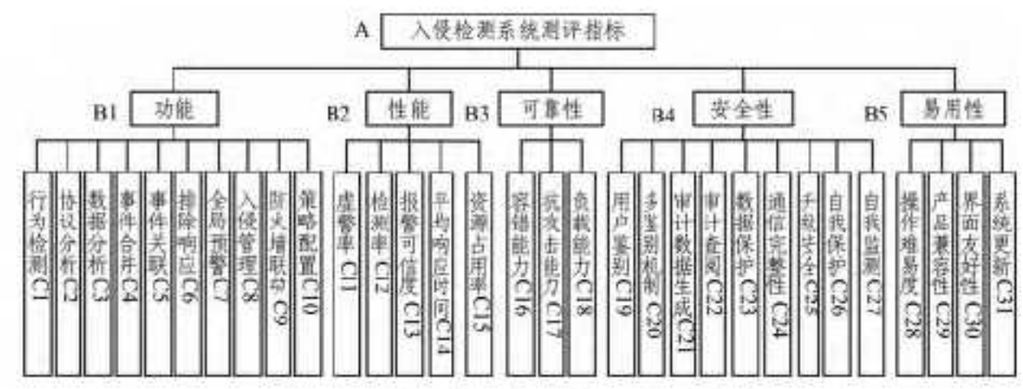

图 1　入侵检测系统综合评价指标体系

本文对该入侵检测系统综合评价指标体系中的部分指标语义解释如下。

2.1　功能指标

(1)行为检测。能够对端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等攻击行为进行检测。

(2)事件合并。能对同类事件采取合并上报，或者能够设置事件合并规则，对符合合并规则的事件信息进行显示。

(3)事件关联。系统可以对同类事件进行分析并报警。

(4)防火墙联动。系统通过所能支持的联动防火墙，按照设定的联动策略自动调整防火墙配置，并且防火墙能实现该配置的功能。

2.2　性能指标

(1)虚警率。系统在检测时出现虚报警告的概率[1]。

(2)报警可信度。系统报警时，受保护对象遭遇入侵攻击的概率。

(3)平均响应时间。从入侵行为发生到入侵检测系统做出响应的平均时间[2]。

2.3　可靠性指标

(1)抗攻击能力。衡量抵抗那些经过特别设计直接以 IDS 为攻击目标的抵抗能力。它主要体现在两个方面：1)程序本身在各种网络环境下能够正常工作；2)程序各个模块之间的通信能够不被破坏，不可仿冒。

(2)负载能力。能维持 IDS 的检测率、虚警率所能达到的最大网络流量、CPU 占用率、内存占用率等资源[3]。

2.4　安全性指标

(1)审计查阅。检测系统应允许授权用户对审计记录进行操作，包括读取、修改和删除审计记录。

(2)数据保护。系统应在遭受攻击时，能够完整保留已经保存的事件数据，能够保护鉴别数据不被未授权查阅和修改[4]。

2.5　易用性指标

(1)操作难易度。包括系统的安装、卸载、界面操作等的难易程度[5]。

(2)产品兼容性。系统所兼容和支持的软硬件平台的情况，包括 CPU、操作系统、基础组件等。

3　多层次混合评价模型

由于图 1 中入侵检测系统综合评价指标体系中的各类指标既有定量、定性指标，又有半定量的指标，如何实现对系统的综合评价，需要采用统一的评价算法对定量、定性及半定量的指标进行统一处理，最终得到综合评价值。

本文的多层次混合评价模型构建的基本思路为：

(1)首先通过采用层次分析法，对目标系统按照综合评价指标体系进行分层处理，确定评价模型为 3 层，第一层为目标系统综合评价，第二层为目标系统所属的质量属性层，第三层为各质量属性所属的指标集；

(2)通过层次分析法计算第二层质量属性层相对于第一层目标系统的权重；

(3)采用变异系数法计算第三层指标集相对于所属的质量属性的权重；

(4)每项指标的最终权重为其质量属性的权重与指标相对于质量属性权重的乘积；

(5)将每项指标最终权重与其指标值的乘积累加得到最终综合评价值。

以下将详细阐述计算过程。

3.1　质量属性层的权重计算

层次分析法又称 AHP 构权法(Analytic Hierarchy Process，AHP)，是将复杂的评价对象排列为一个有序的递阶层次结构的整体，然后在各个评价项目之间进行两两的比较、判断，计算各个评价项目的相对重要性系数，即权重[4]。

本步骤依据层次分析法的思想首先确定指标的量化标准。层次分析法的核心问题是建立一个构造合理且为一致性的判断矩阵，判断矩阵的合理性受到标度的合理性的影响。所谓标度是指评价者对各个评价指标(或者项目)重要性等级差异的量化概念。对于入侵检测系统而言，虽然每项质量属性功能、性能、可靠性、安全性、易用性都对入侵检测系统的综合评价有重要影响，但是影响程度是不同的，通过对各个质量属性的两两评分，来确定各质量属性的相对权重，评分表如表 1 所列。

表 1　评分表

分值 b_{ij}	定义
1	i 与 j 同等重要
3	i 比 j 较为重要
5	i 比 j 更为重要
7	i 比 j 强烈重要
9	i 比 j 极端重要
2、4、6、8	介于上述相邻两级之间重要程度的比较
上述各数的倒数	j 与 i 比较

然后将各质量属性排列成判断矩阵的表格，下发给专家单独进行打分，判断矩阵中第 i 行和第 j 列的元素 b_{ij} 表示质量属性 i 与 j 比较后所得的标度系数。打分完毕，需要计算专家的平均值和标准差，将该结果反馈给专家们，并请专家们再次依据结果提出修改意见得到判断矩阵 B，判断矩阵如表 2 所列。

表 2　判断矩阵

属性 \ 属性	功能	性能	可靠性	安全性	易用性
功能	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
性能	b_{21}	b_{22}	b_{23}	b_{24}	b_{25}
可靠性	b_{31}	b_{32}	b_{33}	b_{34}	b_{35}
安全性	b_{41}	b_{42}	b_{43}	b_{44}	b_{45}
易用性	b_{51}	b_{52}	b_{53}	b_{54}	b_{55}

得到判断矩阵后，需要对该矩阵进行一致性检验，方法如下：

(1)计算判断矩阵每一行数值的乘积并开 n 方根。

1)计算每一行元素的乘积：

$$M_i=\prod_{j=1}^{n}b_{ij},i=1,2,3,\cdots,n \tag{1}$$

2)计算 M_i 的 n 次方根 w_i^*：

$$w_i^*=\sqrt[n]{M_i} \tag{2}$$

对向量 $W^*=[w_1^*,w_2^*,\cdots,w_n^*]$ 正规化，即归一化，其计算公式为：

$$w_i=\frac{w_i^*}{\sum_{i=1}^{n}w_i^*} \tag{3}$$

得到向量 $W=[w_1,w_2,\cdots,w_n]$。

3)计算判断矩阵的最大特征根 $\lambda_{\max}$：

$$\lambda_{\max}=\sum_{i=1}^{n}\frac{(BW)_i}{nw_i} \tag{4}$$

其中，$(BW)_i$ 为 BW 的第 i 个元素。

4)一致性检验

计算一致性指标。

$$CI=(\lambda_{\max}-n)/(n-1) \tag{5}$$

通过计算得出 CI 值，根据表 3 查取相应的平均随机一致性指标 RL。

表 3　平均随机一致性指标

1-9 标度下矩阵阶数	1	2	3	4	5	6	7	8	9
RL	0	0	0.52	0.89	1.12	1.26	1.36	1.41	1.46

计算 CI/RL 的比值，当比值小于 $CI/RL<0.1$ 时，可认为判断矩阵的一致性是可以接受的；否则不通过一致性检验。不通过时，则需要专家重新打分形成新的判断矩阵，直至通过一致性检验。

(2)当判断矩阵 B 通过一致性检验时，取

$$w_{bi}^*=\sqrt[n]{\prod_{j=1}^{n}b_{ij}},1\leqslant i,j\leqslant n \tag{6}$$

作为质量属性 i 的权重值。对 $W_B^*=(w_{b1}^*w_{b2}^*,\cdots,w_{bn}^*)$ 向量进行归一化处理，将归一化后的向量作为质量属性的权重向量[6]。

(3)归一化处理

$$w_{bi}=\frac{w_{bi}^*}{\sum_{1}^{n}w_{bi}^*},1\leqslant i\leqslant n \tag{7}$$

通过归一化后的向量 $W_B=(w_{b1},w_{b2},\cdots,w_{bn})$ 作为质量属性的权重向量。

3.2　指标集的权重计算

在本节中通过变异系数法计算得到指标集的权重。变异系数法(Coefficient of Variation Method)是直接利用各项指标所包含的信息，通过计算得到指标的权重，它是一种客观赋权的方法[7]。此方法的基本思想是：在评价指标体系中，指标取值差异越大的指标，也就是越难以实现的指标，这样的指标更能反映被评价单位的差距。

并且由于在指标集中的指标项数很多的情况下，采用层次分析法，需要两两比较来计算权重，工作量会非常巨大，例如本文的指标数为 31 项，需要进行 $C_{31}^2=465$ 次比较。而采用如变异系数法这样的客观评价法，一方面能减少工作量，另一方面能尽可能地消除人为的主观因素。对于每一个质量属性下的指标集，假设指标集的权重向量为：

$$W_c=(w_{c1},w_{c2},\cdots,w_{cp}) \tag{8}$$

并满足 $\sum_{i=1}^{p}w_{ci}=1$。其中 p 依据每个质量属性下的指标数目而定。计算步骤如下：

(1)对 n 个不同的入侵检测系统按照指标进行测试，再对指标集的指标测试数据进行无量纲化处理，形成标准化矩阵 R，设为 $R=[r_{ij}]_{n\times m}$，其中 n 为入侵检测系统数目，m 为评价指标数目。由于指标集中除了性能能够直接得到测试数据结果，其余指标不能够直接获取定量数据，本文通过采用测试指标的子指标数量与其难度系数的乘积得出：

$$F=\sum_{i=1}^{n}\delta_i*x_i \tag{9}$$

其中，$x_i=\begin{cases}1, & \text{实现了子指标}\\ 0, & \text{没有实现子指标}\end{cases}$，$\delta_i$ 为该项指标的难度系数，该系数为专家对实现该项指标的难度进行打分后的平均值。

(2)分别计算每个指标的平均数和标准差；

$$\bar{x}_i=\sum_{j=1}^{n}x_{ij}/n \tag{10}$$

$$\sigma_i=\sqrt{\sum_{j=1}^{n}(x_{ij}-\bar{x}_i)^2/n} \tag{11}$$

其中，n 为待评价系统数目。

(3)各项指标的变异系数计算公式：

$$V_i=\frac{\sigma_i}{x_i},1\leqslant i\leqslant n \tag{12}$$

式中，V_i 为第 i 项指标的变异系数，也称为标准差系数；σ_i 是第 i 项指标的标准差；$\bar{x}_i$ 是第 i 项指标的平均数。

(4)对变异系数进行归一化处理，得到各指标相对于质量属性的权重：

$$w_{ci}^*=\frac{V_i}{\sum_{i=1}^{p}V_i} \tag{13}$$

(5)最终的指标权重需要将质量属性的权重乘以相对于质量属性权重的指标权重，计算如下：

$$w_{ci}=w_j\times w_{ci}^* \tag{14}$$

其中，w_j 为指标所属的质量属性的权重值。将所有质量属性所属的指标集的权重向量整合成一个向量，记为 $W_c=(w_{c1},w_{c2},\cdots,w_{cm})$，其中 m 为评价指标数。

3.3　综合评价值的计算。

由 3.2 节的计算步骤 1 得到的标准化矩阵 R，与最终的指标权重向量的乘积即为最终的综合评价值 Z：

$$Z=R\times W_C \tag{15}$$

记：

$$z_i=\sum_{j=1}^{m}r_{ij}\times w_{cj} \tag{16}$$

4　实验评价

本实验为了验证本文的多层次混合评价模型是否能有效

对 IDS 进行较为可信的评价，根据第 3 节的多层次混合评价模型的计算方法，开展对 5 种 IDS 进行综合评价。

(1)打分获得判断矩阵。召集 5 位在 IDS 领域的专家，依据表 1 对 5 个 IDS 进行打分，形成初始判断矩阵 B，如表 4 所列。

表 4　初始判断矩阵

属性 \ 属性	功能	性能	可靠性	安全性	易用性
功能	1	1/2	3	2	7
性能	2	1	5	4	8
可靠性	1/3	1/5	1	1/2	4
安全性	1/2	1/4	2	1	5
易用性	1/7	1/8	1/4	1/5	1

(2)获得初始判断矩阵后，对该矩阵进行一致性检验。通过 3.1 节的一致性检验计算步骤，首先计算判断矩阵每行元素的乘积的开方根：

$$w_1^* = \sqrt[5]{1\times1/2\times3\times2\times7}\approx1.838$$

$$w_2^* = \sqrt[5]{2\times1\times5\times4\times8}\approx3.170$$

$$w_3^* = \sqrt[5]{1/3\times1/5\times1\times1/2\times4}\approx0.668$$

$$w_4^* = \sqrt[5]{1/2\times1/4\times2\times1\times5}\approx1.046$$

$$w_5^* = \sqrt[5]{1/7\times1/8\times1/4\times1/5\times1}\approx0.246$$

对向量 $W^* = [w_1^*, w_2^*, w_3^*, w_4^*, w_5^*]$ 归一化得到向量：

$$W = [w_1, w_2, w_3, w_4, w_5]$$
$$= [0.264, 0.455, 0.096, 0.150, 0.035]$$

计算判断矩阵的最大特征根：$\lambda_{\max} = \sum_{i=1}^{5}\frac{(BW)_i}{5w_i} = \frac{1}{5}\left(\frac{1.325}{0.264}+\frac{2.343}{0.455}+\frac{0.525}{0.096}+\frac{0.763}{0.150}+\frac{0.184}{0.035}\right)=5.196$，因此可计算得出：$CI=\frac{5.196-5}{5-1}=0.049$，$\frac{CI}{RL}=\frac{0.49}{1.12}\approx0.044<0.1$。

通过以上计算，该判断矩阵通过一致性检验。

(3)通过以上的一致性检验后，即可获得质量属性的权重向量：

$$W_B = (w_{b1}, w_{b2}, \cdots, w_{b5})$$
$$= [0.264, 0.455, 0.096, 0.150, 0.035]$$

(4)计算指标权重。依据图 1 的入侵检测系统综合评价指标体系，通过对 5 类 IDS 的测试，每项指标测试 5 次，取平均值。依据 3.2 节计算指标集的权重步骤，最终得到系统测试数据及权重值，如表 5 所列。

表 5　系统测试数据及权重值

指标 \ 系统	IDS1	IDS2	IDS3	IDS4	IDS5	平均值 $\bar{x}_i$	标准差 σ_i	变异系数 V_i	权重 w_{ci}^*
C1	89	67	84	95	74	81.8	11.300	0.138	0.029
C2	65	76	78	69	82	74	6.892	0.093	0.019
C3	69	72	65	75	74	71	4.062	0.057	0.012
C4	61	62	57	68	53	60.2	5.630	0.094	0.019
C5	45	37	0	48	0	26	24.073	0.926	0.192
C6	0	8	7	0	0	3	4.123	1.374	0.285
C7	0	12	0	6	9	5.4	5.367	0.994	0.206
C8	24	0	0	27	13	12.8	12.795	0.999	0.207
C9	45	42	37	47	39	42	4.123	0.098	0.020
C10	76	87	83	79	80	81	4.183	0.052	0.011
C11	0.0012	0.0014	0.0008	0.0016	0.0011	0.00122	0.00303	0.249	0.650
C12	0.932	0.912	0.873	0.956	0.947	0.924	0.033	0.036	0.094
C13	87	86	90	83	89	87	2.739	0.031	0.081
C14	0.00454	0.00502	0.00467	0.00454	0.00487	0.00473	0.00212	0.045	0.118
C15	87.54	85.65	84.35	88.43	89.02	86.998	1.953	0.022	0.057
C16	87	85	78	91	89	86	5	0.058	0.317
C17	76	69	73	65	67	70	4.472	0.064	0.350
C18	87	79	81	84	74	81	4.950	0.061	0.333
C19	100	100	100	100	100	100	0	0	0
C20	0	0	17	16	0	6.6	9.044	1.370	0.863
C21	78	81	80	79	79	79.4	1.140	0.014	0.009
C22	90	93	92	92	91	91.6	1.140	0.012	0.008
C23	87	88	84	83	90	86.4	2.881	0.033	0.021
C24	73	74	79	72	75	74.6	2.702	0.036	0.023
C25	65	69	68	71	63	67.2	3.194	0.048	0.030
C26	60	62	59	61	65	61.4	2.302	0.037	0.023
C27	80	83	78	81	86	81.6	3.050	0.037	0.023
C28	85	83	86	89	83	85.2	2.490	0.029	0.242
C29	94	95	94	96	93	94.4	1.140	0.012	0.100
C30	84	86	82	80	84	83.2	2.280	0.027	0.225
C31	65	68	59	66	64	64.4	3.362	0.052	0.433

通过 3.2 节最终的指标集权重计算公式：$W_{ci} = w_j \times w_{ci}^*$ 以及表 4 中的权值，计算得出指标集最终的权值向量：

$$W_C = (w_{c1}, w_{c2}, \cdots, w_{c31})$$
$$= (0.008, 0.005, 0.003, 0.005, 0.051, 0.075, 0.054,$$
$$0.055, 0.005. 0.003, 0.296, 0.043, 0.037, 0.053,$$
$$0.026, 0.030, 0.034, 0.032, 0, 0.192, 0.001, 0.001,$$
$$0.003, 0.005, 0.005, 0.003, 0.003, 0.008,$$
$$0.004, 0.008, 0.015)$$

(5)计算标准化矩阵

由表 4 的测试数据可得到初始指标矩阵 R^*，为了消除不同物理量纲对决策结果的影响，采用文献[4]中改进的归一化

(下转第 443 页)

phic Processor for RSA and ECC[C]// 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors(ASAP'04). ASAP,2004:98-110

[12] Mohammed E, Emarah A E, El-Shennawy K. Elliptic curve cryptosystems on smart cards[C]// 2001 IEEE 35th International Carnahan Conference on Security Technology. Oct 2001:213-222

[13] Koblitz N. Elliptic Curve Cryptosystems [J]. Mathematics of Compution American Mathematical Society, 1987(48):203-309

[14] Johnson D, Menezes A, Vanstone S. The Elliptic Curve Digital Signature Algorithm(ECDSA)[J]. International Journal of Information Security, IJIS, 2001(1):36-63

[15] 王潮,时向勇,牛志华. 基于 Montgomery 曲线改进 ECDSA 算法的研究[J]. 通信学报,2010,31(1):9-13

[16] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C]// Proc. 33rd Hawaii Int'l. Conf. Sys. Sci., Jan., 2000

[17] Clouqueur T, Saluja K K, Ramanathan P. Fault Tolerance in Collaborative Sensor Networks for Target Detection [J]. IEEE Transactions on Computers, 2004, 53(3):320-333

[18] Handy M J, Haase M, Timmermann D. Low energy adaptive clustering hierarchy with deterministic cluster-head selection [C]// Proceedings of the 4th IEEE Conference on Mobile and Wireless Communications Networks. IEEE Communications Society, 2002:368-372

[19] 王潮,贾翔宇,林强. 基于可信度的无线传感器网络安全路由算法[J]. 通信学报,2008,29(11):105-112

(上接第 428 页)

法对矩阵进行标准化处理后,得到标准化矩阵 R:

$$R=\begin{bmatrix}0.218&0.164&0.205&0.232&0.181\\0.176&0.205&0.192&0.187&0.222\\0.195&0.203&0.183&0.211&0.208\\0.203&0.206&0.189&0.226&0.176\\0.346&0.285&0&0.369&0\\0&0.533&0.467&0&0\\0&0.45&0&0.22&0.33\\0.375&0&0&0.422&0.203\\0.214&0.2&0.176&0.224&0.186\\0.188&0.215&0.205&0.195&0.197\\0.203&0.197&0.189&0.207&0.205\\0.2&0.198&0.207&0.191&0.204\\0.208&0.188&0.202&0.208&0.194\\0.199&0.203&0.206&0.197&0.195\\0.202&0.198&0.181&0.212&0.207\\0.217&0.197&0.209&0.186&0.191\\0.215&0.195&0.2&0.207&0.183\\0.2&0.2&0.2&0.2&0.2\\0&0&0.515&0.485&0\\0.196&0.204&0.202&0.199&0.199\\0.197&0.203&0.201&0.201&0.198\\0.201&0.204&0.195&0.192&0.208\\0.196&0.198&0.212&0.193&0.201\\0.194&0.205&0.202&0.211&0.188\\0.195&0.202&0.192&0.199&0.212\\0.196&0.203&0.191&0.199&0.211\\0.199&0.195&0.202&0.209&0.195\\0.199&0.195&0.202&0.209&0.195\\0.199&0.201&0.199&0.204&0.197\\0.202&0.207&0.197&0.192&0.202\\0.202&0.211&0.183&0.205&0.199\end{bmatrix}^{T}$$

(6) 综合评价值计算

由 3.3 节计算公式,可得 5 节中入侵检测系统的最后综合评测值为:

$$Z=R\times W_C=[0.168,0.196,0.249,0.226,0.161]$$

如图 2 所示,综合评测结果显示,IDS3 评测结果最好,IDS4 评测次之,IDS5 最差。

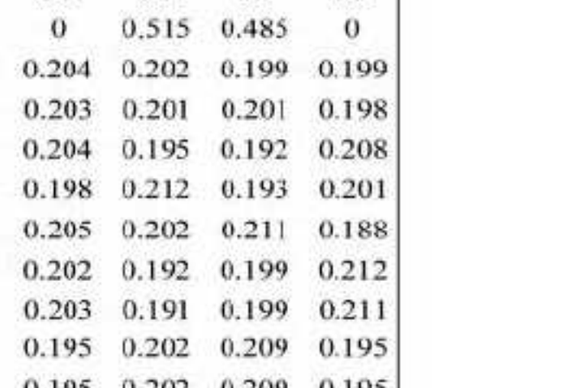

图 2 IDS 综合评测结果

对比表 5 可知,虽然 IDS3 系统在功能方面有 3 项指标为 0,即没有实现该功能,但是由于性能指标以及安全性指标的综合得分高,并且在该两项的权重影响下,评测结果依然是最优的。IDS4 系统在功能方面只有 1 项指标为 0,但是有 3 项性能指标比 IDS3 较差,在性能权重的影响下,综合评测结果比 IDS3 稍差。因此本次实验结果较为真实地反映了入侵检测系统之间的优劣。

如果用户在实际购买 IDS 系统时,还需要综合评估性价比、系统适应场合等因素进行选购,比如性价比最高的 IDS 可能因为没有某一项用户必须要有的重要功能或者检测率没有达到所要求 95% 以上等原因,用户只能退而求其次进行选购。

结束语 本文针对目前入侵检测系统的评价指标体系完整性不足以及大部分采用主观评价法进行评价,对评价模型进行了改进,提出一种基于多层次混合评价模型,该模型算法综合主观和客观评价方法开展对 IDS 的评价,减少了主观因素,同时构建了一套较为完整的指标体系,并且通过本文提出的一种指标量化方法,使得评价结果更具可靠性,对实际选择和评价 IDS 更有现实指导意义。通过实验评测,本文提出的多层次混合评价模型能较为真实地反映入侵检测系统的优劣。本文在指标量化方法中,对指标体系中非性能指标的难度系数采用的是专家打分方法,存在一定的主观因素,在后续的研究工作中将开展对指标难度系数的研究。

参 考 文 献

[1] 甘早斌,何建国. 入侵检测系统的多层次模糊综合评价研究[J]. 计算机应用研究,2006(4):90

[2] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会 GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法[Z]. 2006:1-43

[3] 左国超,段利华. 基于属性测度的入侵检测系统评价方法[J]. 云南大学学报,2006,28(S2):182-186

[4] 曾一五,肖红叶. 统计学导论[M]. 北京:科学出版社,2006:233

[5] 罗嵘. 入侵检测产品的评价指标[J]. 通信技术,2001(2):45-52

[6] 朱珊毅,朱怡安. 基于双层混合法的计算机系统性能评价模型[J]. 微处理机,2010,12(6):114-118

[7] 孙凯,鞠晓峰,李煜华. 基于变异系数法的企业孵化器运行绩效评价[J]. 哈尔滨理工大学学报,2007,12(3):166-167