最优化权值的网络系统风险组合评价模型

张洁卉[1] 潘 超[2] 章 勇[1]
(华中科技大学网络与计算中心 武汉 430074)[1] (湖北经济学院信息与通信工程学院 武汉 430205)[2]

摘 要 网络系统风险受众多因素影响,具有较强的时变性和非线性变化的特点,导致单一模型无法全面描述网络系统风险变化的特点。传统组合模型根据网络系统风险评价确定模型的权值,无法准确描述每一个模型对网络系统风险最终评价结果的贡献,使得网络系统风险评价的准确性差。为了改善网络系统风险评价的效果,文中设计了最优化权值的网络系统风险组合评价模型。首先利用不同模型从不同角度对网络系统风险进行评价,以得到单一模型的预测结果;然后将单一模型的网络系统风险评价结果作为证据体,根据改进证据理论对证据体进行融合,得到网络系统风险的最终评价;最后将提出的方法与其他网络系统风险评价进行了对比测试。测试结果表明,所提模型可以准确地对网络系统风险进行评价,能够反映网络系统风险的变化特点,获得更加理想的网络系统风险评价结果,且评价精度要明显优于其他网络系统风险评价模型。

关键词 网络安全,变化态势,证据体,评价模型,神经网络,支持向量机
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.06.022

Network System Risk Assessment Model with Optimal Weights

ZHANG Jie-hui[1] PAN Chao[2] ZHANG Yong[1]
(Network and Computation Center, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(School of Information and Communication Engineering, Hubei University of Economics, Wuhan 430205, China)[2]

Abstract Network system risk is affected by many factors, and has strong time-varying and non-linear characteristics. As a result, a single model cannot fully describe the characteristics of network system risk change. The traditional combination model cannot accurately describe the contribution of each model on the final evaluation results for network system risk by determining the weight of the model according to the network system risk assessment errors, causing the poor accuracy of network system risk assessment. In order to improve the effect of network system risk assessment, a network system risk assessment model with optimal weights was designed. Firstly, different models are used to evaluate the network system risk from different perspectives, and the prediction results of a single model is obtained. Then, the network system risk assessment results of a single model are taken as an evidence body. According to the improved evidence theory, the evidence body is fused, and then the final evaluation of network system risk is obtained. Finally, the proposed method is compared with other network system risk assessment methods. The test results show that the model can accurately evaluate the network system risk and reflect the changing characteristics of the network security situation. The evaluation accuracy is obviously better than other network system risk assessment methods, and more ideal network system risk assessment results can be obtained.

Keywords Network security, Changing situation, Evidence body, Evaluation method, Neural network, Support vector machine

1 引言

随着网络技术的不断发展,网络用户数量日益增加,网络成为人们交流、沟通的一种重要途径。网络由于是一个开放的系统,因此时刻都有可能受到外界的渗透和攻击,这使得当前网络安全受到了严重挑战[1-3]。网络入侵检测、网络异常状态识别等网络安全防范技术只能检测已经发生异常的网络行为,是一种被动形式的网络安全保护措施,这会使得网络管理员制定相应的防范措施严重滞后,贻误处理威胁的最佳时机,无法有效保证网络的正常运行[4-6]。网络系统风险建模与评价可以对网络将来存在的风险和安全隐患进行识别和分析,可以辅助网络管理员提前制定相应的防范措施,因此如何构

到稿日期:2018-10-12 返修日期:2018-12-18 本文受国家自然科学基金面上项目(61370230)资助。
张洁卉(1982—),女,硕士,主要研究方向为计算机网络、信息安全;潘 超(1980—),男,博士,主要研究方向为模式识别与智能系统,E-mail:pc2379@126.com(通信作者);章 勇(1979—),男,硕士,主要研究方向为计算机网络、信息安全。

建性能优异的网络系统风险评价模型具有重要的实际研究意义[7-9]。

针对网络系统风险建模与评价问题，国内外研究机构、相关科研人员以及高校教师采用了不同技术进行了一系列探索，提出了许多有效的网络系统风险评价模型[11]。当前，网络系统风险建模与评价模型可划分为两类：1）基于定性技术的网络系统风险建模与评价模型，该类方法主要采用知识推理、数学模型对网络系统风险变化特点进行描述，如基于漏洞信息的网络系统风险评价模型、基于危险理论的网络系统风险评价模型、基于博弈论的网络系统风险评价模型，它们从整体上对网络系统风险进行分析，得到网络系统风险所处的状态，但无法对网络系统的风险进行细致刻画，因此其局限性十分明显[12-14]；2）基于定量技术的网络系统风险评价模型，该类方法根据关联分析、聚类分析、隐马尔可夫模型、神经网络、支持向量机等[15-16]算法，通过网络系统风险评价指标和网络系统风险值构建样本，通过训练、拟合网络系统风险评价指标和网络系统风险值之间关系的评价模型，可以较好地对网络系统风险进行定量分析，从而得到确定的评价值，该网络系统风险评价结果的可解释性要优于定性技术，因此该类网络系统风险评价模型成为了当前网络系统风险评价的主要研究方向。定量技术的评价模型又可以划分为两类：单一的网络系统风险评价模型和组合的网络系统风险评价模型。单一方法只能从单一角度对网络系统风险的变化特点进行描述，而网络系统风险受众多因素影响，具有较强的时变性、非线性变化的特点，因此网络系统风险评价的错误较大，无法应用于实际的网络安全管理；组合的网络系统风险评价模型将多种方法组合在了一起，分别从不同角度对网络系统风险的变化特点进行描述，可以考虑不同的网络系统风险影响因素，充分利用网络系统风险的历史相关数据，其评价精度要优于单一方法[17-18]。在组合方法的网络系统风险评价过程中，确定每一种方法的网络系统风险评价权值十分关键，这也是当前组合方法的一个难题，目前有专家法、经验法、等权方法、方差-协方差方法等用于确定权值，以描述每一种方法的网络系统的风险评价贡献，但它们均无法准确描述网络系统的风险评价贡献，权值确定不合理，从而导致最终的网络系统风险评价结果无法达到最优。

在实际应用中，对于不同的网络系统风险评价模型，每种方法的评价效果相同，因此每种权值都具有不确性。证据理论是一种专门处理不确性问题的方法，具有严谨的推理过程[19-20]，因此，为了改善网络系统风险评价的效果，本文设计了最优化权值的网络系统风险组合评价模型，结果表明，本文模型可以准确地对网络系统风险进行评价，能够获得更加理想的网络系统风险评价结果，其整体评价性能要优于其他网络系统风险评价模型。

2　网络系统风险评价的指标体系

网络系统风险评价是一个十分复杂的过程，要获得理想的网络系统风险评价结果，首先须选择最优指标，并将其作为网络评价模型以提供信息源，但是评价指标数量太多，会导致网络系统风险评价建模过程过于复杂，从而使得网络系统风险评价效率低，因此本文根据完整性、易量化等原则，建立网络系统风险评价指标体系，如图 1 所示。

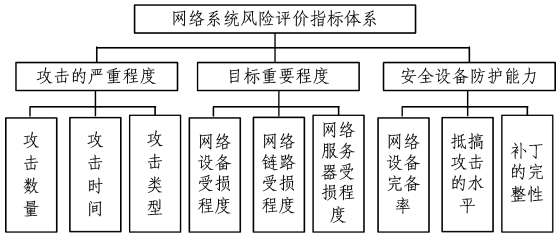

图 1　网络系统风险评价指标体系

Fig. 1　Index system of network system risk assessment

3　最优化权值的网络系统风险组合评价模型

3.1　改进证据理论

设 $\Theta=\{A_1,A_2,\cdots,A_N\}$ 表示辨识框架，共有 n 个证据，它们组成集合 $E=\{E_1,E_2,\cdots,E_n\}$，证据相对应的基本可信度分配函数为 $\{m_1,m_2,\cdots,m_n\}$，$m_i(A_j)$ 为 m_i 分配给 A_j 的基本可信度（BPA），证据合成规则为：

$$m(A)=\begin{cases}0, & A=\varnothing\\ \dfrac{1}{1-k}\sum\limits_{A_i\cap A_j\cap\cdots=A}m_1(A_i)m_2(A_j)\cdots, & A\neq\varnothing\end{cases}\tag{1}$$

其中，$k=\sum\limits_{A_i\cap A_j\cap\cdots=\varnothing}m_1(A_i)m_2(A_j)\cdots m_n(A_k)$。

通常条件下，如果一个证据和其他证据冲突较大，则表示该证据不正常，出现奇异状态，这会影响最后的融合结果，其可信度低。因此本文采用可信度因子 ε 来评价证据的可信度，从而可以对原始证据进行处理，减少证据之间的冲突。ε_i 表示 E_i 的可信度因子，那么可建立如下的可信度矢量：

$$\varepsilon=\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n\}\tag{2}$$

m_i 分配给 A_j 的基本可信度组成数据矩阵 $\boldsymbol{B}_{n\times n}$，那么有 $\boldsymbol{B}_{ij}=m_i(A_j)$。$\boldsymbol{B}$ 的第 i 行为 p_i，则有：

$$p_i(m_i(A_1)m_i(A_2)\cdots m_i(A_n))\tag{3}$$

其中，$i=1,2,\cdots,n$。

p_i 和 p_j 之间的距离 d_{ij} 表示两个证据体的相似度，具体为：

$$d_{ij}=\|p_i-p_j\|=\sqrt{\sum_{k=1}^{N}[m_i(A_k)-m_j(A_k)]^2}\tag{4}$$

所有证据体之间的相似度构成一个距离矩阵 $\boldsymbol{D}_{n\times n}$，具体如下：

$$\boldsymbol{D}=\begin{pmatrix}0 & d_{12} & d_{13} & \cdots & d_{1n}\\ d_{21} & 0 & d_{23} & \cdots & d_{2n}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ d_{n1} & d_{n2} & d_{nw} & \cdots & 0\end{pmatrix}\tag{5}$$

s_i 表示 E_i 和证据集 E 之间的方均欧氏距离，用于描述 E_i 和 E 的一致性，可以反映 E_i 和其他证据之间的差异程度，具体计算公式为：

$$s_i=\frac{1}{2n}\sum_{j=1}^{n}d_{ij}^2\tag{6}$$

s_i 和 ε_i 之间存在一定的联系，设 $\varepsilon_i=f(s_i)$，那么 $f(s_i)$ 的取值范围为 $(0,1]$，而且 ε_i 与 s_i 之间存在一种单调递减的变

化关系，因此可以用一个指数关系曲线对这种关系进行描述，ε_i 可以定义为：

$$\varepsilon_i = f(s_i) = (1-s_i)a^{-s_i} \tag{7}$$

对式(7)进行求导，可以得到：

$$f'(s_i) = (s_i \ln a - \ln a - 1)a^{-s_i} \tag{8}$$

当 $a = \exp(-1)$ 时，可以得到最合理的可信度因子：

$$\varepsilon_i = (1-s_i)\exp(s_i) \tag{9}$$

根据式(9)得到的 ε_i 值，对原始证据进行修正和处理，以获得更好的融合结果。

3.2 评价模型的结构

权值合理确定组合模型的工作过程为：首先建立网络系统风险评价指标，并收集网络系统风险历史数据；然后采用支持向量机(SVM)、RBF 神经网络(RBFNN)、BP 神经网络(BPNN)建立网络系统风险评价模型，并将它们的评价结果作为证据体；最后考虑证据之间的冲突性，使用改进证据理论确定权值，从而得到最终的网络系统风险评价结果。该模型的结构如图 2 所示。

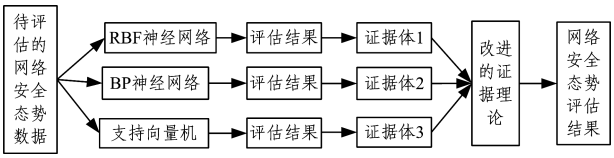

图 2 权值合理确定的网络系统风险评价模型

Fig. 2 Network system risk assessment model with reasonable weights

3.3 网络系统风险评价的初始层

(1)根据完整性、易量化等原则构建如图 1 所示的网络系统风险评价指标体系。

(2)各个指标纲量不一致，会对网络系统风险评价的训练过程产生不利影响，因此对指标值做如下处理：

$$x_i' = \frac{x_i - \min(x_i)}{\max(x_i) - \min(x_i)} \tag{10}$$

其中，max 和 min 分别表示网络系统风险评价指标的最大值和最小值。

(3) 专家根据网络系统风险评价指标值对相应的网络系统风险级别进行估计，建立网络系统风险评价的学习样本。

(4) 分别采用支持向量机、RBF 神经网络、BP 神经网络对网络系统风险训练样本集合进行学习，并对测试样本进行测试，得到每一种模型的网络系统风险评价结果，为后续的网络系统风险评价的融合决策奠定基础。

3.4 网络系统风险评价的决策层

在网络系统风险评价的融合决策过程中，根据初步层中的支持向量机、RBF 神经网络、BP 神经网络的网络系统风险评价结果构造证据体 E，然后使用改进证据理论对证据体 E 进行融合，得到最终的网络系统风险评价结果，具体步骤如下：

(1)根据专家经验和以往网络系统风险评价的历史记录，建立网络系统风险评价的识别框架 $\Theta = \{A_1, A_2, \cdots, A_N\}$。

(2)将支持向量机、RBF 神经网络、BP 神经网络的网络系统风险评价结果作为一个证据体。

(3)确定 $\Theta = \{A_1, A_2, \cdots, A_N\}$ 中的基本可信度(BPA)。

(4)根据证据合成方法得到各证据联合作用下的可信度函数和不确定性描述 $m(\Theta)$。

(5)根据以下规则得到网络系统风险评价结果 A_c，其中 Bel 表示结论的可信度。

规则 1：

$Bel(A_c) = \max\{Bel(A_j)\} Bel(A_c) > \varepsilon$

规则 2：

$Bel(A_c) - Bel(A_j) > \varphi, Bel(A_c) - m(\Theta) > \varphi$

其中，φ 为一个正数。

规则 3：

$m(\Theta) < \gamma$

其中，γ 表示不确定性因子，其为一个正数。

4 网络系统风险评价模型的性能测试与分析

4.1 网络系统风险评价实验数据

本文通过实验分析了基于改进证据理论的网络安全网络评价模型的有效性，实验选择的仿真平台为：Intel(R) 4 核 CPU 2.80 GHz，32 GB RAM，Windows 10 操作系统，采用 VC++ 6.0 进行编程。网络系统风险共分为 5 个级别：很低(1)、低(2)、中(3)、高(4)、很高(5)。它们的样本数量分布如表 1 所列。

表 1 网络系统风险评价的仿真实验数据

Table 1 Simulation data of network system risk assessment

态势级别标签	训练样本数量	测试样本数量
1	100	20
2	200	40
3	150	30
4	80	20
5	200	40

4.2 与单一模型的网络系统风险评价结果的对比

为了正确评价基于组合模型权值合理确定的网络系统风险评价模型(MDS)的有效性，选择持向量机(SVM)、RBF 神经网络(RBFNN)、BP 神经网络(BPNN)进行对比实验。为保证实验结果的客观性，所有模型进行 5 次仿真实验，统计网络系统风险评价的正确率，结果如图 3 所示。对图 3 的结果进行分析可知：

(1)RBF 神经网络、BP 神经网络的网络系统风险评价正确率较低，评价出现错误的概率大，这是因为神经网络属于经验风险最小化原则的机器学习算法，易出现过拟合和欠学习的问题，这使得许多网络系统风险样本的评价结果不准确。

(2)相对于 RBF 神经网络、BP 神经网络，支持向量机的网络系统风险评价正确率更高，这是因为支持向量机是一种基于结构风险最小化原则的机器学习算法，其学习能力和泛化能力更优，不存在过拟合和欠学习的缺陷，但是其网络系统风险评价的正确率低于 85%，无法达到网络安全的实际应用要求。

(3)MDS 的网络系统风险评价正确率要远远高于单一模型，这会使得网络系统风险评价的错误概率大幅度下降，这是

因为本文模型集成了支持向量机、RBF 神经网络、BP 神经网络的优势，可以从不同角度、不同方面对网络系统风险的变化特点进行描述，能够更加有效地区别各种网络系统风险的级别，具有十分明显的优越性。

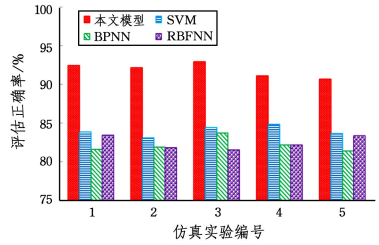

图 3　本文模型与单一模型的网络系统风险评价正确率比较

Fig. 3　Comparison of accuracy rate of network system risk assessment between proposed model and single model

4.3　与其他组合模型的网络系统风险评价结果比较

为了验证改进证据理论的优势，选择文献[11-13]的网络安全评价组合模型进行仿真测试，分别统计网络系统风险评价的正确率和网络系统风险评价的训练时间，实验结果分别如图 4 和图 5 所示。

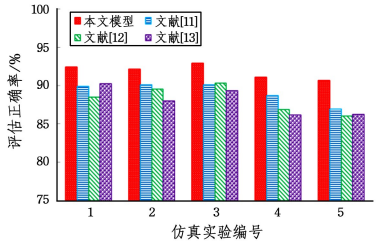

图 4　本文模型与其他组合模型的网络系统风险评价的正确率比较

Fig. 4　Comparison of accuracy rate of network system risk assessment among proposed model and other combined models

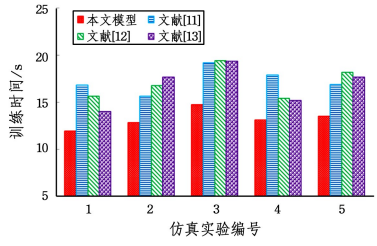

图 5　本文模型与其他组合模型的网络系统风险评价的训练时间比较

Fig. 5　Comparison of training time of network system risk assessment among proposed model and other combined models

从图 4 可以看出，本文模型的网络系统风险评价的正确率高于文献[11-13]的网络安全评价组合模型的正确率，这说明通过引入改进证据理论对各个单模型的网络系统风险评价的贡献率进行刻画，可以建立更好的网络系统风险评价模型。从图 5 可以看出，本文模型的网络系统风险评价的训练时间最少，提高了网络系统风险评价的效率。

结束语　为了提高网络系统风险组合评价的准确性，针对单一模型以及传统组合模型无法全面、高精度地描述网络系统风险的变化特点，本文以提高网络系统风险评价效果为目标，设计了最优化权值的网络系统风险组合评价模型，采用具体仿真实验与其他网络系统风险评价模型进行了对比测试，并对测试结果进行分析，得到了如下结论：

(1)单一模型由于提供的网络系统风险信息量小，无法建立有效的网络系统风险评价模型，导致网络系统风险评价误差大，无法应用于网络系统的安全管理中。

(2)统模型的网络系统风险评价效果虽然优于单一模型，但由于其权值采用经验方式或者平均法确定，无法准确刻画单一模型对网络系统风险评价结果的作用，因此网络系统风险评价结果有待进一步改善。

(3)本文模型采用不同方法对网络系统风险的变化特点进行刻画和建模，基于证据可信度确定权值，可以准确地刻画单一模型对网络系统风险评价结果的作用，使得网络系统风险评价更加客观、可信，而且精度高于网络系统风险对比模型。

本文提出的网络系统风险评价模型为有效评价网络安全风险提供了一种新的研究工具，在网络安全管理领域具有广泛的应用前景。

参 考 文 献

[1]　YUAN X, FENG Z Y, XU W J, et al. Secure connectivity analysis in unmanned aerial vehicle networks [J]. Frontiers of Information Technology & Electronic Engineering, 2018, 19(3): 409-422.

[2]　MOVAHEDI Z, HOSSEINI Z, BAYAN F, et al. Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2): 1287-1309.

[3]　HAN G J, JIANG J F, SHU L, et al. An attack-resistant trust model based on multi-dimensional trust metrics in underwater acoustic sensor network[J]. IEEE Tansactions Mob Computer, 2017, 14(12): 2447-2459.

[4]　LIU Q, CAI Z P, YIN J P, et al. Frameworks and methods of cybersecurity detection [J]. Computer Engineering & Science, 2017, 39(12): 2224-2229. (in Chinese)
刘强，蔡志平，殷建平，等. 网络安全检测框架与方法研究[J]. 计算机工程与科学，2017，39(12)：2224-2229.

[5]　HUANG Q L, MA Z F, YANG Y X, et al. Improving Security and Efficiency for Encrypted Data Sharing in Online Social Networks[J]. Information Security, 2018, 28(7): 104-114.

[6]　FU Y, YU Y H, CHEN Y Q, et al. Network Security Analysis on Attack-defense Behavior Tree[J]. Journal of Sichuan University (Engineering Science Edition), 2017, 49(2): 115-120. (in Chinese)
付钰，俞艺涵，陈永强，等. 基于攻防行为树的网络安全态势分析[J]. 工程科学与技术，2017，49(2)：115-120.

[7]　HU H, YE R G, ZHANG H Q, et al. Quantitative method for network security situation based on attack prediction [J]. Journal on Communications, 2017, 38(10): 122-134. (in Chinese)
胡浩，叶润国，张红旗，等. 基于攻击预测的网络安全态势量化方

法[J]. 通信学报,2017,38(10):122-134.

[8] CHEN Y L,TANG G M,SUN Y F. Assessment of Network Security Situation Based on Immune Danger Theory[J]. Computer Science,2015,42(6):167-170. (in Chinese)
陈妍伶,汤光明,孙怡峰. 基于免疫危险理论的网络安全态势评估[J]. 计算机科学,2015,42(6):167-170.

[9] LIU J W,LIU J J,LU Y L,et al. Application of game theory in network security situation awareness [J]. Journal of Computer Applications,2017,37(S2):48-51,64. (in Chinese)
刘景玮,刘京菊,陆余良,等. 博弈论在网络安全态势感知中的应用[J]. 计算机应用,2017,37(S2):48-51,64.

[10] WEN Z C,CHEN Z G,TANG J. Network Security Assessment Method Based on Cluster Analysis [J]. Journal of Shanghai Jiaotong University,2016,50(9):1407-1414,1421. (in Chinese)
文志诚,陈志刚,唐军. 基于聚类分析的网络安全态势评估方法[J]. 上海交通大学学报,2016,50(9):1407-1414,1421.

[11] MALEKI H,VALIZADEH M H,KOCH W,et al. Markov modeling of moving target defense games [C]// Proceedings of the 2016 ACM Workshop on Moving Target Defense. ACM,2016:81-91.

[12] GE H H,XIAO D,CHEN T P,et al. Quantitative Evaluation Approach for Real-time Risk Based on Attack Event Correlating [J]. Journal of Electronics & Information Technology,2013,35(11):2630-2636. (in Chinese)
葛海慧,肖达,陈天平,等. 基于动态关联分析的网络安全风险评估方法[J]. 电子与信息学报,2013,35(11):2630-2636.

[13] HUANG J M,ZHANG H W,WANG J D,et al. Defense strategies selection based on attack defense evolutionary game model [J]. Information Science,2017,38(1):168-176. (in Chinese)
黄健明,张恒巍,王晋东,等. 基于攻防演化博弈模型的防御策略选取方法[J]. 通信学报,2017,38(1):168-176.

[14] WEN Z C,CHEN Z G,TANG J. Assessing network security situation quantitatively based on information fusion[J]. Journal of Beijing University of Aeronautics and Astronautics,2016,42(8):1593-1602. (in Chinese)
文志诚,陈志刚,唐军. 基于信息融合的网络安全态势量化评估方法[J]. 北京航空航天大学学报,2016,42(8):1593-1602.

[15] HUANG J M,ZHANG H W. A Method for Selecting Defense Strategies Based on Stochastic Evolutionary Game Model[J]. Acta Electronica Sinica,2018,46(9):2222-2228. (in Chinese)
黄健明,张恒巍. 基于随机演化博弈模型的网络防御策略选取方法[J]. 电子学报,2018,46(9):2222-2228.

[16] WHITE J,PARK J S,KAMHOUA C A,et al. Game theoretic attack analysis in online social network services [C]// Proceedings of the 2017 International Conference on Social Networks Technology. IEEE,2017:1012-1019.

[17] LIPPMANN R,HAINES J W. Analysis and results of the DARPA off-line intrusion detection evaluation [C]// Proceedings of the 17th International Workshop on Recent Advances in Intrusion Detection. New York:ACM,2016:162-182.

[18] WU G,CHEN L,SI Z G,et al. An index optimization model for network security situation evaluation [J]. Computer Engineering & Science,2017,39(5):861-869. (in Chinese)
吴果,陈雷,司志刚,等. 网络安全态势评估指标体系优化模型研究[J]. 计算机工程与科学,2017,39(5):861-869.

[19] CHENG J T,AI L,DUAN Z M. Transformer fault diagnosis based on improved evidence theory and neural network integrated method [J]. Power System Protection and Control,2013,41(14):92-96. (in Chinese)
程加堂,艾莉,段志梅. 改进证据理论与神经网络集成的变压器故障诊断[J]. 电力系统保护与控制,2013,41(14):92-96.

[20] LI F W,ZHENG B,ZHU J,et al. A method of network security situation prediction based on AC-RBF neural network[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition),2014,26(5):576-581. (in Chinese)
李方伟,郑波,朱江,等. 一种基于 AC-RBF 神经网络的网络安全态势预测方法[J]. 重庆邮电大学学报(自然科学版),2014,26(5):576-581.