文章编号:1671-4598(2021)12-0046-05 DOI:10.16526/j.cnki.11—4762/tp.2021.12.009 中图分类号:TP312 文献标识码:A

基于小波分解的多尺度 PCA 周期性攻击检测算法

刘学君[1]，张小妮[1]，栾海英[2]，李凯丽[1]，苏 鹏[1]，
黎 杨[1]，晏 涌[1]，沙 芸[1]

(1. 北京石油化工学院 信息工程学院，北京 102617；2. 北京机械工业自动化研究所有限公司，北京 100120)

摘要：在工业控制网络中任何异常入侵行为都直接影响现场控制与决策，工控系统的安全检测迫在眉睫；工业控制系统中存在正弦波攻击，三角波攻击和方波攻击等周期性入侵攻击，这些攻击隐蔽的分布很难被检测出来并且会造成机器的磨损，目前针对该类攻击检测研究较少；针对以上问题，首先采用小波分解把数据分解到各个尺度上，然后采用主成分分析进行局部检测，最后把各个尺度的主成分分析组成一个包含各尺度信息的综合主成分分析模型；通过在公开数据集及自建数据集的周期性攻击实验结果表明，采用该算法比采用单独主成分分析算法进行攻击检测的整体准确率提高 7.4%。

关键词：正弦攻击；三角波攻击；小波变换；主成分分析；异常检测

Multi—scale PCA Periodic Attack Detection Algorithm Based on Wavelet Decomposition

LIU Xuejun[1], ZHANG Xiaoni[1], LUAN Haiying[2], LI Kaili[1], SU Peng[1],
LI Yang[1], YAN Yong[1], SHA Yun[1]

(1. College of Information Engineering, Beijing Institute of Petrochemical Technology, Beijing 102617, China;
2. Beijing Research Institute of Automation for Machinery Industry (RIAMB), Beijing 100120, China)

Abstract: In the industrial control network, any abnormal intrusion behavior directly affects the on—site control and decision—making, so the safety detection of industrial control system is imminent. There are periodic intrusion attacks in industrial control system, such as sine wave attack, triangle wave attack and square wave attack. The hidden distribution of these attacks is difficult to be detected and will cause the wear and tear of the machine. At present, there is little research on this kind of attack detection. In view of the above problems, this paper first decomposes the data to each scale by wavelet decomposition, and then uses principal component analysis for local detection. Finally, the principal component analysis of each scale is composed of a comprehensive principal component analysis model which contains the information of each scale. The experimental results of periodic attacks on public data sets and self built data sets show that the overall accuracy of attack detection using this algorithm is 7.4% higher than that using single principal component analysis algorithm.

Keywords: sinusoidal attack; triangular wave attack; wavelet transform; principal component analysis; anomaly detection

0 引言

随着互联网技术和计算机信息技术的逐渐成熟、工业生产规模的逐渐扩大，把互联网技术应用在工业控制系统当中已经成为一种普遍现象[1]。近年来网络攻击手段越来越多样化也越来越隐蔽，出现的工业控制系统攻击事件不断增多，生产过程的异常或故障造成重大的经济损失、环境灾难甚至人员伤亡，促使国内外十分关注控制系统的信息安全[2]。不同于传统 IT 网络着重研究网络层内的数据安全，工控系统强调的是物理层的信息[3]。一旦业务数据被篡改，就会对整个工控系统工作状态出现误判，因此，对工控系统业务数据攻击进行研究，有利于提高工控系统的安全性。目前该领域的研究是基于工控系统上位机的历史数据，采用状态监控和异常检测算法进行研究，如 Amin 等人[4]对水利灌溉 SCADA 建立被控系统状态模型进行研究以及 Teixeira 等人[5]对电力控制系统的研究，但是他们的研究对于周期性的隐蔽攻击效果有待提高。周期性攻击[6-8]是注入一定幅值的周期性信号，幅值会长时间里在小范围内波动并且低于工控系统的报警线，直接从数据上无法分辨，报警器也不会提示，但是此时

收稿日期:2021-04-12； **修回日期**:2021-06-18。
基金项目:中国航油项目(CNAFKJ2019003)；北京石油化工学院重要科研成果培育项目(BIPTACF—008)；国家重点研发计划项目(2018YFC0824801)。
作者简介:刘学君(1977-)，男，河北唐山人，工学博士，副教授，硕士生导师，主要从事危化品仓储技术、图像处理研究、工控安全方向的研究。
引用格式:刘学君，张小妮，栾海英，等.基于小波分解的多尺度 PCA 周期性攻击检测算法[J].计算机测量与控制，2021，29(12)：46-50.

从设备采集的业务数据是异常的。针对此类工控业务层数据中周期性攻击，本文采用小波变换和多尺度主成分分析，把数据分解到多个尺度进行检测。

1　算法原理

1.1　小波变换

小波变换因其在时间－频率分析中所表现出的优越特性，被广泛应用在信号处理上。它继承和发展了短时傅里叶变换局部的思想，同时又克服了窗口大小不随频率变化等缺点，能够提供一个随频率改变的时频两域的窗口。小波变换能够充分突出某些方面的问题特征，能够对时间（空间）频率的局部化分析，通过伸缩平移运算对信号（函数）逐步进行多尺度细化，最终实现高频和低频处频率细分[9]。张涛等人[6]采用离散小波变换的方法对采集到的数据集进行分析。

小波变换将信号分解为逼近和细节两个过程[10]。信号 $f(t)$ 小波离散变换[11]为：

$$W_f(a,b)=[f,\Phi_{a,b}]=|a|^{-1/2}\sum\nolimits_n f(n)\Phi*\left(\frac{n-b}{a}\right) \tag{1}$$

式中，$\Phi(n)$ 为小波函数，$\Phi*(n)$ 为 $\Phi(n)$ 共轭，a 为尺度参数，b 为位移参数。本文把数据分解为两层，分解后的数据为三维数据，具体的分解如图 1 所示。

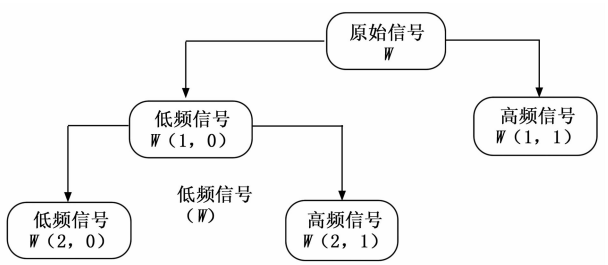

图 1　小波分解示意图

1.2　多尺度主成分分析原理

利用小波分解把数据分为多个尺度每一个尺度作为一个训练集，对每一个训练集做主成分分析（PCA，principal component analysis），根据累计贡献率确定主元个数以及协方差矩阵的特征值和特征向量，来建立单个尺度的 PCA 模型，把每个尺度包含重要信息的 PCA 模型整合成综合的 PCA 模型[12]。为提取单个模型的有效数据以及检测新数据是否受到攻击，引入了 T^2 统计量和 SPE 统计量的控制限[13-14]确定单尺度的 PCA 模型。

T^2 统计量是表征 PCA 模型内部变化的一种预测，具体定义如下[15]：

$$T^2=\frac{k(n-1)}{n-k}F_{k,n-k,\alpha} \tag{2}$$

其中：n 为建模数据的样本个数，α 为显著性水平，在自由度为 $n-k$，k 条件下 F 分布临界值。正常工控下，T^2 应该满足下式：

$$T^2\geqslant T_\alpha^2 \tag{3}$$

T^2 是 T_α^2 统计量的控制限。可以由下式得到：

$$T_\alpha^2=\sum\nolimits_{a=1}^{k}\frac{t_a^2}{\lambda_a} \tag{4}$$

式中，k 为主成分模型中保留的主成分个数，λ_a 为建模数据 X 的协方差矩阵的第 a 个特征值。

SPE 统计量是模型外部数据变化的一种测度，具体定义如下[16]：

$$\theta_i=\sum\nolimits_{j=k+1}^{m}\lambda_j^i \qquad i=1,2,3 \tag{5}$$

$$h_0=1-\frac{2\theta_1\theta_3}{3\theta_2^2} \tag{6}$$

$$SPE=\theta_1\left(\frac{C_a\sqrt{2\theta_2h_0^2}}{\theta_1}+1+\frac{\theta_2h_0(h_0-1)}{\theta_1^2}\right)^{1/h_0} \tag{7}$$

其中：C_a 为正太分布在显著水平 a 下的临界值，λ_j 为 X 的协方差矩阵的特征值。正常工控下，SPE 应满足下式：

$$SPE\geqslant SPE_a \tag{8}$$

SPE_a 是 SPE 统计量的控制限，可有下式计算得到：

$$SPE_a=\sum\nolimits_{j=1}^{m}(x_j-\hat{x}_j)^2 \tag{9}$$

式中，x_j 为第 j 个变量的测量值，$\hat{x}_j$ 为第 j 个变量的主成分模型预测值，m 为矩阵的行数。

正常工控下，SPE 和 T^2 应同时满足：

$$SPE\geqslant SPE_a,T^2\geqslant T_\alpha^2 \tag{10}$$

若其中至少有一个不满足，则表明数据遭受攻击。

2　建模与测试

本文以工控网络数据集来研究周期性攻击检测的具体的建模过程。目前工控方面公开数据集中异常数据一般不含周期性攻击，所以本文构建了 3 种周期性攻击的模型。由于周期性攻击是在幅值和频率上做微小变化，更接近偏差攻击，因此 3 种攻击模型是在偏差攻击模型上进行修改。

假设所有数据 Q 集合数据遭受攻击，则偏差攻击模型定义如下[17]：

$$y(N)=\begin{cases}y(n),n\notin Q;\\ y(n)+E,n\in Q\end{cases} \tag{11}$$

$y(n)$ 表示原始数据，幅值为 E，在部分数据上加上一个小幅值构成偏差攻击。正弦攻击在偏差攻击的基础上添加频率特性攻击，使其隐蔽性更高。正弦攻击模型如下：

$$y(N1)=\begin{cases}y(n),n\notin Q;\\ y(n)+E\sin(n*\omega),n\in Q\end{cases} \tag{12}$$

式中，正弦攻击角频率 ω 决定攻击信号周期，幅值 E 决定攻击强度。

假设方波攻击周期为 N，幅值为 E，把攻击加入集合 Q。则方波攻击模型如下：

$$y(N2)=\begin{cases}y(n),n\notin Q;\\ y(n)+\begin{cases}E,n\in\left(0,\dfrac{N}{2}\right),n\in Q\\ 0,n\in\left(\dfrac{N}{2},N\right),n\in Q\end{cases}\end{cases} \tag{13}$$

三角波攻击与正弦攻击类似，但是正弦攻击相较于三角波攻击更平缓。假设三角波攻击的周期为 N，幅值为 E，把攻击加入集合 Q。三角波攻击模型如下：

$$y(N3)=\begin{cases}y(n),n\notin Q;\\ y(n)+\begin{cases}\dfrac{4E}{N}n,n\in\left(-\dfrac{N}{4},\dfrac{N}{4}\right),n\in Q\\ 2E-\dfrac{4E}{N}N,n\in\left(\dfrac{N}{4},\dfrac{3N}{4}\right),n\in Q\end{cases}\end{cases}\tag{14}$$

式（11）是偏差攻击的模型，根据模型生成异常数据的方法是原始数据叠加一个相较于原始数据较小的数值。式（12）是正弦攻击模型，与偏差攻击模型的区别是叠加的幅值乘上了一个正弦函数，即原始数据叠加数据遵循正弦规律变化。式（13）是方波攻击模型、式（14）是三角波攻击模型，根据模型生成数据的方法与正弦攻击相同。

通过模型生成异常数据后，选取正常数据作为训练集，对选取的训练集做数据预处理，数据预处理包括去中心化和标准化。处理后的数据做小波尺度分解，如（1）式所示，把数据分为多个尺度，具体分解的层数根据实际情况而定。文采用的小波函数是 Daubechies 简称为 dbN，其中 N 为小波的分解阶数。小波 $\psi(t)$ 和尺度函数 $\varphi(t)$ 中的支撑区为 $2N-1$，$\psi(t)$ 的消失矩为 N。本文用到的 $N=2$，dbN 没有明确的表达式，但转换函数 h 的平方模是明确的。

假设 $P(y)=\sum_{k=0}^{N-1}C_k^{N-1+k}y^k$，其中 C_k^{N-1+k} 为二项式的系数[18]，则有：

$$|m_0(\omega)|^2=\left(\cos^2\frac{\omega}{2}\right)p\left(\sin^2\frac{\omega}{2}\right)\tag{15}$$

其中：

$$m_0(\omega)=\frac{1}{\sqrt{2}}\sum\quad h_k e^{-k\omega}\tag{16}$$

Daubechies 小波函数提供了比 Haar 函数更具有效的分析和综合。

采用训练集训练综合模型，首先把正弦攻击、方波攻击和三角波攻击叠加正常数据作为测试集。其次把测试集进行尺度分解，在对应尺度上的 PCA 模型中进行测试。最后如果一个测试集在多个单尺度 PCA 模型当中都检测出了攻击，就采用综合尺度的 PCA 模型即多尺度主成分分析（MSPCA，multi－scale principal component analysis）进行检测，算法流程如图 2 所示。

由图 2 可知，算法的运行步骤如下：

1）首先对训练集数据预处理，在预处理阶段是对数据进行标准化，采用小波滤除噪音，并分解为多个尺度。

2）其次在多个尺度的数据上分别训练单尺度的 PCA 模型，把各个尺度提取出来的重要信息组合成新的矩阵，求取新矩阵的两个控制限得到综合模型。

3）最后在测试集上进行测试，测试集数据进行预处理，然后输入到综合模型中，如果存在数据只要超出一个控制限，那么判定数据为异常数据并输出，反之为正常数据。直到把所有的数据检测完，算法结束。

3 实验结果与分析

3.1 实验步骤

3.1.1 构建数据集

把原始数据集按照 9∶1 的比例划分为训练集和测试集。使用公式（12）～（14）模型构建异常数据，幅值设为原始数据集的数值的 1%～2%，频率设为 100～1 000 之间。根据 3 个模型随机产生 3 组数据。3 组随机数分别随机叠加到部分测试集上，形成 3 组含有异常数据的测试集。

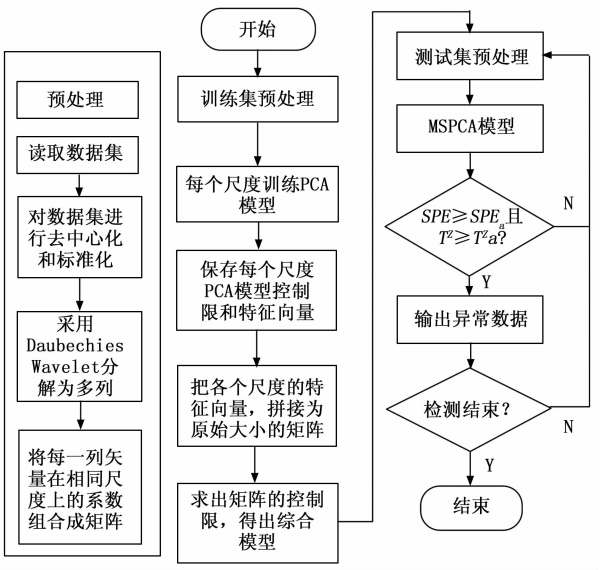

图 2 异常数据检测流程图

3.1.2 训练模型并进行检测

把训练集输入到算法经训练得到综合模型，对测试集进行检测。测试过程中为便于观察实验结果，在算法之中加入显示模块和数据统计模块。显示模块画出各个数据与综合模型两个控制限的距离，并把两个控制限显示在两幅图中，只要超出一个控制限，数据就为异常数据。数据统计模块将会输出异常数据的位置以及异常数据的数目。

3.2 实验方法

本文采用同一训练集分别训练综合模型和 PCA 模型，然后分别统计综合模型和原始 PCA 算法检测出的异常数据数目，来比较两个算法检测效果。

3.3 实验结果

本文采用两个数据集进行实验，并用 python 中 matplotlib 进行绘图。每组实验结果两张图，T^2 统计量图和 SPE 统计量图，图横轴表示样本，纵轴表示统计量值。两张图中的横线表示综合模型的控制限。

3.3.1 密西西比数据集

密西西比州立大学基础设施保护中心于 2014 年建立的工控入侵检测数据集，数据源为天然气管道 SCADA 控制系统网络层数据，包含 4 种类别的攻击，26 个特征和 1 个标签值[18-21]。

1）三角波攻击测试集实验结果：

图 3 和图 4 分是 PCA 和 MSPCA 对三角波攻击的检测结果，三角波的攻击幅度是正常数据±2%。左右两幅图的横线以下为正常数据，超出其中一条都为异常数据。由图 3 和图 4 对比可见，图 4 中检测出的异常数据更多，对数据分解以后再检测的灵敏度要高于原始直接检测的灵敏度。

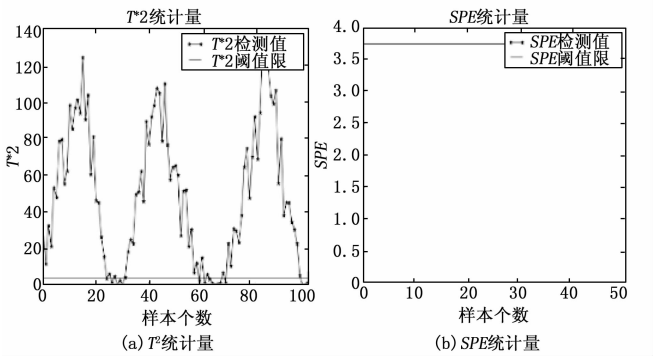

图 3　PCA 检测三角波攻击的结果

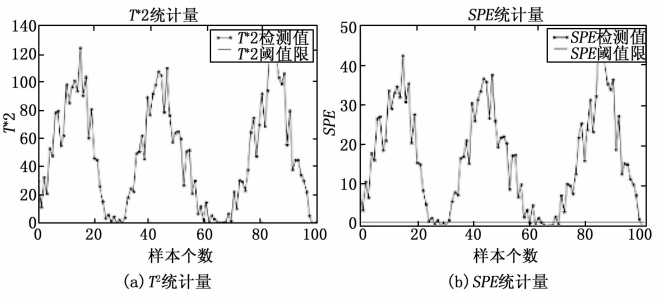

图 4　MSPCA 检测三角波攻击的结果

2）方波攻击测试集实验结果如图 5 和图 6 所示。

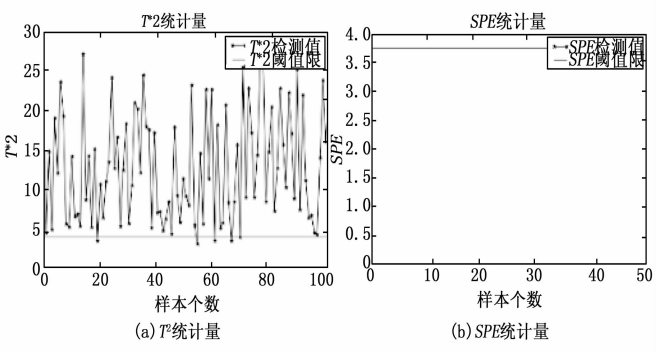

图 5　PCA 检测方波攻击的结果

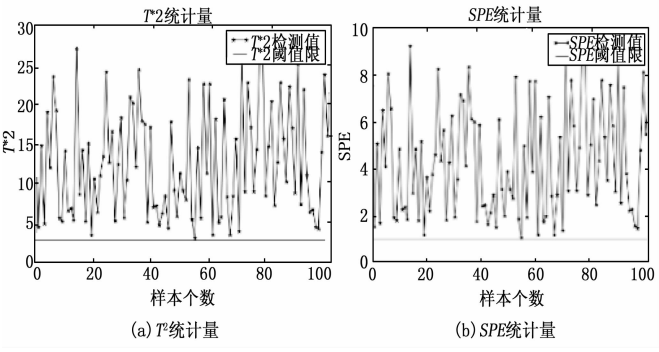

图 6　MSPCA 检测方波攻击的结果

图 5 和图 6 分别用 PCA 和 MSPCA 对方波攻击的检测结果，攻击幅度是正常数据±2%。由两组对比结果可知图 6 中数据分解后检测出来的异常点较多。

3）加入正弦攻击，检测结果如图 7 和图 8 所示。

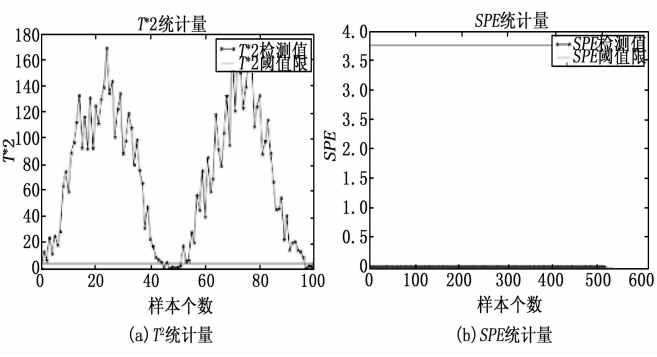

图 7　PCA 检测正弦波攻击的结果

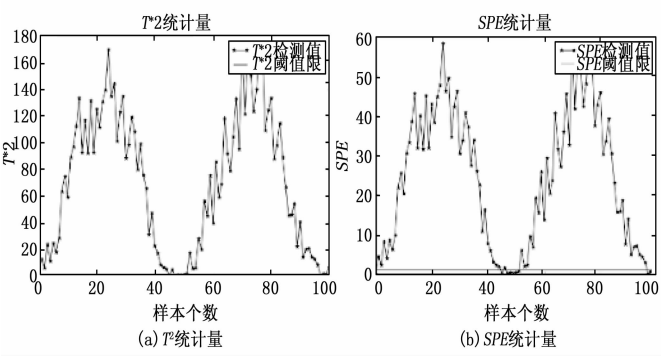

图 8　MSPCA 检测正弦波攻击的结果

图 7 和图 8 为正弦攻击检测结果，攻击幅度是原始数据的 1%，在单尺度检测中仅依靠 T^2 统计，而在 MSPCA 模型当中，是由 T^2 统计和 SPE 统计检测共同决定。由图像可知图 8 中 MSPCA 检测出来的异常数据要多于 PCA 检测出来的数目。

3.3.2　自建数据集实验结果

自建数据集是对某工控系统的多个设备采集数据，其中包括油罐的液位、压力以及温度、管线压力等共包含 131 个特征和 1 个标签。

图 9 和图 10 为某工控系统数据叠加正弦攻击后采用算法检测出来的异常数据，其中攻击幅度为攻击前幅度±1%。

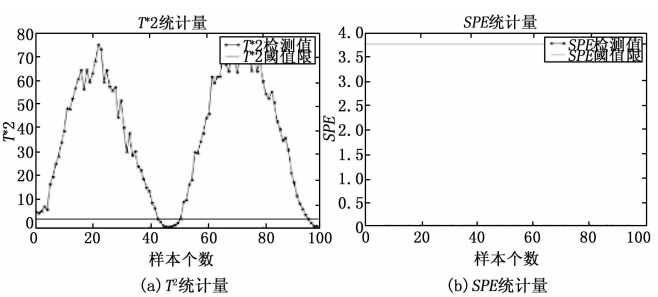

图 9　PCA 检测正弦波攻击的结果

由图 9 和图 10 的检测结果可知，在攻击幅度极小的情况下，图 10 中 MSPCA 检测效果依然比图 9 中 PCA 异常检测效果好。

3.4　实验分析

工控系统为了保证数据的时效性，数据集采集的频率

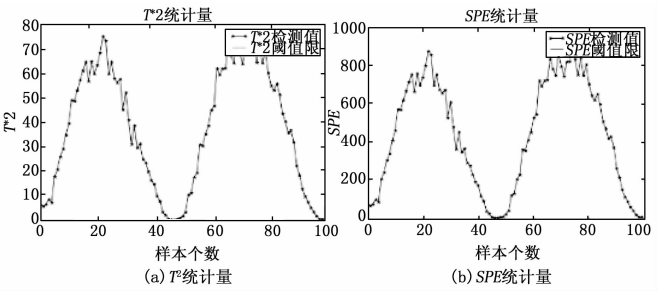

图 10 MSPCA 检测正弦波攻击的结果

比较高，系统设备传感器数据变化量比较小，所以各个攻击类型的攻击幅度比较小控制在 1%～2%之间。通过 3.3 节两个数据集上的几组实验结果图可知，MSPACA 的检测效果要高于 PCA 算法，具体的实验统计数据如表 1 所示。

表 1 正弦攻击检测统计

项目	三角波攻击	方波攻击	正弦攻击
负样本数目	102	102	102
PCA 检测	85	96	91
MSPCA 检测	95	102	98
提高效果/%	9.8	5.8	6.8

由表 1 可知，多尺度的主成分分析在多种类型的攻击的检测结果均优于传统的主成分分析算法，适用于检测相关工控系统业务数据的异常。

4 结束语

针对工业控制系统采集到的各设备运行数据的周期攻击，本文首先采用小波变换进行尺度分解，然后再对每一个尺度做主成分分析记录每个尺度的 PCA 模型，通过指标来筛选出每个尺度有价值的数据，去除冗余，构成 MSPCA 模型，对隐蔽性比较强的周期性攻击提高了检测效果。同时，根据输出的异常数据可以确定受攻击的时间和所攻击的位置。下一步可以围绕提高 MSPCA 的准确率和灵敏程度做进一步研究和探索。

参考文献：

[1] 张凯一，陈铁明，严 春. 工业控制系统安全及异常检测研究进展 [J]. 信息安全研究，2017，3 (7)：624－632.

[2] 王亚楠，王华忠，颜秉勇. 基于 PCA 的过程控制系统欺骗攻击研究 [J]. 信阳师范学院学报（自然科学版），2015，28 (4)：574－578.

[3] 陆耿虹，冯冬芹. 基于改进 C－SVC 的工控网络安全态势感知 [J]. 控制与决策，2017，32 (7)：1223－1228.

[4] AMIN S，LITRICO X，SASTRY S S，et al. Stealthy deception attacks on water SCADA systems [C] //ACM International Conference on Hybrid Systems：Computation & Control，ACM 2010：161.

[5] TEIXEIRA A，AMIN S，SANDBERG H，et al. Cyber security analysis of state estimators in electric power systems [C] //49th IEEE Conference on Decision and Control (CDC)，IEEE，2012.

[6] 张 涛，王道顺，李顺东，等. 对 DCT 域水印系统的周期性攻击 [J]. 清华大学学报（自然科学版），2008 (10)：1675－1678.

[7] 薛田良，刘希懋，张赟宁，等. 周期性拒绝服务攻击下的弹性负荷频率控制 [J]. 控制工程，2021，28 (4)：620－627.

[8] 张衍志，叶小琴. WSN 中基于周期性超宽带距离信息的女巫攻击检测 [J]. 电信科学，2016，32 (8)：110－117.

[9] 蔡 富，孙付平，戴海亮，等. 小波和傅里叶变换在坐标时间序列分析中的应用 [J]. 全球定位系统，2019，44 (4)：40－46.

[10] 宋保业，徐继伟，许 琳. 基于小波包变换－主元分析－神经网络算法的多电平逆变器故障诊断 [J]. 山东科技大学学报（自然科学版），2019，38 (1)：111－120.

[11] 张德峰. MATABLE 小波分析 [M]. 北京：机械工业出版社，2009.

[12] 刘大龙，冯冬芹. 采用多尺度主成分分析的控制系统欺骗攻击检测 [J]. 浙江大学学报（工学版），2018，52 (9)：1738－1746.

[13] CAI B，ZHAO Y，LIU H，et al. A data－driven fault diagnosis methodology in three－phase inverters for PMSM drive systems [J]. IEEE Transactions on Power Electronics，2017，32 (7)：5590－5600.

[14] 杜海莲，苗诗瑜，杜文霞，等. 改进 PCA 方法在化工过程中的故障诊断研究 [J]. 山东科技大学学报（自然科学版），2017，36 (5)：16－22.

[15] 刘丽云，国 蓉，牛鲁娜，等. 基于主元分析方法的化工过程故障诊断与识别 [J]. 化工自动化及仪表，2020，47 (5)：398－406，449.

[16] 单 彪，堵 俊，商亮亮. 基于改进 PCA 空调系统传感器故障检测与诊断 [J]. 控制工程，2020，27 (4)：181－186.

[17] 徐彬彬，洪 榛，赵 磊，等. 网络化倒立摆系统的偏差攻击及检测方法 [C] // 第 30 届中国过程控制会议（CPCC 2019），2019.

[18] 宋 暖，陈大川，栾 爽，等. 基于 Daubechies (dbN) 的飞行器音频特征提取 [J]. 电子制作，2018 (19)：94－95，65.

[19] KRIAA S，PIETRE C L，BOUISSOU M，et al. A survey of approaches combining safety and security for industrial control systems [J]. Reliability Engineering & System Safety，2015，139：156－178.

[20] 陈冬青，张普含，王华忠. 基于 MIKPSO－SVM 方法的工业控制系统入侵检测 [J]. 清华大学学报：自然科学版，2018，58 (4)：380－386.

[21] YONG L，LEUNG K S. Genetic algorithm with adaptive elitist－population strategies for multimodal function optimization [J]. Applied Soft Computing，2011，11 (2)：2017－2034.

[22] LIU E，ZHANG X，XU X，et al. Slice－feature based deep hashing algorithm for remote sensing image retrieval [J]. Infrared Physics & Technology，2020，107：103299.

[23] CHEN W S，YANG H T，HUANG H Y. Optimal design of support insulators using hashing integrated genetic algorithm and optimized charge simulation method [J]. IEEE Transactions on Dielectrics & Electrical Insulation，2008，15 (2)：426－433.

[24] RZEWOZNICZEK M. Towards finding an effective uniform and single point crossover balance for optimization of elastic optical networks [C] //Network Intelligence Conference，IEEE，2015.