计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240600051

一种基于改进 D-S 证据的智慧水利网络安全态势评估方法

夏卓群[1]　周子豪[1]　邓　斌[2]　康　琛[3]
1 长沙理工大学计算机与通信工程学院　长沙 410000
2 长沙理工大学水利与环境工程学院　长沙 410000
3 湖南省水旱灾害防御事务中心网信技术部　长沙 410000
(xiazhuoqun@csust.edu.cn)

摘　要　智慧水利是国家关键信息基础设施的重要行业和领域。网络安全态势评估技术的研究,为智慧水利的数据保护和网络安全建设提供了有力支撑。针对智慧水利网络模型特点以及基于单一 D-S 证据理论的网络安全态势评估模型中存在着主观依赖性、证据冲突大的问题,提出了一种基于改进 D-S 证据理论的智慧水利态势评估方法。首先,面对海量水利数据,使用深度自编码器对数据进行特征学习和过滤降维处理。然后,将处理后的数据交由深度神经网络进行二分类和多分类计算,并将结果融合,得出基本概率分配函数值,其将作为 D-S 证据理论的输入。最后,通过 D-S 证据理论的融合规则得到最终的网络安全态势评估结果。实验结果表明,相较于传统态势评估模型,所提方法能够在提升客观性的情况下,保持较高的准确性。

关键词:智慧水利;网络安全态势感知;D-S 证据理论;深度自编码器;深度神经网络
中图分类号　TN915.08

Security Situation Assessment Method for Intelligent Water Resources Network Based on Improved D-S Evidence

XIA Zhuoqun[1],ZHOU Zihao[1],DENG Bin[2] and KANG Chen[3]
1 School of Computer and Communication Engineering,Changsha University of Technology,Changsha 410000,China
2 School of Hydraulic and Environmental Engineering,Changsha University of Technology,Changsha 410000,China
3 Network Information Technology Department of Hunan Provincial Flood and Drought Disaster Prevention Center,Changsha 410000,China

Abstract　Intelligent water conservancy is an important industry and field of national key information infrastructure. The research on network security situation assessment technology provides powerful support for data protection and network security construction of smart water conservancy. This paper proposes a smart water conservancy situation assessment method based on improved D-S evidence theory,in response to the characteristics of smart water conservancy network models and the problems of insufficient objectivity and large evidence conflicts in network security situation assessment models based on a single D-S evidence theory. Firstly,in the face of massive water conservancy data,deep autoencoders are used to learn features and filter and reduce dimensionality of the data. Then,the processed data is handed over to a deep neural network for binary and multi classification calculations,and the results are fused to obtain the basic probability allocation function value as input for D-S evidence theory. Finally,the fusion rule of D-S evidence theory is used to obtain the final network security situation assessment result. Experimental results show that,compared to traditional situational assessment models,our method can maintain high accuracy while improving objectivity.

Keywords　Intelligent water conservancy,Network security situation awareness,D-S theory of evidence,Deep autoencoder,Deep neural networks

智慧水利工程信息控制系统是国家重要的关键信息基础设施。大型水利工程往往身兼数职,如黄河小浪底水利枢纽工程承担着减游(调沙)、防洪(防凌)、供水、发电、灌溉等许多关系到国计民生的重要职责。因此,如果其控制系统一旦遭受到实质性的网络攻击,将会造成重大影响[1]。如今,针对各种信息系统的威胁、攻击等恶意网络行为不断增长且日益猖獗,逐渐呈现出攻击工具专业化、目的商业化、行为组织化甚至国家化的特点。对于多数水利工程来说,针对发变电系统的攻击会使其失去能源,并产生一系列次要问题;针对供排水及航运系统的攻击会对其自身和当地生产生活造成严重后果;而针对各类液压闸门和阀门的攻击[2],如果成功,将导致灾难性的后果。

当前水利网络安全面临的问题主要体现在:不断变化的网络系统环境中,传统网络设备和安全设备大多独立运行,或

基金项目:湖南省水利厅科技项目(XSKJ2023059-40)
This work was supported by the Hunan Provincial Department of Water Resources Science and Technology Project(XSKJ2023059-40).
通信作者:周子豪(1043082059@qq.com)

者只是根据现有规则进行匹配、报警和处理。它们之间彼此不能互联，或互联程度不足以准确有效地发现、分析和利用各种网络安全事件之间的内部和外部关联关系，从而导致安全威胁的检测和处置不及时，性能效率低，且简单基于规则匹配的误报率、漏报率均较高[3]。网络安全态势感知（Network Security Situational Awareness，NSSA）是解决当前水利网络安全问题的一种新方法，也是当前网络安全领域的研究热点之一。智慧水利网络中的网络安全态势感知通过融合网络安全信息，来实时评估当前的网络安全态势，为网络安全管理员的下一步决策提供支持，降低网络中不安全因素所带来的风险和损失。同时，网络安全态势感知，对增强网络监控能力，提高网络安全应急响应能力并为未来网络安全发展趋势提供预测能力，具有重要意义。

网络安全态势评估的核心是对数据集信息的融合。在数据融合方面，D-S（Dempster/Shafer）证据理论有着非常多的优点。首先，它可以有效处理数据的不确定性问题；其次，D-S可以通过对证据的积累不断减少假设集；最后，它无需知道条件概率以及先验概率。因此，相较于贝叶斯推理法等同类型算法，D-S具有很强的容错能力，能够很好地将信息归类到未知或未定中，并且D-S证据理论对先验效率的依赖性相对于贝叶斯等同类型算法来说较低[4]。但是，D-S理论也存在着较为突出的问题，传统的D-S理论常常采用专家评估法得出基本概率分配函数，会导致存在较大的客观性。为解决这个问题，可使用深度神经网络来自动训练分类计算得出基本概率分配函数，以降低其主观性。在网络安全态势的研究中，由于强容灾能力以及能够通过低代价实现较好效果等特点，深度神经网络备受学者喜爱。但同时深度神经网络在处理大规模数据时也会存在收敛速度慢、分类精度差的问题，本文采用深度自编码先对海量数据进行数据降维和数据过滤，来避免此类问题。

1 相关研究

网络安全态势感知的研究方法复杂多样，其中态势评估、态势预测是网络安全态势感知研究的重点。针对这两大重点模块，学者们将不同的算法融入其中进行实验，并试图建立一个效率高、适应性强、可靠性高的网络安全态势感知模型。

国内外研究中，Wang等[5]将线性加权法融入D-S证据理论中，通过线性加权法对原始数据来源进行修正，提高了D-S对抗冲突的能力，并以此提出了基于改进的D-S的评估模型。该模型提高了D-S对抗冲突的能力，但并未有效解决D-S证据理论在基本概率分配中客观性不足的问题。Chang[6]提出了一种基于卷积神经网络多元融合的网络安全态势感知模型，将卷积神经网络算法、指数加权的D-S融合算法、层次化网络分析法进行多算法融合。与单一算法构建的网络安全态势感知模型相比较，该模型预测的准确性和可靠性均有提高。但该模型使用的卷积神经网络算法也带来了大量的参数计算，使得感知效率有所下降。Xie等[7]所提出的一种基于RBF（Radical Basis Function）神经网络的网络安全态势预测模型，是为了解决态势要素与评估结果之间的不确定性及模糊性问题。但是该模型所使用的方法仅实验于小规模的理想网络中，还需要部署在实际网络环境中进行测试。同样是基于深度学习的研究，Dutt等[8]提出了一种IBLT（Instance-Based Learning Theory）模型，以抵御网络攻击的各类安全工具为基础，能够对网络环境中所存在的攻击行为进行识别，从而提高评估结果的正确率。Hu等[9]提出了一种基于MR-SVM（MapReduce-SVM）的态势感知预测模型，通过使用MapReduce实现多路并发的方法，来提升SVM的计算能力，从而提高预测能力。Covalski等[10]通过模块化软件组件按照多级分层模型互连，提出了一种基于EXEHDA-ISSA（Execution Environment for Highly Distributed Applications-Information Security Situational Awareness）的态势感知模型。Cheng等[11]提出了一种基于实体的网络安全态势要素融合方法，该方法能够对态势要素进行统一描述，并有较高的互补性和较低的冗余性，实现了较好的融合效果。国内现今对于智慧水利网络安全态势的研究中，Jia等[12]针对长江水文急需补齐安全态势感知的短板，结合网络安全存在的问题，探讨了长江水文网络安全态势感知系统的建设目标，以及如何构建网络安全态势感知系统，阐述了系统建设的关键技术和推进的工作策略，为下一步系统建设奠定了基础。Cao等[13]搭建大型调水工程智能运行中心系统整体架构，剖析系统基础设施、数字大脑及业务应用组成内容，并结合引汉济渭工程智能运行中心系统的建设及使用过程，总结阐述了大型调水工程智能运行中心系统的实际应用价值。

态势评估模块是智慧水利网络安全态势感知研究中的核心。本文提出了一种基于D-S证据理论的网络安全态势评估模型DS-DAEDNN（Dempster Shafer-Deep Auto Encoder Deep Neural Networks）。其中，使用深度神经网络（Deep Neural Networks，DNN）来获取基本概率分配函数（Basic Probability Assignment，BPA），避免传统单一D-S证据理论在赋值BPA的过程中存在的主观依赖性问题。同时，使用皮尔逊系统和平均概率值对传统D-S证据理论进行修正，从而避免高冲突证据融合时易产生反直观的结果。最后，使用深度自编码器（Deep Auto Encoder，DAE）对海量高维数据进行特征学习和数据降维，来解决DNN在处理海量数据时存在的准确率不高、时间效率低的问题。

2 态势评估模型

如图1所示，本文提出的网络安全态势评估模型主要包括数据降维模块、态势评估模块和态势输出模块。

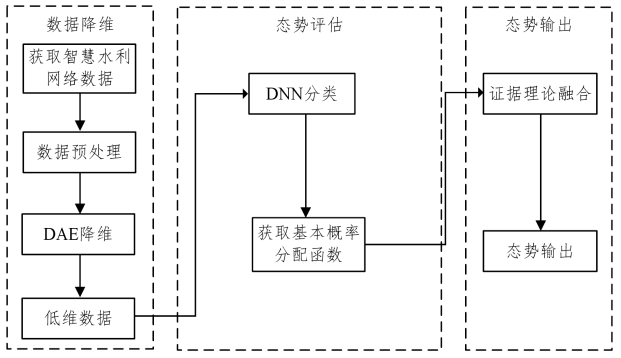

图1 态势评估流程图

Fig. 1 Situation assessment process diagram

在数据降维模块中,采集智慧水利网络运行中的系统要素,如漏洞扫描数据、系统日志数据、防火墙数据等各类安全数据,随后将采集好的数据进行数据预处理,并将预处理后的数据作为 DAE 编码器的输入;在态势评估模块中,将 DAE 所得到的降维数据输入到 DNN 网络进行训练并进行二分类和多分类计算,通过将计算结果融合得到基本概率分配函数;在态势输出模块中,将态势评估模块中计算得出的基本概率分配函数作为 D-S 证据理论的输入,经过 D-S 融合规则得到网络态势值,并输出态势评估结果。

基于 DS-DAEDNN 的网络安全态势评估算法的流程如算法 1 所示。

算法 1 DS-DAEDNN 算法流程

Input:智慧水利网络安全数据集

Output:网络安全态势评估值

1. 输入数据集数据 $n=\{n_1,n_2,\cdots,n_n\}$。
2. 对数据进行预处理。
3. 使用 DAE 算法对数据进行数据降维。
4. 将降维后的低维数据输入 DNN 网络,使用 sigmoid 函数和 softmax 函数分别进行二分类和多分类的训练。
5. 通过二分类所得到的输出值计算入侵攻击概率,并将入侵攻击概率与多分类的训练输出结果融合,共同计算 BPA 值。
6. 将步骤 5 中得到的 BPA 作为 D-S 证据理论的输入,通过 D-S 融合算法得到网络的整体态势值,将其作为最终态势评估输出值。

End

2.1 改进 D-S 证据理论

在数据融合方面,D-S 有着很多先天优势。首先,对信息融合过程中的不确定性问题有比较好的处理能力;其次,D-S 理论可以通过对证据的积累,不断地减少假设集;最后,在处理问题时,不需要将不知道和不确定进行区分,也不需要知道条件概率以及先验概率。证据理论在融合具有高冲突证据时,学者们发现可能会出现融合结果与实际情况相差较大的情况。

针对 D-S 证据理论所存在的不足,学者们进行了长时间的研究,取得了不少成果。本文对 D-S 证据理论中合成证据时所需要的基本概率分配函数进行改进,使得各个证据的权重能够以自适应的方式进行调整,避免出现互相冲突的证据导致融合结果违背实际情况的问题。

本文引入皮尔逊系数来解决上述问题[14]。首先,通过使用皮尔逊系数计算各证据之间是否存在线性相关性,来得到各证据的可信度值,并将该值作为证据的动态权重得到平均概率。其次,计算平均概率与证据之间的度量,得到证据的自适应权重[15]。然后,再对证据加以融合,得到新的证据 BPA。最后,使用 D-S 证据理论中的基本合成规则合成 BPA,得到最终结果。

改进后的 D-S 算法流程如算法 2 所示。

算法 2 D-S 算法流程

Input:未进行处理的证据 BPA

Output:D-S 证据融合所得评估值

1. 使用皮尔逊系数计算各证据之间的相似度:

设 x 和 y 是两个变量,它们之间存在线性关系,用皮尔逊相关系数 P 表示($P\in[-1,1]$)。$P>0$,表明 x,y 呈线性相关;若 $P=0$,则代表 x,y 线性无关。皮尔逊系数的公式如式(1)所示。

$$P_{ij}=\frac{\mathrm{cov}(m_i,m_j)}{\sigma_{m_i}\sigma_{m_j}}=\frac{E((m_i-\mu_{m_8})(m_j-\mu_{m_j}))}{\sqrt{E(m_i^2)-E^2(m_i)}\sqrt{E(m_j^2)-E^2(m_j)}} \tag{1}$$

其中,$\mu_{m_i}=m_i-E(m_i)$,$\mu_{m_j}=m_j-E(m_j)$。

将上述两个证据的相关系数扩展至 $n\times n$ 个证据,可得出相关性矩阵 $\mathbf{P}_{ij}$,如下:

$$\mathbf{P}_{ij}=\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \tag{2}$$

2. 计算证据 m_i 的支持度 SUP_{m_8}:

$$SUP_{m_i}=\sum_{j=1,j\neq i}^{n}P_{ij}(m_i,m_j) \tag{3}$$

3. 计算证据可信度:

通过分析式(3)可知,两个证据支持度越高,m_i 的可信度越高。m_i 可信度公式如式(4)所示。

$$Crd_{m_i}=\frac{SUP_{m_i}}{\sum_{i=1}^{n}SUP_{m_i}},Crd_{m_i}\in[0,1] \tag{4}$$

4. 计算加权平均证据概率:

将可信度值作为各个证据的动态权重,计算平均证据概率:

$$m_{ave}=\sum_{i=1}^{n}m_i\times Crd_{m_i} \tag{5}$$

5. 计算平均概率与到证据之间的度量:

$$d_i=|m_i-m_{ave}| \tag{6}$$

6. 分别计算自适应权重 w_i:

由于度量与权重成反比关系,d_i 越小,说明该证据权重越大。各证据概率权重公式如式(7)所示。

$$w_i=\frac{\frac{1}{d_i}}{\sum_{i=1}^{n}\frac{1}{d_i}} \tag{7}$$

7. 计算各新证据概率 m_i':

$$m_i'=w_im_i \tag{8}$$

8. 使用 D-S 证据理论合成规则将加权平均后的 m_i' 依次融合,并输出最符合决策规则的结果。

End

2.2 DAEDNN 网络

深度自动编码器通过改变原始自动编码器(Auto Encoder,AE)的网络结构来生成 DAE 网络。与 AE 网络相比,DAE 网络在编码器和解码器中都有更多的隐藏层,这可以有效地提高 DAE 的学习能力,同时也使得它更有利于特征学习。

深度神经网络因其准确性和高效性的特点,而被用于网络安全态势评估。相较于传统的神经网络分类算法,DNN 可以在更短的时间内获得更准确的分类结果。

单一的 DNN 网络模型在入侵攻击检测分类场景下具有优异的表现,但在态势评估中,当面对高维、大型结构化数据集时,其最终检测结果的准确性会受到很大影响,导致其态势评估结果与实际网络情况存在显著差异。在 DNN 网络训练前,针对数据集进行特征学习和数据降维是解决上述问题的方法之一。因此,故本文选择将 DAE 作为特征学习和数据降维的工具,并结合 DNN 网络,构建 DAEDNN(Deep Auto Encoder Deep Neural Networks)网络[16]。图 2 所示为基于 DS-DAEDNN 的态势评估模型,其直观展示了 DEADNN 的网络结构。

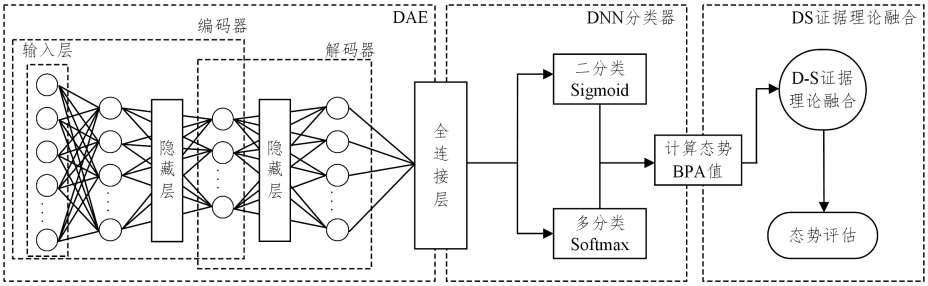

图 2 DAEDNN 模型

Fig. 2 DAEDNN model

DAE 算法对原始数据进行处理的流程如算法 3 所示。

算法 3 DAE 算法流程

Input:原始数据集

Output:重构后的低维数据集

1. 配置编码器、解码器中的隐藏层数,并根据数据集中的特征数配置编码器输入层接口数量。
2. 将预处理数据集输入编码器,并将数据集中的全部特征映射至编码器隐藏层所对应的各个特征表达之中。
3. 这些表征同时也作为解码器的输入,解码器试图将表征重构回原始输入。
4. 通过损失函数比较重构输入数据和原始输入数据,计算损失并使用反向传播算法更新网络权重。
5. 重复步骤 1—步骤 3,直到损失收敛,DAE 网络学习到数据中的所有表征。
6. 解码器输出数据,输出数据拥有输入数据的所有主要特征,能够表示输入数据,但输出数据的特征维度较输入数据低。

End

DNN 算法分类函数如下:

1)本文所使用的二分类激活函数为 sigmoid 函数,该函数的输出结果在区间[0,1]内。在本模型中,sigmoid 函数所输出的数值越靠近 1,则越容易被判定为异常流量。sigmoid 函数的计算如下所示:

$$\sigma(x)=\frac{1}{1+e^{-x}} \tag{9}$$

2)本文采用 softmax 函数作为 DNN 模型的多分类激活函数,虽然 softmax 函数也是将输出映射到 0 和 1 区间,但是与 sigmoid 函数不同的是,softmax 函数所得出的各个类别的输出值相加的和等于 1。因此,本文的 DNN 模型选择将 softmax 函数输出值最大的类别作为预测的类别。softmax 函数的计算如下所示:

$$S(z_i)=\frac{e^{z_i}}{\sum_{j=1}^{K}e^{z_j}} \tag{10}$$

其中,$z=\{z_1,z_2,z_3,\cdots,z_K\}$,$K$ 表示函数 softmax 的输出结果可以被分为 K 个类,z_i 表示每一个所取得的值。

3 实验

3.1 实验环境

实验的硬件环境为:Intel(R) Core(TM) i7-8750H 处理器;显卡为:NVIDIA GeForce GTX 1050 Ti;内存为:16GB。训练和测试实验均在 Windows 64 位操作系统上进行。使用的编程语言和机器学习库为 python3.9 和 TensorFlow2.10。模型的训练和测试均使用 GPU 加速。

本实验所选择的数据集 SWaT[17](Secure Water Treatment)来自新加坡国立大学(NUS)的一个研究项目,该项目旨在通过实验室规模的水处理系统来研究和评估工业控制系统(ICS)的安全性。SWaT 数据集是在该系统上收集的,模拟了真实世界的水处理和分配过程,特别是在面临攻击时的系统行为[18]。该数据集包含了正常操作下的系统行为数据,以及在各种网络攻击场景下的数据。这些攻击包括对系统的物理和逻辑攻击,例如改变化学物质的投加量,改变传感器和执行器信号,重放攻击以操纵进程行为等。

SWaT 数据集包含了 51 个特征和 6 种攻击所产生的主要异常行为类型。该数据集来自于 51 个传感器和执行器,共记录连续 11 天的数据,其中 7 天为正常操作数据,4 天阶段性受到攻击,共遭受 41 次攻击。数据集的详细描述如表 1 所列,其中 N_rate 是正常数据点与测试数据集中所有数据点的比率。

表 1 SWaT 数据集描述

Table 1 SWaT dataset descriptions

属性	详情
数据集名称	SWaT
所含特征种类	51
攻击次数	41
攻击持续时间/min	2～25
训练大小(均为正常数据)	496800
测试大小(含攻击数据)	449919
N_rate/%	88.02

SWaT 数据集中主要异常行为类型以及对应影响因子如表 2 所列。

表 2 SWaT 数据集中异常行为类型

Table 2 SWaT dataset abnormal behavior types

异常行为类型	影响因子
化学品加药系统异常行为	0.3
原水的存储和转移异常行为	0.1
预处理系统异常行为	0.2
膜过滤系统异常行为	0.2
消毒系统异常行为	0.2

3.2 数据集预处理

在 SWaT 数据集环境中,某些特征的最大值和最小值之间存在显著差异。为使特征能够在相同范围之内同时精确保留数据的关系,本文采用最大最小值法将数据进行归一化处理:

$$x'_{ij}=\frac{x_{ij}-x_{i\min}}{x_{i\max}-x_{i\min}} \tag{11}$$

其中,x_{ij} 表示需要归一化处理的数据;$x_{i\max}$ 和 $x_{i\min}$ 是数据中的最大值和最小值;x'_{ij} 表示归一化处理后的输出结果,取值范围为 $x'_{ij}\in[0,1]$。

3.3 实验结果与分析

3.3.1 对比实验

实验采用准确率(Accuracy)、召回率(Recall)以及 F1 值

(F1-Score)作为对比实验中模型的评价指标。

TP 表示被模型预测为攻击样本并与实际相符合的次数；FP 表示被模型预测为正常样本但与实际不相符的次数；TN 表示被模型预测为正常样本并与实际相符合的次数；FN 表示被模型预测为攻击样本但与实际不相符的次数。

准确率(Accuracy)：表示模型预测的攻击样本的正确频率。预测的准确率越高，则代表模型的误报率越低。

$$Accuracy=\frac{TP}{TP+FP} \tag{12}$$

召回率(Recall)：表示模型正确分类的攻击样本与实际攻击样本的百分比，它代表着模型的识别能力。

$$Recall=\frac{TP}{TP+FN} \tag{13}$$

F1 值(F1-Score)：准确率和召回率的调和平均数。

$$F1\text{-}Score=\frac{2\times Accuracy\times Recall}{Accuracy\times Recall} \tag{14}$$

使用 SWaT 数据集测试 5 个模型：DS，SVM，DS-SAEDNN，DAEDNN 和 DS-DAEDNN。选择上述指标作为评价指标，对 5 个模型进行比较分析。不同模型的指标得分如图 3 所示，其中纵坐标表示评价指标的百分数，数值越高，代表模型性能越好。

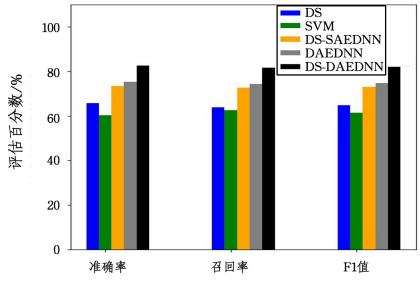

图 3　不同模型的各类指标得分

Fig. 3　Scores of various indicators for different models

由图 3 可知，DS-DAEDNN 模型在准确率、召回率和 F1 值等方面都优于其他 4 种类型的模型。实验结果表明，DS-DAEDNN 不仅提高了对少量训练数据样本的攻击类型的准确率和召回率，而且对大量训练样本的攻击检测性能也并没有降低。DS-DAEDNN 具有更高的准确率和召回率，因此具有更强的泛化能力。与 DS，SVM，DS-SAEDNN 和 DAEDNN 模型相比，DS-DAEDNN 的 F1 值分别增加了约 17.36%，20.67%，9.09%和 7.31%。

3.3.2　网络安全态势量化评估

根据《国家突发公共事件应急预案》[19]对网络安全形势进行分类，如表 3 所列。其中，I 级、II 级、III 级、IV 级、V 级分别为安全、比较安全、基本安全、较不安全、不安全 5 个等级。

表 3　网络安全评估等级表

Table 3　Network security assessment levels

安全等级	态势 BPA
安全(I 级)	(0.8,1.0]
比较安全(II 级)	(0.6,0.8]
基本安全(III 级)	(0.4,0.6]
较不安全(IV 级)	(0.2,0.4]
不安全(V 级)	[0,0.2]

从测试数据集中随机选择不同数量的测试样本，定量评估网络的安全状况。同时，使用不同的模型计算网络安全态势值。从 7 个不同数量的测试样本中获得的网络安全态势值如图 4 所示。

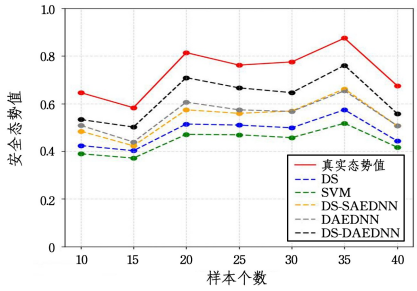

图 4　7 组测试的网络安全态势值

Fig. 4　Network security situation values for 7 sets of tests

由图 4 可见，在样本数较少时，DS-DAEDNN 评估模型的评估结果更接近网络的实际态势值，DS-SAEDNN 评估模型和 DAEDNN 评估模型的评估结果大致相同，而传统 D-S 证据理论评估模型和传统 SVM 评估模型的评估结果则相较于其他评估模型处于劣势。随着样本个数的增加，DS-DAEDNN 网络安全评估模型相较于其他模型的评估结果也更接近实际态势值。因此，基于 DS-DAEDNN 模型计算出的网络安全态势值相较于其他态势评估模型具备更好的可用性。

结束语　本文针对传统 D-S 网络安全态势评估方法在证据融合过程中存在客观性不足、证据冲突大的缺点，结合智慧水利网络的特点，提出了一种基于改进 D-S 证据理论的智慧水利态势评估方法。该方法首先结合了深度自编码器和深度神经网络组成 DAEDNN 模型，用于对网络攻击进行识别。根据识别结果进行二分类和多分类计算，并将计算结果融合得出基本概率分配函数。最后，通过 D-S 证据理论融合计算得出网络安全态势值。本文实验使用 SWaT 数据集对模型进行了训练和测试，实验结果表明，基于 DS-DAEDNN 的网络安全态势评估模型在准确率、泛化能力等方面优于其他模型。

参 考 文 献

[1]　WU K H，LI Y，CHEN F，et al. A method for describing industrial control system network attack using object Petrinet[J]. IEEE Transactions on Electrical and Electronic Engineering，2016，11(2)：216-227.

[2]　ZHAO W B. Research on the Network Security Monitoring System of Smart Water Conservancy Internet of Things[J]. Water Resources Informatization，2021(4)：39-46.

[3]　LI Y J，ZHANG J，YANG X，et al. Discovery of Water Conservancy Network Security Threats Based on Situation Awareness [C]// Proceedings of the 2020(Eighth) China Water Conservancy Informatization Technology Forum. 2020：328-334.

[4]　RIGELSFORD J. Pattern recognition：Concepts，methods and applications[J]. Assembly Automation，2002，22(4).

[5]　DONG W，WANG G，YAN Q，et al. Design of Network Security Situation Awareness and Early Warning System Based on Big Data[C]// 2023 International Conference on Networking，Informatics and Computing (ICNETIC). Palermo，Italy，2023：749-753.

[6]　CHANG L W，LIU X J，QIAN Y H，et al. A Network Security

Situation Awareness Model Based on Multi-source Fusion of Convolutional Neural Networks [J]. Computer Science, 2023, 50(5): 382-389.

[7] XIE L X, WANG Y C, YU J B. Network Security Situation Awareness Based on Neural Networks [J]. Journal of Tsinghua University(Science and Technology), 2013, 53(12): 1750-1760.

[8] DUTT V, AHN Y S, GONZALEZ C. Cyber situation awareness: modeling detection of cyber attacks with instance-based learning theory[J]. Human Factors, 2013, 55(3): 605-618.

[9] HU J, MA D, LIU C, et al. Network Security Situation Prediction Based on MR-SVM [J]. IEEE Access, 2019, 7: 130937-130945.

[10] ALMEIDA R B, COVALSKI V, MACHADOR, et al. A hierarchical architectural model for network security exploring situational awareness[C]// Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing. 2019: 1365-1372.

[11] SI C, ZHANG H, WANG Y, et al. Network Security Situation Elements Fusion Method Based on Ontology[C]// 2014 Seventh International Symposium on Computational Intelligence and Design. Hangzhou, China, 2014: 272-275.

[12] JIA K, WANG L H, LIU D. Preliminary Exploration on the Construction of the Network Security Situation Awareness System for the Hydrology of the Yangtze River [J]. Express Water Resources & Hydropower Information, 2021, 42(3): 79-84.

[13] CAO Q. System Design and Application of the Intelligent Operation Center for Large-scale Water Diversion Projects [J]. Water Resources Informatization, 2022, 6(1): 65-70.

[14] KONG Z J. Research on the Method and Application of Network Security Situation Awareness Based on D-S Evidence Theory [D]. Hohhot: Inner Mongolia University, 2022.

[15] LUO Q Q. Research on Network Security Situation Awareness Based on D-S Theory [D]. Nanjing: Nanjing University of Posts and Telecommunications, 2021.

[16] YANG H Y, ZENG R Y. A Network Security Situation Assessment Method Based on Deep Learning [J]. Journal of Xidian University, 2021, 48(1): 183-190.

[17] GOH J, ADEPU S, JUNEJO K N, et al. A Dataset to Support Research in the Design of Secure Water Treatment Systems [C]// The 11th International Conference on Critical Information Infrastructures Security. Cham: Springer, 2016.

[18] Secure Water Treatment(SWaT) Testbed[EB/OL]. https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/#swat.

[19] 国务院.《国家突发公共事件总体应急预案》(http://www.gov.cn/jrzg/2006-01/08/content_150878.htm), 2006.

XIA Zhuoqun, born in 1977, Ph.D, professor. His main research interest is network security.

ZHOU Zihao, born in 1999, postgraduate. His main research interest is network security.