DOI:10. 3969/j. issn. 1674-1951. 2021. 02. 002

基于GRU-CNN的综合能源网络安全攻击检测方法

An intrusion detection method for integrated energy network based on GRU-CNN

吕政权[1],李朝阳[2],王海峰[1],陈怡君[1],彭道刚[2*]
LYU Zhengquan[1], LI Zhaoyang[2], WANG Haifeng[1], CHEN Yijun[1], PENG Daogang[2*]

(1.国网上海市电力公司培训中心,上海 200438; 2.上海电力大学 自动化工程学院,上海 200090)
(1. State Grid Shanghai Electric Power Company Training Center, Shanghai 200438, China; 2. School of Automation Engineering, Shanghai University of Electric Power, Shanghai 200090, China)

摘 要:在电力系统向综合能源转型与网络攻击技术演进的双重影响下,电力信息安全和防护形势日益严峻,网络攻击检测系统有助于发现电力系统薄弱环节。针对传统研究算法改进一味追求更高检测准确率而忽视特征人工提取过程中信息丢失的问题,提出一种基于门控循环神经网络(GRU)和卷积神经网络(CNN)的攻击检测方法。该方法采用GRU提取原始时间序列特征,利用CNN获得多维度特征,然后结合Softmax分类器实现异常流量的映射。采用该检测方法对KDD99数据集和虚假数据注入攻击(FDIAs)2个试验模型进行训练测试,结果表明,相比传统模型,该方法有较好的分类效果和较高的准确率,验证了方法的有效性与实用性。

关键词:综合能源;攻击检测;网络安全;深度学习;循环神经网络;卷积神经网络;云大物移智链
中图分类号:TM 711 **文献标志码**:A **文章编号**:1674-1951(2021)02-0009-06

Abstract: Influenced by the transformation of power system to an integrated energy one and the evolution of network attack technology, power information security and protection is getting mounting challenges. Network intrusion detection system (NIDS) can identify weaknesses in the power system. Pursuing detection accuracy, but neglecting the missing data in manual feature extraction is the problem in the course of improving the traditional algorithm. Thus, an intrusion detection method based on the Gated Recurrent Unit (GRU) and Convolutional Neural Network (CNN) is proposed. The method uses GRU to extract the original time series features, takes CNN to obtain multi-dimensional features, and realizes the mapping of abnormal traffic with Softmax classifier. The method has been practiced in the training of two experimental models, KDD99 data set and False Data Injection Attack (FDIAs). The results show that the method performs better in classification and detection accuracy than the traditional one, which verifies the effectiveness and practicability of the method.

Keywords: integrated energy; intrusion detection; cyber security; deep learning; GRU; CNN; cloud computing, big data, IoT, mobile internet, AI and blockchain

0 引言

近年来,我国光伏、风电、生物质能等新能源发展迅速,承担缓冲器、聚合器、稳定器的多类储能技术也在不断改进,“云大物移智链”的应用逐渐渗透。为构建综合能源系统,打破传统供能单打独斗的固有模式,实现电气热多能系统的协同规划运行,国家电网公司以实现“清洁、科学、高效、节约、经济用能”为宗旨,整合、设计、规划、协调各种能源,方便可再生能源的安全消纳[1-4]。但伴随着信息化和工业化高层次的深度结合以及信息物理系统的高度集成,网络空间形式日益复杂;同时,现场电力终端设备数量庞大,攻击结合特定业务隐藏在正常业务中,安全风险积累后可能造成严重影响,网络信息安全成为整个电力系统安全、稳定、经济运行的重要保证。目前,网络攻击的针对性、持续性、隐蔽性显著增强,各种威胁源相互交织,呈现多元复杂的局面。2019年,电力系统入侵事件层出不穷,如英国制冷控制系统遭扫描攻击、印度核电站内网访问权限遭窃取、乌克兰核电厂信息泄露、委

收稿日期:2020-08-04;**修回日期**:2021-02-02
基金项目:国网上海市电力公司科技项目(52097019001N)

内瑞拉大规模停电以及南非电力公司被勒索病毒袭击等，能源领域面临来自敌对因素、偶然因素、系统结构和环境因素等多方的信息安全威胁[5]。

继“等保2.0”之后，信息安全愈发受到重视，文献[6]指出，当前综合能源主要面临互联系统风险、智能终端风险和无线安全风险。文献[7]将区块链技术与综合能源相结合，针对不同数据节点补充了检测算法。文献[8]指出，综合能源环境下工控系统面临病毒入侵的威胁，对智能设备的大量应用和通信协议的开放网络表示担忧，对信息质量和时效性给予更高期待。传统的攻击检测按照检测原理和入侵属性不同，分为根据计算机资源情况的异常检测和已知系统弱点攻击模式的误用检测。较多学者针对不同攻击方式研究了相关算法，解滨等[9]提出了一种基于K-means聚类的攻击检测算法，通过调整距离阈值α实现对聚类个数k的动态优化，一定限度提高了检测率。肖琦等[10]建立了随机森林模型作为灰盒算法，对CTU-13数据集中的僵尸网络流量进行检测。Li等[11]引入深度学习算法卷积神经网络（CNN）训练NSL-KDD数据集的41维特征，经过独热编码后转换为图像。但这些方法存在以下问题：泛化性能不佳，只针对特定攻击种类[12]；数据集标签类型有限，影响模型学习效果[13]；浅层学习不能满足数据集动态增长的精度要求等[14]：因此，有必要提出相适应的网络攻击检测方法。

本文提出一种基于门控循环卷积神经网络的综合能源攻击检测模型。通过分析KDD99数据集的4类攻击样本，采集接入分布式电源和电动汽车的假数据注入攻击节点测试系统信号，进行数据采集和特征提取，利用门控循环单元（GRU）和CNN兼顾时间序列的序列与多维特性，用逻辑回归模型进行攻击类别映射分类，以实现综合能源环境下高效准确的网络攻击检测。

1 GRU-CNN混合网络攻击检测模型

1.1 相关理论

随着综合能源的发展，节点结构、连接特征、内容特征、基于时间与主机的流量特征等高维多标签样本被引入，基于先验知识选取局部特征进而提高检测准确率的方法已不适应综合能源场景下的网络安全防护工作，但实时的海量数据契合深度学习算法的特点。门控循环单元是循环神经网络的变体之一，它通过可以学习的门来控制信息流动，更好地捕捉时间序列中时间步长较大的依赖关系[15]，不同于长短期记忆网络的是，GRU具有更为合理的结构、参数与收敛性，因此该方法近年来在学术界广泛应用，特别是应用于自然语言处理方向。它优化了循环神经网络中隐藏状态的计算方式，其中重置门可以用来丢弃与预测无关的历史信息，更新门可以控制隐藏状态如何被候选隐藏状态所更新。本文采用GRU提取综合能源系统的数据特征，引入重置门R_t和更新门Z_t的概念，具体公式如下

$$R_t = \sigma(X_t W_{xr} + H_{t-1} W_{hr} + b_r), \tag{1}$$

$$Z_t = \sigma(X_t W_{xz} + H_{t-1} W_{hz} + b_z), \tag{2}$$

$$\tilde{H}_t = \tanh(X_t W_{xh} + (R_t \odot H_{t-1}) W_{hh} + b_h), \tag{3}$$

$$H_t = Z_t \odot H_{t-1} + (1 - z_t) \odot \tilde{H}_t, \tag{4}$$

式中：t为时间步长；W_{xr}，W_{hr}，W_{xr}，W_{hz}，W_{xh}，W_{hh}为权重参数；b_r，b_z，b_h为偏差参数，皆由训练获得；$\sigma()$为Sigmoid激活函数，将元素值域变换到[0,1]；⊙表示做元素乘法；R_t和Z_t的输入为当前时间步输入X_t与上一隐藏状态H_{t-1}；H_t为隐藏状态；$\tilde{H}_t$为候选隐藏状态。

GRU的输出H_t作为CNN的数据输入，CNN网络依次通过2次卷积、池化进行多维度特征提取，最终实现综合能源系统遭受网络攻击与否的检测，卷积神经网络如图1所示。

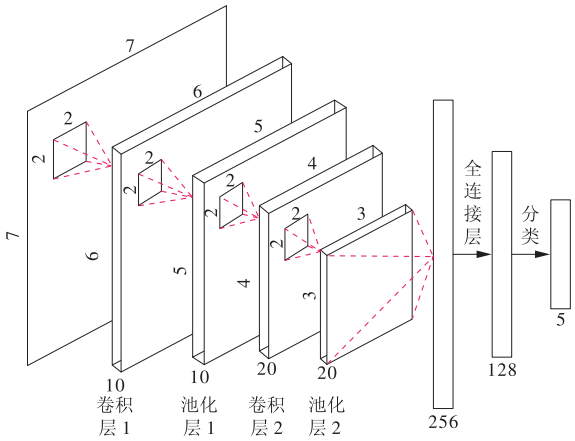

图1 卷积神经网络

Fig. 1 Convolutional neural network

从图1不难看出，卷积层块里的基本单位是卷积层后接最大池化层，在经过多轮处理之后由全连接层进行分类[16]。卷积层用来识别图像里的空间模式，池化层则用来降低卷积层对位置的敏感性，全连接层又叫输出层，起到特征分类器的作用。卷积过程和全连接层标签概率分布公式如下[17]

$$A_{i,j} = f\left(\sum_{m=0}\sum_{n=0} w_{m,n} H_{ti+m,j+n} + b\right), \tag{5}$$

$$S(\tilde{y} = p|x) = softmax(y_p) = \frac{\exp(y_p)}{\sum_{p=1}^{q} y_p}, \tag{6}$$

式中：$A_{i,j}$为卷积层输出；$w_{m,n}$为卷积核矩阵的第m行第n列元素；$H_{ti+m,j+n}$为卷积输入矩阵的第$(i+m)$行第$(j+n)$列元素；b为偏置；f为Relu激活函数；S为后验

概率；x 为全连接层输入；y_p 为输出类别，包含 q 个元素的全连接层输出。

1.2　GRU-CNN模型构建

为保证输出的确定性，本文采用Z-score法对原始时间序列数据进行标准化处理，对于缺失的特征以该特征的均值替代，标准化后的数据 Z 作为GRU模型的输入

$$Z = \frac{x - \mu}{\sigma}, \tag{7}$$

式中：μ 为该特征在整个数据集上的均值；σ 为标准差。

本文提出的模型结合深度学习中循环神经网络较强的记忆性和卷积神经网络较强的特征表达能力，设计并实现了基于GRU-CNN的信息安全攻击检测模型，其网络结构如图2所示。充分考虑综合能源模型数据，将单个传输控制协议（TCP）连接的基本特征、连接内容特征、流量特征、有功无功潮流信息等标准化后的输出作为模型的输入，经GRU提取序列特征后通过2层卷积层（Conv2D）、2层池化层（AvgPool2D）、2层全连接层（Dense）和2层丢弃层（Dropout），获得多维度特征并实现异常流量的映射，确定综合能源网络攻击类型归属。

为解决费时及容易过拟合的问题，本文加入丢弃层，以削弱神经元节点间的联合适应性。在训练阶段随机选取某些元素权值为0，将其从网络中丢弃，增强泛化能力。此外，本文采用Adam算法[18]优化训练效率，结合动量变量和RMSProp算法，为梯度设定相应的学习率。

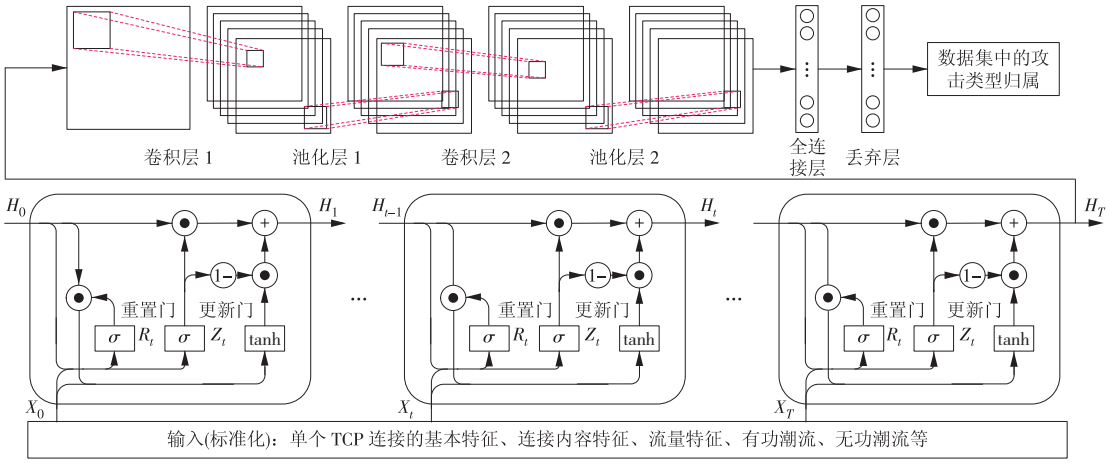

图2　GRU-CNN模型网络结构

Fig. 2　Framework of the GRU-CNN model

2　试验设计

2.1　KDD99数据集

KDD99数据集广泛用于检测评估，作为入侵检测的行业基准，它模拟网络环境中的拒绝服务（DoS）、远程主机未授权访问（R2L）、未授权的本地超级用户特权访问（U2R）和端口扫描（Probing）共4大类39种攻击方式。为方便研究，本文随机抽样数据包中10%的数据贴以异常（attack）标签，正常数据贴以（normal）标签（完整样本分布见表1）；为验证攻击检测模型的有效性和泛化性，训练集中出现22种攻击方式，测试集包含17种未知方式。

数据集中的单个连接由41个特征来描述，其中包括了9种离散类型：协议类型protocol_type；网络服务类型service；连接状态flag；连接主机/端口是否相同land；登录是否成功logged_in；超级用户权限root_shell，su_attempted，is_hot_login，is_guest_login。为方便数据处理，本文将各离散状态字符用数值替代，如TCP、用户数据报协议（UDP）、控制报文协议（ICMP）3种协议类型用数字0，1，2替代。

表1　数据集样本分布

Tab. 1　Data set sample distribution

攻击类别	标签	训练集样本数	测试集样本数
Normal	normal	97 278	60 593
Probing	Ipsweep，mscan，nmap，portsweep，saint，satan	1 247	306
DoS	apache2，back，land，mailbomb，neptune，pod，processtable，smurf，teardrop，udpstorm	391 458	229 853
U2R	buffer_overflow，httptunnel，loadmodule，perl，ps，rootkit，sqlattack，xterm	52	228
R2L	ftp_write，guess_passwd，imap，multihop，named，phf，sendmail，snmpgetattack，snmpguess，spy，warezclient，warezmaster，worm，xlock，xsnoop	1 126	16 189

2.2 虚假数据注入攻击(FDIAs)节点测试系统

为更好地体现综合能源的主题,应对分布式发电、新能源汽车等接入综合能源系统的现状,文献[19]在IEEE 33标准节点系统的基础上做出了修改,模拟FDIAs并检测算法的适用性。如图3所示,分别在节点6引入光伏电源(PV),节点18引入微型燃气轮机(MT),节点22引入电动汽车(EV),节点33引入风力发电机(WT),配置信息见文献[20]。

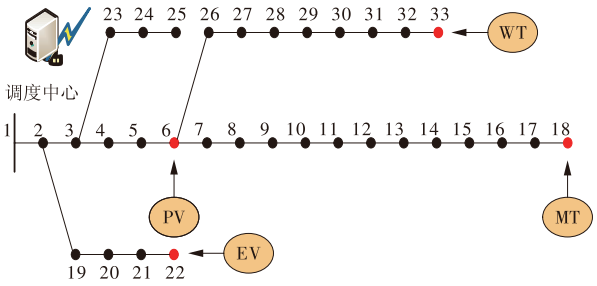

图3 33节点测试系统

Fig. 3 33 nodes in the test system

虚假数据注入攻击作为新兴攻击,一般指攻击者根据电力系统拓扑图操纵量测装置,绕过数据检测集即最大标准化残差,致使电力系统进行错误状态估计的攻击方式[21]。注入向量$\boldsymbol{a}=[a_1,a_2,\cdots,a_m]^{\mathrm{T}}$,状态变量误差向量$\boldsymbol{c}=[c_1,c_2,\cdots,c_n]^{\mathrm{T}}$,不可观察的虚假数据注入攻击用下式表示

$$\|\boldsymbol{r}_{\mathrm{a}}\|=\|\boldsymbol{z}_{\mathrm{a}}-\boldsymbol{H}\boldsymbol{x}_{\mathrm{a}}\|=\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\boldsymbol{x}+\boldsymbol{c})\|, \tag{8}$$

当且仅当$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$时,下式成立

$$\|\boldsymbol{r}_{\mathrm{a}}\|=\|\boldsymbol{z}_{\mathrm{a}}-\boldsymbol{H}\boldsymbol{x}_{\mathrm{a}}\|=\|\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\|<\tau, \tag{9}$$

式中:$\boldsymbol{r}_{\mathrm{a}}$为残差;$\boldsymbol{x}_{\mathrm{a}}$为虚假数据注入后的状态估计量;$\boldsymbol{z}$为量测向量;$\boldsymbol{z}_{\mathrm{a}}$为实际量测向量,$\boldsymbol{z}_{\mathrm{a}}=\boldsymbol{z}+\boldsymbol{a}$;$\boldsymbol{x}$为状态向量;$\boldsymbol{H}$为雅可比量测矩阵;$\tau$为最大标准化残差阈值。

本文虚假数据的注入方式为添加符合正态分布的噪声,考虑攻击者可能采取不同的攻击强度,本文进行了多组对比试验,延用文献[16]对攻击强度影响因素的理解,认为试验主要受到攻击强度和虚假数据概率密度的影响。攻击强度用方差σ^2表示,设置σ^2=5.00,σ^2=0.50,σ^2=0.05共3组强度(分别代表较大、中等及较小强度)进行对比试验;另外,虚假数据注入的概率密度取值范围为0.05~1.00,间隔为0.05。

3 试验结果分析

采用KDD99数据集与小型综合能源系统测试节点作为2组测试环节,利用多语言、可跨平台的图形处理器(GPU)版MXNet搭建试验模型,并使了Intel Core i5-9300H @ 2.4 GHz处理器,搭配NVIDIA GeForce GTX 1660 Ti 6 GB显卡运行所有的试验,试验流程如图4所示。试验1将预测数据与传统的几种机器学习模型进行比较,试验2分别测试模型在3种攻击强度下的概率密度分布。

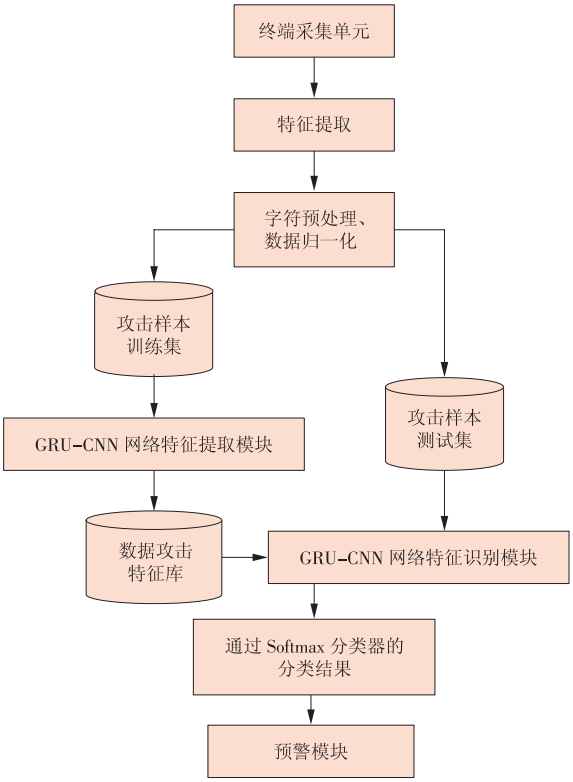

图4 试验流程

Fig. 4 Test procedure

3.1 试验1

KDD99模型的正确率将从准确率(A)、召回率(R)和误报率(F)3个方向进行说明,变量定义如下:真正例P_{t}表示检测出正常标签normal;真反例N_{t}表示检测出具体异常标签;伪正例P_{f}和伪反例N_{f}分别表示错误检测正常与异常样本,计算公式及检测结果如下。

$$A=\frac{P_{\mathrm{t}}+N_{\mathrm{t}}}{P_{\mathrm{t}}+N_{\mathrm{f}}+P_{\mathrm{t}}+N_{\mathrm{t}}}, \tag{10}$$

$$R=\frac{P_{\mathrm{t}}}{P_{\mathrm{t}}+N_{\mathrm{f}}}, \tag{11}$$

$$F=\frac{P_{\mathrm{f}}}{P_{\mathrm{f}}+N_{\mathrm{t}}}。 \tag{12}$$

将本文的GRU-CNN攻击检测系统与原始GRU,CNN模型及文献[12]给出的几种传统模型检测结果进行对比,结果见表2。由表2可见:本文模型在准确率和误报率方面显著优于其他模型,优越性明显;即使R方面和其他模型大致相同,但整体上看,GRU-CNN的深度学习模型不失为一种良好的攻击检测算法;由于4种攻击类型在数据集中的量级不同,限制了小数量级攻击类型的检测识别,这也是准确率不容易继续提高的主要原因。

表2　试验结果对比

Tab. 2　Comparation of test results　%

模型	*A*	*R*	*F*
GRU-CNN	92.18	71.81	0.42
GRU	82.11	53.44	9.54
CNN	84.03	60.62	11.23
SVM	77.36	62.77	7.32
DT	80.33	71.66	8.22
ANN	81.40	69.99	3.23
ELM	84.29	77.18	6.30

3.2　试验2

采用修改后的小型综合能源系统节点进行测试，图5为低、中、高攻击强度下准确率与概率密度的关系。由图5可以清楚地发现：攻击强度越高，攻击特征越明显，在同一概率密度下的准确率起始值越高（图中为92.5%，93.6%，95.8%）；随着概率密度的增大，均能实现99.0%左右高准确率的收敛，且收敛速度随着攻击强度的提高而加快。

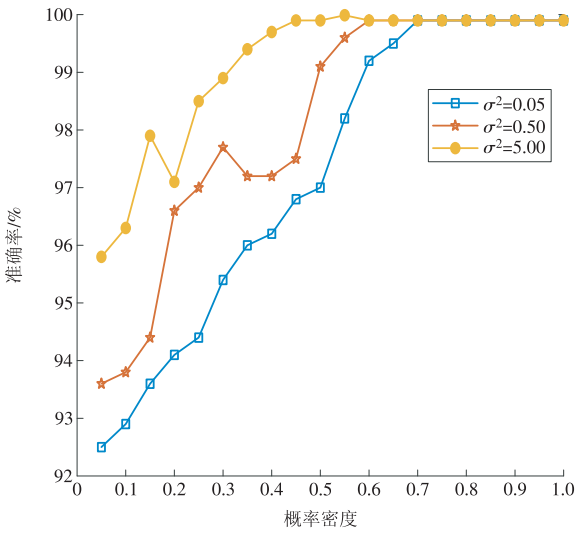

图5　各攻击强度下准确率与概率密度的关系

Fig. 5　Relationship between accuracy rates and probability densities under various attack intensities

4　结束语

为了解决电力综合能源系统信息安全问题，本文提出一种基于GRU-CNN的综合能源系统攻击检测模型，通过KDD99异常流量数据集和小型综合能源节点测试系统虚假数据注入攻击2个试验可以看出，GRU-CNN攻击检测模型在综合能源系统网络攻击检测中具有一定的有效性。相比于其他传统方法，采用GRU和CNN分别提取时间序列特性和多维度特性作为表征，有效提升了攻击检测的准确率。此外，如何检测拥有不同量级标签的数据集、如何检测更高维度多节点测试系统以及在真实综合能源系统应用是下一步研究的重点。

参考文献：

[1]葛少云，曹雨晨，刘洪，等.考虑可靠性约束的综合能源微网供能能力评估[J].电力系统自动化，2020，44(7)：31-41.
GE Shaoyun，CAO Yuchen，LIU Hong，et al. Evaluation of energy supply capability for multi-energy microgrid considering reliability constraint[J]. Automation of Electric Power Systems，2020，44(7)：31-41.

[2]孙浩，陈永华.综合能源系统多能流联合仿真技术研究[J].华电技术，2020，42(5)：66-72.
SUN Hao，CHEN Yonghua. Research on multiple energy flow co-simulation technology applied integrated energy system[J]. Huadian Technology，2020，42(5)：66-72.

[3]杨晓巳，陶新磊.综合能源技术路线研究[J].华电技术，2019，41(11)：22-25.
YANG Xiaosi，TAO Xinlei. Research on integrated energy technical route [J]. Huadian Technology，2019，41(11)：22-25.

[4]王珺，顾伟，张成龙，等.智能社区综合能源优化管理研究[J].电力系统保护与控制，2017，45(1)：89-97.
WANG Jun，GU Wei，ZHANG Chenglong，et al. Research on integrated energy management for smart community[J]. Power System Protection and Control，2017，45(1)：89-97.

[5]肖建荣.工业控制系统信息安全[M].北京：电子工业出版社，2015.

[6]YANG Y，WU F，LIU Y. Remote access：A residental power monitor and control system [J]. IEEE Potentials，2015，34(4)：18-23.

[7]郭鹤旋.区块链在能源互联网安全机制上的应用研究[D].保定：华北电力大学，2019.

[8]李存斌，李小鹏，田世明，等.能源互联网电力信息深度融合风险传递：挑战与展望[J].电力系统自动化，2017，41(11)：17-25.
LI Cunbin，LI Xiaopeng，TIAN Shiming，et al. Challenges and prospects of risk transmission in deep fusion of electric power and information for energy internet[J]. Automation of Electric Power Systems，2017，41(11)：17-25.

[9]解滨，董新玉，梁皓伟.基于三支动态阈值K-means聚类的入侵检测算法[J].郑州大学学报(理学版)，2020，52(2)：64-70.
XIE Bin，DONG Xinyu，LIANG Haowei. An algorithm of intrusion detection based on three-way dynamic threshold K-means clustering [J]. Journal of Zhengzhou University (Natural Science Edition)，2020，52(2)：64-70.

[10]肖琦，苏开宇.基于随机森林的僵尸网络流量检测[J].微电子学与计算机，2019，36(3)：43-47.
XIAO Qi，SU Kaiyu. Botnet traffic detection based on

random forest algorithm[J]. Microelectronics & Computer, 2019,36(3):43-47.

[11]LI Zhipeng, QIN Zheng, HUANG Kai, et al. Intrusion detection using convolutional neural networks for representation learning[C]// International Conference on Neural Information Processing. Heidelberg: Springer, 2017: 858-866.

[12]滕少华,陈成,霍颖翔.小样本纠错的多层入侵检测分类研究[J].广东工业大学学报, 2020,37(3):9-16.
TENG Shaohua, CHEN Cheng, HUO Yingxiang. A multi-fold self correction small-sample classifier for intrusion detection [J]. Journal of Guangdong University of Technology, 2020,37(3):9-16.

[13]王蓉,马春光,武朋.基于联邦学习和卷积神经网络的入侵检测方法[J].信息网络安全, 2020,20(4):47-54.
WANG Rong, MA Chunguang, WU Peng. An intrusion detection method based on federated learning and convolutional neural network[J]. Netinfo Security, 2020, 20 (4):47-54.

[14]冯文英,郭晓博,何原野,等.基于前馈神经网络的入侵检测模型[J].信息网络安全, 2019,12(9):101-105.
FENG Wenying, GUO Xiaobo, HE Yuanye, et al. Intrusion detection model based on feedforward neural network[J]. Netinfo Security, 2019,12(9):101-105.

[15]阿斯顿 张,李沐,扎卡里,等.动手学深度学习[M].北京:人民邮电出版社,2019.

[16]李元诚,曾婧.基于改进卷积神经网络的电网假数据注入攻击检测方法[J].电力系统自动化, 2019,43(20): 97-104.
LI Yuancheng, ZENG Jing. Improved convolutional neural based detection method for false data injection attack[J]. Automation of Electric Power Systems, 2019, 43 (20): 97-104.

[17]何彦,凌俊杰,王禹林,等.基于长短时记忆卷积神经网络的刀具磨损在线监测模型[J].中国机械工程,2020, 31(16):1959-1967.
HE Yan, LING Junjie, WANG Yulin, et al. In-process tool wear monitoring model based on LSTM-CNN[J]. China Mechanical Engineering,2020,31(16):1959-1967.

[18]何梦乙,覃仁超,刘建兰,等.基于Adam-BNDNN的网络入侵检测模型[J].计算机测量与控制,2020,28(2): 58-62.
HE Mengyi, QIN Renchao, LIU Jianlan, et al. Network intrusion detection model based on Adam-BNDNN [J]. Computer Measurement & Control,2020,28(2): 58-62.

[19]孙江山,刘敏,邓磊,等.基于自适应无迹卡尔曼滤波的配电网状态估计[J].电力系统保护与控制, 2018,46 (11):1-7.
SUN Jiangshan, LIU Min, DENG Lei, et al. State estimation of distribution network based on AUKF [J]. Power System Protection and Control, 2018,46(11):1-7.

[20]潘正宁.含分布式发电和储能装置的三相潮流算法[D].南京:东南大学, 2014.

[21]陈碧云,李弘斌,李滨.伪量测建模与AUKF在配电网虚假数据注入攻击辨识中的应用[J].电网技术, 2019,43 (9):3226-3236.
CHEN Biyun, LI Hongbin, LI Bin. Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network [J]. Power System Technology, 2019,43(9):3226-3236.

(本文责编:刘芳)

作者简介:

吕政权(1985—),男,上海人,高级工程师,硕士,从事电力安全演练策划组织工作(E-mail:lvzhengq@163.com)。

彭道刚*(1977—),男,上海人,教授,博士,从事智能发电、综合智慧能源与能源互联网等研究(E-mail: pengdaogang@126.com)。