Journal of Electric Power Science and Technology

Volume 36 | Issue 5 Article 5

11-16-2021

Research on network security situation awareness of intelligent distribution transformer terminal unit based on RBF-SVM

Haitao Wu
Shenzhen Power Supply Bureau Co., Ltd.,Shenzhen 518010 ,China

Shanglin Dai
Shenzhen Power Supply Bureau Co., Ltd.,Shenzhen 518010 ,China

Zhongwei Qiao
Shenzhen Power Supply Bureau Co., Ltd.,Shenzhen 518010 ,China

Haolan Liang
School of Electrical and Information Engineering,Changsha University of Science and Technology,Changsha 410114 ,China

Xiangjun Zeng
School of Electrical and Information Engineering,Changsha University of Science and Technology,Changsha 410114 ,China

See next page for additional authors

Research on network security situation awareness of intelligent distribution transformer terminal unit based on RBF-SVM

Authors

Haitao Wu, Shanglin Dai, Zhongwei Qiao, Haolan Liang, Xiangjun Zeng, and Dongqi Liu

基于 RBF-SVM 智能配变终端的网络安全态势评估

吴海涛[1],代尚林[1],乔中伟[1],梁皓澜[2],曾祥君[2],刘东奇[2]

(1.深圳供电局有限公司,广东 深圳 518010;2.长沙理工大学电气与信息工程学院,湖南 长沙 410114)

摘　要:面向台区部署的智能配变终端受自身漏洞及通信网络脆弱性等多方面的影响,易受到网络攻击。针对智能配变终端存在的安全问题,提出一种基于 RBF－SVM 智能配变终端网络安全态势评估方法。首先,分析该终端可能遭受的网络攻击,提取相应的安全检测指标,并将检测指标数据归一化处理;然后构建基于高斯(RBF)核函数的非线性支持向量机(SVM)分类器,采用 k 折交叉验证与网格搜索法确定该分类器的最优参数 C 和 g,建立智能配变终端安全态势评估模型;最后将检测指标数据样本代入模型中进行训练和测试。结果表明所提方法与随机森林和逻辑回归等方法相比较,具有更高的准确率,可实现终端安全态势评估,对电力终端安全防护具有一定的实用价值。

关　键　词:智能配变终端;安全态势;SVM;RBF;随机森林

DOI:10.19781/j.issn.1673-9140.2021.05.005　　**中图分类号**:TM77　　**文章编号**:1673-9140(2021)05-0035-06

Research on network security situation awareness of intelligent distribution transformer terminal unit based on RBF-SVM

WU Haotao[1],DAI Shanglin[1],QIAO Zhongwei[1],LIANG Haolan[2],ZENG Xiangjun[2],LIU Dongqi[2]

(1. Shenzhen Power Supply Bureau Co., Ltd.,Shenzhen 518010,China;2. School of Electrical and Information Engineering, Changsha University of Science and Technology,Changsha 410114,China)

Abstract:Due to its own vulnerabilities and the vulnerability of the communication network, the intelligent distribution transformer terminal deployed for the station area is vulnerable to network attacks. For solving the security problems existing in the intelligent distribution transformer terminal, this paper proposes an intelligent distribution transformer terminal network security situation awareness method based on RBF-SVM. Firstly, the potential network attack that the terminal may suffer is analyzed, the corresponding security detection indicators areextracted and normalized. Then, a nonlinear support vector machine (SVM) classifier based on the Gaussian (RBF) kernel function is conducted. The k-fold cross-validation and grid search method is applied for determining the optimal parameters of C and g for the classifier, and the Security Situation Awareness model of the intelligent distribution transformer terminal is established. Finally, the test index data are substituted into the model for training and testing. The results show that compared with s random forest and logistic regression methods, the proposed method has a higher accuracy rate, can realize terminal security situation awareness, and canbe used for practical power terminal security protection.

Key words:intelligent distribution transformer terminal unit;security situation awareness;SVM;RBF;random forest

收稿日期:2020-08-16;**修回日期**:2021-01-01

基金项目:国家重点研发计划(2018YFB0904900,2018YFB0904903)

通信作者:梁皓澜(1993-),女,博士研究生,主要从事电力系统网络安全、电力系统保护与控制研究;E-mail:2631650704@qq.com

随着能源互联网的推进,配电网逐步向信息化、智能化的配电物联网方向发展。面向台区部署的智能配电变压器终端作为配电物联网的基础元件和核心设备,其应用是推动配电网向能源互联网转型发展的关键环节[1]。

为满足能源物联网中智能配电网的功能需求,智能配电终端进行升级改造,成为边缘架构下配电网中的"边"和"端"融合体,其不仅具备对低压设备信息采集和边缘计算的功能,而且能够根据台区监测到的数据进行保护控制。它是推动整个配电网实现设备互联、信息互联和能源互联的关键节点[1]。

随着配电物联网的不断推进,大量智能终端设备以及多元用户接入电网,电网逐步形成了开放互动网络环境,导致电力终端安全防护受到巨大的挑战。开放环境下多元电力终端用户供需互动用电,即将超越现有电网纵向加密、横向隔离的分级分区信息安全防护格局,一旦威胁侵入、吸附于终端设备,突破边界防护,就畅通无阻,易引发重大电网安全事故。如 2015 年乌克兰遭受黑客利用电力终端为攻击跳板攻击电力控制系统,导致大规模停电,严重影响当地人民的日常生活[2-3]。智能配变终端作为终端设备及多元用户接入电网的第一道门户,易遭受网络攻击,其安全性直接关系到电网的安全稳定运行。因此,研究智能配变终端的网络安全态势评估的意义重大。

在网络安全态势评估研究方面,文献[4]首次提出网络安全态势的理论;文献[5]研究了网络安全态势评估模型;文献[6]将网络安全态势评估应用到电力信息系统中,依据评估框架和在线评估算法,构建了电力信息系统安全态势在线评估系统;文献[7]提出了一种应用到智能电网中的广域感知模型;文献[8]将网络安全态势感知应用到配电网,提出了一种基于同步相量测量装置的配电网安全态势感知方法。上述文献在网络安全态势感知理论、模型及其在电力领域的应用方面做了大量研究,但是对于配电物联网中具有边缘计算功能的智能配变终端的网络安全态势评估,仍缺乏直接的指导意义。

针对智能配变终端自身系统漏洞及其脆弱性易遭受网络攻击的问题,该文首先提出一种基于径向基函数—支持向量机(radial basis function-support vector machine,RBF-SVM)智能配变终端网络安全态势评估方法;然后,通过提取智能配变终端安全检测指标,选取 SVM 机器学习算法搭建智能配变终端安全态势感知模型,实现对智能配变终端网络安全态势的评估;最后,利用 python[9] 编写算例对所提方法进行测试和比较,验证其有效性。

1 面向台区的智能配变终端

1.1 智能配变终端的概念及功能

智能配变终端,即智能化配电变压器监测终端(distribution transformer supervisory terminal unit,TTU),安装于柱上变压器台区,具备对配电变压器 0.4 kV 低压设备实现电能分配、电能计量、无功补偿以及供用电信息的自动测量、采集、保护、监控及安全防护等功能[10]。

TTU 是实现低压配电自动化、用户用电采集、各类新型业务的边缘融合与云边协同的关键边缘节点,以"硬件平台化、软件 APP 化"为理念,基于 Linux 操作系统,应用分布式边缘计算、容器等技术,实现业务 APP 同硬件及操作系统的解耦应用;通过云端协同满足台区基础运行信息监测分析、台区需求侧管理、低压配网运维管控、信息模型标准化、主站终端协同控制等要求。智能配变终端架构如图 1 所示。

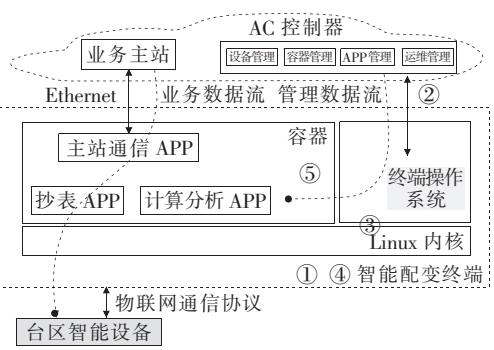

图 1 智能配变终端架构

Figure 1 The architecture of intelligent distribution transformer terminal unit

1.2　智能配变终端可能遭受的网络攻击

智能配变终端因自身操作系统的漏洞和外部通信协议的脆弱性，容易遭受网络攻击，根据攻击检测的数据源，智能配变终端可能遭受的网络攻击如下[11-12]。

1)资源耗尽攻击。攻击者利用智能配变终端通信协议缺陷，发送大量伪造的 TCP 连接请求，使终端 CPU 满负荷运行以及导致终端系统内存不足，资源耗尽，致使终端系统瘫痪，服务暂停。

2)泛洪(Flooding)攻击。攻击者向智能终端系统发出大量的报文和制造大量的通信数据流量，耗尽终端 IP 资源，导致其无法向其他终端设备提供正常服务。

3)暴力破解。攻击者利用密码字典，使用穷举法尝试可能的账号名和密码组合，直到试验出正确的密码。

4)权限漏洞。攻击者有可能利用智能配变终端里的权限漏洞获取管理员权限，进而向连接在网络的其他终端发布虚假和恶意的信息，攻击更多节点。

5)恶意代码攻击。攻击者通过物理接触的方式向终端植入恶意控制程序，如果获得成功，它就可以进入管理系统控制整个设施，威胁电网安全。

2　基于 RBF-SVM 的终端安全风险评估模型

该文通过提取智能配变终端的网络安全检测指标数据样本，基于 RBF-SVM 构建智能配变终端安全态势评估模型来实现对配变终端设备的网络安全态势感知。

2.1　智能配变终端信息安全评估指标提取

为了应对网络攻击，智能配变终端必须具备妥当的安全机制来保护设备的核心功能不受侵害。利用终端正常运行时和存在恶意行为运行时捕获的流量数据、终端监测系统监测自身的资源的内存占有率、安全认证访问次数、看门狗定时器定时报警次数以及 CPU 功耗等指标数据，综合评估智能配变终端是否存在异常。配变终端安全检测指标详情如表 1 所示。

表 1　配变终端安全检测指标

Table 1　Details of Security detection indexes for TTU

检测类型	描述	指标	数据
访问核验	监视终端系统是否出现未通过安全认证的越权访问	访问校验错误次数	系统登录以来未通过安全认证的越权访问累计次数
网络报文流量监视	监视 TTU 通信接口的网络报文流量	网络报文 20 s 峰值流量	统计接口的 20 s 数据流量的累计峰值
系统资源使用监视	判断系统是否遭到资源耗尽攻击，监视 CPU 负荷情况与系统内存使用情况	5 min CPU 负载率平均值和 CPU 内存占用率	统计 5 min CPU 负载率平均值和 CPU 内存占用率平均值
看门狗定时器监视	监视终端内部硬件或者软件错误，预设一个时间值，当预期任务没有完成，看门狗定时器就会到时，并发出信号	看门狗定时器报警次数	上电以来看门狗定时器报警累计次数
CPU 功耗监视	在终端的电源部分外接采样电阻采集终端的功耗信息(采样电阻电压)，监视 CPU 模块运行时是否出现恶意代码攻击	以 250 KSa/s 的采样速率采集终端设备 CPU 模块运行时产生的能耗数据，每 5 s CPU 模块运行产生的功耗	统计 5 s CPU 模块运行的功耗平均值

2.2　SVM 分类器

SVM 是机器学习中的一种有监督学习模型[13-14]，可用于分类问题和回归分析。在得到智能配变终端安全检测指标后，将其指标进行数据统计作为输入特征，进而构建分类器，找到最优参数，进行测试与验证。

假设给定一个特征空间 R^n 上的训练数据集，即

$$T=\{(\boldsymbol{x}_1,y_1),(\boldsymbol{x}_2,y_2),\cdots,(\boldsymbol{x}_i,y_i)\},\quad i=1,2,\cdots,N \tag{1}$$

式中　$\boldsymbol{x}_i$ 为特征向量，$\boldsymbol{x}_i\in R^n$；y_i 为 $\boldsymbol{x}_i$ 的类别标签，$y_i\in\{+1,-1\}$。

若存在超平面能够对训练数据集线性可分，即

$$\boldsymbol{w}\cdot\boldsymbol{x}+b=0 \tag{2}$$

$$y_i(\boldsymbol{w}\cdot\boldsymbol{x}_i+b)\geqslant 1,i=1,2,\cdots,N \tag{3}$$

式(2)、(3)中　$\boldsymbol{w}$ 为超平面的法向量；b 为位移项。

对训练集数据进行训练，求出最大间隔分离的超平面 $\boldsymbol{w}$ 和 b 的最优解，即

$$\begin{cases}\min\limits_{w,b} & \dfrac{1}{2}\|\boldsymbol{w}\|^2\\ \text{s.t} & y_i(\boldsymbol{w}\cdot\boldsymbol{x}_i+b)\geqslant 1,i=1,2,\cdots,N\end{cases} \tag{4}$$

分类决策函数为

$$f(\boldsymbol{x})=\mathrm{sign}(\boldsymbol{w}\cdot\boldsymbol{x}+b) \tag{5}$$

然而,智能配变终端的训练数据并非线性可分,为了解决这个问题,对每个样本点 $(\boldsymbol{x}_i,y_i)$ 引进一个松弛变量 $\varepsilon_i\geqslant 0$ 和惩罚 $C>0$,将其转化为凸二次规划问题,即

$$\begin{cases}\min\limits_{w,b}\ \dfrac{1}{2}\|\boldsymbol{w}\|^2+C\sum\limits_{i=1}^{N}\varepsilon_i\\ \text{s.t}\ y_i(\boldsymbol{w}\cdot\boldsymbol{x}_i+b)\geqslant 1-\varepsilon_i\\ \quad\varepsilon_i\geqslant 0,i=1,2,\cdots,N\end{cases} \tag{6}$$

将此问题通过对偶算法求最优解,对式(6)中每一个不等式约束引进拉格朗日乘子 α_i、μ_i,最优化问题式(6)的拉格朗日函数为

$$L(\boldsymbol{w},b,\varepsilon,\alpha,\mu)=\frac{1}{2}\|\boldsymbol{w}\|^2+C\sum_{i=1}^{N}\varepsilon_i-\sum_{i=1}^{N}\alpha_i(y_i(\boldsymbol{w}\cdot\boldsymbol{x}_i+b)-1+\varepsilon_i)-\sum_{i=1}^{N}\mu_i\varepsilon_i \tag{7}$$

其中,$\alpha_i\geqslant 0$,$\mu_i\geqslant 0$。

最优化问题式(6)的对偶问题为

$$\begin{cases}\min\limits_{w,b,\varepsilon}\ \dfrac{1}{2}\sum\limits_{i=1}^{N}\sum\limits_{j=1}^{N}\alpha_i\alpha_j y_i y_j(x_i\cdot x_j)-\sum\limits_{i=1}^{N}\alpha_i\\ \text{s.t}\ \sum\limits_{i=1}^{N}\alpha_i y_i=0\\ \quad 0\leqslant\alpha_i\leqslant C,i=1,2,\cdots,N\end{cases} \tag{8}$$

当所构建的分类平面为非线性超平面时,需要使用一个变换将原空间数据映射到新空间,所以将对偶问题目标函数式(8)中的内积 $\boldsymbol{x}_i\times\boldsymbol{x}_j$,用核函数 $K(\boldsymbol{x}_i\times\boldsymbol{x}_j)=\phi(\boldsymbol{x}_i)\phi(\boldsymbol{x}_j)$ 来代替。此时对偶问题的目标函数为

$$\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_i\alpha_j y_i y_j(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)-\sum_{i=1}^{N}\alpha_i \tag{9}$$

其中,核函数选择高斯(RBF)核,即

$$K(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)=\exp\left(-\frac{\|\boldsymbol{x}_i-\boldsymbol{x}_j\|}{2\sigma^2}\right) \tag{10}$$

最终的分类决策函数为

$$f(x)=\mathrm{sign}\left(\sum_{i=1}^{N}\alpha_i^* y_j K(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)+b^*\right) \tag{11}$$

式中 α_i^*、b^* 均为对偶问题的解。

由于 SVM 分类器使用的核函数为高斯核函数,分类效果受到 C 和高斯核半径 g 的影响,因此模型训练阶段需要对参数进行寻优。该文采用带交叉验证[15]与网格搜索法[16]对 C 和 g 进行优化选择。

2.3 智能配变终端信息安全风险评估模型

智能配变终端网络安全态势评估模型搭建步骤如下。

1)选取某智能配变终端进行模拟攻击,根据表 1 所列的安全检测指标提取数据样本。

2)对智能配变终端安全检测指标数据进行归一化处理,使所有特征都位于同一量级来消除其对分类模型的影响[17]。

3)采用交叉验证和网格搜索法对 C 和 g 进行最优选择,搜索范围为[10^{-3},10^{-4}]两两进行组合,并用交叉验证的平均正确率对所选择的超参数的泛化能力进行评估,选择使得交叉验证的平均正确率最高的 C 和 g 作为 SVM 分类器的超参数。

4)构建智能配变终端的网络安全态势评估模型,对测试数据进行分析,测试该模型的准确率。最后选择一组数据样本,进行安全态势评估。

3 模型仿真与分析

为了量化实验结果,作出以下定义。

1)以智能配变终端系统正常运行时,提取到的检测指标数据为正样本,用 P 表示,即标记不存在安全风险的正类别为 1;以智能配变终端系统掺杂人为攻击运行时,提取到的检测指标数据为负样本,用 N 表示,即标记存在安全风险的负类别为 0。

2)以掺杂人为攻击时,检测到的指标数据判定为正样本的数目,用 F_{P}(假正例)表示;以未遭受网络攻击的系统正常运行时,获取的检测数据判定为正样本的数量,用 T_{P}(真正例)表示。

3)以掺杂人为攻击时,检测到的指标数据判定为负样本的数目,用 T_{N}(真反例)表示;以未遭受网络攻击的系统正常运行时,获取的检测数据判定为负样本的数量,用 F_{N}(假反例)表示。

因此,可获得 4 个评价指标,分别为精准率、召回率、准确率、综合评价指标,即

$$p_{\mathrm{recision}}=\frac{T_{\mathrm{P}}}{T_{\mathrm{P}}+F_{\mathrm{P}}} \tag{12}$$

$$R_{\mathrm{ecall}}=\frac{T_{\mathrm{P}}}{T_{\mathrm{P}}+F_{\mathrm{N}}} \tag{13}$$

$$A_{\mathrm{ccuracy}}=\frac{T_{\mathrm{P}}+T_{\mathrm{N}}}{T_{\mathrm{P}}+T_{\mathrm{N}}+F_{\mathrm{P}}+F_{\mathrm{N}}} \tag{14}$$

$$F_1 = \frac{2P_R}{P+R} \tag{15}$$

真正类率(true positive rate，TPR)，敏感度，即分类器所识别出的正实例占所有正实例的比例，其计算形式为

$$T_{PR} = \frac{T_P}{T_P + F_N} \tag{16}$$

假正类率(false positive rate，FPR)，特异度，即分类器错认为正类的负实例占所有负实例的比例，其计算形式为

$$F_{PR} = \frac{F_P}{T_P + F_N} \tag{17}$$

该文利用 python 编写采用交叉验证和网格搜索法对 SVM 分类器参数寻优，构建 SVM 分类器，将样本数据进行训练仿真分析，得到的结果如图 2 所示。当 C 和 g 分别取 1 和 0.1 时，交叉验证的平均正确率最高达到 91.11%。

对 C 和 g 进行优化选择后，构建 SVM 智能配变终端安全态势评估模型，同时将该文选取的 SVM 与随机森林、逻辑回归算法[13-14]进行比较，ROC 曲线结果如图 3～5 所示。可得出该文采用的算法的测试集与训练集的敏感度(红色线)明显比其他 2 种算法高。3 种算法的评价指标比较结果如表 3 所示。

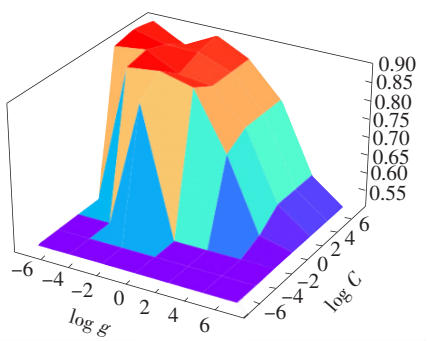

图 2　交叉验证网格搜索参数优化

Figure 2　Cross-validation grid search parameters Optimization

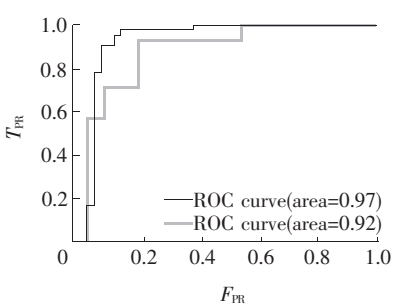

图 3　ROC 曲线(RBF-SVM)

Figure 3　ROC curve (RBF-SVM)

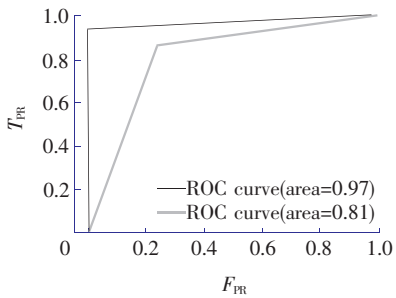

图 4　ROC 曲线(随机森林)

Figure 4　ROC curve (random forest)

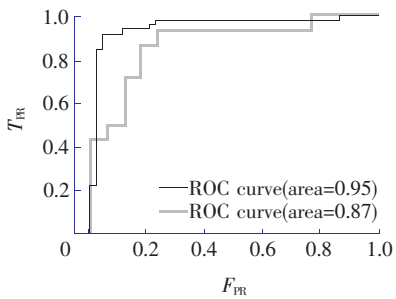

图 5　ROC 曲线(逻辑回归)

Figure 5　ROC curve (logistic regression)

表 3　3 种算法的评价指标比较结果

Table 3　Evaluation indicatorscomparison of three algorithms

算法	$A_{ccuracy}$	$P_{recision}$	R_{ecall}	F_1	AUC
SVM	0.839	0.800	0.857	0.828	0.916
DT[11]	0.806	0.750	0.857	0.800	0.811
LR	0.774	0.769	0.714	0.741	0.874

由表 3 可知，该文选取的 SVM 算法的准确率、精准率等 4 个评价指标都优于其他 2 种算法。由此可知，该文应用的方法可实现对终端异常情况和安全态势进行识别与评估。

选取一组新增数据样本[A：20，B：30，C：45%，D：34%，E：30，F：0.007 01]代入该文基于 RBF-SVM 构建的安全态势评估模型中进行评估，该数据通过模型得到的输出结果为 0，即可判断配变终端不存在安全风险。

4　结语

针对面向配电台区部署的智能配变终端可能遭受的网络攻击，首先提出了一种基于 RBF-SVM 的智能配变终端网络安全态势评估方法，利用交叉验证和网格搜索法寻找 SVM 分类器的最优参数；然后构建智能配变终端网络安全评估模型；最后将该

文采取的方法与随机森林、逻辑回归 2 种算法进行比较，所提的方法优于其他 2 种算法，即表明该方法能够有效评估终端是否存在网络安全风险，对电力系统终端信息安全防护具有一定的借鉴价值。后续可在终端安全检测指标和数据样本特征提取方面进行完善和补充，并开展进一步的研究。

参考文献：

[1] 张冀川，陈蕾，张明宇，等. 配电物联网智能终端的概念及应用[J]. 高电压技术，2019，45(6)：1729-1736.
ZHANG Jichuan，CHEN Lei，ZHANG Mingyu，et al. Conception and application of smart terminal for distribution internet of things[J]. High Voltage Engineering，2019，45(6)：1729-1736.

[2] 李中伟，佟为明，金显吉，等. 智能电网信息安全防御体系与信息安全测试系统构建 乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化，2016，40(8)：147-151.
LI Zhongwei，TONG Weiming，JIN Xianji，et al. Construction of cyber security defense hierarchy and cyber security testing system of smart grid：thinking and enlightenment for network attack event to national grid of ukraine and israel[J]. Automation of Electric Power Systems，2016，40(8)：147-151.

[3] 梅生伟，王莹莹，陈来军. 从复杂网络视角评述智能电网信息安全研究现状及若干展望[J]. 高电压技术，2011，37(3)：672-679.
MEI Shengwei，WANG Yingying，CHEN Laijun. Overviews and prospects of the cyber security of smart grid from the view of complex networks theory[J]. High Voltage Engineering，2011，37(3)：672-679.

[4] Bass T，Gruber D. A glimpse into the future of ID[J]. USENIX & SAGE，1999，24：40-45.

[5] Bass T. Intrusion detection systems and multisensor data fusio：creating cybersapce situational awareness[J]. Communications of the ACM，2000，43(4)：99-105.

[6] 镐俊杰，王丹，杨东海. 电力信息系统网络安全态势在线评估框架与算法研究[J]. 电力系统保护与控制，2013，41(9)：116-120.
HAO Junjie，WANG Dan，YANG Donghai. Research of security situation online-assessing framework and algorithm in electric power information system[J]. Power System Protection and Control，2013，41(9)：116-120.

[7] Alcaraz C，Lopez J. Wasam：a dynamic wide-area situational awareness model for critical domains in smart grids[J]. Future Generation Computer Systems，2014，30：146-154.

[8] 田书欣，李昆鹏，魏书荣，等. 基于同步相量测量装置的配电网安全态势感知方法[J]. 中国电机工程学报，2021，41(2)：617-632.
TIAN Shuxin，LI Kunpeng，WEI Shurong，et al. Security situation awareness approach for distribution network based on synchronous phasor measurement unit[J]. Proceedings of the CSEE，2021，41(2)：617-632.

[9] Severance C. Guido van rossum：the modern era of python[J]. Computer，2015，48(3)：8-10.

[10] 王程斯. 基于 ARM 的电网智能配变终端设计研究[J]. 电网与清洁能源，2021，37(1)：54-61.
WANG Chengsi. Design and research of smart distribution and transformation terminal based on ARM[J]. Power System and Clean Energy，2021，37(1)：54-61.

[11] 刘东奇，曾祥君，王耀南. 基于信息熵的智能配电变压器终端安全态势评估[J]. 南方电网技术，2020，14(1)：18-23.
LIU Dongqi，ZENG Xiangjun，WANG Yaonan. Security situation assessment of intelligent distribution transformer terminal unit based on information entropy[J]. Southern Power System Technology，2020，14(1)：18-23.

[12] 王宇，李俊娥，周亮，等. 针对嵌入式终端安全威胁的电力工控系统自愈体系[J]. 电网技术，2020，44(9)：3582-3594.
WANG Yu，LI June，ZHOU Liang，et al. A self-healing architecture for power industrial control systems against security threats to embedded terminals[J]. Power System Technology，2020，44(9)：3582-3594.

[13] 李航. 统计学习方法：第 2 版[M]. 北京：清华大学出版社，2019：112-141.

[14] Cortes C，Vapnik V. Support vector networks[J]. Machine learning，1995，20(3)：273-297.

[15] Kennedy J，Eberhart R. Particle swarm optimization[C]//International Conference on Neural Networks，Perth，Australia：IEEE，1995.

[16] 王健峰，张磊，陈国兴，等. 基于改进的网格搜索法的 SVM 参数优化[J]. 应用科技，2012，39(3)：28-31.
WANG Jianfeng，ZHANG Lei，CHEN Guoxing，et al. A parameter optimization method for an SVM based on improved grid search algorithm[J]. Applied Science and Technology，2012，39(3)：28-31.

[17] 肖汉光，蔡从中. 特征向量的归一化比较性研究[J]. 计算机工程与应用，2009，45(22)：117-119.
XIAO Hanguang，CAI Congzhong. Comparison study of normalization of feature vector[J]. Computer Engineering and Applications，2009，45(22)：117-119.