DOI:10.20033/j.1003-7241.(2025)01-0097-04.

电力工控网络0day漏洞风险自动识别技术

胡朝辉[1,2]，陈善锋[1]，杨逸岳[1]

（1.南方电网数字电网研究院股份有限公司，广东 广州 510080；
2.华南理工大学 电子与信息学院，广东 广州 510641）

摘 要：为了准确识别漏洞风险，提出一种电力工控网络0day漏洞风险自动识别方法。将电力工控网络根据需求转换为二维数据，经过归一化处理获取灰度矩阵，采用二维小波阈值去噪方法对数据去噪处理。将常规序列特征提取规则作为基本单元，采用特征提取方法提取电力工控网络0day漏洞风险特征，构建特征集合，将集合中的全部数据映射到二维平面上，通过维诺图区分数据，实现电力工控网络0day漏洞风险自动识别。实验结果表明，所提方法可以有效提升漏洞风险自动识别结果的准确性，同时还能够有效缩短识别时间。

关键词：电力工控网络；0day；漏洞风险；自动识别
中图分类号：TP393 文献标识码：A 文章编号：1003-7241(2025)01-0097-04

Automatic Identification Technology for 0day Vulnerability Risk in Power Industrial Control Network

HU Zhao-hui[1,2], CHEN Shan-feng[1], YANG Yi-yue[1]

(1. Digital Grid Research Institute, China Southern Power Grid, Guangzhou 510080 China;
2. South China University of Technology, School of Electronic and Information Engineering, Guangzhou 510641 China)

Abstract: In order to accurately identify vulnerability risks, an automatic identification method for 0day vulnerability risks in power industry control networks is proposed. It converts the power industry control network into two-dimensional data according to requirements, obtains the grayscale matrix through normalization processing, and uses two-dimensional wavelet threshold denoising method to denoise the data. Using conventional sequence feature extraction rules as the basic unit, feature extraction methods are used to extract the 0day vulnerability risk features of the power industry control network, and a feature set is constructed. All data in the set is mapped onto a two-dimensional plane, and data is distinguished through a Vinot map to achieve automatic identification of 0day vulnerability risk in the power industry control network. The experimental results show that the proposed method can effectively improve the accuracy of vulnerability risk automatic identification results, while also effectively reducing identification time.

Keywords: power industrial control network; 0day; vulnerability risk; automatic recognition

0 引言

工业控制系统是电力以及交通领域基础建设的重要组成部分，同时也是促进经济发展的重要条件。互联网技术的飞速发展，使其和电力工控系统之间联系更加密切，在有效推动电力企业发展的同时，也带来了一系列安全隐患。电力工控系统作为关乎我国民计民生的重要基础设施[1-2]，一直以来都是网络安全攻击的重点目标。

和传统电网相比，智能电网信息安全的复杂程度更高一些，同时具有比较复杂的接口以及不同的通信方式。由于网络的机型以及设备不同，所以采用统一的连接方式也具有一定的难度。尤其是智能电网信息安全具有传统互联网以及电网工控系统双重威胁的特点，所以展开电力工控网络漏洞风险识别具有十分重要的意义。国内相关专家也展开了大量研究，获取了比较满意的研究成果，例如杨至元等人[3]主要通过Cyber-net算法完成网络风险识别。梁海镇等人[4]主要通过最大流最大分割定理实现电网静态安全关键断面识别。邓松等人[5]主要通过函数挖掘获取系统数据的风险特征，同时借助混合GEP完成风险安全识别。在以上几种识别方法的基础上，提出一种电力工控网络0day漏洞风险自动识别方法。经实验测试结果表明，所提方法不仅可以有效降低识别时间，同时还能够获取更加满意的识别结果。

收稿日期：2023-07-03

1 风险自动识别方法

1.1 电力工控网络数据去噪

小波阈值去噪的主要目的是针对含有噪声的数据展开小波变换处理，同时将其分解为多个不同的层，进而获取对应的小波系数，将小波系数阈值处理，获取全新的小波系数；对最新获取的小波系数展开重构，进而获取重构后的数据，即为去噪处理之后的数据。现阶段，小波变换的阈值去噪方法现阶段存在以下两个方面的问题，分别为阈值的确定以及阈值函数的选取。

阈值的选取会直接对去噪结果产生影响，假设阈值的取值比较小，则数据中的小波系数和细节信息会更多地被保留，但是在数据中存在的噪声也会相应增加；反之，假设选择的阈值比较小，则数据中保留的噪声就会相对较少，但是数据中一些有利用价值的信息也将会被删除。所以，确定阈值的取值范围具有十分重要的意义。

针对其他阈值选择方法而言，通过固定阈值门限准则可以更快更简单地获取阈值，同时还能够获取比较满意的去噪效果，具体计算公式如下：

$$H=\sigma\sqrt{\log_2 N} \tag{1}$$

式中，H代表阈值；σ代表噪声标准；N代表电力工控网络数据的规模。

σ的取值可以采用分解处理之后的高频系数绝对值中值展开估计，详细的计算式如下：

$$\sigma=\frac{\left|\tilde{\omega}_{i,j}\right|}{0.6745} \tag{2}$$

式中，$\tilde{\omega}_{i,j}$代表最新的小波系数。

分析现阶段已有阈值函数，通过其特性可以划分为两种不同的类型，分别为：

（1）硬阈值函数

硬阈值函数需要将全部不低于设定阈值的小波系数保留下来，而剩余部分的取值则全部设置为0，对应的数学公式为：

$$\tilde{\omega}_{i,j}=\begin{cases}\omega_{i,j},\left|\omega_{i,j}\right|\geq H\\0,\omega_{i,j}<H\end{cases} \tag{3}$$

（2）软阈值函数

软阈值准则就是将小波系数中低于阈值的系数取值全部设定为0，剩余部分则是减去阈值本身，对应的数学表达式为：

$$\tilde{\omega}_{i,j}=\begin{cases}\operatorname{sgn}\left(\omega_{i,j}\right)\left(\left|\omega_{i,j}\right|-H\right),\left|\omega_{i,j}\right|\geq H\\0,\omega_{i,j}<H\end{cases} \tag{4}$$

但是经过分析发现，软硬阈值函数存在明显的不足，同时还会导致计算结果存在偏差。为了有效解决上述问题，以下主要使用软硬阈值函数的加权平均阈值函数，具体表达式如下：

$$\tilde{\omega}_{i,j}=\begin{cases}(1-\beta)\omega_{i,j}+\beta\operatorname{sgn}\left(\omega_{i,j}\right)\left(\left|\omega_{i,j}\right|-H\right),\left|\omega_{i,j}\right|\geq H\\0,\omega_{i,j}<H\end{cases} \tag{5}$$

$$\beta=\frac{H}{\left|\omega_{i,j}\right|}\exp\left(-\frac{\left|\omega_{i,j}\right|-H}{\left|\omega_{i,j}\right|+H}\right) \tag{6}$$

式中，β代表加权因子。

通过分析以上公式可知，全新的阈值函数不但具有连续性，同时更加适用于电力工控网络数据去噪处理。

以下主要通过二维小波阈值去噪方法对电力工控网络数据展开去噪处理[6-7]，详细的操作流程如下所示：

（1）设定电力工控网络样本数据，同时经过转换使其成为全新的二维数据集。

（2）对二维数据集中的全部数据归一化处理，进而获取如式(7)所示的二维灰度矩阵数据$B_{m,n}$：

$$B_{m,n}=\begin{bmatrix}b_{1,1},b_{1,2},b_{1,3},\cdots,b_{1,n}\\b_{2,1},b_{2,2},b_{2,3},\cdots,b_{2,n}\\b_{3,1},b_{3,2},b_{3,3},\cdots,b_{3,n}\\\vdots\quad\quad\vdots\\b_{m,1},b_{m,2},b_{m,3},\cdots,b_{m,n}\end{bmatrix} \tag{7}$$

式中，$b_{m,n}$代表二维灰度矩阵数中的元素。

（3）对二维数据集中的数据展开小波分解处理，同时为原始含有噪声的电力工控网络数据选择最佳小波基，同时展开多层分解处理，进而获取一组小波系数。

（4）完成步骤(3)后，阈值处理全新的小波系数，同时确定阈值的取值范围，对其展开半软阈值函数处理，进而获取如公式(8)所示的估计系数$N_{x,y}$：

$$N_{x,y}=\frac{\left|\tilde{\omega}_{i,j}\right|}{(\sigma\cdot\beta)\times B_{m,n}} \tag{8}$$

（5）通过二维小波对电力工控网络数据展开重构处理，同时采用小波系数展开小波重构处理，获取重构处理之后的电力工控网络数据。

（6）对重构处理之后的数据展开反归一化处理，进而获取去噪后的电力工控网络数据$f_{(i,j)}$，如式(9)所示：

$$f_{(i,j)}=\frac{\left|\tilde{\omega}_{i,j}\right|\cdot\sum_{H=2}B_{m,n}}{\operatorname{sgn}\left(\omega_{i,j}\right)\cdot N_{x,y}} \tag{9}$$

1.2 电力工控网络0day漏洞风险自动识别

根据时间序列可以详细记录某个目标对象的变化规律，同时形成不同的关系序列，将其全部集合在一起，即可构建时间序列。在时间序列分析方法中，比较常用的方法就是时间序列分解法(STL)，根据时间序列的组成绘制阈值对应的预测曲线，最终达到数据预测分析的目的。

STL算法具有操作简单以及鲁棒性强等优势，更加适合对规律性比较强的时间序列展开回归分析。通过现有的时间序列分析方法以及思想，构建一种特征提取模型[8]，具体如图1所示。

特征序列存在的主要意义就是为了完成特征提取，同时借助规则方法完成数据的空间转换，构建全新的特

征序列，使其可以获取更加满意的特征提取结果。

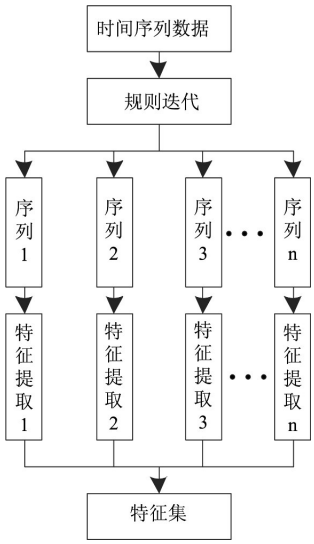


图1 特征提取模型

特征提取是为了获取时间序列中相对完整且规则的序列，进而提取对应的特征。在实际操作过程中，可以序列作为研究对象展开具体的分析和研究。针对现阶段比较单一的特征序列而言，需要分别统计不同类型的特征[9-10]。同时将各个类型的特征全部封装处理，使其成为相对较小的模块，然后对其融合处理，最终构建一个相对完整的特征，方便后续的使用以及分析。

电力工控网络数据是比较典型的一维时间序列 $X_{m,n}$，对应的表达形式为：

$$X_{m,n}=\begin{bmatrix} x_{1,1},x_{1,2},x_{1,3},\cdots,x_{1,n} \\ x_{2,1},x_{2,2},x_{2,3},\cdots,x_{2,n} \\ x_{3,1},x_{3,2},x_{3,3},\cdots,x_{3,n} \\ \vdots \quad\quad \vdots \\ x_{m,1},x_{m,2},x_{m,3},\cdots,x_{m,n} \end{bmatrix} \tag{10}$$

将时间序列划分为 k 段，则对应的表达形式为：

$$X_{STL}=\left\{x_{m,n}\left|\left(t_i,v_i\right)\right|\times x_{kl}\right\} \tag{11}$$

式中，X_{PLR} 代表时间的划分结果；t_i 代表采样时间；v_i 代表直线的左端值；x_{kl} 代表电力工控网络数据属性集。

通过上述分析，采用STL算法提取电力工控网络0day漏洞风险特征，详细的操作步骤为：

(1) 在设定时间序列中抓取电力工控网络0day漏洞风险特征点，获取重要特征点[11-12]；

(2) 经过对比分析，将无利用价值的特征点删除，构建全新的序列，同时对新序列重新编号处理，采用特征将原序列采用分段线性的方式描述；

(3) 通过STL方法将时间序列实行线性分段处理，同时将其转换为二维平面上的点，为后续电力工控网络0day漏洞风险自动识别提供简单且精确的数据源。

通过维诺图，以此为依据区分数据，达到电力工控网络0day漏洞风险自动识别的目的，详细的操作流程如图2所示。

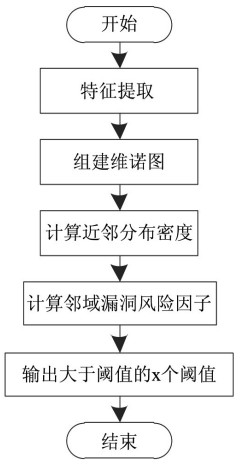


图2 电力工控网络0day漏洞风险自动识别流程图

通过构建的维诺图依次计算近邻分布密度 V_{pi} 以及邻域漏洞风险因子 U_{pi}，如公式(12)所示：

$$\begin{cases} V_{pi}=\dfrac{x_{m,n}\left|\left(t_i\left|v_i\right.\right)\right.}{\mathrm{sgn}\left(\omega_{i,j}\right)\cdot N_{x,y}} \\ U_{pi}=\dfrac{B_{m,n}\times\beta\,\mathrm{sgn}\left(\omega_{i,j}\right)}{N_{x,y}} \end{cases} \tag{12}$$

将计算结果按照从小到大的顺序排列，输出最终取值大于阈值的取值，即为最终的电力工控网络0day漏洞风险自动识别结果。

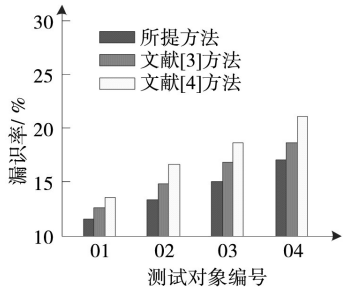
2 实验结果与分析

为了验证所提电力工控网络0day漏洞风险自动识别方法的有效性，选取小型电力工况网络作为研究对象。

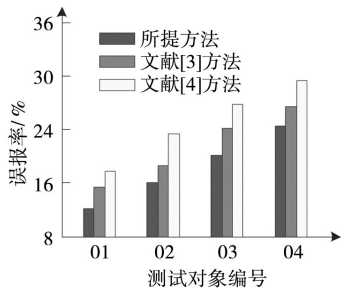
表1 不同方法的电力工控网络0day漏洞风险自动识别失误次数对比结果分析

测试样本数量/个	电力工控网络0day漏洞风险自动识别失误次数/次		
	所提方法	文献[3]方法	文献[4]方法
100	5	8	10
150	8	13	16
200	11	15	17
250	13	18	21
300	16	22	24
350	20	24	27
400	23	26	30
450	26	31	35
500	30	35	38
550	34	37	41
600	37	42	45
650	41	45	48
700	45	48	52
750	50	55	58
800	56	60	64

为了验证识别结果的有效性，实验主要选取电力工控网络 0day 漏洞风险自动识别失误次数、误报率、漏识率作为测试指标，详细的实验测试结果表 1 和图 3 所示。



(a) 不同方法的漏识率测试结果对比



(b) 不同方法的误报率测试结果对比

图 3 不同方法的电力工控网络 0day 漏洞风险自动识别结果测试对比

由表 1 和图 3 中的实验数据可知，三种测试指标均是衡量识别结果准确性的，三项测试指标的取值越低，则说明识别结果越准确。经过具体对比分析可知，所提方法的电力工控网络 0day 漏洞风险自动识别失误次数、漏识率以及误报率明显更低一些，充分证明所提方法可以获取比较满意的识别结果。

为了测试所提方法的识别效率，选取识别时间作为测试结果，详细的实验测试结果如图 4 所示。

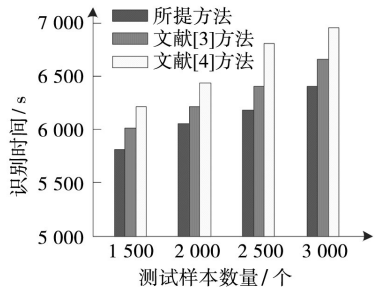


图 4 不同方法的电力工控网络 0day 漏洞风险自动识别时间测试结果对比

分析图 4 中的实验数据可知，各个方法的电力工控网络 0day 漏洞风险自动识别时间会随着测试样本数量的增加呈现上升趋势，但是与另外两种方法相比，所提方法的上升趋势相对平缓一些，且识别时间明显更低一些，充分说明所提方法可以以更快的速度完成识别。

3 结束语

随着信息技术的飞速发展使其在各个领域都得到了十分广泛的应用，尤其是电力工控系统中更是占据十分重要的地位。有效促进电力企业的发展和进步，随之而来的安全问题也成为关注的热点内容。提出一种电力工控网络 0day 漏洞风险自动识别方法。经实验测试结果表明，所提方法可以有效降低识别时间，同时还能够准确识别漏洞风险确保电力工控网络的稳定运行。但是所提方法还有很多需要解决的问题，后续将对其展开更加深入的研究，使其可以得到更加广泛的应用。

参考文献：

[1] 赵悦琪，赵德政，林浩，等．工业控制系统安全防护体系研究[J]．电子技术应用，2021，47(1)：69－72，77．

[2] 汪祖民，田纪宇，王宝凤．改进天牛须搜索算法的工控系统入侵检测[J]．计算机工程与设计，2021，42(8)：2108－2114．

[3] 杨至元，张仕鹏，孙浩，等．基于 Cyber－net 与学习算法的变电站网络威胁风险评估[J]．电力系统自动化，2020，44(24)：19－27．

[4] 梁海镇，陈丽丹，李峰，等．基于最大流最小割的电网静态安全关键断面辨识方法[J]．电网技术，2022，46(3)：1084－1092．

[5] 邓松，蔡清媛，高昆仑，等．基于函数挖掘的能源信息物理系统数据安全风险识别算法[J]．中国电力，2021，54(3)：23－30，37．

[6] 李志军，张鸿鹏，王亚楠，等．排列熵—CEEMD 分解下的新型小波阈值去噪谐波检测方法[J]．电机与控制学报，2020，24(12)：120－129．

[7] 赵永梅．VMD 和小波阈值重构的电力电缆局部放电信号去噪法[J]．西安科技大学学报，2021，41(4)：739－746．

[8] 陈继明，许辰航，李鹏，等．基于时频分析与分形理论的 GIS 局部放电模式识别特征提取方法[J]．高电压技术，2021，47(1)：287－295．

[9] 韦恒，黄超，杨彦，等．基于数据挖掘技术的电网设备参数风险识别方法研究[J]．自动化技术与应用，2022，41(2)：47－50，97．

[10] 白冰．GABP 神经网络算法模型在计算机网络安全评估的应用研究[J]．自动化技术与应用，2022，41(1)：83－86．

[11] 陶耀东，贾新桐，吴云坤．一种工业控制系统漏洞风险评估方法[J]．小型微型计算机系统，2020，41(3)：603－609．

[12] 叶子维，郭渊博，琚安康．动静态特征结合的漏洞风险评估及缓解方法[J]．计算机应用研究，2020，37(4)：1161－1165．

作者简介：胡朝辉(1986－)，男，研究生，高级工程师，研究方向：网络安全。