第47卷 第10期 2023年5月25日
DOI：10.7500/AEPS20220813001
电力系统自动化
Automation of Electric Power Systems
Vol. 47 No. 10 May 25，2023

基于空间特征的电网同步量测虚假数据注入攻击检测

郑 瑶[1]，张 颉[2]，姚文轩[1]，邱 伟[1]，唐思豪[1]
（1. 湖南大学电气与信息工程学院，湖南省长沙市 410082；2. 电力物联网四川省重点实验室，四川省成都市 610041）

摘要： 随着电力系统向能源互联新生态逐渐迈进及网络层和物理层的深度耦合，网络攻击对电力系统的威胁不断提升。源身份欺骗攻击作为一种新型且复杂、强隐秘性的虚假数据注入攻击，可导致电网控制系统判断错误，引发系统瘫痪。针对这一问题，提出一种基于空间特征的电网同步量测虚假数据注入攻击检测方法。该方法通过变分模态分解和改进离散正交S变换提取同步量测装置不同位置的空间特征，实现在不损失量测数据空间特征的基础上，提取量测数据的身份认证信息；结合轻量型卷积神经网络评估量测数据遭受源身份攻击的可能性，加速检测响应速度。通过实际多点同步量测数据的检测结果，验证了该方法的有效性。

关键词： 广域测量系统；同步量测数据；虚假数据注入攻击；卷积神经网络

0 引言

随着无线通信技术在电力物联网中的广泛应用及风力、光伏等可再生能源和智能量测装置在电网中的逐步接入，电力系统不断向能源互联的新生态迈进[1]。电力系统的网络层和物理层深度耦合，系统控制水平和能源效率得以不断提升。但电力系统的脆弱性节点一旦暴露，安全性就可能受到外界网络攻击的威胁[2-3]，如乌克兰因网络攻击突发的停电事故[4]。广域测量系统（wide area measurements system，WAMS）中同步相量测量单元（phasor measurement unit，PMU）的数据传输标准[5-6]缺乏完善的网络通信安全机制，在量测数据的传输过程中，容易遭受虚假数据注入攻击和全球定位系统（global positioning system，GPS）信号欺诈等多种网络攻击[7-8]。虚假数据注入攻击中出现了一种新型隐秘性极强的源身份欺骗攻击方式，此攻击方式通过获取不同同步测量装置的数据权限，使得原有同步测量装置的量测数据和其他装置相混合，其攻击数据可能来自WAMS中相邻位置的同步量测装置，导致攻击数据非常接近原真实数据，使电网控制系统难以识别[9]，甚至可能将进一步引发系统瘫痪。这对电网控制系统提出了更高的防御要求。

近年来，虚假数据注入攻击成为网络攻击的主要欺骗手段。研究发现，电网频率量测数据中可提取独特地域特征信息作为数据源的检测依据[10-11]，文献[12-13]通过实际多点频率数据实现数据源位置识别。文献[14-16]采用变分模态分解（variational mode decomposition，VMD）算法或小波变换等现代信号处理方法和各类智能算法结合的方式检测网络攻击。文献[17]提出一种针对发电机动态状态估计的虚假数据注入攻击方法。上述方法对于判断和检测多种网络攻击分类的情况进行了分析和检测，但没有考虑源身份欺骗攻击。针对虚假数据注入攻击中新型、复杂、高欺骗性的源身份欺骗攻击，文献[18]提出一种基于集成经验模式分解和快速傅里叶变换（fast Fourier transform，FFT）的特征提取技术和机器学习的虚假混合数据网络攻击检测算法，文献中最小攻击率为10%，没有考虑网络攻击率更小的情况。文献[9]提出一种多粒度级联森林算法学习特征潜在关系的方法，但没有考虑不同攻击率下的识别精度。

针对此类隐秘性强的源身份欺骗攻击，提高识别精度和速度是本文算法的主攻方向，提升测试算法在不同攻击率下的识别精度。首先，为获得高识别精度，需要充分提取同步量测装置在不同位置的信息，本文提出量测数据空间特征提取算法，利用量测频率数据所包含的空间位置，作为该位置的身份认证信息。然后，为保证识别速度，提出结合小参数量、低复杂度的轻量型卷积神经网络（light

收稿日期：2022-08-13；修回日期：2022-10-23。
上网日期：2023-03-16。
国家自然科学基金资助项目（52177078）；湖南省自然科学基金资助项目（2022JJ30151）；电力物联网四川省重点实验室开放课题资助项目（PIT-F-202201）；中国博士后科学基金资助项目（BX20220102）。

convolutional neural network，LCNN）空间特征检测算法。最后，实现针对电网同步量测数据中源身份欺骗网络攻击的快速、精准检测。

1　同步量测数据网络攻击检测原理

不同于其他网络攻击，源身份欺骗攻击的数据来源于其他位置同步量测装置的正常数据，其攻击数据非常接近原真实数据，引发WAMS中应用程序的行为混乱，甚至可进一步导致电网系统瘫痪。本文提出量测数据空间特征的提取算法，结合LCNN空间特征识别算法，实现针对源身份欺骗攻击的快速、精准检测。

1.1　攻击检测算法结构

不同地点的量测数据表现出不同特征[12]，由此提出，假设通过提取电网正常运行数据中的空间位置信息，并依据此空间特征作为电网正常运行时网络攻击检测的身份信息，结合卷积神经网络，达到检测电网正常运行时是否遭受网络攻击的目的，并通过实际多点同步量测数据验证。研究提出一种存在源身份欺骗攻击时的同步量测数据攻击检测方法，如图1所示，主要由同步量测数据的空间特征提取算法和LCNN攻击检测网络组成。量测数据的空间特征提取算法主要过程为：首先，通过VMD算法提取量测频率数据的本征模态函数（intrinsic mode function，IMF），去除直流分量，获得扰动分量，使用改进离散正交S变换（improved discrete orthonormal Stockwell transform，IDOST）提取各扰动分量中的空间特征，此方式获取的空间特征可在较大程度上提取其空间信息；然后，进入LCNN攻击检测网络，主要通过2层卷积、2层批量标准化（batch normalization，BN）、2层池化和2层全连接，并在第2层全连接层中使用dropout丢弃部分神经元，最后使用softmax分类器进行特征分类。

图1　电网同步量测虚假数据注入攻击检测结构
Fig. 1　Detection architecture of false data injection attack for grid synchronous measurement

1.2　量测数据空间特征提取

为了实现攻击检测方法的高精度获取，需要充分提取同步量测装置在不同位置的空间特征。图1中，源身份欺骗攻击的虚假数据来源于其他同步量测装置，判断数据是否被攻击和识别攻击来源，需要先提取各个量测装置数据的空间特征。采用9个量测位置的数据作为攻击检测的身份识别号，用D_i（$i=1,2,\cdots,9$）表示，其中，i表示量测位置的编号，如附录A图A1所示。D_i的频率曲线存在一个直流分量和扰动分量，粗线表示直流分量，扰动分量为直流分量基础上的小扰动值。假设不同量测位置扰动分量含有该位置的空间信息，作为量测数据网络攻击的检测依据。量测数据空间特征的提取程度决定攻击检测方法的识别精确度，其大小影响特征检测网络的响应速度。因此，如何消除直流分量，获得扰动分量，进一步提取空间特征是实现源身份欺骗攻击检测的重要步骤，以下将主要分析如何通过VMD算法和IDOST实现空间特征提取。

本文从以下2个步骤提取不同量测位置的空间特征：步骤1去除D_i在t时段量测数据$f(t)$的直流分量，提取t时段扰动分量$y(t)$；步骤2通过IDOST算法计算$y(t)$空间特征。

步骤1：提取扰动分量$y(t)$。采取VMD算法[19]将非线性非平稳性的量测数据$f(t)$分解为多个I_τ目标模态，其中，τ为模态数。VMD算法提取量测数据$f(t)$中的I_τ，如式（1）所示。经过计算二次梯度分解得到I_τ，满足如式（2）所示约束条件，并通过引入二次惩罚参数α和Lugrange乘子求解I_τ的约束变分问题的最优解，从而将原始信号$f(t)$分解为多个IMF分量。

$$u_\tau(t)=A_\tau(t)\cos\varphi_\tau(t) \tag{1}$$

式中：$u_\tau(t)$为t时段的模态函数；$A_\tau(t)$为模态分量I_τ在t时段的幅值；$\varphi_\tau(t)$为模态分量I_τ在t时段的相位。

$$\begin{cases}\min\limits_{u_\tau(t),\omega_\tau(t)}\left\{\sum\limits_\tau\left\|\partial_t\left[\left(\delta(t)+\dfrac{\mathrm{j}}{\pi t}\right)u_\tau(t)\right]\mathrm{e}^{-\mathrm{j}\omega_\tau(t)}\right\|_2^2\right\}\\ \text{s.t.}\quad\sum\limits_\tau u_\tau(t)=f(t)\end{cases} \tag{2}$$

式中：∂_t为t的偏导数；$\omega_\tau(t)$为$u_\tau(t)$的频率中心；$\delta(t)$为单位脉冲函数。

通过VMD算法实现对$f(t)$的分解，如附录A图A2(a)所示，采用观察中心频率的方法确定VMD算法的模态数$\tau=6$，即量测数据$f(t)$分解为6个I_τ（$\tau=1,2,\cdots,6$）分量，分别从高频到低频对应不同的频率分量，其中，I_6反映了$f(t)$的整体变化趋势，即直流分量。通过$f(t)-I_6$计算得到扰动分量$y(t)$，如附录A图A2(b)所示。

步骤2：采用IDOST提取扰动分量$y(t)$的空间特征。相比于FFT提取频域信息，S变换（Stockwell transform，ST）[20]能提取$y(t)$在时频域的特征，但ST的冗余表示导致计算效率低下。为克服这一缺点，采用具有有效空间表示的离散正交

S变换(discrete orthonormal Stockwell transform, DOST)[21]计算$y(t)$特征,从而得到量测数据的空间特征。文献[22]提出一种快速算法降低计算复杂度,使得$O(N^2)$的DOST降低至$O(N\log_2 N)$,其中,$O(\cdot)$为复杂度函数,N为扰动分量点数。但此时得到的空间特征矩阵仍含有大量的冗余信息,增加了LCNN检测时间和复杂度,由此提出IDOST,在不损失原有DOST特征矩阵结构的基础上,压缩空间特征矩阵,为小参数的LCNN检测网络提供可能,由此提升网络攻击检测速度。IDOST计算公式如式(3)所示。

$$y_{\mathrm{DS}}(v,q)=\frac{1}{N}\sum_{k=0}^{L-1}y(t_k)D_\beta(t_k;\,v,q) \tag{3}$$

式中:$y_{\mathrm{DS}}(v,q)$为扰动分量函数;t_k为第k个时段;L为$2^{\log_2(N-2)}$;v为频带中心;q为时间定位;β为频带中心v的频带宽度;$D_\beta(t_k;\,v,q)$为正交基函数。

DOST公式如附录A式(A1)和式(A2)所示,推导出某倍频数m下的DOST系数矩阵,如图A3所示。图中:系数矩阵由$\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_m\}$多个矩阵块组成,系数$(v;\,\beta,q)$根据式(A3)和式(A4)计算得到。图A4中,单个矩阵块中的数值均相同,即DOST特征矩阵中同一系数矩阵下的每一列和每一行值相同,这些冗余数据将随着矩阵的增大而增加。多个倍频数下的标准正交基函数下的系数矩阵组成如图A4(a)所示的DOST特征矩阵,为实现小参数的LCNN检测网络,可压缩特征矩阵。

在不损失原有DOST特征矩阵结构的基础上,提出IDOST算压缩空间特征,实现步骤如下:

步骤1:根据对称性压缩矩阵大小。文献[22]提出实信号的正频带p和负频带$-p$的基函数共轭对称,将$v=v+0.5$代入附录A式(A2),如式(4)所示。根据对称性,此时$y(t)$空间特征矩阵的大小为$N/2\times N$。

$$\begin{cases} D_\beta(t_k;\,v,q)=\mathrm{j}\mathrm{e}^{-\mathrm{j}\pi q}\dfrac{\mathrm{e}^{-\mathrm{j}2\alpha\left(v-\frac{\beta}{2}\right)}-\mathrm{e}^{-\mathrm{j}2\alpha\left(v+\frac{\beta}{2}\right)}}{2\sqrt{\beta}\sin\alpha} \\ \alpha=\pi\left(\dfrac{k}{N}-\dfrac{q}{\beta}\right) \end{cases} \tag{4}$$

$$\begin{cases} D_\beta(t_k;\,v,q)=1 & m=0 \\ D_\beta(t_k;\,v,q)=\mathrm{e}^{\frac{-\mathrm{j}2k\pi}{N}} & m=1 \\ v=2^{(m-1)}+2^{(m-2)} & m=2,3,\cdots,\log_2(N-1) \\ \beta=2^{(m-1)} & m=2,3,\cdots,\log_2(N-1) \\ q=0,1,\cdots,\beta-1 & m=2,3,\cdots,\log_2(N-1) \end{cases} \tag{5}$$

步骤2:去除重复特征点。由附录A式(A3)推导出图A4(a)特征矩阵的最小行数为1,最小列数为N/β,可进一步减小最小列数,重新组成DOST空间特征矩阵,如图2所示。

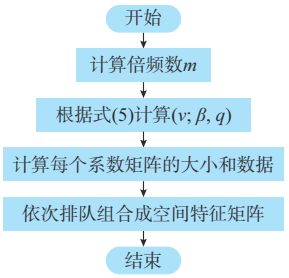

图2　IDOST空间特征矩阵流程图
Fig. 2　Flow chart of IDOST spatial feature matrix

IDOST空间特征矩阵示意图如附录A图4(b)所示。通过式(5)可计算系数$(v;\,\beta,q)$,此时,在倍频数m下的系数矩阵大小为$\beta\times L/\beta$,空间特征矩阵大小为$N/2\times 2^{\log_2(N-2)}$。当$m=0$和$m=\log_2(N-1)$时,IDOST空间特征矩阵的系数矩阵中最小行数和列数均为1,系数矩阵中所有列均减小为原来的N/β,且均为重复信息,不损失原DOST系数矩阵特征,如图A5(d)所示。当$N=256$时,对比压缩前后的特征如图A5(c)和图A5(d)所示。此时,DOST输入的扰动分量为实信号,正频带和负频带对称,图A5(c)为DOST特征矩阵上半部分,IDOST空间特征矩阵不会损失和破坏原DOST特征矩阵信息和结构。

扰动分量$y(t)$中t值的合理选取对于LCNN中网络层数和每层中卷积核个数十分重要。当$t=N$时,N值过大,网络层数和卷积核个数增加,加深网络复杂度和增大网络参数;N值过小,特征信息不足,网络难以学习。以下将探寻N值的合理选取。DOST输入向量或矩阵需满足$N=2^\kappa$,其中,κ为正整数,因此,讨论N为128、256和512时,经过IDOST计算$y(t)$的空间特征矩阵信息,并将不同N值的空间特征矩阵代入卷积神经网络中分析其检测精度值。如附录A图A5所示,$N=128$时,特征矩阵大小为64×32,信息较少,网络不足以分析;$N=512$时,特征矩阵大小为256×128,包含的特征信息更多,需要增加卷积核个数,以达到一定的检测精确度;$N=256$时,矩阵大小为128×64,此时,网络层数为2,卷积核大小相较于$N=512$时可以进一步减小,且检测精确度不变。综上,考虑LCNN参数和IDOST输入要求,选取$N=256$。

1.3　LCNN检测空间特征

为了实现欺骗攻击的检测，需要一种空间特征检测算法。本文提出一种小参数量LCNN空间特征检测算法，压缩空间特征矩阵，从输入端减小检测算法的计算压力；通过分析扰动分量$y(t)$中t值的合理选取，探索检测算法的网络层数，从结构上减小算法复杂度。LCNN模型主要由2层卷积、2层BN、2层池化和2层全连接组成，用于学习和识别量测数据的空间特征。

1）卷积层-BN层-池化层

LCNN单个卷积层中将空间特征作为输入信号x，以卷积的形式获取不同空间特征中所含信息，如式(6)所示。此时的卷积输出特征如附录A图A6的卷积层1和2所示。

$$Z_{C,n}=g(w_n*x+b_n) \tag{6}$$

式中：$Z_{C,n}$为第n个滤波器核的卷积输出特征；w_n为第n个滤波器核的权值；b_n为第n个滤波器核的偏置项；*为一维卷积运算符号；$g(\cdot)$为激活函数；x为输入信号。

由附录A图A6可知，通过卷积层1之后的效果并不明显，但增加BN层，使每层神经网络的输入保持相同分布，减小空间特征的变化值，经标准化后，卷积层之后的特征更接近输入的空间特征，标准化如式(7)所示。输出$Z_{B,n}$通过γ与β的线性变换得到新的值，如式(8)所示。

$$\sigma^2=\frac{1}{\varpi}\sum_{n=1}^{\varpi}\left(Z_{C,n}-\frac{1}{\varpi}\sum_{n=1}^{\varpi}Z_{C,n}\right)^2 \tag{7}$$

$$Z_{B,n}=\gamma\frac{Z_{C,n}-\frac{1}{\varpi}\sum_{n=1}^{\varpi}Z_{C,n}}{\sqrt{\sigma^2+\varepsilon}}+\partial \tag{8}$$

式中：ϖ为滤波器核的数量；ε为常量；σ^2为方差；γ、∂为训练参数。

在BN层之后，LCNN的结构中设置一个最大池化层，如附录A图A6池化层1和2所示。此时，提取的特征和输入的空间特征不再相似，为深层特征信息。池化层通过以固定的步幅滑动来选择$Z_{B,n}$特定区域η中的最大值，池化层1和2为2×2的最大池化下采样，即沿空间特征的高度和宽度均向下采样2个步长，丢弃75%激活神经，减小网络参数和计算量，控制LCNN过拟合。最大池化层的输出$Z_{P,n}$可以表示为：

$$Z_{P,n}=\max_{T\in[jw,jw+\eta]}\{Z_{B,n}\} \tag{9}$$

式中：w为池化区域的宽度；T为区域η的序列集。

2）全连接层1和2

利用全连接层来处理多维结构的高级特征，连接前一层中所有的激活神经，实现攻击检测。设置Z_f为全连接层1的输出，在最后一层全连接层2中，使用softmax分类器对学习到的不同量测位置的空间特征进行分类，softmax分类器的输出定义为：

$$p(y=\rho|Z_f)=\frac{e^{z_f}}{\sum_{\xi=1}^{\rho}e^{z_f}} \tag{10}$$

式中：y为输出类；ρ为空间特征类的个数。

通过以上步骤，LCNN学习到不同量测位置的空间特征，特征层的可视化如附录A图A6所示，每一列表示单个样本在不同特征层的训练结果。

LCNN具体参数设计如附录A表A1所示，LCNN总参数量为2 109 108个，每个参数为32位浮点数，由此可以计算出模型所占系统内存空间约为7.7 MB。相比于CNN经典模型如Inception-v3、AlexNet和VGG16，其模型内存空间分别约为100、200、500 MB，需要消耗更多计算资源。

2　网络攻击检测方法测试

2.1　量测数据集测试

为验证攻击检测的准确性，使用WAMS中某9个不同量测位置的频率数据集作为数据库，每个数据集采样率为10 Hz，采样时间为100 min，采样点数为60 000个。此时，电网同步量测数据来源于电网正常运行状态，当电网中出现多次短路、断路或者振荡等情况需要进一步收集数据。选取数据库中各数据集前90%数据为训练集，10%为测试集，单个样本点数为256，不同样本之间相隔80点。由此，训练集样本数为6 075，测试集样本数为675，测试集中不同位置的量测数据相混合。附录A图A7表示9个电网同步量测装置的相对地理位置。

创建不同攻击率下的虚假混合数据。假定某测试集，用D_j表示($j=1,2,\cdots,n$)，在某时段被D_i($i\neq j,i=1,2,\cdots,n$)攻击或者被任意篡改，攻击时间长短和位置不定，如附录A图A8所示。图中：实线表示D_j原量测数据，中间虚线表示D_i攻击数据，A点表示D_i攻击开始位置，从A点开始，D_i数据被攻击，到B点攻击停止。调整B点位置，可得到测试集在不同源身份欺骗攻击率下的虚假混合数据攻击样本测试集。验证测试集在不同攻击率下的攻击检测精确度，测试集中不同D_i的测试样本数为75，样本攻击率指单个测试集中攻击样本占样本数的比例，可以分为D_i($i=1,2,\cdots,9$)的0%攻击率(正常信号)和非0%攻击率，其中，非0%攻击率包括攻击率为4%、8%、20%、40%和80%的情况。

2.2　虚假混合数据网络攻击测试集验证分析

在同一量测数据集下，对比不同数据特征提取方法和特征检测网络，验证所提出的攻击检测方法。当测试集为0%攻击率（正常信号）和非0%攻击率时，6种不同算法的测试精确度和算法各个部分的测试时间如表1所示。

表1　算法性能比较

Table 1　Performance comparison of algorithms

方法	算法名称	0%攻击率精确度/%	非0%攻击率精确度/%	时间/ms
1	FFT-DBN[23]	89.56	84.68	9.90
2	FFT-LCNN	90.89	85.63	10.87
3	VMD-DOST-LCNN	93.63	88.72	113.31
4	VMD-IDOST-DBN	91.48	86.48	52.80
5	VMD-IDOST-SAE	91.85	85.71	53.30
6	VMD-IDOST-LCNN	94.96	89.01	54.20

首先，对比表1中不同方法的测试精确度。表1中特征提取为FFT的方法1和2，在相同FFT参数下，LCNN检测网络精度高于深度置信网络（deep blief network，DBN）；对比方法3和6，在相同VMD算法和LCNN参数条件下，对比DOST和IDOST算法，说明IDOST实现空间特征矩阵压缩，保证检测算法精确度，检测时间缩短约50%；进一步对比采用同参数的VMD-IDOST提取数据特征，特征检测网络模型为DBN、堆叠自编码器（stacked auto-encoder，SAE）和LCNN，如表1中方法4至方法6，LCNN在不同场景下检测精确度最高。

其次，对比表1中不同方法的检测时间。从表1中可知，单个数据源检测时间最短为方法1，但精确度最低；方法6检测时间最长，但此时单个测试样本的测试时间满足实时性要求，且检测精确度最高；对比方法1、2和6，方法6通过IDOST空间特征提取，检测精度提高4%以上；方法4、5和6的测试时间相隔不到2 ms，但方法6通过采用LCNN，检测精确在0%攻击率和非0%攻击率下分别达到94.96%和89.01%，精度相对较高。综合考虑，选定方法6实现攻击检测，其网络结构为方法6的VMD-IDOST-LCNN。

为验证攻击检测方法的特征提取能力，采用t分布邻域嵌入（t-distributed stochastic neighbor embedding，t-SNE）算法将全连接层2中激活函数之前的特征层和测试集数据输入t-SNE函数中，并降维到三维空间实现可视化，得到测试集数据的三维t-SNE图，如附录A图A9所示。0%攻击率量测数据特征识别的可视化结果如图A9(a)所示，同一地点下的正常量测数据的特征单一聚合。当量测数据遭受源身份欺骗攻击时，攻击检测方法的特征提取能力如图A9(b)所示，同一数据集下量测数据的数据特征包含虚假混合数据网络攻击数据和正常数据特征。由此可以得出混合输入的测试集样本在经过空间特征提取和LCNN学习后，同一特征聚集，不同量测数据特征可明显区分。

当测试集攻击率为40%时，如附录A图A9(b)所示，4个地点被源身份欺骗攻击，其攻击检测结果如图A10所示。虚线框内表示为虚假混合数据网络攻击的攻击区域，虚线框外为正常数据样本，当攻击检测方法在测试集攻击率为40%时，能准确识别网络攻击，此时测试集的精确度为88.89%。

验证D_i(i=1，2，…，9)在0%攻击率（正常信号）和非0%攻击率时攻击检测的精确度。如图3所示，最上方的两条曲线分别为D_i在0%攻击率检测精确度和非0%攻击率的平均检测精确度的变化趋势。对比2条曲线可以看出，在非0%攻击率下，测试集的平均检测精确度低于0%攻击率值，平均下降5.00%，前者稳定在89.01%，后者为94.81%，两条曲线的变化趋势相同，且均存在一个最低点D_2，分别为79.20%和82.67%，攻击检测方法对D_2的攻击检测识别较弱。各个D_i非0%攻击率的差值如图3所示，其中，检测精确度差值最大为4.00%，最小为1.33%。由此可以分析，在不同攻击率下，攻击检测方法都能有效识别，小图中红色纵向线上的绿色节点表示非0%攻击率下不同攻击率的平均精确度值，根据平均精确度可判别D_6和D_9精确度最高为95.20%，D_2最低为79.20%，其他均高于84.00%，平均精确度稳定在89.01%。

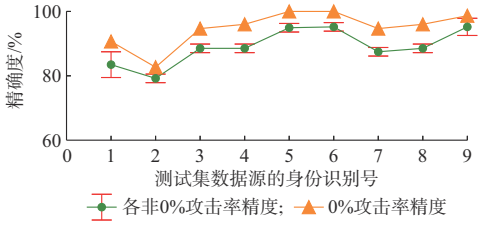

图3　不同攻击率下的测试集精度

Fig. 3　Accuracy of test set with different attack rates

3　结语

本文针对在WAMS中电网同步量测装置遭受虚假数据注入攻击问题，提出一种基于空间特征的电网同步量测数据检测方法，实现快速、多数据源的源身份欺骗攻击检测。所提方法具备以下3个方面特点：1）为提高攻击检测精度，采用空间特征提取算法，多点空间特征的三维t-SNE可视化图表明，算法可充分提取多点量测数据的空间位置信息；2）为提

高攻击检测算法响应速度，使用IDOST得到压缩空间特征，并结合小参数量、低复杂度的LCNN特征检测算法，通过多种攻击检测算法比较表明，能在提高精确度的同时保障检测速度；3）通过实测频率数据表明，攻击检测方法能快速且精准地识别量测数据是否遭受虚假数据注入攻击。本文电网同步量测数据来源于电网正常运行状态，当电网中出现多次短路、断路和振荡等情况时，是否能精确提取其空间特征需要进一步的收集数据并分析。本文主要提出一种针对源身份欺骗网络攻击的检测算法，未来可进一步结合电力系统控制策略，保障系统在虚假数据注入攻击下的稳定运行。

附录见本刊网络版（http://www.aeps-info.com/aeps/ch/index.aspx），扫英文摘要后二维码可以阅读网络全文。

参 考 文 献

[1] 杨挺，翟峰，赵英杰，等.泛在电力物联网释义与研究展望[J].电力系统自动化，2019，43(13)：9-20.
YANG Ting, ZHAI Feng, ZHAO Yingjie, et al. Explanation and prospect of ubiquitous electric power Internet of Things[J]. Automation of Electric Power Systems, 2019, 43(13): 9-20.

[2] 徐飞阳，薛安成，常乃超，等.电力系统自动发电控制网络攻击与防御研究现状与展望[J].电力系统自动化，2021，45(3)：3-14.
XU Feiyang, XUE Ancheng, CHANG Naichao, et al. Research status and prospect of cyber attack and defense on automatic generation control in power system[J]. Automation of Electric Power Systems, 2021, 45(3): 3-14.

[3] 周元刚，刘绚，张波.基于多阶段传输的智能变电站安全通信策略[J].电力系统自动化，2021，45(22)：105-114.
ZHOU Yuangang, LIU Xuan, ZHANG Bo. Security communication strategy for smart substation based on multi-stage transmission[J]. Automation of Electric Power Systems, 2021, 45(22): 105-114.

[4] 赵俊华，梁高琪，文福拴，等.乌克兰事件的启示：防范针对电网的虚假数据注入攻击[J].电力系统自动化，2016，40(7)：149-151.
ZHAO Junhua, LIANG Gaoqi, WEN Fushuan, et al. Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks[J]. Automation of Electric Power Systems, 2016, 40(7): 149-151.

[5] IEEE standard for synchrophasor data transfer for power systems: IEEE C37.118.2—2011[S]. Institute of Electrical and Electronics Engineers, 2011.

[6] 国家质量监督检验检疫总局，中国国家标准化管理委员会.电力系统实时动态监测系统第2部分：数据传输协议：GB/T 26865.2—2011[S].北京：中国标准出版社，2011.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China. Real-time dynamic monitoring systems of power system: Part 2 protocols for data transferring: GB/T 26865.2—2011 [S]. Beijing: Standards Press of China, 2011.

[7] 王琦，李梦雅，汤奕，等.电力信息物理系统网络攻击与防御研究综述（一）建模与评估[J].电力系统自动化，2019，43(9)：9-21.
WANG Qi, LI Mengya, TANG Yi, et al. A review on research of cyber-attacks and defense in cyber physical power systems: Part one modelling and evaluation[J]. Automation of Electric Power Systems, 2019, 43(9): 9-21.

[8] 汤奕，李梦雅，王琦，等.电力信息物理系统网络攻击与防御研究综述（二）检测与保护[J].电力系统自动化，2019，43(10)：1-9.
TANG Yi, LI Mengya, WANG Qi, et al. A review on research of cyber-attacks and defense in cyber physical power systems: Part two detection and protection[J]. Automation of Electric Power Systems, 2019, 43(10): 1-9.

[9] CUI Y, BAI F F, LIU Y L, et al. Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5807-5818.

[10] GARG R, HAJJ-AHMAD A, WU M. Geo-location estimation from electrical network frequency signals[C]// 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, May 26-31, 2013, Vancouver, Canada: 2862-2866.

[11] HAJJ-AHMAD A, GARG R, WU M. ENF-based region-of-recording identification for media signals [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1125-1136.

[12] YAO W X, ZHAO J C, TILL M J, et al. Source location identification of distribution-level electric network frequency signals at multiple geographic scales[J]. IEEE Access, 2017, 5: 11166-11175.

[13] CUI Y, LIU Y L, FUHR P, et al. Exploiting spatial signatures of power ENF signal for measurement source authentication[C]// 2018 IEEE International Symposium on Technologies for Homeland Security, October 23-24, 2018, Woburn, USA.

[14] QIU W, TANG Q, ZHU K Z, et al. Cyber spoofing detection for grid distributed synchrophasor using dynamic dual-kernel SVM[J]. IEEE Transactions on Smart Grid, 2021, 12(3): 2732-2735.

[15] QIU W, TANG Q, ZHU K Z, et al. Detection of synchrophasor false data injection attack using feature interactive network[J]. IEEE Transactions on Smart Grid, 2021, 12(1): 659-670.

[16] 孙凯祺，邱伟，李可军，等.面向快速频率响应系统的网络攻击防御控制策略[J].中国电机工程学报，2021，41(16)：5476-5486.
SUN Kaiqi, QIU Wei, LI Kejun, et al. Cyber attack defense control for fast frequency response system[J]. Proceedings of the CSEE, 2021, 41(16): 5476-5486.

[17] 李扬，李智，陈亮，等.发电机动态状态估计中的一种虚假数据注入攻击方法[J].电工技术学报，2020，35(7)：1476-1488.
LI Yang, LI Zhi, CHEN Liang, et al. A false data injection attack method for generator dynamic state estimation [J]. Transactions of China Electrotechnical Society, 2020, 35(7):

1476-1488.
[18] LIU S Y, YOU S T, YIN H, et al. Model-free data authentication for cyber security in power systems[J]. IEEE Transactions on Smart Grid, 2020, 11(5): 4565-4568.
[19] DRAGOMIRETSKIY K, ZOSSO D. Variational mode decomposition[J]. IEEE Transactions on Signal Processing, 2014, 62(3): 531-544.
[20] STOCKWELL R G, MANSINHA L, LOWE R P. Localization of the complex spectrum: the S transform[J]. IEEE Transactions on Signal Processing, 1996, 44(4): 998-1001.
[21] STOCKWELL R G. A basis for efficient representation of the S-transform[J]. Digital Signal Processing, 2007, 17(1): 371-393.
[22] WANG Y W, ORCHARD J. Fast discrete orthonormal Stockwell transform[J]. SIAM Journal on Scientific Computing, 2009, 31(5): 4000-4012.
[23] 李海平,齐卓砾,胡君朋.基于FFT-DBN的行星齿轮箱齿面磨损故障智能判定方法研究[J].测控技术,2020,39(12):50-54.
LI Haiping, QI Zhuoli, HU Junpeng. Intelligent judgment of tooth wear fault problems for planetary gearbox based on FFT-DBN[J]. Measurement & Control Technology, 2020, 39(12): 50-54.

郑 瑶(1995—),女,博士,主要研究方向:同步相量网络安全和电力系统分析。E-mail:ggbondqie@hnu.edu.cn
张 颉(1983—),男,博士,主要研究方向:电网数字化、人工智能、电力北斗、5G和数字孪生等。E-mail:18161273371@163.com
姚文轩(1988—),男,通信作者,教授,博士生导师,主要研究方向:智能电网、广域同步相量测量技术与应用、电能质量监控。E-mail:wenxuanyao@hnu.edu.cn

(编辑 杨松迎)

Spatial Feature Based Detection of False Data Injection Attack on Synchronous Grid Measurements

ZHENG Yao[1], *ZHANG Jie*[2], *YAO Wenxuan*[1], *QIU Wei*[1], *TANG Sihao*[1]
(1. College of Electrical and Information Engineering, Hunan University, Changsha 410082, China;
2. Power Internet of Things Key Laboratory of Sichuan Province, Chengdu 610041, China)

Abstract: As the power system gradually moves toward a new ecosystem of energy interconnection and the deep coupling of the network layer and physical layer, the threat of network attacks on the power system keeps rising. The source identity (ID) spoofing attack, as a new and complex, strong stealthy false data injection attack, can cause the grid control system to misjudge and cause system paralysis. To address this problem, a spatial feature based method is proposed for detecting false data injection attacks on synchronous measurements of power grids. It has extracted different spatial features of the synchronous measurement devices at different locations by variational modal decomposition (VMD) and improved discrete orthonormal Stockwell transform (IDOST), so as to extract the authentication information of the measurement data without losing the spatial features of the measurements. Combined with the light convolutional neural network (LCNN) to evaluate the likelihood of measurement data being attacked by source ID to enhance the speed of detection response. The effectiveness of the method is verified by the detection results of actual multi-point synchronous measurement data.

This work is supported by National Natural Science Foundation of China (No. 52177078), Hunan Provincial Natural Science Foundation Project of China (No. 2022JJ30151), Power Internet of Things Key Laboratory of Sichuan Province Open Subject Project of China (No. PIT-F-202201) and China Postdoctoral Science Foundation (No. BX20220102).

Key words: wide area measurement system; synchronous measurement data; false data injection attack; convolutional neural network