DOI:10.13878/j.cnki.jnuist.20220913006

戚梦逸[1]　刘涅煊[1]　陶晓峰[1]　吕朋朋[1]

基于相量测量的状态估计攻击检测方法

摘要

针对电力系统中基于相量测量技术状态估计的虚假数据注入攻击难以被成功检测的问题,本文提出一种面向电力系统线性状态估计的攻击智能检测方法.采用自编码器对电网测量数据进行多次特征提取,逐渐降低特征维度;提取信息通过 softmax 层进行有监督学习,从而得到基于堆叠自编码器的攻击检测算法.针对自编码器的过度拟合问题,进一步提出基于降噪自编码的攻击检测方法.采用 IEEE-118 节点测试系统对所提出的方法进行仿真验证,结果表明所提出的攻击检测方法计算精度和效率高于其他方法.

关键词

自编码器;相量测量;状态估计;攻击检测

中图分类号 TM743

文献标志码 A

0　引言

随着现代信息技术在智能电网中的广泛应用,针对电网的恶意信息攻击严重威胁着电网的安全运行.电网的状态监测和数据采集系统是信息攻击的主要对象.黑客在测量设备或者信息传送通道注入错误信息,从而导致调度中心数据库发生错误,影响电力系统的安全运行.

文献[1]分析了信息攻击风险在模型中的传播机制,并定量推演了信息流交互对电网运行状态的影响;文献[2]通过分析信息攻击下配电网控制系统信息空间与物理空间的风险传递作用,提出一种信息物理风险传递模型.尽管电力系统调度中心状态估计能够对不良数据进行检测[3],当黑客发起信息攻击,状态估计的不良数据检测将会检测到该信息攻击,从而将数据进行剔除或修正,然而,虚假数据注入攻击[4]则不会被检测到,从而对电力系统安全运行造成影响.通过假设黑客能够获取完整的电网拓扑结构和参数,针对电力系统状态估计的虚假数据注入攻击得以实施[5].文献[6]提出一种基于数据驱动的稀疏虚假数据注入攻击策略,从而在异常值情况下成功实施稀疏虚假数据注入攻击.

除了信息攻击方法外,虚假数据注入攻击检测方法也成为学者们的研究热点.例如:文献[7]提出一种基于博弈论的关键测量设备的分阶段动态虚假数据注入攻击防御方法;文献[8]提出一种基于聚类算法与状态预测检测法的虚假数据注入攻击检测技术;文献[9]基于时序近邻保持嵌入方法,在提取局部空间结构特征的基础上,同时获得与时间相关的动态特征,从而有效检测虚假数据注入攻击;文献[10]提出一种基于极端梯度提升结合无迹卡尔曼滤波的电网虚假数据注入攻击检测方法,进而检测与修正虚假数据注入攻击.为保证虚假数据注入攻击在电网运行中能被高效实时检测,文献[11]提出一种面向监视控制与数据采集和相量测量单元混合量测的智能电网恶性数据在线防御方法.

此外,随着人工智能技术[12]的快速发展,基于数据驱动的信息攻击检测方法也随之出现.例如:文献[13]引入自注意力机制计算各时间步隐状态的线性加权和作为量测序列的深层特征,进而提出一种基于双向门控循环单元和自注意力的检测方法;文献[14]基于云自适应粒子群优化脉冲神经网络构建配电网伪量测模型对虚假数据注

收稿日期 2022-09-13

资助项目 国家自然科学基金(62105160)

作者简介

戚梦逸,男,工程师,主要研究方向为电力计量等.1561994323@qq.com

1　南瑞集团有限公司(国网电力科学研究院有限公司),南京,211106

入攻击进行辨识.自编码器[15]是解决攻击检测问题的一个有效途径.自编码器采用无监督学习方式提取数据特征,引起了众多学者的关注[16].文献[17]为了消除积雪覆盖时空变化研究中云遮挡的影响,构建了一种降噪自编码神经网络模型,实现云下积雪参数的补全,提高了积雪产品的覆盖面积;文献[18]对于直流线性模型,设计了数据驱动的编、解码方案,构建了基于编码策略的虚假数据攻击检测方法;文献[19]将自编码器成功应用于仅含有少量标签测量数据的虚假数据注入攻击检测中.针对单层自编码器无法提取原始数据中全部信息的问题,可以将多个自编码器组合在一起,上一级自编码器的输出作为下一级的输入,进而形成堆叠自编码器.

本文提出一种数据驱动的面向智能电网相量测量状态估计攻击检测方法.该方法将多个自编码器结合在一起,逐级提取原始测量数据的特征,进而形成堆叠自编码器.利用大量历史数据对堆叠自编码器进行训练,训练后的堆叠自编码器可以用于电力系统信息攻击检测.先对原始测量数据进行拓扑错误和不良数据检测与辨识,再将检测后的测量数据作为堆叠自编码器的输入进行计算,从而得到信息攻击检测结果.

1 电力系统线性状态估计

状态估计是电力系统调度中心能量管理系统的重要组成部分.当前电网中采用的状态估计均为非线性状态估计.随着相量测量技术的发展,母线电压和线路电流相量可以直接测量,因此,线性状态估计成为可能.

1.1 测量方程

电力系统的线路模型通常采用 π 型等值电路,如图 1 所示.

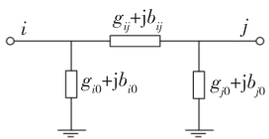

图 1 线路 π 型等值电路

Fig. 1 Line π equivalent circuit

相量测量系统能够直接对支路电流相量进行测量.由线路的 π 型等值电路可以得到支路电流实部和虚部与母线电压相量之间的线性方程:

$$\begin{bmatrix} I_{ij,\mathrm{r}} \\ I_{ij,\mathrm{i}} \end{bmatrix} = \begin{bmatrix} g_{ij}+g_{i0} & -(b_{ij}+b_{i0}) & -g_{ij} & b_{ij} \\ b_{ij}+b_{i0} & g_{ij}+g_{i0} & -b_{ij} & -g_{ij} \end{bmatrix} \begin{bmatrix} e_i \\ f_i \\ e_j \\ f_j \end{bmatrix}, \tag{1}$$

其中:$I_{ij,\mathrm{r}}$ 和 $I_{ij,\mathrm{i}}$ 分别为支路 ij 电流的实部和虚部;g_{ij} 和 b_{ij} 分别为支路 ij 的电导和电纳;g_{i0} 和 b_{i0} 分别为母线 i 对地电导和电纳;e_i 和 f_i 分别为母线 i 的电压实部和虚部;e_j 和 f_j 分别为母线 j 的电压实部和虚部.智能电网中相量测量系统除了能够对支路电流相量进行直接测量,还可以对母线电压相量和节点注入电流相量进行直接测量.因此,线性状态估计的测量量包括节点电压、支路电流和注入电流的实部和虚部.测量量 $\boldsymbol{z}$ 与状态量 $\boldsymbol{x}$ 之间的线性关系可表示为

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{v}, \tag{2}$$

其中:$\boldsymbol{z}$ 为测量向量,$\boldsymbol{z} = [(\boldsymbol{z}_{\mathrm{U}})^{\mathrm{T}}(\boldsymbol{z}_{\mathrm{B}})^{\mathrm{T}}(\boldsymbol{z}_{\mathrm{IN}})^{\mathrm{T}}]^{\mathrm{T}}$,$\boldsymbol{z}_{\mathrm{U}} = [\cdots z_{e_i} z_{f_i} \cdots]^{\mathrm{T}}$,$\boldsymbol{z}_{\mathrm{B}} = [\cdots z_{\mathrm{Br}ij} z_{\mathrm{BI}ij} \cdots]^{\mathrm{T}}$,$\boldsymbol{z}_{\mathrm{IN}} = [\cdots z_{\mathrm{Ir}i} z_{\mathrm{II}i} \cdots]^{\mathrm{T}}$.$\boldsymbol{z}_{\mathrm{U}}$,$\boldsymbol{z}_{\mathrm{B}}$ 和 $\boldsymbol{z}_{\mathrm{IN}}$ 分别为节点电压、支路电流和注入电流相量的测量向量;z_{e_i} 和 z_{f_i} 分别为母线 i 电压实部和虚部的测量值;$z_{\mathrm{Br}ij}$ 和 $z_{\mathrm{BI}ij}$ 分别为支路 ij 电流的实部和虚部测量值;$z_{\mathrm{Ir}i} z_{\mathrm{II}i}$ 分别为母线 i 注入电流实部和虚部的测量值.$\boldsymbol{x}$ 为状态向量,$\boldsymbol{x} = [\cdots \quad e_i f_i e_j f_j \quad \cdots]^{\mathrm{T}}$;$\boldsymbol{v}$ 为测量误差向量,$\boldsymbol{v}$ 服从均值为 0 方差为 σ^2 的高斯分布;$\boldsymbol{H}$ 为测量矩阵.

1.2 线性状态估计

加权最小二乘状态估计的基本原理是使得测量量的误差加权平方和最小.由于测量方程为线性方程,因此,采用加权最小二乘进行状态估计无需迭代计算.线性状态估计的目标函数为

$$J(\boldsymbol{x}) = [\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x}]^{\mathrm{T}} \boldsymbol{R}^{-1} [\boldsymbol{z} - \boldsymbol{H}\boldsymbol{x}], \tag{3}$$

式中:J 为目标函数;$\boldsymbol{R}$ 为对角矩阵,第 i 个对角元素为 $1/\sigma_i^2$,σ_i 为第 i 个测量量的测量误差标准差.则状态量的估计值 $\hat{\boldsymbol{x}}$ 为

$$\hat{\boldsymbol{x}} = [\boldsymbol{H}^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{H}]^{-1} \boldsymbol{H}^{\mathrm{T}} \boldsymbol{R}^{-1} \boldsymbol{z}. \tag{4}$$

由于数据采集和传输过程中受到干扰,相量测量系统不可避免存在不良数据.为了避免坏数据对状态估计结果造成较大误差,在得到状态量估计值后还需要进行不良数据检测.将估计结果 $\hat{\boldsymbol{x}}$ 带入目标函数,计算目标函数值 $\hat{J} = (\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}})^{\mathrm{T}} \boldsymbol{R}^{-1} (\boldsymbol{z} - \boldsymbol{H}\hat{\boldsymbol{x}})$,当存在不良数据情况时,则 $\hat{J}$ 较大.因此,可以设定阈值 ε,当测量数据不含有不良数据情况时,状态估计

目标函数小于 ε，当存在不良数据时，则会大于 ε. 由此可以进行不良数据检测.若存在不良数据则需要通过不良数据辨识依次将不良数据剔除.

2 面向线性状态估计的信息攻击

黑客通过其所获取的电网拓扑和参数信息，将特定的攻击数据注入测量量，对原有测量数据进行篡改，使得状态估计结果偏离真实值.与不良数据不同，攻击数据能够使得估计结果的目标函数小于设定的阈值 ε，从而躲过状态估计的不良数据检测而不被发现.假设黑客能够获取电网拓扑信息以及线路参数，根据如下规则生成攻击向量 $\boldsymbol{a}$：

$$\boldsymbol{a}=\boldsymbol{Hc}, \tag{5}$$

其中，$\boldsymbol{c}$ 为无攻击和有攻击情况下状态量估计值的偏差，即信息攻击后状态估计得到的状态量估计值 $\hat{\boldsymbol{x}}_c=\hat{\boldsymbol{x}}+\boldsymbol{c}$.信息攻击后的测量向量为 $\boldsymbol{z}_a=\boldsymbol{z}+\boldsymbol{a}$.此时，无攻击和有攻击两种情况下测量向量的估计残差的差值为

$$\hat{\boldsymbol{r}}_a-\hat{\boldsymbol{r}}=\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}\hat{\boldsymbol{x}}-\boldsymbol{Hc}-\boldsymbol{z}+\boldsymbol{H}\hat{\boldsymbol{x}}=\boldsymbol{a}-\boldsymbol{Hc}, \tag{6}$$

式中，$\hat{\boldsymbol{r}}_a$ 为被攻击测量量残差.由于攻击向量 $\boldsymbol{a}=\boldsymbol{Hc}$，所以式(6)中估计残差的差值为0.这表明当攻击向量 $\boldsymbol{a}=\boldsymbol{Hc}$ 时，信息攻击能够躲过不良数据检测.基于上述攻击方法，黑客可以通过篡改电网数据采集系统中的数据 $\boldsymbol{z}$，将其修改为 $\boldsymbol{z}_a=\boldsymbol{z}+\boldsymbol{a}$. 电力系统调度中心的状态估计程序无法检测到该攻击行为，从而得到错误的状态估计结果，对电网安全运行造成威胁.

3 攻击检测

由于电网状态估计无法检测虚假数据注入攻击，为了确保电网的安全稳定运行，需要通过攻击检测算法对测量数据进行检测，判断是否受到攻击.自编码器是一种典型的分类算法，能够通过提取测量量中的特征信息判断测量量是否受到攻击.

自编码器是一种无监督学习神经网络，由编码器和解码器两部分组成.最简单的自编码器有 3 层结构，编码器将输入进行编码，变为中间结果，中间结果再经过解码器还原为原始输入.这样处理的目的是将输入量进行降维，用更少的特征表征隐含在输入中的数据.编码器对输入量进行降维特征提取，该特征向量再作为解码器的输入，如图 2 所示. $\boldsymbol{z}$ 为测量向量，作为自编码器的输入量；$\boldsymbol{y}$ 为 $\boldsymbol{z}$ 的降维特征向量，输出向量 $\tilde{\boldsymbol{z}}$ 为原始输入量 $\boldsymbol{z}$ 的重构.自编码器通常有如下 4 种应用：降维、特征检测、生成与训练数据类似的数据、数据压缩.

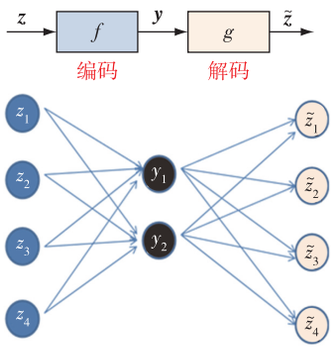

图 2 编码器原理

Fig. 2 Encoder principle

自编码器的目标是使得输出向量最大程度上还原原始输入，因此，训练过程的损失函数 J_a 为

$$J_a=\arg\min\|\boldsymbol{z}-\tilde{\boldsymbol{z}}\|^2. \tag{7}$$

编码器和解码器的激活函数分别为

$$\boldsymbol{y}=f(\boldsymbol{z})=\boldsymbol{W}_1\boldsymbol{z}+\boldsymbol{b}_1, \tag{8}$$

$$\tilde{\boldsymbol{z}}=g(\boldsymbol{y})=\boldsymbol{W}_2\boldsymbol{y}+\boldsymbol{b}_2, \tag{9}$$

式中：f 和 g 分别为编码器和解码器的激活函数；$\boldsymbol{W}_1$ 和 $\boldsymbol{W}_2$ 为权重矩阵；$\boldsymbol{b}_1$ 和 $\boldsymbol{b}_2$ 为偏置向量.

电网的测量量中往往含有随机噪声，为了避免随机噪声对编码器造成影响以及过拟合问题，需要对自编码器进行降噪处理，使其具有鲁棒性，进而得到基于降噪自编码器的电力系统信息攻击检测方法.为了防止自编码器的过度拟合问题，训练过程中在输入数据 $\boldsymbol{z}$ 的基础上加入噪声，使得编码器具有一定的鲁棒性，进而加强模型的泛化能力，即降噪自编码器.降噪自编码的训练过程如图 3 所示.

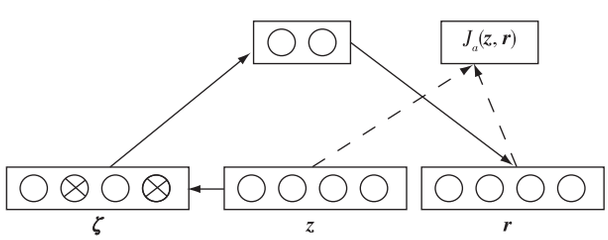

图 3 降噪自编码

Fig. 3 Denoising autoencoder

降噪自编码器在训练之前需要在输入量 $\boldsymbol{z}$ 上以一定的概率将其中的元素置零，从而构造出含有噪声的输入量 $\boldsymbol{\zeta}$.然后将 $\boldsymbol{\zeta}$ 作为编码器的输入进行解码和编码.将重构数据 $\boldsymbol{r}$ 与原始数据 $\boldsymbol{z}$ 进行误差迭代计算，这样训练得到的编码器就具有鲁棒性.

在攻击检测中,当自编码器训练完成后,仅有编码器会用于检测过程,而解码器则不再使用.单一编码器难以提取输入量的所有信息,所以将多个编码器首尾相连,上一层编码器的输出作为下一层的输入,编码器的输出个数逐渐减少,逐层提取特征向量,进而形成堆叠自编码器.堆叠自编码器采用无监督的方式进行逐层训练,直到最后一层编码器训练完成.堆叠自编码器最后一层需要加入一个 softmax 层.softmax 层需要通过有监督的学习进行训练,其输出结果为 0 和 1,分别表示无攻击和受到攻击两种情况.

4 仿真分析

采用 IEEE 118 节点数据对本文提出的方法进行验证,算例如图 4 所示.测量数据均采用相量测量数据,即母线电压和电流的幅值和相角,测量量数量为 852 个.将测量量作为攻击检测的输入量.电源和负荷功率通过蒙特卡罗仿真进行模拟,电力系统状态量通过 MATPOWER[20] 潮流计算获得.潮流计算结果作为真值,在真值基础上叠加随机误差作为测量值.电压幅值和相角的测量误差标准差分别取 2% 和 2°.选择 10 个状态量作为被攻击的状态量,并使这些状态量的状态估计结果与真值的偏离范围为-2 至 2 之间,则攻击向量 $\boldsymbol{a}=\boldsymbol{Hc}$,被攻击的测量量为 $z_a=z+\boldsymbol{a}$. 训练集包含 20 000 组正常测量数据和 3 000 组攻击数据;测试集包含 5 000 组正常测量数据和 500 组攻击数据.堆叠自编码器包含 5 个编码器和一个 softmax 层,输入量 z 的维数为 852,4 个编码器的输出维数分别为 500、200、100 和 50.

采用混淆矩阵对检测性能进行定量分析.混淆矩阵中检测结果分为 4 种:真正(True Positive,TP)表示实际受到攻击则检测为有攻击;真负(True Negative,TN)表示实际没有受到攻击而检测为无攻击;假正(False Positive,FP)表示实际没有受到攻击而检测为有攻击;假负(False Negative,FN)表示实际受到攻击而检测为无攻击.通过准确率 A、精确率 P 和

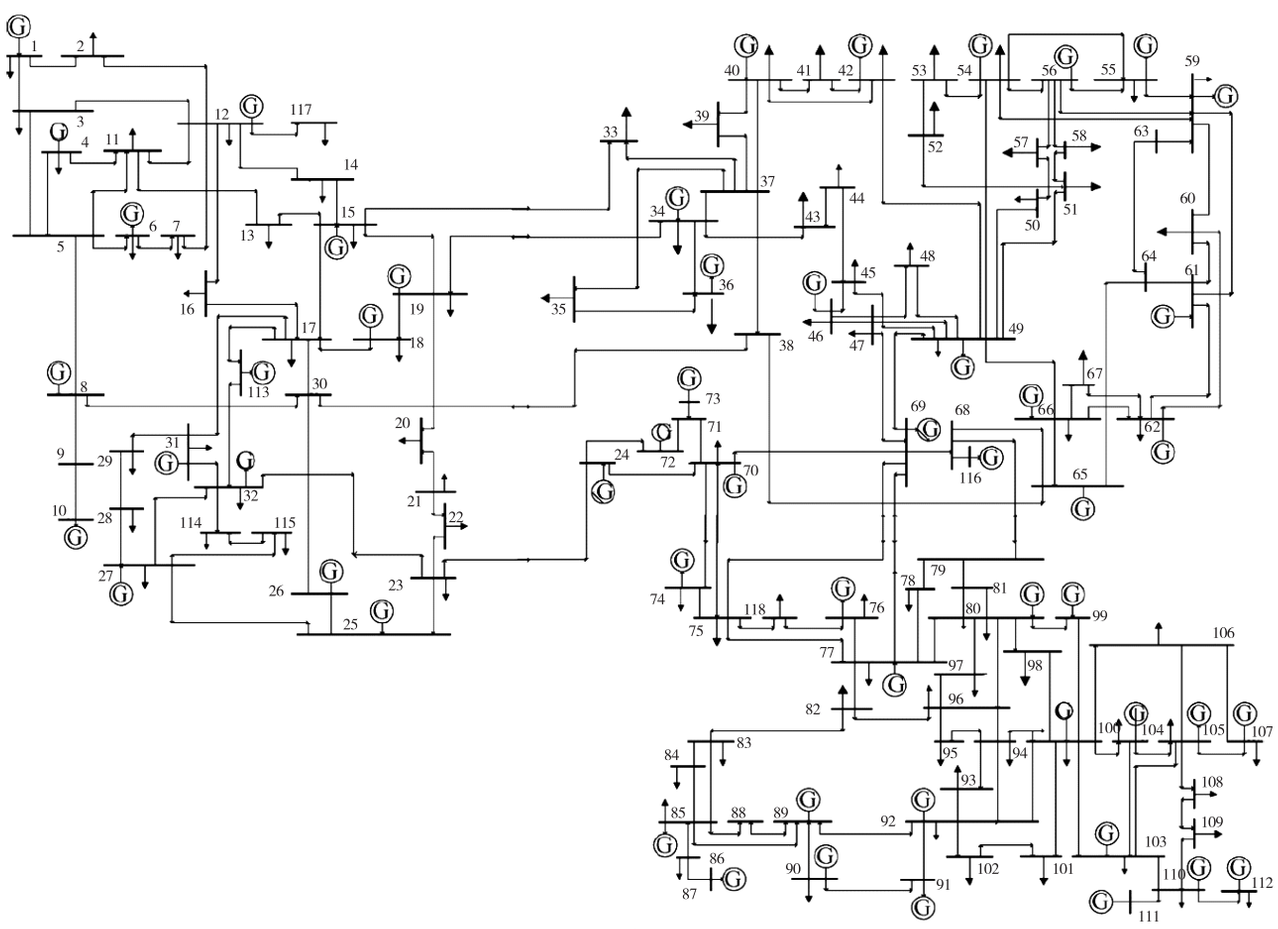

图 4 IEEE 118 节点测试系统

Fig. 4 IEEE 118 node test system

召回率 R 对所提出的攻击检测检测方法进行定量评价:

$$A=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}}, \tag{10}$$

$$P=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}}, \tag{11}$$

$$R=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}. \tag{12}$$

分别采用多层感知机(MultiLayer Perceptron,MLP)、支持向量机(Support Vector Machine,SVM)、深度神经网络(Deep Neural Network,DNN)和堆叠自编码器(Stacked AutoEncoder,SAE)对虚假数据注入攻击进行检测.多层感知机的神经元个数为 50,输出值大于 0.5 则检测为有攻击,否则检测为无攻击.深度神经网络有 10 个隐含层,每层神经元个数为 400.上述 4 种检测方法的结果如表 1 所示.可见 MLP 和 SVM 的召回率相对较低,说明有大量的攻击未被检测到,无法满足实用要求.尽管 DNN 召回率高于 MLP 和 SVM,但是与 SAE 相比仍存在较大差距.基于 SAE 的攻击检测方法准确率、精确率和召回率均高于其他 3 种方法.

表 1　虚假数据注入攻击检测结果

Table 1　Detection rates of false data injection attack　%

方法	A	P	R
MLP	92.30	67.11	30.20
SVM	94.29	82.07	47.60
DNN	97.45	93.48	77.40
SAE	**99.69**	**98.79**	**97.80**

为了进一步分析本文提出的攻击检测性能的影响因素,以下分别从编码器神经元设置和编码器个数设置 2 个方面进行仿真计算.

1)神经元设置

① 形式 1.编码器 1:100 个神经元;编码器 2:70 个神经元;编码器 3:40 个神经元;编码器 4:10 个神经元.

② 形式 2.编码器 1:500 个神经元;编码器 2:200 个神经元;编码器 3:100 个神经元;编码器 4:50 个神经元.

③ 形式 3.编码器 1:50 个神经元;编码器 2:100 个神经元;编码器 3:200 个神经元;编码器 4:500 个神经元.

以上 3 种神经元设置下堆叠自编码器信息攻击检测结果如表 2 和表 3 所示.从混淆矩阵可以看出形式 1 和形式 3 分别有 87 个和 142 个攻击没有被检测到,同时,分别有 18 个和 27 个正常测量被检测为受到攻击.形式 1 和形式 3 的检测效果与形式 2 相比较差.从检测精度指标中也可以看出,形式 2 的准确率、精确率和召回率都为最高.这是由于形式 1 的神经元个数较少,无法充分提取原始测量数据的内在信息.形式 3 虽然具有较多的神经元,但是输入端编码器神经元数量少,无法提取足够信息,尽管编码器 4 含有 500 个神经元仍然会有较多的错误检测结果.由此可以看出,堆叠自编码器的多个编码器合理的神经元个数设置对于提高攻击检测精度有直接影响.输入层的编码器神经元个数太少则无法充分反映原始输入数据的特征信息,即使末端编码器神经元个数增加,也不能提升检测精度.因此,神经元个数通常需要逐层递减,才能够充分挖掘原始输入数据的有效信息.

表 2　不同神经元设置下检测结果

Table 2　Detection results under different neuron settings

形式	TP	FP	FN	TN
1	413	18	87	4 982
2	489	6	11	4 994
3	358	27	142	4 973

表 3　不同神经元设置下检测精度指标

Table 3　Detection accuracy indexes under different neuron settings　%

形式	A	P	R
1	98.09	95.82	82.60
2	99.69	98.79	97.80
3	96.93	92.99	71.60

2)编码器个数设置

堆叠自编码器由多个编码器构成,为了分析编码器个数对检测结果的影响,分别构造如下 3 种堆叠自编码器结构:

① 结构 1,1 个编码器,神经元个数为 500 个.

② 结构 2,2 个编码器,神经元个数分别为 500 和 200.

③ 结构 3,4 个编码器,神经元个数分别为 500、200、100 和 50.

上述 3 种结构的堆叠自编码器攻击检测结果如表 4 和表 5 所示.由混淆矩阵和精度指标都可以看出结构 1 和结构 2 堆叠自编码器攻击检测结果与结构 3 相比较差.这是由于结构 1 和结构 2 的自编码器层数较少,各层之间神经元个数相差较大,无法逐层提

取出原始数据的全部有用信息.

表 4　不同编码器个数设置下检测结果

Table 4　Detection results under different number of encoders

结构	TP	FP	FN	TN
1	226	64	274	4 936
2	415	11	85	4 989
3	489	6	11	4 994

表 5　不同编码器个数设置下检测精度指标

Table 5　Detection accuracy indexes under different number of encoders　%

结构	*A*	*P*	*R*
1	93.85	77.93	45.20
2	98.25	97.42	83.00
3	99.69	98.79	97.80

为进一步验证所提出的基于降噪自编码(Denoising Autoencoder,DAE)攻击检测方法的鲁棒性,对测量量 z 加入不同数量的随机误差,利用 DAE 和 SAE 两种方法分别进行信息攻击检测.在训练降噪自编码时需要将测量量随机置零.图 5 给出了测量量中含有不同比例误差值时 DAE 和 SAE 两种方法的检测准确率.可见随着测量量中误差比例的增加检测准确率明显下降,同时,基于降噪自编码的检测方法与自编码检测方法相比准确率更高,这是由于降噪自编码具有更高的鲁棒性.

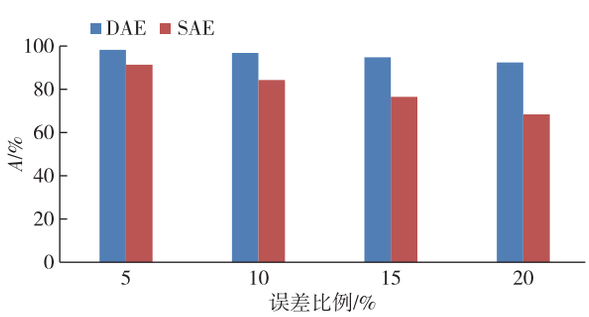

图 5　不同误差比例检测准确率

Fig. 5　Detection accuracies under different error ratios

降噪自编码在训练过程中需要对输入量按照一定比例进行随机置零,图 6 给出了降噪自编码器输入量置零比例对检测精度的影响.可见,当测量量中误差比例较小时,训练过程中置零比例越大检测准确率越低;当误差比例达到 10%时,训练置零比例为 10%的检测精度最高.因此,降噪自编码攻击检测方法并非置零比例越高越好,而是当置零比例与误差比例相近时才能够得到较高的检测精度.

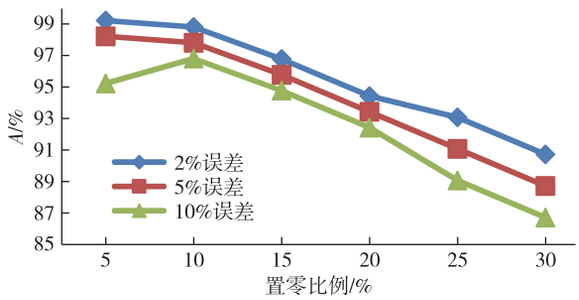

图 6　不同置零比例检测准确率

Fig. 6　Detection accuracies under different zero-setting ratios

5　结语

针对电力系统线性状态估计信息攻击难以被检测为不良数据的问题,提出一种完全基于数据驱动的攻击检测方法.该方法将多个自编码进行联合,逐层提取原始数据中的有用信息,进而构造基于堆叠自编码器的攻击检测方法.针对过度拟合问题,进一步提出基于降噪自编码的攻击检测方法.仿真结果表明,堆叠自编码器的检测效果对编码器神经元个数和编码器个数较为敏感.神经元数量以及编码器个数较少都会导致堆叠自编码器无法完全提取原始的特征,从而使得检测效果变差.通过选择合适的编码器结构,基于堆叠自编码器的信息攻击检测方法与多层感知机、支持向量机和深度神经网络相比具有更好的检测性能.降噪自编码具有更高的鲁棒性,并且当置零比例与误差比例相近时能够得到最佳的检测精度.

参考文献

References

[1] 邓勇,彭敏放,刘靖雯.电力信息物理系统建模和信息攻击机制分析[J].电力系统及其自动化学报,2021,33(10):10-17
DENG Yong, PENG Minfang, LIU Jingwen. Modeling of cyber power physical system and analysis of information attack mechanism[J]. Proceedings of the CSU-EPSA, 2021,33(10):10-17

[2] 安宇,刘东,陈飞,等.考虑信息攻击的配电网信息物理运行风险分析[J].电网技术,2019,43(7):2345-2352
AN Yu, LIU Dong, CHEN Fei, et al. Risk analysis of cyber physical distribution network operation considering cyber attack[J]. Power System Technology, 2019, 43(7):2345-2352

[3] 褚晨杰,吕干云,吕经纬,等.基于 PMU/SCADA 混合量测的电力系统鲁棒状态估计[J].南京工程学院学报(自然科学版),2020,18(4):14-19

CHU Chenjie,LÜ Ganyun,LÜ Jingwei,et al.Robust state estimation of power system based on PMU and SCADA hybrid measurement[J].Journal of Nanjing Institute of Technology (Natural Science Edition),2020,18(4):14-19

[4] 王艳丽,吕海翠,宋佳.高效物联网虚假数据注入攻击智能防御仿真[J].计算机仿真,2020,37(9):258-261,337
WANG Yanli,LÜ Haicui,SONG Jia.Intelligent defense simulation of high efficient Internet of Things false data injection attack[J].Computer Simulation,2020,37(9):258-261,337

[5] 田继伟,王布宏,李腾耀,等.智能电网虚假数据注入攻击研究进展与展望[J].网络空间安全,2019,10(9):73-84
TIAN Jiwei,WANG Buhong,LI Tengyao,et al.Research progress and prospects of false data injection attacks in smart grid[J].Cyberspace Security,2019,10(9):73-84

[6] 田继伟,王布宏,尚福特,等.基于数据驱动的稀疏虚假数据注入攻击[J].电力自动化设备,2017,37(12):52-59
TIAN Jiwei,WANG Buhong,SHANG Fute,et al.Sparse false data injection attacks based on data driven[J].Electric Power Automation Equipment,2017,37(12):52-59

[7] 蔡星浦,王琦,郤伟,等.基于多阶段博弈的电力 CPS 虚假数据注入攻击防御方法[J].电力建设,2019,40(5):48-54
CAI Xingpu,WANG Qi,TAI Wei,et al.A multi-stage game based defense method against false data injection attack on cyber physical power system[J].Electric Power Construction,2019,40(5):48-54

[8] 阮兆文,孟干,周冬青,等.智能电网中的虚假数据注入攻击检测方法研究[J].自动化与仪器仪表,2019(3):49-52
RUAN Zhaowen,MENG Gan,ZHOU Dongqing,et al.Research on false data injection attack detection method in smart grid[J].Automation & Instrumentation,2019(3):49-52

[9] 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
ZENG Junrao,LI Peng,GAO Lian,et al.Detection of false data injection attacks in smart grids based on time neighbor preserving embedding (TNPE)[J].Journal of Safety Science and Technology,2021,17(3):124-129

[10] 刘鑫蕊,常鹏,孙秋野.基于 XGBoost 和无迹卡尔曼滤波自适应混合预测的电网虚假数据注入攻击检测[J].中国电机工程学报,2021,41(16):5462-5476
LIU Xinrui,CHANG Peng,SUN Qiuye.Grid false data injection attacks detection based on XGBoost and unscented Kalman filter adaptive hybrid prediction[J].Proceedings of the CSEE,2021,41(16):5462-5476

[11] 刘鑫蕊,吴泽群.面向智能电网的空间隐蔽型恶性数据注入攻击在线防御研究[J].中国电机工程学报,2020,40(8):2546-2559
LIU Xinrui,WU Zequn.Online defense research of spatial-hidden malicious data injection attacks in smart grid[J].Proceedings of the CSEE,2020,40(8):2546-2559

[12] Hu K,Chen X,Xia Q F,et al.A control algorithm for sea-air cooperative observation tasks based on a data-driven algorithm[J].Journal of Marine Science and Engineering,2021,9(11):1189

[13] 陈冰,唐永旺.基于 Bi-GRU 和自注意力的智能电网虚假数据注入攻击检测[J].计算机应用与软件,2021,38(7):339-344,349
CHEN Bing,TANG Yongwang.False data injection attacks detection in smart grid based on Bi-GRU and self-attention[J].Computer Applications and Software,2021,38(7):339-344,349

[14] 陈碧云,李弘斌,李滨.伪量测建模与 AUKF 在配电网虚假数据注入攻击辨识中的应用[J].电网技术,2019,43(9):3226-3236
CHEN Biyun,LI Hongbin,LI Bin.Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network[J].Power System Technology,2019,43(9):3226-3236

[15] 罗仁泽,王瑞杰,张可,等.残差卷积自编码网络图像去噪方法[J].计算机仿真,2021,38(5):455-461
LUO Renze,WANG Ruijie,ZHANG Ke,et al.Image denoising method of residual convolution auto-encoder network[J].Computer Simulation,2021,38(5):455-461

[16] 张忠林,杨朴舟.基于自编码器语义哈希的大规模文本预处理[J].计算机仿真,2019,36(3):225-229,260
ZHANG Zhonglin,YANG Puzhou.Large scale text preprocessing based on self-encoder semantic hashing[J].Computer Simulation,2019,36(3):225-229,260

[17] 张永宏,陈帅,王剑庚,等.一种基于降噪自编码神经网络的积雪产品去云方法[J].南京信息工程大学学报(自然科学版):2023,15(2):169-179
ZHANG Yonghong,CHEN Shuai,WANG Jiangeng,et al.Cloud removal for snow products based on denoising autoencoder artificial neural network[J].Journal of Nanjing University of Information Science & Technology (Natural Science Edition),2023,15(2):169-179

[18] 史晗璋,谢林柏,吴治海,等.基于编码策略的电网假数据注入攻击检测[J].信息与控制,2021,50(4):419-426
SHI Hanzhang,XIE Linbo,WU Zhihai,et al.Detection of false data injection attacks in power grid based on coding schemes[J].Information and Control,2021,50(4):419-426

[19] Zhang Y,Wang J H,Chen B.Detecting false data injection attacks in smart grids:a semi-supervised deep learning approach[J].IEEE Transactions on Smart Grid,2021,12(1):623-634

[20] Zimmerman R D,Murillo-Sánchez C E,Thomas R J.MATPOWER:steady-state operations,planning,and analysis tools for power systems research and education[J].IEEE Transactions on Power Systems,2011,26(1):12-19

南京信息工程大学学报(自然科学版),2023,15(4):460-467
Journal of Nanjing University of Information Science & Technology(Natural Science Edition),2023,15(4):460-467

Detection of cyber attack against phasor measurement state estimation

QI Mengyi[1] LIU Niexuan[1] TAO Xiaofeng[1] LÜ Pengpeng[1]
1 NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106

Abstract It is difficult to successfully detect the false data injection attacks against the linear state estimation based on phasor measurement techniques in power systems. Here, we propose an intelligent method to detect false data injection attacks. First, the auto-encoder is used to extract the features of the power grid measurement data, which is done repeatedly to gradually reduce the feature dimension. Then the finally extracted feature is subjected to supervised learning through the Softmax layer, so as to obtain an attack detection algorithm based on stacked auto-encoders. Second, the attack detection approach is improved through noise reduction to solve the over fitting of auto-encoders. Finally, the proposed method is simulated and verified by IEEE-118 node test system, and the results show that the proposed attack detection method has high computational accuracy and efficiency.

Key words auto-encoder; phasor measurement; state estimation; attack detection