doi: 10.7690/bgzdh.2026.05.008

基于改进 D-S 的电力监控网络复合攻击活动检测方法

谢志奇，曾体健，张玉吉
（贵州乌江水电开发有限责任公司，贵阳 550002）

摘要：为解决以往电力监控网络复合攻击活动检测方法存在检测准确度不高的问题，提出基于改进 D-S 的电力监控网络复合攻击活动检测方法。对原始数据进行归一化计算和降噪处理，利用改进 D-S 理论，从数据的原始特征中提取更为精准和重要的特征并分类，构建网络攻击数据检测模型，通过计算输入数据的当前状态，对电力监控网络复合攻击活动检测方法进行设计。实验结果表明：与以往的电力监控网络复合攻击活动检测方法相比，所提检测方法在不同网络攻击数据集中的平均误码率仅为 3.2%，检测准确度更高。

关键词：改进 D-S；电力监控网络；网络攻击活动；检测方法；方法设计
中图分类号：TP309.2　　**文献标志码：**A

Compound Attack Activity Detection Method For Electric Power Monitoring Network Based on Improved D-S

Xie Zhiqi, Zeng Tijian, Zhang Yuji
(*Guizhou Wujiang Hydropower Development Co*., *Ltd*., *Guiyang* 550002, China)

Abstract: In order to solve the problem of low detection accuracy in the previous detection methods of compound attack activities in power monitoring network, a detection method of compound attack activities in power monitoring network based on improved D-S is proposed. The original data is normalized and denoised, and the improved D-S theory is used to extract more accurate and important features from the original features of the data and classify them, and then the network attack data detection model is constructed. By calculating the current state of the input data, the power monitoring network compound attack activity detection method is designed. The experimental results show that compared with the previous detection methods, the average bit error rate of the proposed detection method is only 3.2% in different network attack data sets, and the detection accuracy is higher.

Keywords: improved D-S; power monitoring network; network attack activity; detection method; method design

0　引言

电力监控网络能够实时反映当前状态下电力系统的运行状态，实时监控电网中电力的传输和分配。随着网络技术的快速发展，电力监控网络在实际应用中存在很大的网络安全威胁，不仅会影响到电力系统的正常供电，而且会降低电力系统运行的效率和可靠性，给电网企业带来极大的经济损失[1]。此外，电力系统的网络攻击会对兵工领域造成威胁，一定程度上影响军事设施和武器系统的正常运行。针对上述问题，许多学者将各种新兴技术引入了电力监控网络攻击检测方法。

文献[2]提出基于机器学习技术的电力监控网络复合攻击活动检测方法，利用机器学习提取网络攻击数据的特征，利用焦点损失构建网络攻击检测模型的损失函数，提高数据的分类能力，减小数据处理压力，完成网络攻击检测，但该方法的检测精度不高。文献[3]提出基于深度学习的电力监控网络符合攻击活动检测方法，在深度学习的支持下，降低电力数据的维度，保持数据的均衡性，利用潮流传输作为指标，构建电力网络攻击检测模型，实现电力网络攻击数据的检测，但该方法的数据分类精度不高。文献[4]提出基于人工智能技术的电力监控网络复合攻击活动检测方法，利用人工智能技术，实现电力监控数据的高精度分类，对传感器中注入的虚假数据进行准确识别，利用生成的区间残差数值作为检测网络攻击的重要手段，但该方法检测时间过长。

在以往研究的基础上，笔者设计了基于改进 D-S 的电力监控网络复合攻击活动检测方法。通过对电力监控网络数据的预处理，利用改进 D-S 提取相关的数据特征，最终实现电力监控网络攻击活动的检测。

收稿日期：2024-12-08；**修回日期：**2025-01-09
基金项目：乌江公司项目(JG0120210125)
第一作者：谢志奇(1979—)，男，湖北人。

1　电力监控网络复合攻击活动检测方法设计

1.1　电力监控网络攻击数据预处理

现有的网络攻击数据种类繁多，且大部分网络攻击数据均存在冗余数据和噪声数据[5]。这些垃圾数据的存在，会影响到网络攻击检测方法对网络攻击数据的分类精度，从而影响最终的检测结果[6]；因此，主要从数据的归一化和降噪 2 方面进行处理。其中，归一化是数据处理的基本操作，能够提高数据检测的精度[7]。同时，由于电力数据中经常存在无穷大等非数值数据，因此，在进行归一化处理时，还要进行数据的填充。其具体的处理过程为：

$$\left.\begin{aligned} X&=(x-\mu)/\sigma \\ X_1&=\frac{\sum\log|k_i|}{N_{k_i}}\left[1-\kappa\Gamma\left(\sum k_i/N_{k_i}\right)\right] \end{aligned}\right\}。\tag{1}$$

式中：X 为归一化后的数据值；x 为需要进行预处理的数据；μ 为预处理数据的均值；σ 为预处理数据的标准差；X_1 为数据的填充结果；k_i 为第 i 个电力监控网络攻击数据；N_{k_i} 为在第 i 个电力监控网络攻击数据的第 k 个特征属性，$N_{k_i}=Xk_i$；κ为数据的填充系数；$\Gamma(\ )$为归一化数值整合值。通过上述计算，完成数据的归一化处理。网络攻击数据的噪声问题会直接影响到数据特征提取的精度[8]。在进行噪声处理时，可以将噪声数据视为异常数值对其进行处理。其具体处理过程如图 1 所示。

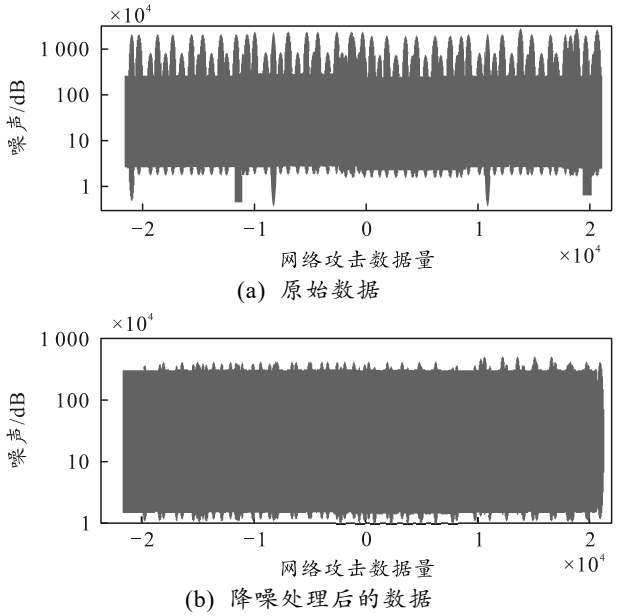

图 1　网络攻击数据的降噪处理

从图 1 可以看出：经过噪声处理后的数据峰值变小，且稳定性变得更强，具有很强的抗干扰性。对于类型不同的数据，降噪效果也会存在些许不同，数据之间存在的特征也会有明显区别。通过上述对网络攻击数据的归一化计算和噪声处理，降低了网络攻击数据中无效数据的存在，为后续网络攻击数据的特征提取提供了方便[9]。同时，将网络攻击数据进行预处理，能够降低数据计算的压力，提高数据特征提取的精度[10]。至此，电力监控网络攻击数据的预处理完成。

1.2　基于改进 D-S 的数据特征提取

完成网络攻击数据的预处理后，需要对数据进行特征提取。在进行特征提取时，为了能够通过原始数据获得更加灵活的特征信息，提高检测精度[11]，采用改进 D-S 理论，进行网络攻击数据的特征提取。其中，改进 D-S 理论在特征提取中的应用结构如图 2 所示。

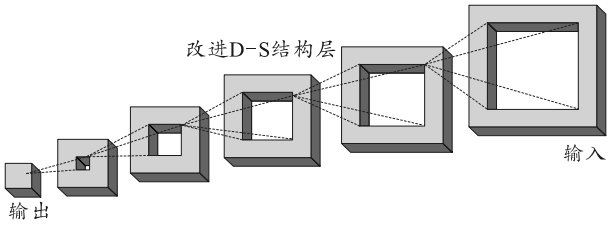

图 2　改进 D-S 理论应用结构

图 2 中，将预处理后的数据输入到上述结构中，输入数据会在改进 D-S 理论中被多次调整。在上述结构中设置一个初始参数，再根据每次输出的结果进行不断调整，并缩小特征提取的范围，直到输出最为准确的特征提取结果[12]。同时，在改进 D-S 理论中，多层结构的融合增强了网络攻击数据的原始特征。其提取的最终数据结果为：

$$e_m=g(e_{m-1}\otimes v_m+b_m)。\tag{2}$$

式中：e_m 为最终提取的网络攻击数据特征；$g(\ )$为在进行特征提取时使用激活函数；v_m 为改进 D-S 理论在进行特征提取时的权重系数；b_m 为网络攻击特征；e_{m-1} 为在前一次数据特征提取的结果；e_0 为网络攻击数据的输入样本。完成上述计算后，为提高最终的检测精度，对提取的数据特征进行降维处理，处理过程为：

$$e_m^*=\mathrm{pool}(e_m)。\tag{3}$$

式中：e_m^* 为进行降维处理后的数据特征；pool( )为降维函数。通过上述计算，完成数据特征的降维处理，为之后构建数据检测模型奠定基础。至此，基于改进 D-S 的数据特征提取完成。

1.3　构建网络攻击检测模型

利用特征提取预处理后的网络攻击数据，对原有的数据特征进行有效特征提取，再利用特征映射选取关联性较强的特征，将不同的数据特征编码到网络中，并计算出新输入数据和拟合数据之间的误差，从而构建网络攻击检测模型[13]。构建的网络攻击检测模型如图 3 所示。

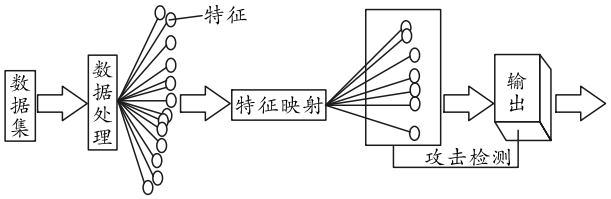

图 3　网络攻击特征检测模型

图 3 中，利用输入数据的有效特征进行重构，从而生成与输入数据相似的拟合数据，计算数据的输入值和生成的拟合值之间的差值，来判定数据当前的状态，并将数据划分为正常数据和异常数据[14]。如果当前输入的数据处于异常状态，那么输出的数值将会大于正常数据的数值。具体的分类过程如图 4 所示。

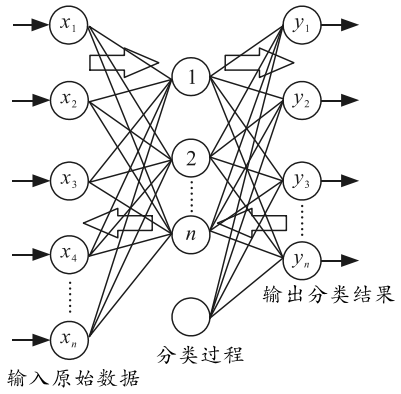

图 4　数据分类过程

图 4 中，根据输入初始数据特征，对数据进行简单分类，再通过数据的分布特点和内部特征，进行数据精准分类，为后续检测网络攻击数据提供依据。在完成上述对数据的分类后，生成的样本数据为：

$$H=\begin{bmatrix} h_1(x_1) & h_2(x_1) & \cdots & h_L(x_1) \\ h_1(x_2) & h_2(x_2) & \cdots & h_L(x_2) \\ \vdots & \vdots & & \vdots \\ h_1(x_N) & h_2(x_N) & \cdots & h_L(x_N) \end{bmatrix}_{N\times L}。\tag{4}$$

式中：H 为输出的样本集；$h_L(x_N)$为单个样本数据。在上述公式基础上，生成网络攻击检测数学模型：

$$f(x)=\sum_{i=1}^{L}\boldsymbol{\alpha}_i G(\boldsymbol{K}x_i+b)\bullet h_i(x)。\tag{5}$$

式中：$\boldsymbol{\alpha}_i$ 为不同样本数据的权重向量；$G(\ )$为数据特征的激活函数；x_i 为样本数据；$f(x)$为样本数据的输出数值；$\boldsymbol{K}$ 为数据的权重矩阵；b 为样本数据在计算过程中出现的偏差。通过上述计算，生成网络攻击检测的数学模型。至此，网络攻击监测模型的构建完成。

1.4　实现网络复合攻击活动检测

在上述设计的基础上，进行网络复合攻击活动的检测。在检测过程中，先对输入数据状态进行计算，具体计算过程为：

$$c=\frac{N_1-N_2}{N_2}=\frac{1}{l(1+\Delta\varepsilon)}-1。\tag{6}$$

式中：N_1 为输入数据的原始数值；N_2 为输入数据的拟合数据；l 为拟合系数；$\Delta\varepsilon$ 为输入数据原始数值和拟合数值之间的差值；c 为输入数据当前的状态数值。通过上述计算输入数据当前的状态值，然后对该状态数值进行判定，具体判定过程为：

$$d=\begin{cases}1, & c\in[c_{\min},c_{\max}] \\ 0, & \text{otherwise}\end{cases}。\tag{7}$$

式中：d 为对输入数据进行状态判定的结果；$c_{\min}$ 为输入数据的最小状态值；$c_{\max}$ 为输入数据的最大状态值。通过上述计算得出 d 的数值，决定当前电力监控网络的状态。当 c 的数值处在标准范围内，此时 d=1，说明当前数据为正常数据，当前电力监控网络处于正常状态。检测方法将继续检测其他数据。如果 c 的数值并未在标准范围内，此时 d=0，说明当前数据为异常，电力监控网络处于异常状态，此时电力监控网络会发出警告[15]。至此，基于改进 D-S 的电力监控网络复合攻击活动检测方法的设计完成。

2　实验测试

2.1　实验准备

为验证设计的基于改进 D-S 的电力监控网络复合攻击活动检测方法在实际应用中的效果，进行了仿真实验。

本实验以美国麻省理工学院林肯实验室提供的 DARPA1999 作为报警信息源，建立攻击场景。实验平台为 Matlabr2010b。

实验中，为保证实验结果的准确性，抽取了 10 组网络攻击数据集，并将抽取的数据集划分为正常样本数和异常样本数，方便后续实验的进行。实验数据集的具体分类情况如表 1 所示。

表 1　实验数据集的分类情况

序号	实验数据集	正常样本数	异常样本数
1	Normal	56 000	37 000
2	Generic	40 000	188 873
3	Exploits	33 396	11 143
4	Fuzzers	14 145	6 060
5	DoS	122 264	4 089
6	Reconnaissance	10 795	3 496
7	Analysis	2 000	677
8	Backdoor	1 746	583
9	Shellcode	1 133	378
10	Worms	130	44

表 1 中，数据集的样本数量庞大，测试时，需要设置相应的实验参数，以确保实验的顺利进行。实验参数如表 2 所示。

表 2　实验参数的设置

序号	实验参数	参数设置
1	CPU	Intel(R) Core(TM)i5-10210U
2	内存	16 GB
3	编程环境	Python3.7
4	操作系统	Windows 10

在上述实验参数的设置下进行实验测试。Matlab 平台提供了一些 Python 调用库，这些库可以在 Matlab 中直接调用 Python 函数或模块。可以使用这些库来调用 Python 3.7 编程环境中的函数或模块，并在 Matlab 中使用返回的结果。具体的实验环境如图 5 所示。

图 5　具体的实验环境

为保证实验结果的可靠性，设置了对比实验。其中，笔者设计的基于改进 D-S 的电力监控网络复合攻击活动检测方法为方法 1，基于 Apriori 算法的电力监控网络复合攻击活动检测方法为方法 2，基于孤立森林算法的电力监控网络复合攻击活动检测方法为方法 3。

该实验设计流程为：

1) 整个实验过程中使用相同的实验数据集进行验证比较，从攻击数据集中选取部分训练数据为本次实验用数据集。

2) 将 D-S 作为复攻击检测模型的参数训练算法，使用经典一阶 Forward 算法作为评价函数。将实验用攻击数据集用于 D-S 的训练。

3) 将 D-S 作为复攻击检测模型的参数训练算法，使用二阶 Forward 算法作为评价函数。将实验用攻击数据集用于改进 D-S 模型的训练。

4) 启动淘汰机制从算法结束条件开始逐渐增加，统计不同预测值即 2 个模型的最优值，确定检测值，再将控制参数的值从 0.1 开始逐渐递增至 1。

5) 将 TQPSO 和 QPSO 算法作为复合攻击预测模型的参数训练算法，使用二阶 Forward 算法作评价函数。将实验用攻击数据集用于检测模型的训练。

6) 实验从攻击数据集中随机选取一条攻击序列，送入步骤 5)中训练产生了 2 个攻击场景，进入攻击场景识别、攻击意图计算和攻击检测过程。

2.2　实验结果与讨论

以检测方法的误码率为评价指标，对比 3 种检测方法的好坏。误码率的计算过程为：

$$P=m/M。\tag{8}$$

式中：P 为检测方法的误码率；m 为在检测过程中，正常样本被误报成异常样本的数量；M 为正常样本的数量。通过式(8)计算出 3 种检测方法在不同数据集的误码率。方法 1、2、3 的实验结果如图 6 所示。

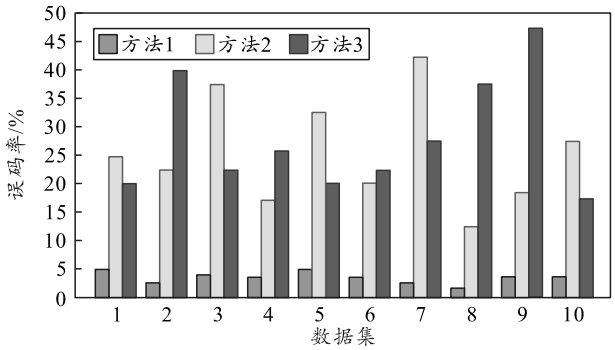

图 6　不同方法的实验结果

从图 6 中可以看出：在不同的数据集中，方法 1 的误码率较低，均低于 5%；方法 2 和 3 的误码率较高，方法 2 的误码率最高为 45%左右，方法 3 的误码率最高为 50%左右。同时，方法 1 的平均误码率为 3.2%，方法 2 的平均误码率为 26.3%，方法 3 的平均误码率为 33.3%，由此可知，方法 1 的平均误码率最小。笔者在实际应用中，设计的基于改进D-S的电力监控网络复合攻击活动检测方法误码率较低，检测准确度更高，有更好的应用效果，具有一定的优势，保障了军事设施和武器系统的正常运行。

3　结束语

综上所述，笔者设计的电力监控网络复合攻击

活动检测方法利用改进 D-S 理论，提取网络攻击数据的特征，构建网络攻击数据检测模型，提高了检测精度。同时，在数据检测前，对网络攻击数据进行归一化计算和降噪处理，降低了数据运算压力，提高了数据检测速度。此外，在实验测试中，该方法检测准确度较高，实际应用效果较好，对相关检测技术的发展和进步有一定的参考价值。

参考文献：

[1] 王庆, 李朝东, 陈伟, 等. IPDU 在电力监控系统网络安全防护中的应用研究[J]. 黄山学院学报, 2022, 24(3): 21−24.

[2] 东晓, 王潇煜, 谢丹丹, 等. 基于 Apriori 算法的稳控装置通信系统网络攻击检测方法[J]. 电力信息与通信技术, 2022, 20(9): 1−8.

[3] 李晶晶. 孤立森林算法在网络潜在攻击检测方法中的应用研究[J]. 九江学院学报(自然科学版), 2022, 37(4): 72−74, 92.

[4] 单瑞卿, 畅广辉, 李翔硕, 等. 考虑攻击方身份的电力监控系统网络安全风险分析[J]. 电力科学与技术学报, 2022, 37(5): 3−16.

[5] 曹一家, 赵一睿, 施星宇, 等. 考虑针对变电站网络攻击风险的脆弱元件筛选方法[J]. 电力系统自动化, 2023, 47(8): 25−33.

[6] 王青, 赵璇, 周绍生. IT2 模糊网络系统在网络攻击下的 H_∞控制[J]. 杭州电子科技大学学报(自然科学版), 2023, 43(2): 54−60.

[7] 于宗超, 王文博, 金倩倩, 等. 基于人工智能的电力系统网络攻击检测研究综述[J]. 高电压技术, 2022, 48(11): 4413−4426.

[8] 郭方洪, 郑祥康, 邓超, 等. 直流微电网无界虚假数据注入网络攻击检测与系统恢复方法[J]. 电力系统自动化, 2023, 47(2): 146−153.

[9] 许训炜, 沈希澄, 解相朋, 等. 基于数据驱动的源网荷储协同控制系统网络攻击关联性分析[J]. 浙江电力, 2023, 42(2): 76−82.

[10] 罗予东, 陆璐. 基于人工神经网络和遗传算法的网络攻击检测[J]. 计算机工程与设计, 2021, 42(9): 2446−2454.

[11] 秦云涛. 基于网络流量解析的网络攻击检测系统的设计与实现[J]. 信息与电脑(理论版), 2021, 33(17): 207−210.

[12] 刘世良, 裴生雷. 基于一种改进型事件触发传输机制的网络欺骗性攻击下的电力系统负荷频率控制[J]. 中南民族大学学报(自然科学版), 2023, 42(3): 365−372.

[13] 张保俊, 伍益明, 应晨铎, 等. 面向网络攻击和隐私保护的多智能体系统分布式共识算法[J]. 通信学报, 2023, 44(3): 117−127.

[14] 麻文刚, 张亚东, 禹倩, 等. 基于 CB-CNN 与分割残差优化的列控系统网络攻击流量检测[J]. 铁道学报, 2023, 45(4): 62−76.

[15] 苏江文, 宋立华. 基于无监督学习的电力系统网络潜在多步攻击实时检测方法[J]. 电气自动化, 2023, 45(2): 15−17.

****

（上接第 27 页）

[4] 周燕, 肖莉. 基于改进关联聚类算法的网络异常数据挖掘[J]. 计算机工程与设计, 2023, 44(1): 108−115.

[5] 蒋华, 李星, 王慧娇, 等. 基于数据索引结构的跨级高效用项集挖掘算法[J]. 计算机应用, 2023, 43(7): 2200−2208.

[6] 高淑萍, 徐振曦, 宋国兵, 等. 基于小波阈值去噪和 CEEMD 的混合三端直流输电线路故障测距[J]. 电力系统保护与控制, 2022, 50(3): 29−40.

[7] 张岩, 李新月, 王斌, 等. 基于深度学习的鲁棒地震数据去噪[J]. 石油地球物理勘探, 2022, 57(1): 12−25.

[8] 孙曙光, 张婷婷, 王景芹, 等. 基于连续小波变换和 MTL-SEResNet 的断路器故障程度评估[J]. 仪器仪表学报, 2022, 43(6): 162−173.

[9] 戴仁昶, 王亚伟, 刘广一, 等. 电力系统预想故障分析 GPU 并行和图并行计算的比较研究[J]. 电网技术, 2021, 45(6): 2064−2069.

[10] 黄春, 姜浩, 全哲, 等. 面向深度学习的批处理矩阵乘法设计与实现[J]. 计算机学报, 2022, 45(2): 225−239.

[11] 叶铃, 雷迎科, 陈悦, 等. 基于 k-means 算法的直扩信号信息及伪码序列盲估计方法[J]. 信号处理, 2021, 37(8): 1533−1540.

[12] 吴颖豪, 刘虹, 张岐山. 基于改进成对约束扩充的标签传播聚类算法[J]. 计算机应用研究, 2022, 39(12): 3592−3597.

[13] 陈勇, 郭云柱, 王威, 等. 模糊 K-Harmonic-Kohonen 网络的 FTIR 光谱数据聚类分析[J]. 光谱学与光谱分析, 2023, 43(1): 268−272.

[14] 刘卫明, 张弛, 毛伊敏. 采用 N-list 结构的混合并行频繁项集挖掘算法[J]. 计算机科学与探索, 2022, 16(1): 120−136.

[15] 廖彬, 黄静莱, 王鑫, 等. SCEA: 一种适应高维海量数据的并行聚类集成算法[J]. 电子学报, 2021, 49(6): 1077−1087.