DOI:10.3876/j.issn.1000-1980.2018.05.014

基于模糊校正的深度时序信息安全评估算法

魏明桦[1,2],郑金贵[1]

(1.福建农林大学作物科学学院,福建 福州 350007;2.福州职业技术学院信息技术工程系,福建 福州 350108)

摘要:针对现有信息安全评估算法对多专家主观态度偏差的处理不足,并且传统时序机器学习模型无法应对时间段内偏差积累等问题,提出一种基于深度模糊校正的深度时序信息安全评估算法。该算法首先通过三角模糊函数构建专家模糊评估指标,并采用改进的加权DS证据推理校正指标,然后创建损失和可能性矩阵特征,最后使用深度时序网络评估信息安全。在MIT数据集上进行了仿真实验,实验分别分析了特征是否能够应对多专家冲突,以及评估算法的正确率,鲁棒性和时间效率等指标。实验结果表明,本文提出的算法拥有更强的模糊评价能力,对专家间的冲突意见处理能力更强,在时序上的信息安全评估更准确,鲁棒性更高,但是算法效率却得到了保持。

关键词:三角模糊函数;损失矩阵;可能性矩阵;加权DS证据推理;RNN-LSTM

中图分类号:TN914 **文献标志码**:A **文章编号**:1000-1980(2018)05-0464-07

An evaluation algorithm of information security based on fuzzy adjustment feature matrices and deep time sequence model

WEI Minghua[1,2], **ZHENG Jingui**[1]

(1. *School of Crop Science and Technology*, *Fujian Agriculture and Forestry University*, *Fuzhou* 350007, *China*;
2. *School of Information and Technology*, *Fuzhou Polytechnic*, *Fuzhou* 350108, *China*)

Abstract: The conventional algorithm can not deal with the deviant attitude of different experts in the evaluation of information security. At the same time, it adopts shallow machine learning models and mishandled the deviation accumulating problem. In the study, we proposed a novel evaluation algorithm of information security based on the fuzzy adjustment feature matrices and the deep time sequence model. In the proposed algorithm, the triangle fuzzy function was applied to build the expert's evaluation indexes. Then, the improved weight DS theory of evidence was used to adjust the indexes. After that, the loss matrix and possibility matrix are constructed. The information security was evaluated by a deep neural model in proposed model. In the simulations of MIT dataset, we explored whether the feature matrices will cope with the conflicts of experts or not, and the accuracy, performance and robustness of estimation were also checked. It can be found that the proposed algorithm has a better ability to evaluate the fuzzy system, and the ability for coping with the conflicts of experts is also better, achieving a better accuracy and robustness with the reservation of performance.

Key words: triangle fuzzy function; loss matrix; possibility matrix; weight DS evidence; RNN-LSTM

在日益复杂的网络结构与动态变化的信息交互场景中,产业网络依赖性导致信息安全直接关系到各个领域。为了减少信息安全对各个领域产生的风险,信息安全评估研究成为了热点[1]。信息安全评估通过网

基金项目:福州市科技计划项目(2015-G-84)

作者简介:魏明桦(1980—),男,副教授,博士,主要从事计算机网络技术、农业高新技术产业化研究。E-mail:weiminhualw@163.com

通信作者:郑金贵,教授。E-mail:jgzheng@fjau.edu.cn

引用本文:魏明桦,郑金贵.基于模糊校正的深度时序信息安全评估算法[J].河海大学学报(自然科学版),2018,46(5):464-470.
WEI Minghua, ZHENG Jingui. An evaluation algorithm of information security based on fuzzy adjustment feature matrices and deep time sequence model[J]. Journal of Hohai University(Natural Sciences),2018,46(5):464-470.

络过去与现在的状态评估网络未来的状态,可以提升网络防御主动性,并为信息事件的操作和决策提供大量重要的依据,将攻击网络、传播病毒等危害降至最低[2]。

早期的多位专家评判方法,根据不同专家的评判结果进行权重评判,剔除偏离程度较大的评判指标,计算有效评判指标的均值作为评估结果[3]。近年来的时序网络评估算法引入了时序机器学习模型,研究者通过 Markov 随机链[4]对时序数据处理,开启了基于时序模型的信息安全评估方法。然而,Markov 随机链虽然可以模拟序列数据,但并未考虑数据的全局性,具有时域上的局限性。为了解决局限问题,BPNN/SVM/PSO 等机器学习算法相继引入到信息安全评估中,并利用专家知识构建推理规则,再利用推理规则结合模型进行信息安全评估。

目前,通过模糊评价系统构建模糊形式的专家推理规则,再采用模型进行分类和预测,成为主流的信息安全评估方法[5]。专家主观评价的先决条件是影响主观评价产生偏差的主要原因,偏差会随着时序积累,积累的偏差对信息安全评估带来更大的误差和冲突。传统时序机器学习模型对时序数据前后的关系处理不足,最终导致时序信息安全评估算法效果不佳。

为了解决这些问题,笔者提出一种基于模糊校正的深度时序信息安全评估算法,首先通过三角模糊函数构建专家模糊评估指标,并采用改进的加权 DS 证据推理校正指标,然后创建损失和可能性矩阵特征,最后使用深度时序网络评估信息安全。由于经过校正后的模糊特征可以减小专家间的主观判断产生偏差和冲突,并且循环神经网络适合处理时序数据[6-7]。在这样 2 个条件下,时序信息安全评估将会获得效率更高,鲁棒性更好的结果。

1　模糊校正特征矩阵构建

传统模糊评价系统缺少客观指标,其评价隶属度会产生大量冲突,这些冲突会导致校正过程中丢弃大量评估指标。经过校正丢弃后的指标难以构建成熟的特征矩阵用于评估。本文通过 4 个步骤构建模糊校正特征矩阵,以解决传统模糊评价系统隶属度的冲突问题:(a)确定影响信息系统安全的角色,并进行专家评估;(b)采用三角模糊函数作为评价专家评估的客观量化标准,构建模糊专家态度;(c)利用改进的加权 DS 理论对模糊专家态度校正,丢弃少量带来冲突的指标;(d)经过校正后的模糊专家态度,用于构建模糊校正特征矩阵,用于信息安全评估。

1.1　三角模糊函数构建

在信息系统安全的初级定义过程中,通常需要专家通过主观感受给出定义。主观感受分为清晰和不清晰 2 种状态,对于不清晰的描述,需要采用更客观的量化工具进行精确量化,这时候一般采用三角模糊函数 (x_0,x_1,x_2) 对特征进行描述[8]。三角模糊函数的量化标准通过欧式距离确定,欧式距离计算结果用于判断模糊函数之间的距离,用于量化不同专家的主观安全评判信息。由于多个专家之间存在隶属度冲突,在量化完成后需要使用校正算法丢弃冲突指标。

1.2　改进的加权 DS 证据推理

DS 证据推理用来表达不精确的概率,采用概率区间的方式表达,对模糊的表达更为明确。模糊特征校正中通常采用 DS 算法[9],该算法假设信息安全状态集合 Ψ,该集合上的 Dempster 规则通过信任函数关系表示。

假设 m_1、m_2 分别是对应信任函数的概率值,相应集合的焦元分别为 $A_1,A_1,\cdots,A_k$ 和 $B_1,B_1,\cdots,B_r$,二者之间的关系表示为

$$K=\sum_{A_i\cap B_j=\varphi} m_1(A_i)m_2(B_j) \tag{1}$$

式中:K——焦元交集的信任函数概率值。

通过式(2)可以计算 A、B 焦元的交集 C 焦元,该焦元的概率赋值函数可以表示为

$$m(C)=\begin{cases}\dfrac{\sum\limits_{A_i\cap B_j=C} m_1(A_i)m_2(B_j)}{1-K} & \forall C\in\Psi, C\neq\varphi\\ 0 & C=\varphi\end{cases} \tag{2}$$

当参数 $K\neq1$,得到确定概率值 m;当参数 $K=1$,则现有的概率值 m_1、m_2 相互矛盾,不能进行基本概率组

合,DS 推理规则将其丢弃。

在信息安全评估过程中,多个证据之间存在冲突是很常见的情况,概率赋值的冲突将造成大量评估指标丢弃,这样的校正不利于信息安全评估。为了解决传统 DS 推理丢弃规则的不足之处,引入证据相容度,计算 m_1、m_2 之间的相容度系数[10]:

$$R_{12}(u)=\frac{m_1(u)m_2(u)}{\frac{1}{2}(m_1^2(u)+m_2^2(u))} \tag{3}$$

式中:$R_{12}(u)$——相容度系数;u——信息安全评估中某一证据。

当存在多个专家的意见时,将其扩展到 $n\times n$ 个变量之间,即可获得两两相容度系数形成的相容矩阵:

$$\boldsymbol{R}=\begin{bmatrix} R_{11} & \cdots & R_{1n} \\ \vdots & & \vdots \\ R_{n1} & \cdots & R_{nn} \end{bmatrix} \tag{4}$$

$\boldsymbol{R}$ 中的数值表示各专家意见之间的支撑程度,支撑程度越高,说明可信度越高。绝对相容程度为

$$S_i(u)=\sum_{j=1,i\neq j}^{n}R_{ij}(u) \tag{5}$$

理想状态下,相容程度为 $n-1$,则最终的可信程度:

$$T_i(u)=\frac{S_i(u)}{n-1} \tag{6}$$

改进的 DS 证据推理在校正专家意见冲突之前,将每个意见的可信度作为基本概率的权重,通过加权的方式重新计算基本概率赋值,即可避免因为证据冲突过大而导致大量意见丢弃的情况。

1.3 特征矩阵计算

在信息安全评估中,一般在系统中定义 4 个关键角色:(a)专家评估角色:通过多个专家的主观安全信息评估构成,$E_x=\{E_{x1},E_{x2},\cdots,E_{xk}\}$;(b)威胁信息角色:$T_h=\{T_{h1},T_{h2},\cdots,T_{hn}\}$;(c)资产信息角色:$Q=\{q_1,q_2,\cdots,q_t\}$;(d)脆弱元组角色:$P=\{p_1,p_2,\cdots,p_s\}$;其中,$k,t,s,n=1,2,\cdots$。

在一个信息系统中,威胁信息、资产信息和脆弱元组是风险发生的主要对象,还需要制定每个专家给出的评估信息。在 4 个关键角色基础上构建模糊校正特征矩阵,分别构建可能性矩阵(风险发生前)和损失矩阵(风险发生后)。多个专家给出的威胁信息 m_{ij} 和脆弱信息 n_{ij} 可以通过改进的加权 DS 证据推理计算获得:

$$m_{ij}=w_{ij}m_{ij}\mid_{E_{x1}}+w_{ij}m_{ij}\mid_{E_{x2}}+\cdots+w_{ij}m_{ij}\mid_{E_{xk}}\quad(i=1,2,\cdots,n;j=1,2,\cdots,s) \tag{7}$$

$$n_{ij}=w_{ij}n_{ij}\mid_{E_{x1}}+w_{ij}n_{ij}\mid_{E_{x2}}+\cdots+w_{ij}n_{ij}\mid_{E_{xk}}\quad(i=1,2,\cdots,s;j=1,2,\cdots,t) \tag{8}$$

可能性矩阵 $\boldsymbol{N}(n_{ij})_{s\times t}$ 中,n_{ij} 表示第 i 种威胁信息角色利用第 j 种脆弱元组造成损失的可能性大小,可能性大小归一化至[0,1]区间内;损失矩阵 $\boldsymbol{M}(m_{ij})_{n\times s}$ 中,m_{ij} 为第 i 种脆弱元组角色对第 j 种资产信息角色产生的影响,影响大小归一化至[0,100]区间内。

经过加权 DS 理论的决策,可以获得 2 个矩阵 $\boldsymbol{M}\in\boldsymbol{R}_{n\times s}$、$\boldsymbol{N}\in\boldsymbol{R}_{s\times t}$ 作为模糊校正特征矩阵。网络信息安全的状态随着时间变化,在不同时间段产生的模糊校正特征矩阵将被输入至时序机器学习预测模型中进行训练和评估。

2 深度时序信息安全评估预测

近年来,机器学习逐渐成为信息安全评估的有效工具。在时序特征上的机器学习模型,由最早的浅层 Markov 随机场模型,到如今的深度时序学习模型,对时序数据的处理能力逐渐增强。由模糊校正提取的特征在时序化产生的特征矩阵,在时序化机器学习模型中可以预测出评估结果。

循环神经网络(RNN)是近年来兴起的深度神经网络模型,在提取时序特征关键特征和预测未来有更好的效果[11]。在 RNN 模型中的 LSTM 单元[12],能够通过门结构限制信息传递,保证误差有效,在时序特征(如,语音特征、文本特征等)的训练和预测上均取得了不错的效果。图 1 给出了 RNN-LSTM 单元的结构,LSTM 由 4 个受限门组成,分别是输入门、遗忘门、输出门和状态单元,图中 f、g、h 为激活函数。

各个门对信息传递的限制通过文献[13-14]给出。在 RNN 模型中,由于网络的长度与时间采样点长度相同,所以 BP 的传播是从最后一个时间点逐渐向第一个时间点传播,即伴随时间的误差反向传播算法(BPTT)[15]。最终通过训练好的 RNN 模型即可对时序化模糊校正特征矩阵进行预测,对于每个时间段,均可以给出当前时间段中的信息安全评估结果。

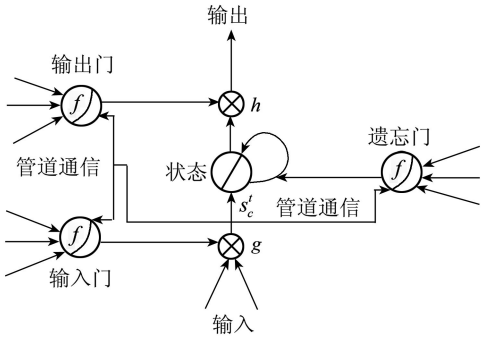

图 1　RNN-LSTM 单元结构

Fig. 1　RNN- LSTM structure

3　实验结果与分析

3.1　实验数据集

实验采用的 MIT Lincoln Lab2000DARPA 数据集的网络拓扑结构见文献[16]。在该数据集中,一共给出 1 000 个样本,每个样本的样本点为 512 个。提取每个样本在时序下的模糊校正特征矩阵,并将其中 90% 的数据作为训练数据,10% 的数据作为验证数据。根据表 1 专家可以对每个样本给出主观评估值,并提取模糊校正特征矩阵。

表 1　信息安全评估等级和三角模糊函数关系

Table 1　Relationship of information security and triangle fuzzy function

安全评估等级	损失([0,100])	可能性([0,1])
低	[0,10,20]	[0, 0.1,0.2]
较低	[10,30,40]	[0.1,0.3,0.4]
中等	[30,50,60]	[0.3, 0.5,0.6]
较高	[60,80,70]	[0.6,0.8,0.7]
高	[80,90,100]	[0.8,0.9,1]

3.2　模糊校正特征矩阵实验结果

在模糊校正特征矩阵提取中,邀请了 30 位专家进行安全评估实验。为了验证特征的有效性,选取 3 位意见冲突大的专家作为验证对象。假设资产集合为 $Q=\{q_1,q_2\}$;威胁信息角色为 $T_h=\{T_{h1},T_{h2}\}$;脆弱元组角色为 $P=\{p_1,p_2,p_3\}$,3 位专家评估值经过 DS 证据推理后的结果见表 2,3 位专家对可能性等级的评判结果见表 3。

表 2　专家对损失等级的评判

Table 2　Expert judgment of loss level

脆弱元组角色	E_{x1}		E_{x2}		E_{x3}	
	q_1	q_2	q_1	q_2	q_1	q_2
p_1	较高	高	较高	中等	高	很高
p_2	中等	较低	较高	低	较低	高
p_3	高	低	高	较低	中等	低

表 3　专家对可能性等级的评判

Table 3　Expert judgment of possibility level

脆弱元组角色	E_{x1}		E_{x2}		E_{x3}	
	T_{h1}	T_{h2}	T_{h1}	T_{h2}	T_{h1}	T_{h2}
p_1	高	高	较高	较高	高	较高
p_2	中等	较低	较高	低	较低	较高
p_3	较高	低	高	中等	中等	较低

由式(7)(8)可得到损失矩阵和可能性矩阵:

$$\boldsymbol{M}=\begin{bmatrix}(72.32,83.24,94.39) & (63.28,77.48,28.45)\\(25.39,43.38,58.98) & (23.83,31.85,52.87)\\(58.89,73.27,89.64) & (6.23,16.37,32.87)\end{bmatrix} \tag{9}$$

$$\boldsymbol{N}=\begin{bmatrix}(0.54,0.73,0.94) & (0.33,0.46,0.68) & (0.53,0.72,0.83)\\(0.64,0.84,0.96) & (0.23,0.39,0.58) & (0.36,0.24,0.47)\end{bmatrix} \tag{10}$$

经过 RNN 预测可以得到 3 位专家归一化的评估结果:

$$\boldsymbol{R}=\begin{bmatrix}(46.37,0.43)\\(53.74,0.67)\\(62.37,0.38)\end{bmatrix} \tag{11}$$

从结果中可以看出,经过改进的加权 DS 证据推理获得的 3 位专家结果的差异性不大,不会因为冲突过大导致丢弃重要评估意见,相应的特征矩阵预测准确率更高,鲁棒性更高。

3.3　RNN 预测实验结果

经过 30 个专家进行安全评估打分,并提取模糊校正特征矩阵。在时间 T 内,可能性矩阵和损失矩阵组

成的输入特征为 $\boldsymbol{S}\in\boldsymbol{R}_{2\times T}$,相应的 RNN 模型输入神经元设为 2 个,深度设为 T,输出通过 1 个神经元给出预测值。在实际训练过程中,由于特征非线性,激活函数 f 选择 ReLu,激活函数 g 选择 tanh,激活函数 h 选择 sigmoid[17],以保证 LSTM 的激活。时序特征处理选择 RMSprop 方法作为 BPTT 的学习率更新方法。为了防止过拟合,每一轮 BPTT 迭代完成采用 dropout=0.5 丢弃冗余特征[18],网络训练最大的迭代次数 ITR 为 200。

经过 200 次迭代,RNN 网络趋向于平稳收敛,并验证 100 个测试样本给出预测值。将数据集中给出的预测标签作为真实值,并比较 RNN-LSTM 模型的预测值进行比较(图 2)。表 4 给出了 10 个关键威胁点的检测对比结果。

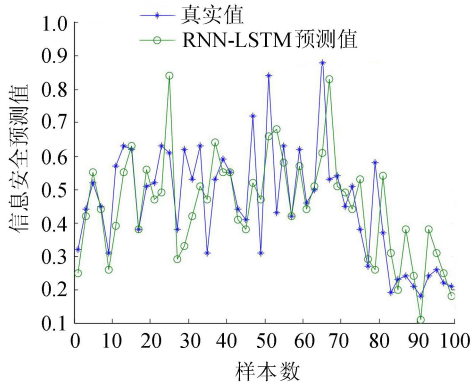

图 2 真实值与 RNN 输出值比较

Fig. 2 Comparison of RNN result and actual value

表 4 关键威胁点的 RNN 信息安全评估结果

Table 4 Evaluating result of RNN information security in key threaten points

样本编号	RNN 输出	真实输出	RNN 威胁级别	真实威胁级别
13	0.76	0.73	较高	中等
25	0.78	0.75	较高	较高
35	0.73	0.78	中等	较高
39	0.65	0.71	中等	中等
46	0.68	0.65	中等	中等
59	0.83	0.86	较高	较高
67	0.90	0.88	高	较高
86	0.87	0.91	较高	高
93	0.68	0.68	中等	中等
100	0.66	0.65	中等	中等

本文提出的算法在特征提取上和模型深度上都进行了优化。在横向对比上,选择当前特征矩阵效果最好的双重复模糊集算法(DFS)[19]以及对时序特征矩阵分类效果最好的 GA-SVM 算法[20]和模糊小波神经网络(FWNN)算法[21]进行对比。在特征矩阵对比中,预测算法采用相同的 RNN 预测结构;在时序模型对比中,特征提取采用相同的模糊校正特征矩阵。图 3 给出了不同算法的预测对比结果;表 5 则给出了 10 个关键威胁点不同算法之间的对比值。另外,为了验证算法效率的问题,将本文算法与当前 3 种预测效果最好的算法从训练效率,预测效率和均方误差进行了对比(表 6)。

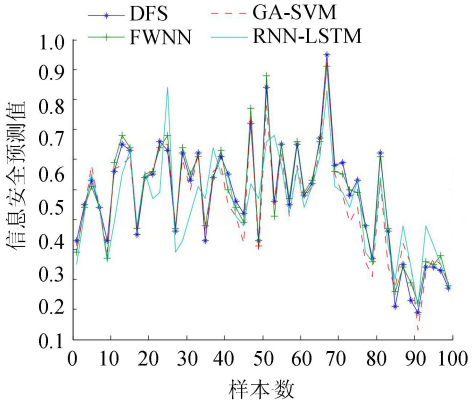

图 3 4 种不同模型的输出值比较

Fig. 3 Output results of four different models

表 5 关键威胁点不同模型信息安全预测对比结果

Table 5 Result of information security from four different models in key threaten points

样本编号	RNN-LSTM	DFS	FWNN	GA-SVM
13	0.76	0.72	0.70	0.65
25	0.78	0.70	0.62	0.50
35	0.73	0.65	0.68	0.68
39	0.65	0.68	0.47	0.43
46	0.68	0.73	0.55	0.31
59	0.83	0.80	0.75	0.74
67	0.90	0.91	0.90	0.53
86	0.87	0.79	0.64	0.44
93	0.68	0.58	0.73	0.64
100	0.66	0.88	0.70	0.55

表 6 不同算法的迭代时间与均方误差对比结果

Table 6 Errors and time consumption of four different models

算法	训练效率/s	预测效率/ms	均方误差
RNN-LSTM	>1 800	220	0.072
DFS	293	183	0.182
GA-SVM	287	239	0.216
FWNN	3 422	218	0.283

3.4 实验结果分析

经过对模糊校正特征矩阵和 RNN 模型的对比实验,可以分析出以下 3 个重要结论:(a)在关键威胁时间点的信息安全评估上,模糊校正特征矩阵在处理专家意见冲突中,可以保护有效信息免受校正剔除。通过改进的加权 DS 证据推理校正后的时序特征,更适合于深度时序模型的预测。(b)在关键威胁检测上,从特征矩阵的

对比来说,本文提出的模糊校正特征矩阵比双重模糊矩阵在预测准确率和鲁棒性上略有提升。在预测模型对比上,本文构建的 RNN 模型比传统浅层模型有了较大的提升。(c)模型训练与效率对比上,RNN 深度模型的均方误差更低,但是 RNN 模型的深度更大,迭代、优化和计算所需要的时间消耗更大,主要由深度模型的特性决定。然而,在预测效率上,由于 RNN-LSTM 只通过网络参数计算,在效率上与传统浅层机器学习模型对比差距不大。

4　结　　语

提出了一种基于模糊校正的深度时序信息安全评估算法。该算法首先通过三角模糊函数构建专家模糊评估指标,并采用改进的加权 DS 证据推理校正指标,然后创建损失和可能性矩阵特征,最后使用深度时序网络评估信息安全。改进的加权 DS 证据推理对专家评价的冲突和偏差处理能力强,深度网络 RNN 模型对时序数据的预测也拥有更高的准确率和鲁棒性。然而,由于仿真实验建立在有限量的数据集之上,RNN 模型的深度还有限。今后的工作在于构建更复杂的网络拓扑结构,获取更大量的安全评估数据。通过更深的模型构建出适应性和扩展性更强的信息安全评估模型。

参考文献:

[1] 赖欣,黄邦菊. 空管自动化系统信息安全评估研究[J]. 计算机科学,2014,41(增刊 1):474-476,493. (LAI Xin, HUANG Bangju. Research on information security evaluation of air pipe automation system[J]. Journal of Computer Science, 2014,41(Sup1):474-476,493. (in Chinese))

[2] 张堃,张培建,吴建国,等. 大型控制系统信息安全评估研究[J]. 控制工程,2014,21(4):524-528. (ZHANG Kun, ZHANG Peijian, WU Jianguo, et al. Research on information security evaluation of large control system[J]. Control Engineering, 2014, 21(4):524-528. (in Chinese))

[3] 焦波,李辉,黄赫东,等. 基于变权证据合成的信息安全评估[J]. 计算机工程,2012,38(21):126-128,132. (JIAO Bo, LI Hui, HUANG Hedong, et al. Information security assessment based on variable weight evidence[J]. Journal of Computer Engineering, 2012,38(21):126-128,132. (in Chinese))

[4] 敖琪,张根宝. 基于马尔科夫的多路控制器可靠性及安全评估[J]. 自动化仪表,2014(3):60-63,72. (AO Qi, ZHANG Baogen. Reliability and safety assessment of markov's multipath controller[J]. Process Automation Instrumentation, 2014(3): 60-63,72. (in Chinese))

[5] 马丽仪,张露凡,杨宜,等. 基于模糊神经网络方法的信息系统安全风险评价研究[J]. 中国安全科学学报,2012,22(5): 164-169. (MA Liyi, ZHANG Lufan, YANG Yi, et al. Research on security risk evaluation of information system based on fuzzy neural network[J]. China Safety Science Journal, 2012,22(5):164-169. (in Chinese))

[6] 魏明桦,郑金贵. 基于改进 BP 神经算法的农产品价格预测模型的构建与实现[J]. 唐山师范学院学报,2014(2):66-68. (WEI Minghua, ZHENG Jingui. Construction and realization of agricultural product price forecasting model based on improved BP neural algorithm[J]. Journal of Tangshan Normal University,2014(2):66-68. (in Chinese))

[7] 陈超,陈性元,杨英杰,等. 基于粗糙集和 D-S 证据理论的系统安全评估[J]. 计算机工程,2013,39(10):138-142. (CHEN Chao, CHEN Xingyuan, YANG Yingjie, et al. System safety assessment based on rough set and D-S evidence theory[J]. Journal of Computer Engineering, 2013,39(10):138-142. (in Chinese))

[8] 王霞. 多属性决策的三角模糊函数方法[J]. 辽宁工程技术大学学报(自然科学版),2010,29(5):850-853. (WANG Xia. The triangular fuzzy function method for multi-attribute decision making[J]. Journal of Liaoning University of Engineering Technology (Natural Science Edition), 2010,29(5):850-853. (in Chinese))

[9] JÜRG K, MONNEY P A. A mathematical theory of hints: an approach to the Dempster-Shafer theory of evidence[M]. Berlin: Springer Science & Business Media, 2013.

[10] 崔艳丽,吴洪博. L_n^* 系统中理论的相对发散度和相对相容度[J]. 模糊系统与数学,2011,25(6):53-59. (CUI Yanli, WU Hongbo. The relative divergence and relative compatibility of the theory in the L_n^* system[J]. Fuzzy Systems and Mathematics, 2011,25(6):53-59. (in Chinese))

[11] CHO K, AARON C, YOSHUA B. Describing multimedia content using attention-based encoder-decoder networks[J]. IEEE Transactions on Multimedia,2015, 17 (11):1875-1886.

[12] WENINGER F, JOHANNES B, BJÖRN S. Introducing currennt: the munich open-source cuda recurrent neural network toolkit [J]. The Journal of Machine Learning Research, 2015,16(1):547-551.

[13] GREFF K, SRIVASTAVA R K, KOUTNÍK J, et al. LSTM: a search space odyssey[J]. IEEE Transactions on Neural Networks and Learning Systems,2017:28(10), 2222-2232.
[14] SHI Xingjian, CHEN Zhourong, WANG Hao, et al. Convolutional LSTM network: a machine learning approach for precipitation nowcasting[J]. Advances in Neural Information Processing Systems,2015,5:802-810.
[15] HANSON J,YANG Y,PALIWAL K,et al. Improving protein disorder prediction by deep bidirectional long short-term memory recurrent neural networks[J]. Bioinformatics,2016, 33(5):685-692.
[16] ZUECH R,KHOSHGOFTAAR T M,WALD R. Intrusion detection and big heterogeneous data: a survey[J]. Journal of Big Data, 2015, 2(1):3.
[17] 李卫.深度学习在图像识别中的研究及应用[D].武汉:武汉理工大学,2014.
[18] SCHMIDHUBER J. Deep learning in neural networks: an overview[J]. Neural Networks, 2014, 61:85-117.
[19] 关昕,郭俊萍,王星. 基于改进DS理论的双重模糊信息安全评估[J]. 计算机工程与应用,2017,53(2):112-117. (GUAN Xin, GUO Junping, WANG Xing. Double fuzzy information security assessment based on improved DS theory[J]. Computer Engineering and Applications, 2017,53(2):112-117. (in Chinese))
[20] 谢浩,樊重俊,李岩,等. 基于GA-SVM的机场数据中心信息安全风险评估[J]. 信息安全与通信保密,2015(6):104-107. (XIE Hao, FAN Chongjun, LI Yan, et al. Information security risk assessment of airport data center based on ga-svm[J]. Information Security and Communication Security,2015(6):104-107. (in Chinese))
[21] 赵冬梅,刘金星,马建峰. 基于模糊小波神经网络的信息安全风险评估[J]. 华中科技大学学报(自然科学版),2009,37(11):43-45,49. (ZHAO Dongmei, LIU Jinxing, MA Jianfeng. Information security risk assessment based on fuzzy wavelet neural network[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition),2009,37(11):43-45, 49. (in Chinese))

(收稿日期:2017-12-15 编辑:刘晓艳)

·简讯·

第十三届全国土力学及岩土工程学术大会将在天津市召开

4年一度的全国土力学及岩土工程学术大会是我国岩土工程领域历史最为悠久、影响最为深远的学术会议之一。由中国土木工程学会土力学及岩土工程分会主办,天津大学、天津城建大学、天津建筑学会岩土力学与地下工程专业委员会承办的第十三届全国土力学及岩土工程学术大会将于2019年7月在天津市召开。

当前是我国基础设施工程建设飞速发展的时期,伴随着高速轨道交通、高速铁路、高速公路、城市地铁、超高超限建筑、海洋资源开发等重大工程,提出了许多新的土力学及岩土工程问题。第十三届学术大会将以“岩土工程品质提升与可持续发展”为主题,对我国近年来土力学与岩土工程领域的最新研究进展进行广泛的学术交流。会议征文内容包括:岩土的基本性质与本构关系,岩土工程勘察、测试与评价技术,基础工程与地基处理,地下工程及深基坑工程,岩土工程数值仿真与信息化技术,土动力学与岩土地震工程,特殊土与边坡工程,环境岩土工程,岩土工程中的新技术与新材料,地质灾害预警与防治,重大岩土工程实录,岩土工程机械设备与施工技术等12个方向。

(本刊编辑部供稿)