

DOI:10.19651/j.cnki.emt.2108047

基于 DKPCA 的电力信息系统虚假 数据注入攻击检测方法^{*}

陆孝锋^{1,2} 李鹏^{1,2} 高莲^{1,2} 杨家全³(1. 云南大学信息学院 昆明 650500; 2. 云南省高校物联网技术及应用重点实验室 昆明 650500;
3. 云南电网有限责任公司电力科学研究院 昆明 650217)

摘要: 电力信息系统的虚假数据注入攻击(FDIA)通过恶意篡改对应物理系统的状态数据,影响电网的正常运行。本文提出一种基于动态核主元分析(DKPCA)的虚假数据注入攻击检测方法,目的是解决电力信息系统中 FDIA 事件的时间相关性(动态性)问题,以及非线性变量难以分离问题。该方法通过构建动态增广矩阵解决了变量间的动态自相关性,利用核矩阵将非线性变量映射到高维空间转化为线性变量,引入主元分析建立 DKPCA 模型求得统计量的控制限,实时检测数据判断是否有故障发生。通过在 IEEE-30 节点系统上进行实验仿真,与 KPCA、PCA、NPE、TNPE 等检测方法比较,结果显示 DKPCA 模型检测率高达 100%,同时保持较低的误报率 0.2%。证明了所提方法可以实时检测电力信息系统中的攻击数据,有效避免故障漏报,确保电力信息系统数据安全。

关键词: 动态性;非线性;虚假数据注入攻击;攻击检测;动态核主元分析

中图分类号: TM773 **文献标识码:** A **国家标准学科分类代码:** 510.99

False data injection attack detection method based on dynamic kernel principal component analysis for power information system

Lu Xiaofeng^{1,2} Li Peng^{1,2} Gao Lian^{1,2} Yang Jiaquan³(1. School of Information, Yunnan University, Kunming 650500, China; 2. Internet of Things Technology and Application Key Laboratory of Universities in Yunnan, Kunming 650500, China;
3. Electric Power Research Institute, Yunnan Power Grid Cop, Kunming 650217, China)

Abstract: False data injection attack (FDIA) in power information system affects the normal operation of power grid by maliciously tampering with the state data of corresponding physical system. This paper proposes a false data injection attack detection method based on dynamic kernel principal component analysis (DKPCA), in order to solve the time correlation of FDIA events in power information system (dynamic) problem, and the problem that it is difficult to separate nonlinear variables. This method solves the dynamic autocorrelation between variables by constructing a dynamic augmented matrix, uses the kernel matrix to map nonlinear variables into high-dimensional space and convert them into linear variables, introduces principal component analysis to establish DKPCA model, obtains the control limit of statistics, and judges whether there is a fault by detecting data in real time. The experimental simulation is carried out on IEEE-30 node system. Compared with KPCA, PCA, NPE, TNPE and other detection methods, the results show that the detection rate of DKPCA model is as high as 100%, while maintaining a low false positive rate of 0.2%. It is proved that the proposed method can detect the attack data in power information system in real time, effectively avoid fault omission and ensure the data security of power information system.

Keywords: dynamic; non-linear; false data injection attack; attack detection; dynamic kernel principal component analysis

0 引言

随着物联网时代的到来,电网已经成为复杂的电力信

息系统^[1]。2009 年在第 32 届中国控制会议上专家们^[2]首次提出了虚假数据注入攻击(false data injection attack, FDIA)的概念。文献^[3]提出 FDIA 的攻击目标是电力系

收稿日期:2021-10-10

^{*} 基金项目:国家自然科学基金(61763049)、云南省应用基础研究重点课题(2018FA032)、云南省中青年学术和技术带头人后备人才项目(202105AC160094)资助

统的状态数据,即系统中各电源和负荷点功率、枢纽点电压、平衡点的电压和相位角。Umar 等^[4]提出它通过影响数据的状态空间结构来干扰系统决策,成功避开不良数据检测(bad data detection, BDD),达到危及电力系统安全的目的。例如 2015 年圣诞节前夕,乌克兰境内电网受到网络攻击,其中 FDIA 尤为严重,导致乌克兰大规模停电,造成十分严重的经济损失^[5]。

针对 FDIA 的研究目前有两条主线,一条主线是研究如何有效构建 FDIA^[6]。Xia 等^[7]提出 FDIA 的稀疏攻击向量构建方法,该构建方法需要攻击者准确的获取电力系统的量测雅可比矩阵。Yu 等^[8]提出在无法获取电力信息系统状态空间方程和雅可比矩阵的情况下,利用主元分析(principal component analysis, PCA)构建 FDIA,该构建方法更具有泛化性。上述方法,都是根据电力系统的静态模型来构建 FDIA,忽略了电力系统的动态特性。Qiu 等^[9]考虑发电机的动态和静态潮流,建立电力系统的动态模型,提出了一种能够通过 BDD 的 FDIA 构建方法,与现有的静态攻击方案相比,所提出的方案更具有隐蔽性。

另一条主线是研究如何精确检测 FDIA,该研究方向有两个:基于卡尔曼滤波器的检测方法、基于数据驱动的检测方法。

文献[10]提出基于卡尔曼滤波器的检测方法操作快捷简便易上手,得以被广泛用于攻击检测。文献[11]提出使用卡尔曼滤波技术,受限于电力系统配置信息、拓扑结构、状态估计和坏数据检测机制等,研究人员很难获取到详细的参数信息,也就无法设置阈值,无法检测攻击。为了克服该缺点,文献[12]提出基于机器学习和深度学习的 FDIA 检测方法被提出使用。He 等^[13]提出利用历史量测数据构建深度学习模型,通过模型识别 FDIA 的行为特征,根据实时数据的行为特征检测 FDIA。Ganjkhani 等^[14]提出结合状态估计器和深度学习检测 FDIA,该方法增加多个隐藏层来提高检测精度。Yang 等^[15]提出使用变分模态分解提取量测值的特征,利用长短期记忆网络进行训练,检测 FDIA。上述的检测方法能够成功检测到部分 FDIA,检测精度并不高,同时电力信息系统攻击数据难以获取,使得标记数据集的过程变得十分困难。针对该问题曾俊尧等^[16]提出基于时序近邻保持嵌入算法,根据文献生成攻击数据,解决了攻击数据难以获取的问题,保留数据局部特征的同时提取数据的时间相关性,提高了 FDIA 的检测率。该方案并没有解决 FDIA 的非线性问题和动态性问题,有待于其他学者进一步研究。

针对非线性问题和动态性问题,本文提出基于动态核主元分析(dynamic kernel principal component analysis, DKPCA)的 FDIA 检测方法。该方法利用核矩阵映射低维非线性变量,同时构建动态增广矩阵保留变量之间的动态自相关性,再引入主元分析建立 DKPCA 离线模型,输入正常历史量测数据建立平方预测误差(squared prediction

error, SPE)统计限,从而检测 FDIA。DKPCA 模型不依赖电力信息系统的拓扑矩阵和状态空间方程,也不依赖故障数据,仅仅需要正常数据构建统计限,是一种便于工程应用的数据驱动的方法,且该方法保留了变量之间的动态自相关性,解决量测数据的非线性问题和数据不平衡问题,使得检测率明显提高。

1 相关背景

1.1 问题描述

状态估计的基本原理^[17]是利用数据采集与监视控制系统(supervisory control and data acquisition, SCADA)中的仪表采集量测数据,根据量测数据来估计电力系统的运行状态。本文中,将重点讨论直流电网的状态估计^[18]。相比较交流电网,直流电网具有更高的可靠性和易操作性。在直流模型中,量测值包含电压相角量测、有功和无功注入功率量测,线路的有功和无功传输功率量测,数据采集中心的量测值表示为 $\mathbf{z} = (z_1, z_2, \dots, z_n)^T$, n 表示该量测数据空间维度 n 维,系统状态表示为 $\mathbf{x} = (x_1, x_2, \dots, x_m)^T$, m 表示系统状态空间维度 m 维。量测值和系统状态通过直流潮流方程式表达^[19]:

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \quad (1)$$

式中: $\mathbf{e} = (e_1, e_2, \dots, e_n)^T$ 和 \mathbf{H} 分别表示量测噪声空间维度 n 维和雅可比矩阵。

传统的 BDD 将量测值残差的 2-范数与阈值 τ 进行比较,来检验是否存在坏数据。这种情况下, BDD 工作原理可以表示为^[20]:

$$R = \|\mathbf{z} - \mathbf{H}\mathbf{x}\|_2 \geq \tau \quad (2)$$

若实时采集的量测值的残差 2-范数大于阈值 τ , 存在坏数据,否则系统运行正常。

FDIA 的目的就是误导电力信息系统将错误的状态估计 $\hat{\mathbf{x}} = \mathbf{x} + \mathbf{c}$ 作为一个有效的状态估计。其中 $\mathbf{c} \neq 0$, \mathbf{c} 表示电力系统状态的偏差, $\hat{\mathbf{x}}$ 表示受到 FDIA 后的状态估计。

为了实现这一点,攻击者将控制中心接收到的量测值更改为 $\hat{\mathbf{z}} = \mathbf{z} + \mathbf{a}$, 系统模型表示为^[21]:

$$\hat{\mathbf{z}} = \mathbf{H}\mathbf{x} + \mathbf{e} + \mathbf{a} \quad (3)$$

式中: $\mathbf{a} = (a_1, a_2, \dots, a_n)^T$ 表示攻击向量, $\hat{\mathbf{z}}$ 为受到 FDIA 后的量测值。

一般来说,一个非结构化的攻击向量 \mathbf{a} 很可能被上述式(2)中的传统 BDD 识别出来,因此为了规避 BDD,攻击向量进行结构化 $\mathbf{a} = \mathbf{H}\mathbf{c}$, 其中 \mathbf{c} 表示由于虚假数据的注入状态变量中引入的误差向量。同时量测值的残差 2-范数是不变的:

$$\|\hat{\mathbf{z}} - \mathbf{H}\hat{\mathbf{x}}\| = \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\mathbf{x} + \mathbf{c})\| = \|\mathbf{z} - \mathbf{H}\mathbf{x}\| \quad (4)$$

如式(4)所示攻击可以绕过 BDD。电力信息系统误以为 $\hat{\mathbf{x}} = \mathbf{x} + \mathbf{c}$ 是一个有效估计,从而引来一个误差向量 \mathbf{c} 。

此时,采用BDD模型无法检测实时数据中的FDIA,这将危害电力信息系统的安全稳定运行。

综上所述,FDIA表现了极强的隐蔽性和多样性,本文提出基于DKPCA的FDIA检测模型来解决此类问题。

1.2 动态核主元成分分析

DKPCA的核心思想是先构造一个动态时滞矩阵,在原数据矩阵中加入时滞,得到增广矩阵;通过核函数将低维非线性的数据映射到高维得到线性数据;最后在高维特征空间进行主元分析。一句话概括就是DKPCA将输入空间中的非线性问题转化为特征空间中的线性问题同时提取特征向量的动态自相关性。

考虑检测过程的时间相关性,时间序列模型可以表示如下:

$$\mathbf{X}_i(k) = [\mathbf{X}_i(k)^\top, \mathbf{X}_i(k-1)^\top, \dots, \mathbf{X}_i(k-d)^\top] \quad (5)$$

式中: d 表示动态矩阵的时滞,下角标 i 表示当前向量为时间序列, k 表示当前时刻, $k-1$ 表示上一时刻,依次往下, $\mathbf{X}_i(k)$ 为 k 时刻训练样本的观测值。

构造动态时滞矩阵:

$$\mathbf{X}_i^d = \begin{bmatrix} \mathbf{x}_i^\top(k) & \mathbf{x}_i^\top(k-1) & \dots & \mathbf{x}_i^\top(k-d) \\ \mathbf{x}_i^\top(k-1) & \mathbf{x}_i^\top(k-2) & \dots & \mathbf{x}_i^\top(k-d-1) \\ \dots & \dots & \dots & \dots \\ \mathbf{x}_i^\top(k \ (k_i \ d)) & \mathbf{x}_i^\top(k \ (k_i \ d) \ 1) & \dots & \mathbf{x}_i^\top(k \ k_i) \end{bmatrix} \quad (6)$$

式中:数据 $\mathbf{x}(k) \in R^m (k=1,2,\dots,n)$, n 表示样本个数,通过非线性映射 $\Phi(\cdot)$ 映射到高维空间 F ,如下表示:

$$\lambda \mathbf{v} = \mathbf{C}^F \mathbf{v} \quad (7)$$

式中: \mathbf{C}^F 是特征空间中的协方差矩阵, λ 是协方差矩阵中的非零特征值, \mathbf{v} 表示特征向量, $\Phi(\cdot)$ 表示内积核函数。

假设高维空间 F , 映射过程中去均值处理,则协方差表示为:

$$\mathbf{C}^F = \frac{1}{n} \sum_{j=1}^n \Phi(x_j) \Phi(x_j)^\top \quad (8)$$

式(8)用核矩阵表示:

$$[\mathbf{K}_{ij}] = \mathbf{K}_{ij} = \langle \Phi(x_i), \Phi(x_j) \rangle \quad (9)$$

式中: \mathbf{K} 为 $n \times n$ 的核矩阵, \mathbf{K}_{ij} 表示 $\Phi(x_i) \Phi(x_j)$ 的点积。

进行简化:

$$n\lambda \boldsymbol{\alpha} = \mathbf{K} \boldsymbol{\alpha}, \boldsymbol{\alpha} = [\alpha_1, \dots, \alpha_n]^\top \quad (10)$$

式中: $\boldsymbol{\alpha}$ 为映射空间中的相关系数,特征值 $n\lambda$ 对应的特征向量, $n\lambda$ 又为 \mathbf{K} 的特征值。

根据以往文献选择符合数据分布的核函数,本文使用高斯径向基核函数 $K = \exp\left(\frac{-\|x-y\|^2}{2\sigma^2}\right)$ 构造核函数。

对复杂的高维空间进行均值中心化处理:

$$\overline{\mathbf{K}}_{ij} = \mathbf{K}_{ij} - \mathbf{I}_l \mathbf{K}_{ij} - \mathbf{K}_{ij} \mathbf{I}_l + \mathbf{I}_l \mathbf{K}_{ij} \mathbf{I}_l \quad (11)$$

式中: \mathbf{I}_l 表示元素都是 $1/n$ 的 $l \times l$ 矩阵, \mathbf{K}_{ij} 为进行均值中心化处理的核矩阵。

因此,对于DKPCA,特征空间中的主元分析转换成了

对核矩阵的特征值分解问题,如下表示:

$$\mathbf{t}_k = \langle \mathbf{v}_k, \Phi(\mathbf{x}_k) \rangle = \sum_{i=1}^n \boldsymbol{\alpha}_i^k \langle \Phi(x_i), \Phi(x) \rangle = \sum_{i=1}^n \boldsymbol{\alpha}_i^k k(x_i, x), k=1, \dots, n \quad (12)$$

式中: \mathbf{v}_k 表示特征向量, \mathbf{t}_k 为映射 $\Phi(\cdot)$ 在特征向量 \mathbf{v}_k 上投影的第 k 个核主元向量, $\boldsymbol{\alpha}_i^k$ 为规范化系数向量。

2 基于DKPCA的FDIA检测模型

本次实验检测FDIA用SPE作为标准, Spe_{online} 表示SPE统计量,反映了在某一时刻观测值对主元模型的偏离程度,是模型外部数据变化的一种评价标准,显示了数据在残差空间中的投影变化,定义如下:

$$Spe_{online} = \|\Phi(\mathbf{x}) - \Phi_k(\mathbf{x})\|^2 = \sum_{i=1}^N t_i^2 - \sum_{i=1}^K t_i^2 \quad (13)$$

式中: N 为样本个数, K 为非零特征值个数, t_i 表示 i 时刻的值对主元模型的偏离程度, $\|\Phi(\mathbf{x}) - \Phi_k(\mathbf{x})\|^2$ 表示测量样本在剩余子空间上的欧几里得距离,通过该距离定义故障及检测的正常区域。

相应的 Spe_{lim} 表示SPE控制限,如下所示:

$$Spe_{lim} = \frac{s}{2m} \chi_\alpha^2 \left(\frac{2m^2}{s} \right) \quad (14)$$

式中: s 为 Spe_{online} 的方差, m 为 Spe_{online} 的均值, α 为检验水平,上述参数服从 χ^2 分布。

基于DKPCA算法的FDIA检测模型,首先确立正常量测数据的控制线 Spe_{lim} ,接着采集实时量测数据输入到DKPCA模型中得到相应统计量 Spe_{online} ,比较统计量与控制限,判断是否存在FDIA。

基于DKPCA的FDIA检测模型,需要经过模型训练和实时监控两个阶段,其中模型训练:使用历史量测数据对模型进行训练,计算 Spe_{lim} 控制限;实时监控:对采集到的实时量测数据进行归一化处理,计算 Spe_{online} 统计量是否超过模型训练所得到的控制限,来检测是否存在FDIA。

本文所提出的基于DKPCA的FDIA检测模型详细步骤如下所示。

1) 离线建模过程

(1) 对采集到的历史量测数据进行归一化处理。

(2) 确定时滞,构造动态增广矩阵,计算增广矩阵各维度均值、方差。

(3) 根据式(10)计算核矩阵并根据式(11)进行中心化处理,核矩阵中心化: $\overline{\mathbf{K}}_{ij} = \mathbf{K}_{ij} - \mathbf{I}_l \mathbf{K}_{ij} - \mathbf{K}_{ij} \mathbf{I}_l + \mathbf{I}_l \mathbf{K}_{ij} \mathbf{I}_l$

(4) 对中心化处理以后的核矩阵进行特征分解,根据式(11)映射得到核主元向量 \mathbf{t}_k 。

(5) 建立DKPCA离线模型。

(6) 根据式(14)计算 Spe_{lim} 控制限。

2) 实时监控过程

(1) 采集实时量测数据。

- (2)对数据进行归一化处理。
- (3)处理后的数据输入 DKPCA 模型。
- (4)根据式(13)计算实时数据的 Spe_{online} 统计量。
- (5)根据 Spe_{lim} 控制限来判断 Spe_{online} 统计量是否超限,超限则存在 FDIA。

本文提出应用于 FDIA 检测的 DKPCA 模型流程如图 1 所示。

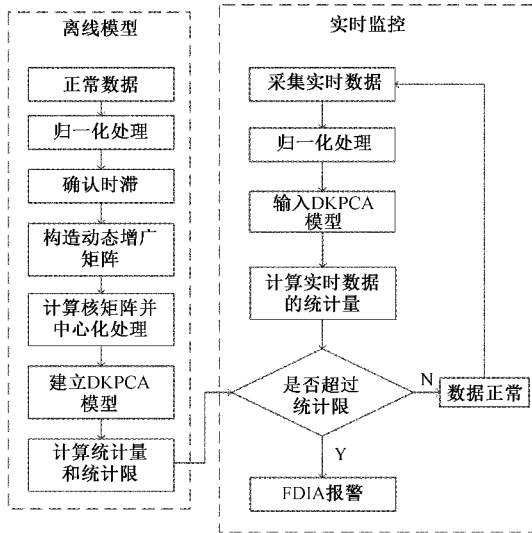


图 1 基于 DKPCA 的 FDIA 检测模型

算法 1 为 DKPCA 检测的伪代码。

算法 1 基于 DKPCA 的 FDIA 检测伪代码

```

1:采集正常历史量测数据作为训练数据集;
2:确定时滞  $s=1$ ;
3:构建动态增广矩阵,
   for  $i=s+1: N // N$  为样本个数
        $j=i-h$ ;
        $k1=i$ ;
        $k2=i-1$ ;
       ...
4:设定核矩阵参数为:  $type='gauss'; width='128'$ ;
5:利用核矩阵提取低维非线性分量;
6:建立 DKPCA 模型;
7:训练数据通过 DKPCA 模型,计算控制限  $Spe_{lim}$ ;
8:输入受攻击的数据实行在线监测,
   for  $i=1,2,3 \dots$ 
9:计算实时量测数据的统计量  $Spe_{online}$ ;
10: if  $Spe_{online} \geq Spe_{lim}$ 
    存在 FDIA
  else
    数据未遭受攻击
  end
    
```

3 实例仿真及分析

本文仿真实验选择 MATPOWER7.1 工具箱中的 IEEE-30 节点系统,模拟负荷曲线产生动态非线性的量测数据,验证 DKPCA 模型的检测效果。在 IEEE-30 节点系统中导入 case30,生成量测数据,每条量测数据包含 112 条量测值,其中量测值包括总线有功功率、总线无功功率、各支路有功功率和各支路无功功率。平衡节点以外的 29 个电压相角是带估计状态变量,如图 2 所示。

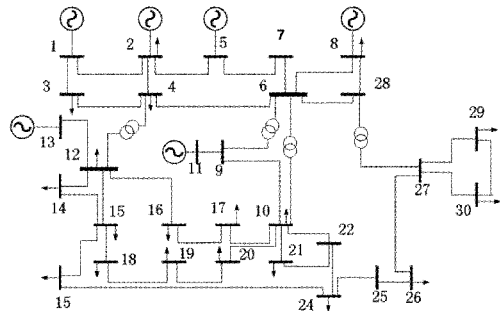


图 2 IEEE-30 节点系统示意图

算法参数设置如下:在 DKPCA 模型中,动态矩阵的时滞设置为 1,核函数为高斯函数,显著性水平为 99%。对比实验中,核主元分析(kernel principal component analysis, KPCA)、PCA、领域保持嵌入(neighborhood preserving embedding, NPE)、时间扩展领域保持嵌入(temporal extension of neighborhood preserving embedding, TNPE)主元个数以主元贡献度为 90% 的标准选出,控制限 Spe_{lim} 以 99% 的置信度为标准。

3.1 电网攻击数据的生成

本次仿真实验选择 MATPOWER7.1 工具箱 IEEE-30 节点系统来生成量测数据,根据 FDIA 攻击原理构造攻击量测数据,如图 3 所示,FDIA 攻击后状态变量的位置分布与 FDIA 攻击前基本一致,部分状态变量位置偏移原始状态变量。

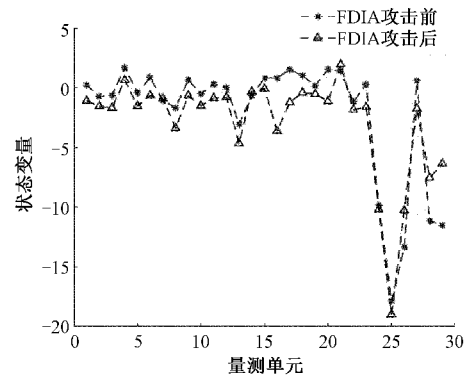


图 3 IEEE-30 节点系统状态变量示意图

如图 4 所示,攻击数据的量测值发生剧烈变化。为了验证该实验的准确性,进行了大量实验证明攻击数据与正

常数据的残差2-范数基本一致,表明了构造的攻击数据能规避BDD模型,使得电力信息系统进行错误的状态估计。

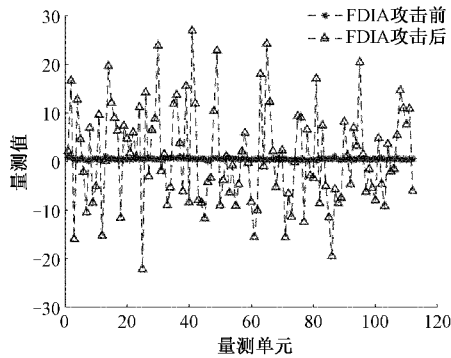


图4 IEEE-30节点系统量测值示意图

3.2 正常量测数据误报率分析

检测FDIA通常以误报率和检测率作为指标。正常量测数据检测实验以误报率作为指标^[22],分别选取两组长度相同的正常量测数据,数据长度分别为1000和2000,如表1所示。

表1 实验数据分配

实验	训练数据	测试数据
1	1~1000	1001~2000
2	1~2000	2001~4000

正常量测数据检测实验的误报率结果如表2所示,NPE、PCA误报率较高,TNPE、KPCA误报率较低,DKPCA的误报率最低,分别为0和0.2%,效果最佳。

表2 正常量测数据误报率分析

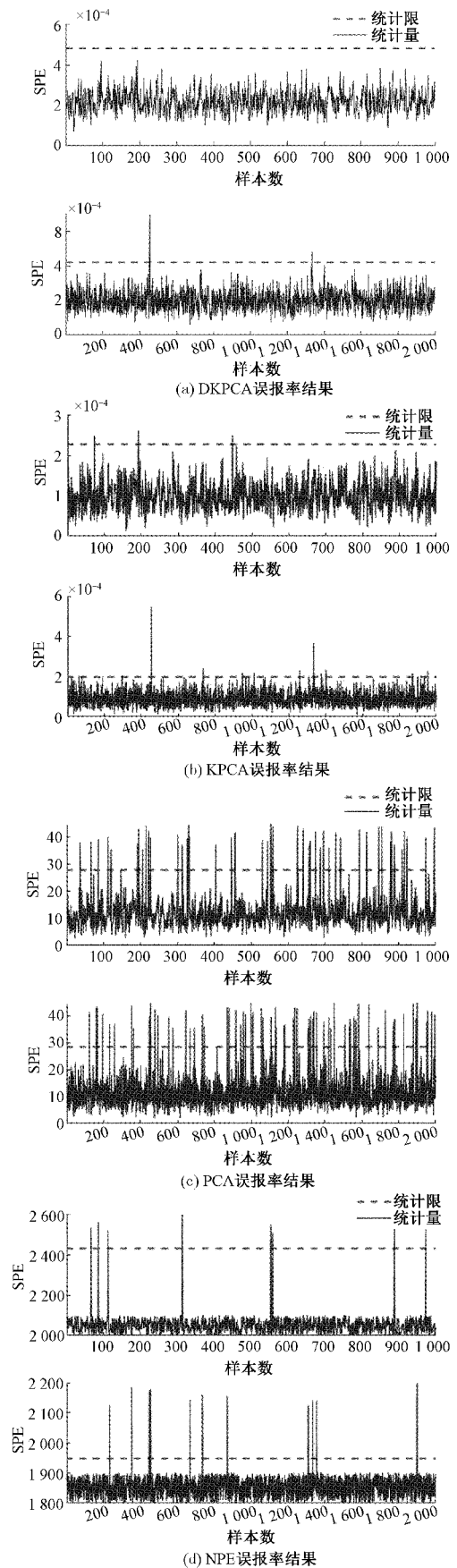
指标	实验	误报率/%				
		NPE	TNPE	PCA	KPCA	DKPCA
SPE	1	0.80	0.30	4.90	0.30	0
	2	0.55	0.45	3.45	1.05	0.20

如图5所示,给出了实验1和实验2的检测结果对比,综合比较5种算法的实验结果,KPCA、PCA、NPE、TNPE都出现了多次误报,图5(a)所示,DKPCA仅仅在2000条数据进行测试时,出现了4次误报。由于FDIA的特殊性,可能会导致数据在某一时段突然波动,监控超过控制线,这属于正常现象,所以DKPCA故障检测模型有更好的自适应性。

3.3 虚假数据注入攻击检测率分析

FDIA数据检测实验中以攻击检测率作为指标^[23]。用1500条正常量测数据训练模型得到 Spe_{lim} 控制限,输入另外的1500条数据进行测试,测试的数据中1~500条为正常量测数据,501~1500条为FDIA数据。

实验结果如表3所示,NPE、TNPE检测率不合格,PCA检测率达到96.5%,能够检测大部分攻击数据,KPCA、DKPCA检测率达到100%,效果最佳。



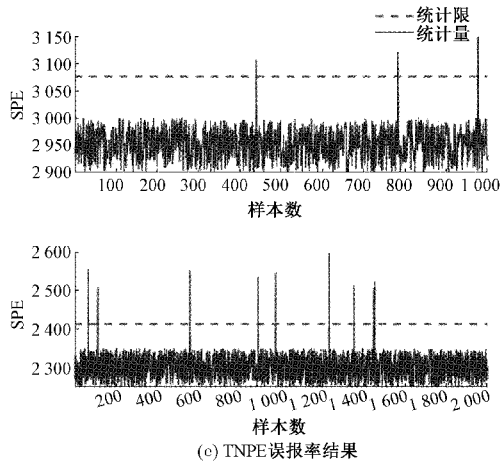


图 5 正常数据误报率结果对比

表 3 攻击数据检测率

指标	故障检测率/%				
	NPE	TNPE	PCA	KPCA	DKPCA
SPE	77.4	66.7	96.5	100	100

如图 6(a) 所示, NPE 和 TNPE 检测率极低, 分别为

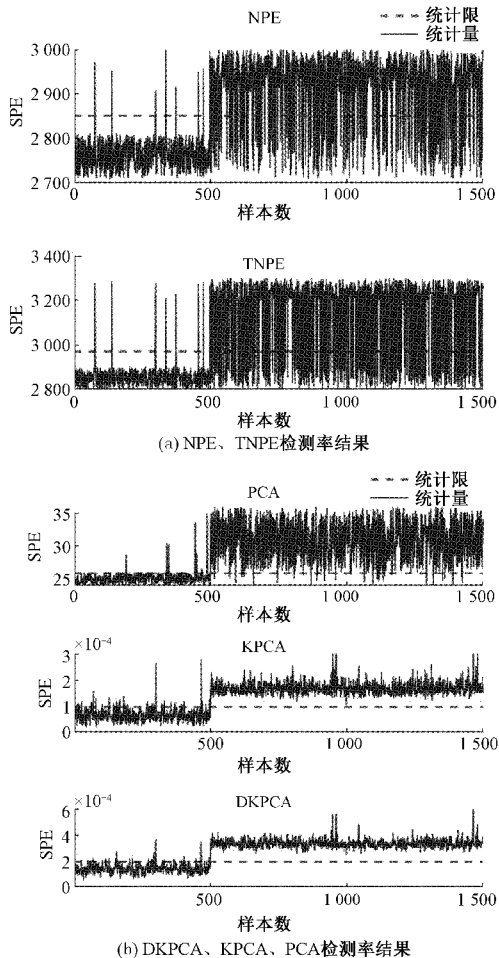


图 6 FDIA 攻击数据检测结果对比

77.4%、66.7%, 达不到实际应用的要求。图 6(b) 所示, 实验结果证明 DKPCA 在降低模型误报率的同时, 并没有削弱故障检测率, 甚至达到了完美的检测率 100%。由此可见 DKPCA 模型更适合用于 FDIA 的故障检测。

4 结 论

针对电力信息系统数据非线性问题和动态性问题, 本文提出基于 DKPCA 的电力信息系统 FDIA 检测方法, 是一种便于工程应用的数据驱动的方法。

首先在主元分析的基础上引入核函数, 构造核主元分析来优化模型结构, 利用核矩阵映射非线性数据到高维空间转换为线性数据, 降低了计算复杂度, 释放了大量计算机内存, 通过嵌入动态模型构造动态核主元分析, 依靠动态时滞增广矩阵处理时序问题, 提取了数据随时间变化的动态特征, 使得投影得到的低维空间不仅和原始变量空间具有相似的空间结构, 而且具有相似的时序动态结构, 因而包含了更多的特征信息, 减少了特征信息的丢失。

通过在 IEEE-30 节点系统多次仿真证明, 基于 DKPCA 的 FDIA 检测方法误报率接近 0, 检测率高达 100%, 模型性能优于 NPE、TNPE、PCA、KPCA 等方法, 为电力信息系统攻击检测提供一种好的办法。由于量测数据中通常存在误差和干扰, 未来的研究工作中, 还需要在现有的检测算法基础上, 提高算法模型的抗干扰能力, 加强算法模型对不同类型 FDIA 的检测能力及自我学习更新能力。

参 考 文 献

- [1] 王玉军, 卢敏, 孙云枫, 等. 基于大数据技术的电网历史数据管理设计实现[J]. 电子测量技术, 2020, 43(3): 30-34.
- [2] 白英伟, 管萸, 李慧聪, 等. 省级电网一体化全电量采集系统的设计与应用[J]. 电子测量技术, 2019, 42(8): 22-27.
- [3] DING Y, MA K, PU T, et al. A deep learning-based classification scheme for false data injection attack detection in power system [J]. Electronics, 2021, 10(12): 1459-1461.
- [4] UMAR S, FELEMBAN M. Rule-based detection of false data injections attacks against optimal power flow in power systems [J]. Sensors, 2021, 21(7): 2478-2478.
- [5] 程逸帆, 乔飞, 侯珂, 等. 区域微电网群两级能量调度策略优化研究[J]. 仪器仪表学报, 2019, 40(5): 68-77.
- [6] 张淑清, 要俊波, 张立国, 等. 基于改进深度稀疏自编码器及 FOA-ELM 的电力负荷预测[J]. 仪器仪表学报, 2020, 41(4): 49-57.
- [7] XIA M, DU D, FEI M, et al. A novel sparse attack vector construction method for false data injection in smart grids[J]. Energies, 2020, 13(11): 29-40.

- [8] YU Z H, CHIN W L. Blind false data injection attack using PCA approximation method in smart grid[J]. IEEE Transactions on Smart Grid, 2015, 6(3): 1219-1226.
- [9] QIU A, DING Z, WANG S. A descriptor system design framework for false data injection attack toward power systems[J]. Electric Power Systems Research, 2020, 192(10):106932-106935.
- [10] 王建平,郑成强,徐晓冰,等.基于卡尔曼滤波的微电网同步并网研究[J].电子测量与仪器学报,2017,197(5):809-815.
- [11] 杨奕贤,郭力,王洪达,等.基于数据驱动的直流微电网虚假数据注入攻击快速防御策略[J].电力自动化设备,2021,41(5):145-151.
- [12] 何西,涂春鸣,于力.配电网状态估计量测处理方法及抗虚假数据注入攻击策略[J].高电压技术,2021,47(7):2342-2349.
- [13] HE Y, MENDIS G J, JIN W. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism [J]. IEEE Transactions on Smart Grid,2017,8(5):2505-2516.
- [14] GANJKHANI M, FALLSH S N, BADA KHSHAN S, et al. A novel detection algorithm to identify false data injection attacks on power system state estimation [J]. Energies, 2019,12(11):1-19.
- [15] YANG L, ZHAI Y, LI Z. Deep learning for online AC false data injection attack detection in smart grids: An approach using LSTM-Autoencoder [J]. Journal of Network and Computer Applications, 2021,193(5): 103178-103180.
- [16] 曾俊娆,李鹏,高莲,等.基于TNPE的智能电网虚假数据注入攻击检测[J].中国安全生产科学技术,2021,17(3):124-129.
- [17] YANG L Q, LI Y C, LI Z J. Improved-ELM method for detecting false data attack in smart grid [J]. International Journal of Electrical Power and Energy Systems, 2017,91:183-191.
- [18] 李春,张代红,李登武.基于CNN-LSTM的配电网供电能力研究[J].国外电子测量技术,2019,38(9): 16-21.
- [19] ZHANG C, CHEN H, GUO M, et al. DC power flow analysis incorporating interval input data and network parameters through the optimizing-scenarios method[J]. International Journal of Electrical Power & Energy Systems, 2018, 96(1):380-389.
- [20] 李雪,钟慧欣,孙庆,等.基于快速回归算法的虚假数据攻击构造新方法[J].仪器仪表学报,2018,39(3): 179-189.
- [21] WANG Y J, SUN F M, LI X H. Compound dimensionality reduction based multi-dynamic kernel principal component analysis monitoring method for batch process with large-scale data sets[J]. Journal of Intelligent & Fuzzy Systems, 2020,38(1):1-10.
- [22] 袁川来,廖庸邑,孔玲爽,等.时间约束的改进分层模糊Petri网的配电网故障诊断方法[J].电子测量与仪器学报,2020,34(3):126-134.
- [23] TONG R N, LI P, LANG X, et al. A novel adaptive weighted kernel extreme learning machine algorithm and its application in wind turbine blade icing fault detection[J]. Measurement, 2021,185(12):110009-110010.

作者简介

陆孝锋,硕士研究生,主要从事智能电网攻击检测、电力大数据处理。

E-mail:1395949326@qq.com

李鹏(通信作者),副教授,博士,主要从事智能电网运行和控制、电力信息物理融合系统。

E-mail:lipeng@ynu.edu.cn

高莲,博士,讲师,主要从事电气设备状态检测与故障诊断、电力系统分析、运行与控制。

E-mail:962245641@qq.com

杨家全,硕士,主要从事智能电网故障分析。

E-mail:yjquan@163.com