文章编号: 1001-0920(2019)11-2330-07 DOI: 10.13195/j.kzyjc.2019.0592

基于自适应鲁棒性的入侵检测模型

吴亚丽†, 李国婷, 付玉龙, 王晓鹏

(1. 西安理工大学 自动化与信息工程学院，西安 710048；
2. 西安理工大学 陕西省复杂系统控制与智能信息处理重点实验室，西安 710048)

摘 要: 传感器与网络技术的迅猛发展促进了信息物理系统的发展与应用. 而传统网络系统的入侵检测技术已经发展成熟,信息物理系统(CPS)可以在借鉴传统网络系统入侵检测技术的基础上,结合自身特性进行改进. 针对CPS所处地理位置复杂及网络传输不可靠导致的检测鲁棒性不高的问题,提出基于稀疏降噪自编码网络(SDAE)的入侵检测算法;同时,考虑到CPS对模型适应性及推广性的需求,将基于差分变换的头脑风暴优化算法(DBSO)与改进的自编码网络相结合,形成基于DBSO优化SDAE(DBSO-SDAE)的检测算法. 该算法具有自动提取入侵数据最优特征表示的能力,同时在进一步提高模型鲁棒性的前提下,可极大地增强模型的适应性. 仿真结果表明,所提出的DBSO-SDAE模型与其他模型相比,具有较高的鲁棒性、自适应性及较优的检测实时性,可极大地满足CPS对检测算法的高需求.

关键词: 信息物理系统；鲁棒性；自适应性；入侵检测；自编码网络；头脑风暴优化算法

中图分类号: TP183 **文献标志码:** A

A new intrusion detection model based on adaptability and robustness

WU Ya-li†, LI Guo-ting, FU Yu-long, WANG Xiao-peng

(1. School of Automation and Information Engineering, Xi'an University of Technology，Xi'an 710048, China；
2. Shaanxi Province Key Laboratory of Complex System Control and Intelligent Information Processing, Xi'an University of Technology，Xi'an 710048, China)

Abstract: The rapid development of sensor and network technology promotes the development and application of cyber physical system, while the intrusion detection technology of the traditional network system has matured. The cyber physical system (CPS) can be improved in combination with its own characteristics based on the traditional intrusion network technology. The geographic location of CPS is complex and the network transmission is unreliable, which lead to that the detection robustness is not high. Aiming at this problem, an intrusion detection algorithm based on sparse denoising auto-encoders (SDAE) is proposed. What's more, CPS requires models to be adaptive and generalized, so difference brain storm optimization (DBSO) based optimization of SDAE (DBSO-based optimization of SDAE, DBSO-SDAE) detection algorithm is formed by combining DBSO with improved auto-encoders. The algorithm can automatically extract the optimal feature representation of intrusion data and greatly enhance the adaptability of the model while further improving the robustness of the model. The simulation results show that the DBSO-SDAE model proposed in this paper has higher robustness, adaptability and better real-time detection than other models, which greatly satisfies the high demand of CPS for detection algorithms.

Keywords: cyber physical system; robustness; adaptability; intrusion detection; auto-encoders; brainstorm optimization algorithm

0 引 言

信息物理系统(CPS)通常被定义为计算与物理过程的深度结合,它将计算和通信功能与对物理世界中的实体的监视和控制集成在一起[1]. 近几年来,传感器与网络技术的迅猛发展促进了信息物理系统的发展与应用,例如,机器人控制系统[2]、汽车系统[3]、水利[4]及电力[5]系统等. 但是,CPS也面临着各种各样的随机故障和网络攻击的威胁,极大地制约了CPS的发展. 相较于传统的网络安全,任何蓄意的网络攻击都会对被控制的物理对象甚至依赖它的人造成难以

收稿日期: 2019-05-01；**修回日期:** 2019-08-20.

基金项目: 国家重点研发计划重点专项项目 (2018YFB1703004); 国家自然科学基金青年基金项目 (61503299, 61502385).

责任编委: 李韬.

†通讯作者. E-mail: yliwu@xaut.edu.cn.

想象的损害. 入侵检测作为一种积极主动的防御技术,是及时发现潜在网络威胁、制定合理防御策略的主要手段,是网络安全技术体系中重要的组成部分. 它能够通过收集和分析相关网络数据及时发现攻击行为,降低安全威胁. 因此,研究CPS的入侵检测显得尤为重要.

目前,传统的网络系统已经有逐步成型的入侵检测技术,CPS可以借鉴传统网络的入侵检测技术,并结合系统自身特性进行调整. 由于传感器设备和网络技术的不断发展,CPS生成数据的维度和数量更甚于传统网络,传统的入侵检测方法在处理海量高维数据方面面临巨大挑战. 而深度学习作为表征学习的代表适宜处理大规模数据,能够直接从复杂的原始数据中自动学习高层次的特征数据,免去了手工特征提取对专家知识的依赖. 实际上,检测算法越强大,能耗就越大. 文献[6-7]结合了各自CPS系统特点,均考虑资源消耗及负载问题,在一定程度上都是以牺牲精度为前提的. 但是,信息物理系统需要更好的安全性能. 文献[3]针对不同攻击的时间上下文将深度学习与计算卸载相结合,取得较好的结果,并以检测延时为准则建立数学模型,验证了其可行性. 因此,本文采用深度学习算法建立入侵检测模型.

在深度学习算法中,自动编码器利用大量未标记数据,通过数据特征提取来降低特征维数,在入侵检测中具有较好的特征提取和降维能力. 在传统的网络系统中,文献[8-9]均采用自编码网络进行入侵检测,并取得了较好的成果,但若要适用于CPS系统,仍然需要考虑两个问题:一是CPS系统对检测系统的鲁棒性有着较高的要求,而部分CPS系统所处地理位置复杂,传感器传输信息存在噪声,因此有必要提高检测系统的鲁棒性;二是CPS系统的特殊性要求模型能够适应和扩展数据漂移,不断发现新的系统威胁和漏洞,而现有模型结构选择费时费力,模型不能根据数据的不同分布特征自适应提取本质特征,不具有可适性和推广的能力,不能运用于多个CPS实例. 因此,本文将头脑风暴优化算法(brain storm optimization, BSO)与改进的自动编码器相结合,旨在提高模型的鲁棒性及自适应性.

本文提出的方法主要创新点表现在: 1) 考虑到CPS对鲁棒性的较高需求,将噪声引入自编码网络,旨在提升模型的鲁棒性; 2) 基于BSO与改进自编码相结合的方式自适应地获得入侵数据的最优特征表示,免去费时费力的人工提取,避免网络结构对检测精度及鲁棒性的影响,在进一步提高鲁棒性的同时使模型更具有适应性和推广能力; 3) 模型能够针对入侵数据的不同特征进行自适应调整,并对已知和未知攻击都具备较高的检测率.

1　基于鲁棒性的网络模型框架

CPS系统对鲁棒性的需求更甚于传统网络系统,传感器设备的偶然故障和网络传输的不可靠性是导致检测系统鲁棒性低的主要原因,究其缘由是低质量带噪声数据引起的. 因此,有必要对检测系统进行降噪处理,以提高其鲁棒性.

1.1　叠加稀疏自编码网络

1.1.1　自编码网络

CPS将计算和通信功能与对物理世界中的实体的监视和控制集成在一起,所带来的结果是数据维度和规模的剧增,而自编码网络将有监督与无监督相结合,能够对数据进行特征提取及降维,从而学习到特征最本质的表示.

自动编码网络(auto-encoders, AE)是2007年Bengio等[10]提出的,通过对输入数据进行无监督的逐层特征变换,将原空间的样本特征表示变换为新的特征空间并自动学习分层特征表示. AE由3部分组成,即输入层、隐层和输出层,其表示如图1所示,其中输入层和输出层具有相同的维度.

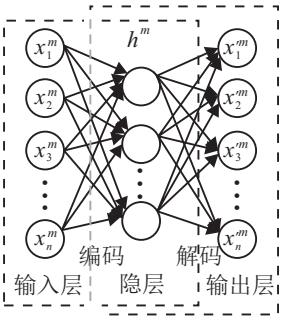


图 1　单层自编码机

编码过程为计算输入层数据x到隐层的数据h的过程. 解码过程为将隐层的数据h重新恢复出输入层数据即输出层数据x'的过程,表示为

$$\begin{cases} h = S_f(W_1 x + b), \\ x' = S_g(W_2 h + d). \end{cases} \tag{1}$$

其中: W_1为输入层与隐层的权值矩阵; W_2为隐层和输出层的权值矩阵; b、d分别为隐层的偏置向量和输出层的偏置向量; S_f、S_g为sigmoid函数,目的是为了提高网络的非线性能力. 函数表示为

$$\mathrm{sigmoid}(x) = \frac{1}{1+\mathrm{e}^{-x}}. \tag{2}$$

为了减少参数,将输入层与隐层之间的权值矩阵W_1和隐层与输出层的权值矩阵的转置W_2'取为W,其公式表示为

$$W_1 = W_2' = W. \tag{3}$$

故AE参数有3个,分别为W、b、d. 训练的目标是最小化输出与输入之间的差异,目标函数为

$$\arg\min_{W,b,d}[c(x,x')] = \frac{1}{2}\|x-x'\|^2. \tag{4}$$

其中:x'是在x给定的情况下由W、b、d来调节的;$c(x,x')$为每个训练样本的训练目标,总训练目标为

$$c(x,x') = \sum_{i=1}^{m}\frac{1}{2m}\|x-x'\|^2, \tag{5}$$

其中m为训练样本的数量.

训练完成后,隐层的输出h是学习到的特征,将其作为自编码网络中下一层AE的输入. 多层AE即构成了堆栈自编码机(stacked auto-encoder, SAE),然而由于SAE不具有分类特性,将SAE与分类器结合成为堆栈自编码网络.

分类器采用softmax分类器,训练样本集合为$\{(x^{(1)},y^{(1)}),(x^{(2)},y^{(2)}),\cdots,(x^{(m)},y^{(m)})\}$,$m$为样本个数,其中第$i$个训练样本为$x^{(i)}$,其标签为$y^{(i)}\in\{1,2,\cdots,k\}$,$k$为类别数,则softmax回归的假设为

$$h_\theta(x^{(i)}) = \begin{bmatrix} p(y^{(i)}=1\mid x^{(i)};\theta)\\ p(y^{(i)}=2\mid x^{(i)};\theta)\\ \vdots\\ p(y^{(i)}=k\mid x^{(i)};\theta)\end{bmatrix} = \frac{1}{\sum_{j=1}^{k}\mathrm{e}^{\theta_j^{\mathrm{T}}x^{(i)}}}\begin{bmatrix}\mathrm{e}^{\theta_1^{\mathrm{T}}x^{(i)}}\\ \mathrm{e}^{\theta_2^{\mathrm{T}}x^{(i)}}\\ \vdots\\ \mathrm{e}^{\theta_k^{\mathrm{T}}x^{(i)}}\end{bmatrix}. \tag{6}$$

向量$h_\theta(x^{(i)})$的每一个元素$p(y^{(i)}=k|x^{(i)};\theta)$代表样本$x^{(i)}$属于第$j$类的概率(向量的元素和为1),$\theta_1,\theta_2,\cdots,\theta_k$为模型参数向量,则模型的代价函数定义如下:

$$J(\theta) = -\frac{1}{m}\Big[\sum_{i=1}^{m}\sum_{j=1}^{k}1\{y^i=j\}\log\frac{\mathrm{e}^{\theta_j^{\mathrm{T}}x^{(i)}}}{\sum_{j=1}^{k}\mathrm{e}^{\theta_j^{\mathrm{T}}x^{(i)}}}\Big] + \frac{\lambda}{2}\sum_{j=1}^{k}\sum_{r=0}^{n}\theta_{rj}^2. \tag{7}$$

其中:$1\{\cdot\}$表示指示函数,花括号内表达式为真时指示函数值为1,否则为0;等号右边第2项为权重衰减项,用于解决参数冗余带来的数值问题,同时增强网络的泛化能力. λ为权值衰减系数. 利用式(7)对网络模型进行总体评价,评价函数值越小,检测精度越高.

1.1.2 稀疏约束

为了使模型更具有高效性,在原有的SAE的基础上引入稀疏限制条件. 受生物神经网络启发,将大量神经元在同一时刻处于抑制状态,只有少量神经元被激发. 在本文的自编码网络中使用的激活函数为sigmoid函数,则当神经元的输出接近1时为激活状态,而输出接近0时为抑制状态. 为了使神经元j的活跃度接近于稀疏性参数ρ(通常取值接近于0),可使

$$\rho = \overline{\rho}_j. \tag{8}$$

加入稀疏限制后,损失函数为

$$J_{\mathrm{SSAE}} = c(x,x') + \beta\sum_{j=1}^{N}\mathrm{KL}(\rho\parallel\overline{\rho}_j). \tag{9}$$

其中:等号右边第1项为均方误差重构项;第2项为稀疏惩罚项;β为稀疏惩罚项权重;N为隐藏层中神经元数量;j为第j个神经元;$\mathrm{KL}(\rho\parallel\overline{\rho}_j)$是以$\rho$和$\overline{\rho}_j$为均值的两个伯努利随机变量间的相对熵,用来比较两个变量的相似度.

1.2 噪声输入

传感器监测点失效、异常及传输不稳定产生了不可靠低质量带噪声数据,低质量带噪声数据导致系统较低的鲁棒性. 鲁棒性的定义为当输入包含一些失真时,网络仍可学习到有用的特征,也即要求检测模型依然能够从噪声数据中捕获输入分布中的有用结构.

噪声输入的思想在文献[11]中就有提出,实验表明该方法具有较好的效果;文献[12]提出了关于噪声信道的鲁棒编码;在前者基础上文献[13]引入了降噪参数提高自编码网络鲁棒性,在偏差模型的基础上,从几何流行学习角度、随机算子角度、信息论角度、生成模型的角度对算法进行了分析.

输入加噪后其模型改变如下:

$$\tilde{x}\sim q_d(\tilde{x}\mid x). \tag{10}$$

原始输入x通过随机映射得到损坏输入$\tilde{x}$,在分析中为保证算法的一般性,未特定针对某种噪声,将损坏输入$\tilde{x}$输入到网络,得到重构输出层数据$\tilde{x}'$,即

$$\begin{cases} h = S_f(W_1\tilde{x}+b),\\ \tilde{x}' = S_g(W_2h+d).\end{cases} \tag{11}$$

则有新的重构误差函数如下:

$$\arg\min_{W,b,d}c(x,\tilde{x}') = \sum_{i=1}^{m}\frac{1}{2m}\|x-\tilde{x}'\|^2. \tag{12}$$

使$\tilde{x}'$尽可能接近损坏的输入x,与SAE不同的是$\tilde{x}'$是$\tilde{x}$的确定函数而不是x的,而$\tilde{x}$是通过随机映射得到的,同时更符合实际的噪声数据,从而进一步提高了模型的鲁棒性.

1.3 鲁棒性定量评价标准

Huber[14]从稳健统计的角度系统地给出了鲁棒过程所满足的3个层面:一是模型需要具有较高的精

度或有效性;二是对于模型假设出现的较小偏差,只对算法性能产生较小的影响;三是对于模型假设出现的较大偏差,而不对算法性能产生“灾难性”的影响. 在文献[15]中,以均方误差作为衡量语音模型鲁棒性好坏的度量方式;在文献[16]中,为了定量分析每个跟踪系统的鲁棒性能,使用中心位置误差和重叠率两种度量方式;文献[17]针对农作物叶片病害问题,以加入噪声前后偏离度作为评价鲁棒性好坏的定量体现;文献[18]针对语音识别的噪声问题,以相对精度为对比作为鲁棒性好坏的定量体现.

综上所述,借鉴文献[15-18]中的鲁棒性定量评价标准并结合Huber从稳健统计的角度系统地给出鲁棒性3个层面的概念,选择检测率AC及加入噪声前后检测率的偏离度作为鲁棒性量化评价标准,具体内容如下.

为了更好地评价模型,本文选取入侵领域常用的AC作为评价指标,其评价公式为

$$\mathrm{AC}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{FN}+\mathrm{FP}+\mathrm{TN}}. \tag{13}$$

其中: TP为划分为攻击类的攻击样本数量, TN为划分为正常类别的正常样本的数量, FP为分类为攻击类的正常样本数, FN为分类为正常类别的攻击样本数量.

偏离度的定义公式为

$$D=\frac{|\mathrm{AC}_{t_0}-\mathrm{AC}_{t_1}|}{\mathrm{AC}_{t_0}}\times 100\%. \tag{14}$$

其中: AC_{t_0}为噪声等级为0时的检测精度; AC_{t_1}为噪声等级为t_1时的检测精度; D为偏离度,偏离度越小代表系统鲁棒性越好越稳定.

2　基于自适应鲁棒性的网络模型框架

CPS需要模型具有较好的自适应性,能根据数据的不同分布特征自适应提取本质特征以获得较好的精度及鲁棒性,故有必要引入自适应鲁棒模型框架.

2.1　差分头脑风暴优化算法

为了在提高模型鲁棒性的同时解决模型的自适应问题,减少因模型结构、降噪参数等选取不当对精度及鲁棒性的影响,从而解放人力,减少不必要的计算资源开销,使模型能根据不同数据分布特征自适应提取最本质特征,本文引入头脑风暴优化算法(brain storm optimization, BSO)[19]. BSO是Shi在2011年第二届国际智能群体大会(ICSI11)上提出的一种新的群体智能优化算法,主要受人类头脑风暴会议所启发. 该算法利用聚类思想搜索局部最优解,通过局部最优比较得到全局最优解,利用变异思想提高了算法的多样性,避免了算法陷入局部最优. BSO在许多领域得到了广泛的应用,具有很好的发展前景. 具体算法步骤如下.

Step 1: 对种群初始化;

Step 2: 对个体进行评价和聚类;

Step 3: 通过变异产生新个体;

Step 4: 对种群和聚类中心进行更新;

Step 5: 如果达到最大迭代次数,则输出最优个体,否则转到Step2.

文献[20]提出了差分的变异方法,具有较好的性能,已在许多文献中进行了研究和应用[21-22]. 基于差分变异的头脑风暴优化(difference brain storm optimization, DBSO)算法的BSO可以根据种群的个体分布进行自适应调整,降低计算复杂度,提高运行速度. 与基于高斯变异的经典BSO相比, DBSO更适合于入侵检测领域. 因此,本文将DBSO应用于SDAE来优化网络框架及降噪参数. DBSO与BSO整体结构相同,仅在Step 3用差分变异代替高斯变异产生新个体.

2.2　入侵检测模型

为了获得最优的网络结构及降噪参数,提取CPS系统入侵数据的最本质特征,提高检测率,基于DBSO的基本原理,提出一种新的入侵检测算法——基于DBSO优化的SDAE(DBSO-based optimization of SDAE, DBSO-SDAE),省去了复杂的人工调整步骤,减少了宝贵的计算资源. 最后,在提高鲁棒性的同时实现自适应特征提取模型框架.

头脑风暴算法优化隐藏层层数、节点数及降噪参数的具体过程如下:

1) 初始化.

引入头脑风暴算法,设置种群规模NP、最大迭代次数I、算法超参数.

2) 产生可行隐藏层层数、节点数及降噪参数的集合.

为减少模型参数,各隐藏层节点数个数相同. 因此,取自编码网络的隐藏层层数L、隐藏层节点数N和降噪参数V为决策变量,即决策变量的个数为3. 种群中第i个个体p^i为

$$p^i=[L^i,N^i,V^i]. \tag{15}$$

种群规模为NP,即随机的产生NP个个体. $L^i\in[1,2,\cdots,\max_L]$, $N^i\in[1,2,\cdots,\max_N]$, $V^i\in[0,1]$分别为隐藏层的层数、节点数及降噪参数.

3) 确定个体评价指标.

由于隐藏层层数、节点数及降噪参数共同影响着网络模型的检测精度及鲁棒性,对个体的评价指标与网络模型总的评价标准检测精度有关. 需要在保持较高检测精度的同时选出具有较高鲁棒性的降噪

参数及网络框架,其评价函数如下:

$$\arg\max_{N,L,V} T = \alpha \mathrm{AC}_{\mathrm{noise}} + \eta \mathrm{AC}_0. \tag{16}$$

其中:$\alpha+\eta=1$,α、η为权重系数. 由鲁棒性定义可知,当给输入加入噪声时,网络仍可学习到有用的特征,即要求网络仍能拥有较好的检测精度. 因此,$\mathrm{AC}_{\mathrm{noise}}$为加入噪声后的检测精度,目的是为了使网络具有较高的鲁棒性,AC_0为不加噪声时的检测精度,目的是为了使网络具有较高的检测精度.

4) 个体评价与聚类.

将2)中产生的NP个个体集合分别代入自编码网络模型中,以评价函数T作为个体的评价指标,对种群中每一个个体进行评价.

本文采用k-means进行聚类,不同的是,本文将聚类用于目标空间,即以个体在目标空间中的欧氏距离作为相似度标准.

5) 对种群与聚类中心进行更新.

对隐藏层层数及节点数以很小的概率用任意解替代聚类中心,以增加种群的多样性. 在得到选择个体后,对其进行差分变异来产生新个体,过程如下:

$$X^d_{\mathrm{new}} = X^d_{\mathrm{selected}} + \mathrm{rand} \times (x_1 - x_2). \tag{17}$$

其中:X^d_{new}为新产生个体的第d维,X^d_{selected}为选择个体的第d维,x_1、x_2为选择的两个不同个体.

6) 判断是否达到终止条件.

判断迭代次数I是否达到设定的最大迭代次数$I_{\max}$. 若是,则进入7);否则,返回4),重新进行个体评价与聚类,迭代次数为$I=I+1$.

7) 输出最优个体.

输出针对该数据集对应的自编码网络模型的最优个体,即隐藏层层数、节点数及降噪参数,并将最优个体参数作为网络模型的最优结构,代入后续的网络训练.

总体步骤流程框图如图2所示.

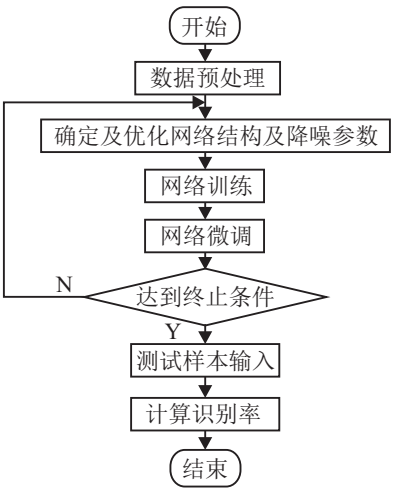


图 2 DBSO-SDAE算法流程

3 实验仿真

3.1 数据集选择

NSL-KDD数据集是由著名的KDD99流量数据集[23]处理和改进后产生的,在异常检测系统中得到了广泛的应用. 数据集中的攻击都是CPS中常见的几种攻击;且CPS要求模型既能检测已知攻击,也能检测未知攻击. 而NSL-KDD测试集中存在训练集中未曾出现的新攻击,因此,本实验采用NSL-KDD数据集对模型进行验证.

3.2 降噪参数对网络性能的影响实验

本节引入的噪声为掩蔽噪声,将其加入训练样本中,将干净的原始数据随机以一定噪声比例随机置零,并输入到稀疏自编码网络中,探究降噪参数对网络性能的影响,其结果如图3所示.

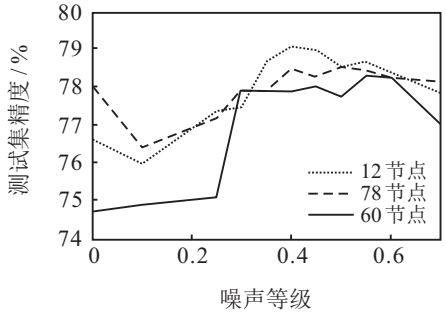


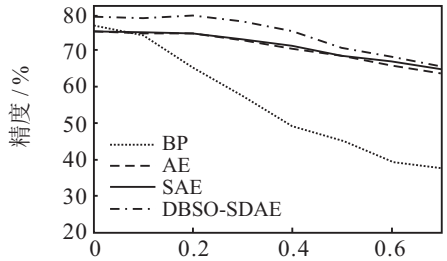
图 3 降噪参数对网络性能的影响

在图3中,降噪参数为0代表输入干净的数据,即未被加入噪声. 由图3可以看出,当降噪参数增加到一定范围内时,可以提高网络泛化能力,提高检测精度,从而验证了噪声的输入可以使自动编码器学习到更加鲁棒的高层特征,减弱过拟合现象.

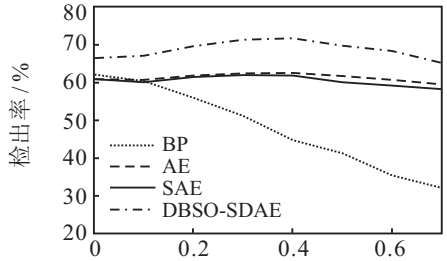
同时,原本性能最佳的78节点在加入降噪参数后上升幅度最小,而性能最差的60节点上升幅度最大. 对于12节点而言,在一定噪声比例下,其测试精度反超原本最优的78节点. 降噪参数的加入使原有系统机制发生改变,从而影响了最优解,使原本最优的节点个数不再最优. 因此,有必要考虑噪声因素在提高鲁棒性的同时重新选择最优的网络结构.

3.3 入侵检测模型DBSO-SDAE实验

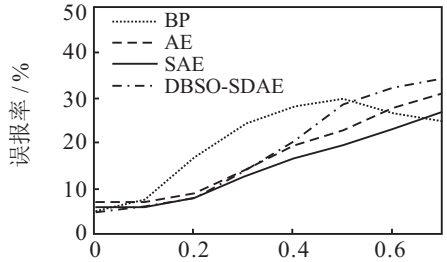
利用DBSO-SDAE模型自适应得到的最优网络层数、节点个数及降噪参数为[1, 17, 0.52]. 考虑到传感器设备的偶然故障及传输的不可靠性,有必要对网络模型的鲁棒性进行验证. 在测试样本中加入均值为0、方差为噪声等级Q的高斯噪声(噪声等级为0～0.7),以测试精度及偏离度为指标验证网络鲁棒性. 本次实验采用控制变量法,以相同结构网络为基础,加入不同程度的噪声,每个数据由10次均值求得,得到实验结果如图4所示.



(a) 噪声等级对精度影响



(b) 噪声等级对检出率影响



(c) 噪声等级对误报率影响

图4　噪声等级对检测性能的影响

由图4可知,本文提出的算法在噪声等级为0时对精度、检出率及误报率均有所改进. 同时,在加入噪声时,指标精度、检出率和噪声等级较低时的误报率均表明算法有较高的鲁棒性,仅在加入的噪声等级过高时,误报率逊于其他算法. 这是由于误报率和检出率为一对矛盾度量,在噪声等级过高导致精度过低时,检出率的提高是以大幅度牺牲误报率为代价的. 而当精度较高时,误报率和检出率的提高相互牺牲程度降低. 因此,本文将精度作为主要的度量指标. 由图4(a)很明显能够看出自编码网络相较于BP网络有很强的鲁棒性,而DBSO-SDAE在加入等级为0～0.3的噪声时精度基本持平,相较于其他自编码网络其变化最缓慢,说明其衰减最慢,对噪声的抵抗能力最强,同时在整个噪声加入的过程中,DBSO-SDAE检测精度最高,也同样验证了其具有最强的鲁棒性.

通过精度的偏离度可以更具说服力地判断4个模型的稳定程度,如表1所示.

表1　4种模型精度偏离度

$Q=0.4$	BP	AE	SAE	DBSO-SDAE
偏离度/%	35.47	5.91	5.24	**4.99**

由表1可知,在噪声等级为0.4时,BP偏离程度达到35.47%,DBSO-SDAE模型偏离度最小,仅有4.99%的数据波动,且在噪声等级为0～0.4之间时DBSO-SDAE模型的偏离度均小于或远小于其他模型. 但如图4(a)所示,在噪声等级为0.4～0.7之间,本文所提模型偏离度与SAE持平或略高于SAE,但其整体检测精度仍远高于其他模型. 其原因在于本文所提模型初始精度远高于SAE,但模型对噪声的抵抗程度是有限度的,当噪声等级大于0.4时,意味着归一化后,在[0,1]的数据集中加入方差大于0.4的噪声,模型均无法从现有数据中获得更有效的信息. 由上述分析可知,DBSO-SDAE模型数据稳定性最高,相对于其他模型有更强的鲁棒性.

利用DBSO-SDAE模型自适应选出的最优参数为隐藏层层数为1层、隐藏层节点数为17个、降噪参数为0.52训练网络,并在测试集KDDtest+上进行测试,得到测试结果如表2所示.

表2　各算法AC值对比

测试集	J48[24]	朴素贝叶斯[24]	NB 树[24]	随机树[24]
test+/%	81.05	76.56	82.02	81.59
测试集	BP	CNN	SSAE	DBSO-SDAE
test+/%	77.92	79.21	78.27	**82.04**

表2列举了不同算法的AC值,与其他算法相比,本文提出的DBSO-SDAE模型有着较高的检测精度.

考虑到检测算法模型对测试阶段的实时性有着较强的需求,加入实时性仿真对比如表3所示.

表3　算法测试时长对比

算法	BP	CNN	DBSO-SDAE
测试时间/s	0.037	0.395	**0.014**

由表3可知,本文提出的模型在测试数据量为22 544时,所需的检测时长仅为0.014 s,与其他模型相比,具有较高的实时性,其原因在于所选出的网络结构简单、参数过少,但尽管网络结构简单,依然拥有较高精度.

综上,由实验分析可得,DBSO-SDAE模型不仅有较优的鲁棒性,还能自适应选择最优网络参数,获得较高的检测精度及较优的实时性.

4　结　论

由于计算与物理过程的深度结合,CPS对传统入侵检测提出了更高的鲁棒性和自适应性的需求. 本文结合CPS自身特点,提出了基于自适应鲁棒性的DBSO-SDAE检测模型. 将稀疏自编码网络加入噪声,通过重构误差的学习方式,使网络能够学习到更具鲁棒性的高层次表示. 并将DBSO与SDAE相结

合,使模型在提高鲁棒性的同时能自适应地根据数据的不同分布特征提取本质特征,获得较好的精度及鲁棒性. 实验表明,该方法具有较强鲁棒性和自适应性,且无论针对已知入侵类型和未知入侵类型,均具有很好的检测性能,从而为CPS的入侵检测提供了一种新的具有较强鲁棒性及自适应性的检测方式.

参考文献(References)

[1] Lee E A. Cyber physical systems: Design challenges[C]. International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC). Orlando: IEEE, 2008: 363-369.

[2] Li Z, Yang C, Su C, et al. Vision-based model predictive control for steering of a nonholonomic mobile robot[J]. IEEE Transactions on Control Systems Technology, 2016, 24(2): 553-564.

[3] Loukas G, Vuong T, Heartfield R, et al. Cloud-based cyber-physical intrusion detection for vehicles using deep learning[J]. IEEE Access, 2018, 6: 3491-3508.

[4] Yang T H, Yang S C, Kao H M, et al. Cyber-physical-system-based smart water system to prevent flood hazards[J]. Smart Water, 2018, 3(1): 1-13.

[5] Wu J, Li Y N, Li S Y. State estimation for distributed cyber-physical power systems under data attacks[J]. Control and Decision, 2016, 31(2): 331-336.

[6] Alpaño P V S, Pedrasa J R I, Atienza R. Multilayer perceptron with binary weights and activations for intrusion detection of cyber-physical systems[C]. TENCON 2017-2017 IEEE Region 10 Conference. Penang: IEEE, 2017: 2159.

[7] Alheeti K M A, Gruebler A, McDonald-Maier K D. An intrusion detection system against malicious attacks on the communication network of driverless cars[C]. 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). Las Vegas: IEEE, 2015: 916-921.

[8] Sun J, Wang X, Xiong N, et al. Learning sparse representation with variational auto-encoder for anomaly detection[J]. IEEE Access, 2018, 6: 33353-33361.

[9] Yan B, Han G. Effective feature extraction via stacked sparse auto-encoders to improve intrusion detection system[J]. IEEE Access, 2018, 6: 41238-41248.

[10] Bengio Y, Lamblin P, Popovici D, et al. Greedy layer-wise training of deep networks[C]. Proceedings of the Twentieth Annual Conference on Neural Information Processing Systems. Vancouver: MIT Press, 2007: 153-160.

[11] Von Lehmen A, Paek E G, Liao P F, et al. Factors influencing learning by backpropagation[C]. IEEE International Conference on Neural Networks. New York: IEEE, 1988: 335-341.

[12] Doi E, Balcan D C, Lewicki M S. Robust coding over noisy overcomplete channels[J]. IEEE Transactions on Image Processing, 2007, 16(2): 442-452.

[13] Vincent P, Larochelle H, Bengio Y, et al. Extracting and composing robust features with denoising autoencoders[C]. Proceedings of the 25th International Conference on Machine Learning. New York: ACM, 2008: 1096-1103.

[14] Huber P J. Robust statistics[M]. Berlin: Springer, 2011: 5-22.

[15] Tan T, Qian Y M, Hu H, et al. Adaptive very deep convolutional residual network for noise robust speech recognition[J]. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 2018, 26(8): 1393-1405.

[16] Gao J Y, Yang X S, Zhang T Z, et al. Robust visual tracking method via deep learning[J]. Chinese Journal of Computers, 2016, 39(7): 1419-1434.

[17] Zeng W H. Deep convolutional neural network for robustness identification of crop leaf diseases[D]. Hefei: School of Information Science and Technology, University of Science and Technology of China, 2018.

[18] Huang L X, Wang Y N, Zhang X Y, et al. Research on noise robustness of speech recognition based on deep auto-encoder neural network[J]. Computer Engineering and Applications, 2017, 53(13): 49-54.

[19] Shi Y H. Brain storm optimization algorithm[C]. Advances in Swarm Intelligence. Heidelberg: Springer, 2011: 303-309.

[20] Zhan Z H, Zhang J, Shi Y H, et al. A modified brain storm optimization[C]. IEEE Congress on Evolutionary Computation. Brisbane: IEEE, 2012: 1-8.

[21] Wu Y L, Jiao S B. Brain storm optimization algorithm theory and application[M]. Beijing: Science Press, 2017: 1-68.

[22] Wu Y L, Fu Y L, Wang X R, et al. Difference brain storm optimization algorithm based on clustering in objective space[J]. Control Theory & Applications, 2017, 34(12): 1583-1593.

[23] Ruan Z, Miao Y, Lei P, et al. Visualization for big data security — A case study on KDD99 cup data set[J]. Digital Communications & Networks, 2017, 3(4): 250-259.

[24] Tavallaee M, Bagheri E, Lu W, et al. A detailed analysis of the KDD CUP 99 data set[C]. 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. Ottawa: IEEE, 2009: 1-6.

作者简介

吴亚丽(1975−), 女, 副教授, 博士, 从事智能优化算法理论及应用、复杂系统建模与优化等研究, E-mail: yliwu@xaut.edu.cn;

李国婷(1994−), 女, 硕士生, 从事深度学习优化算法的研究, E-mail: guotingl@foxmail.com;

付玉龙(1994−), 男, 硕士生, 从事多目标群智能优化算法及其应用的研究, E-mail: yloongf@foxmail.com;

王晓鹏(1995−), 女, 硕士生, 从事资源受限项目调度的研究, E-mail: xiaopengW7394@163.com.

(责任编辑: 闫 妍)