基于 Transformer 编码器的智能电网虚假数据注入攻击检测

陈 冰[1] 唐永旺[2]

[1](河南工业大学漯河工学院电气电子工程系 河南 漯河 462000)

[2](中国人民解放军战略支援部队信息工程大学信息系统工程学院 河南 郑州 450002)

摘 要 针对当前基于循环神经网络的智能电网虚假数据注入攻击(False Data Injection Attacks, FDIA)检测方法无法同时利用量测样本中前后参数信息和样本间参数关联关系的问题,提出一种基于 Transformer 编码器的 FDIA 检测框架。对连续时间样本数据进行归一化处理,结合相对位置信息得到连续时间样本向量。引入 Transformer 编码器,通过多头自注意力机制计算长距离依赖关系,得到连续时间样本的特征表示。将该特征表示输入到全连接神经网络层和 Softmax 层,输出后一时刻样本受到注入攻击的概率。在 IEEE 14-bus 和 IEEE 30-bus 中的仿真实验结果表明该方法切实可行,相较于次优结果,准确率平均提高 7.41%,正报率平均提高 4.51%,误报率平均降低 60.99%。

关键词 Transformer 编码器 连续时间 多头注意力 智能电网 虚假数据

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2022.07.051

FALSE DATA INJECTION ATTACKS DETECTING BASED ON TRANSFORMER ENCODER IN SMART GRID

Chen Bing[1] Tang Yongwang[2]

[1](*Department of Electrical and Electronic Engineering, Henan University of Technology Luohe Institute of Technology, Luohe 462000, Henan, China*)

[2](*School of Information System Engineering, PLA Support Force Information Engineering University, Zhengzhou 450002, Henan, China*)

Abstract The current detection method based on the recurrent neural network for false data injection attacks(FDIA) in smart grid cannot simultaneously use the front-back parameter information in single measurement sample and the parameter relationship between the samples. To solve this problem, we propose the FDIA detection method based on transformer encoder. The continuous time sample data was normalized, and the continuous time sample vector was obtained by combining the relative position information. We introduced the transformer encoder to calculate the long-distance dependence through the multi-head self-attention mechanism, and then gained the feature representation of continuous time sample. The feature representation was input into the neural network layer and Softmax layer, and the probability of injection attack at the next moment was output. The simulation results in IEEE 14-bus and IEEE 30-bus show that this method is feasible. And compared with the sub-optimal results, the average accuracy rate is increased by 7.41%, the positive report rate is increased by 4.51%, and the false alarm rate is decreased by 60.99%.

Keywords Transformer encoder Continuous time Multi-head attention Smart grid False data

0 引 言

智能电网以其可靠、高效和经济的传输特点成为现代电力系统最重要的组成部分,然而智能电网严重依赖数据通信和大规模数据处理技术,容易遭到各种恶意网络攻击[1]。尽管已经颁布了很多针对智能电网安全的通信标准、官方指南和监管法律(如 IEC 61850-90-5、NISTIR7628 等),恶意网络攻击仍活跃于智能电网中。

虚假数据注入攻击(False Data Injection Attacks, FDIA)是 Liu 等[2]提出的恶意网络攻击技术,被证明

收稿日期:2020-03-01。**陈冰**,讲师,主研领域:电气工程,人工智能。**唐永旺**,助工。

是一种对智能电网状态估计产生严重影响的恶意网络攻击行为。其通过规避现有数据注入监测系统,篡改电网的状态估计数据,诱导电网控制中心作出错误决策,导致整个智能电网出现故障。如何高效地检测 FDIA,对于保障智能电网安全运行具有重要意义。

传统的 FDIA 检测思路主要归为两种[3-4]。一种是策略性的保护部分关键基础测量数据的安全,避免恶意数据注入的发生。如:Kim 等[5]提出两种快速贪婪算法分别用于选择待保护的测量子集数据和寻找存储安全相量测量单元的位置。Bi 等[6]利用图形分析研究方法引入到 FDIA 检测中,提出精确、低复杂度的近似算法来选择保护系统中最小的数据测量值。另一种是通过独立检验每个状态变量进行 FDIA 检测。例如:Liu 等[7]考虑到电网状态时间测量的内在低维度以及 FDIA 的稀疏性质,将 FDIA 检测视为低秩矩阵分离问题,并提出核规范最小化和低秩矩阵分解两种优化方法来解决该问题。Ashok 等[8]提出了一种在线 FDIA 检测算法,该算法利用统计信息和状态变量的预测来检测量测异常。

近年来随着智能电网通信数据量级的增加和 FDIA 方法的不断升级,传统方法在进行 FDIA 检测时越来越力不从心。机器学习以及深度学习算法逐渐应用在智能电网恶意网络攻击检测中,并较传统检测方法检测性能有明显提高[9-13]。Ozay 等[14]利用监督和半监督机器学习方法完成对高斯分布式攻击的分类。Esmalifalak 等[15]设计了一种基于分布式支持向量机的标签数据模型和一种无监督学习的统计异常检测器。He 等[11]采用条件深度信念网络有效学习了 FDIA 的高维时间行为特征。Niu 等[16]利用卷积神经网络提取和长短时记忆网络(Long Short Term Memory Network,LSTM)学习量测状态序列的时间和空间关系特征,进而实现 FDIA 检测。James 等[17]基于小波变换和单向门控循环单元(Gated Recurrent Unit,GRU)进行系统状态连续估计,检测序列状态中的 FDIA。Wang 等[18]利用 3 层 LSTM 作为序列编码器,学习 FDIA 样本的特征,在测试数据中准确率高达 90%。深度学习算法可以自动学习电网中各节点的状态量测数据特征,发现异常状态序列或对异常序列分类,整个过程不需要人工设定特征。

然而,现有基于循环神经网络[16-18](Recurrent Neural Network,RNN)的 FDIA 检测方法在训练量测值时仅使用了多层单向的 RNN 训练框架,单向的 RNN 模型在处理序列数据时只能利用已经出现过的序列元素,忽略了未来的序列信息,导致模型性能下降,影响特征最终的提取效果。这些方法中只选取 RNN 最后一个时刻的隐状态或者各时刻隐状态的拼接作为提取的特征,无法突出注入攻击数据的特征。因为注入攻击向量不一定会对状态量测数据的每一维都均匀地注入攻击,有可能只对一部分维数的数据进行攻击。另外,这些方法只针对单个样本参数(电压、电流、有用功、支路电流等)进行分析,没有考虑连续时间样本参数之间的关联关系。再者,RNN 的顺序性决定其训练缓慢,因为长序列需要更多的处理步骤,反复循环的结构也使训练更加困难。

Transformer[19]是当前机器翻译领域的主流模型,利用基于注意力机制的编码器和解码器直接学习源语言内部关系和目标语言内部关系。相较于 RNN,Transformer 无循环结构,可以并行处理序列中的所有元素,从整个样本序列中挖掘与当前预测元素关系紧密的上下文元素,Transformer 编码器具有更强的特征提取能力。

考虑到 Transformer 以上优点以及量测数据序列元素互相依赖、关系紧密的特点,本文提出一种基于 Tansformer 编码器的 FDIA 检测框架,输入两个连续时间量测样本,对后一时刻的样本进行检测。首先,对连续时间样本数据进行归一化处理,结合连续时间样本中元素相对位置信息得到连续时间样本向量。然后,采用 Tansformer 编码器对量测序列进行建模,通过多头自注意力机制计算长距离依赖关系,挖掘结合样本中和样本间测量值的特征表示。最后,将该特征表示输入到全连接神经网络层和 Softmax 层,输出后一时刻样本受到注入攻击的概率,完成 FDIA 检测。

1　相关背景

1.1　虚假数据注入攻击

在电力系统中,待估计的状态变量包括电压幅值 $V\in\mathbf{R}^n$ 和相位角 $\theta\in([-\pi,\pi])^n$,n 是总线数量。令 $\boldsymbol{z}=[z_1,z_2,\cdots,z_m]^{\mathrm{T}}\in\mathbf{R}^m$ 表示量测向量,$x=[x_1,x_2,\cdots,x_{2n}]^{\mathrm{T}}\in\mathbf{R}^{2n}$ 代表状态变量,$\boldsymbol{e}=[e_1,e_2,\cdots,e_m]^{\mathrm{T}}\in\mathbf{R}^m$ 代表量测误差向量。在标准直流系统下,可忽略电阻,电压幅值均为 1,仅考虑带有相位角的状态变量,量测值和状态变量的关系如式(1)所示。

$$\boldsymbol{z}=\boldsymbol{T}\boldsymbol{x}+\boldsymbol{e} \tag{1}$$

式中:$\boldsymbol{T}$ 是 $m\times n$ 的拓展结构雅可比矩阵。求使加权残差平方和最小的状态估计变量 $\boldsymbol{x}$,目标函数如式(2)所示。

$$\boldsymbol{j}(x)=(\boldsymbol{z}-\boldsymbol{T}\boldsymbol{x})^{\mathrm{T}}\boldsymbol{R}^{-1}(\boldsymbol{z}-\boldsymbol{T}\boldsymbol{x}) \tag{2}$$

式中:$\boldsymbol{R}$ 是协方差矩阵。利用加权最小二乘法求解式(2)的目标函数,如式(3)所示。

$$\hat{\boldsymbol{x}} = (\boldsymbol{T}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{T})^{-1}\boldsymbol{T}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{z} \tag{3}$$

令 $\boldsymbol{a} = [a_1, a_2, \cdots, a_m]^{\mathrm{T}}$ 表示虚假注入攻击向量,则量测值向量表示为 $\boldsymbol{z}_a = \boldsymbol{z} + \boldsymbol{a}$,$\boldsymbol{x}_a$ 是利用带有虚假注入向量的量测值向量 $\boldsymbol{z}_a$ 估计的状态变量,$\boldsymbol{x}_a = \hat{\boldsymbol{x}} + \boldsymbol{c}$,$\boldsymbol{c}$ 表示攻击后对状态变量的非零干扰向量,如果攻击者已知电网完整的拓扑信息,即已知矩阵 $\boldsymbol{T}$,则可以构建不可观察的 FDIA[20]。

1.2 注意力机制

注意力机制的本质是将一个查询向量和一组键值向量对映射到输出,查询向量与键向量用于计算每个值向量对应的权重,值向量的加权和为输出。常用的注意力函数为加法注意力(additive attention)和点乘注意力(dot-product attention)[21],由于点乘注意力可以利用高度优化的矩阵乘法运算,高效且更加节省空间,因此本文选取放缩点积注意力,其计算流程如图 1 所示,其中:$\boldsymbol{Q}$ 代表查询向量矩阵;$\boldsymbol{K}$ 代表键向量矩阵;$\boldsymbol{V}$ 代表值向量矩阵;$\boldsymbol{Q}$ 和 $\boldsymbol{K}$ 中每个向量的维度为 d_k,$\boldsymbol{V}$ 中每个向量维度为 d_v。

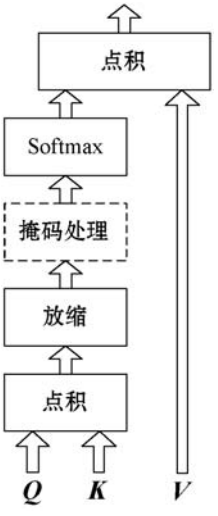

图 1 放缩点积注意力计算流程

首先将 $\boldsymbol{Q}$ 和 $\boldsymbol{K}$ 的点积除以 $\sqrt{d_k}$ 进行缩放,让梯度更稳定;掩码处理用于遮蔽无意义的填充位置,而本文量测数据均有意义,因此将掩码处理步骤省略;然后利用 Softmax 函数计算各值向量的权重;最后进行加权求和,如式(4)所示。

$$Attention(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = \mathrm{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_k}}\right)\boldsymbol{V} \tag{4}$$

2 基于 Transformer 的 FDIA 检测方法

本文利用 Transformer 编码器提取攻击样本的特征,提出基于 Transformer 编码器的 FDIA 检测框架,其训练结构如图 2 所示。

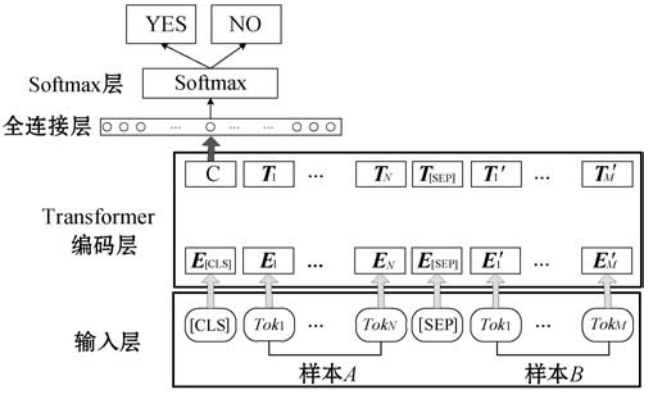

图 2 本文提出的 FDIA 检测模型框架

该框架主要分为输入层、Transformer 编码层、全连接层和 Softmax 层四大部分,[CLS]是样本之间的分类符,表示样本 A 之后的连续时间样本 B 是否受到虚假数据注入攻击。[SEP]是样本之间的分隔符,为便于区分连续时间样本的切割点。该训练框架将连续时间样本 A、B 作为模型输入,通过 Transformer 编码层提取单样本各测量值之间的特征和两个连续时间样本 A、B 整体之间的特征,用于判断样本 B 是否被注入攻击。

2.1 输入层

输入层的作用是将样本 A、B 向量化,将 Tok_i 的向量、相应的位置向量、分割向量进行求和[22],如图 3 所示。

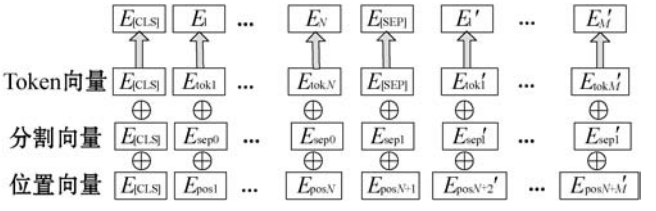

图 3 输入层向量化的过程

由于 Transformer 编码器中没有循环或者卷积结构,无法使用序列元素的位置信息,因此对序列编码时需要添加位置信息。相对位置编码表示如下:

$$PE(pos,2i) = \sin(pos/10\ 000^{2i/d_{\mathrm{model}}}) \tag{5}$$

$$PE(pos,2i+1) = \cos(pos/10\ 000^{2i/d_{\mathrm{model}}}) \tag{6}$$

式中:pos 代表位置;i 代表维度。相对位置编码的每个维度均采样于正弦曲线,根据式(7)和式(8)可知任意位置的编码 $PE(pos+k)$ 都可由 $PE(pos)$ 的线性函数表示,该特点为模型捕捉序列元素之间的相对位置关系提供便利。

$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta \tag{7}$$

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta \tag{8}$$

2.2 Transformer 编码层

Transformer 编码层由三层的双向 Transformer 编码

器构成,具体结构如图 4 所示。

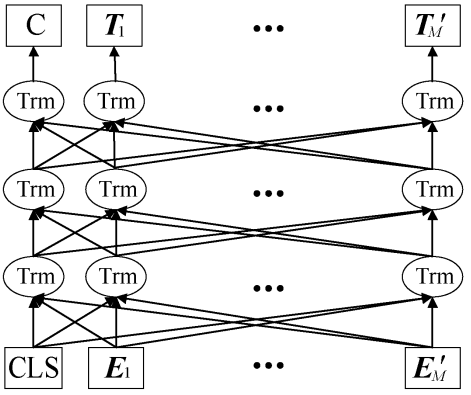

图 4　Transformer 编码层

图 4 中每个 Trm 均代表一个 Transformer 编码器;E_i表示输入的词向量,由 Tok_i的向量、位置向量、分割向量的和组成;T_i表示第 i 个 Token 在经过 Transformer 编码层处理之后得到的特征向量,其模型结构如图 5 所示。

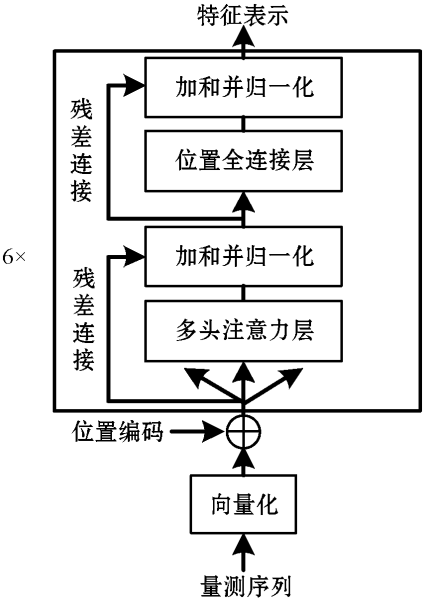

图 5　Transformer 编码器

Transformer 编码器由 6 个相同的编码层堆叠而成,每个编码层又包括两个子层,分别为多头自注意力层和位置全连接层。为了更好地优化深度网络,整个网络使用了残差连接和层归一化。因此,每层输出可以表示为 $LayerNorm(x+Sublayer(x))$,其中 $Sublayer(x)$ 为各层的功能函数。为了使模型正常训练,模型中的所有子层以及嵌入层都需要产生维度 d_{model}的输出。

(1) 多头注意力机制。一次自注意力计算关注到的序列关系有限,而量测数据中的功率、电压、电流、有用功率、无用功率、总功率和分支功率等数据之间关系多样,因此本文采用多头注意力使编码器同时关注来自不同位置的不同表示子空间的信息,其具体计算流程如图 6 所示。

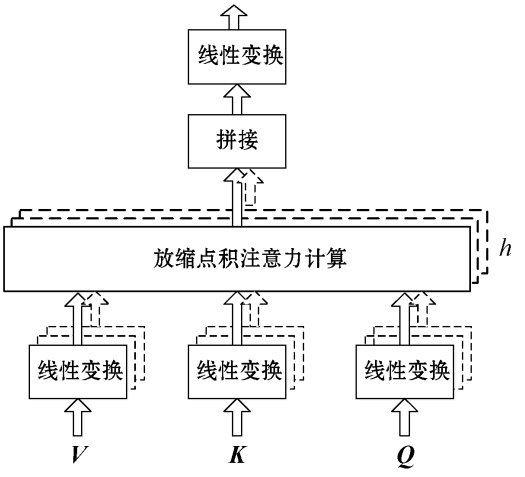

图 6　多头注意力机制计算流程

图 6 中,首先将 $\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$ 线性变换后分 h 次输入到放缩点乘注意力模型,h 即为多头注意力的头数,每次线性变换的参数矩阵不同。然后将 h 次的放缩点积注意力结果拼接后再进行一次线性变换得到多头注意力的结果。计算公式如下:

$$Multihead(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = \text{Concat}(head_1, head_2, \cdots, head_h)\boldsymbol{W}^O \tag{9}$$

$$head_i = Attention(\boldsymbol{Q}\boldsymbol{W}_i^Q, \boldsymbol{K}\boldsymbol{W}_i^K, \boldsymbol{V}\boldsymbol{W}_i^V) \tag{10}$$

式中:线性变换参数矩阵 $\boldsymbol{W}_i^Q \in \mathbf{R}^{d_{\text{model}} \times d_k}$,$\boldsymbol{W}_i^K \in \mathbf{R}^{d_{\text{model}} \times d_k}$,$\boldsymbol{W}_i^V \in \mathbf{R}^{d_{\text{model}} \times d_v}$,$\boldsymbol{W}^O \in \mathbf{R}^{hd_v \times d_{\text{model}}}$。

(2) 位置全连接前馈网络。位置全连接前馈网络分两层,用于处理每个位置的多头注意力计算结果,其输入和输出的维度相同。第一层的激活函数是 ReLU,第二层是线性激活函数,如果多头注意力层输出表示为 $\boldsymbol{X}$,则 FFN 可表示为:

$$FFN(x) = \max(0, \boldsymbol{X}\boldsymbol{W}_1 + \boldsymbol{b}_1)\boldsymbol{W}_2 + \boldsymbol{b}_2 \tag{11}$$

式中:$\boldsymbol{W}_1$、$\boldsymbol{b}_1$ 和 $\boldsymbol{W}_2$、$\boldsymbol{b}_2$ 分别是两个激活函数的参数。Transformer 编码器通过对输入的序列不断进行注意力机制层和普通的非线性层交叠得到最终的序列表示。

2.3　全连接层和 Softmax 层

对于量测数据训练集 C,给定输入样本 $A: x^1, x^2, \cdots, x^N$,样本 $B: x^1, x^2, \cdots, x^M$ 和对应标签 y。[CLS]在最后一个 Transformer 编码器的隐藏层输出记为 $\boldsymbol{C} \in \mathbf{R}^{d_{\text{model}}}$,经过全连接层和 Softmax 层后对 y 进行预测:

$$P(y \mid x^1, x^2, \cdots, x^N, x^1, x^2, \cdots, x^M) = \text{Softmax}(\boldsymbol{C}\boldsymbol{W}_f + \boldsymbol{b}) \tag{12}$$

式中:$\boldsymbol{W}_f$是全连接层的权重矩阵;$\boldsymbol{b}$ 为偏置;$P(y \mid x^1, x^2, \cdots, x^N, x^1, x^2, \cdots, x^M)$ 是 Softmax 层计算的概率结果。则模型训练的目标为最大化目标函数 $L(C)$:

$$L(C) = \sum_{(x,y)} P(y \mid x^1, x^2, \cdots, x^N, x^1, x^2, \cdots, x^M) \tag{13}$$

FDIA 检测模型训练完毕后,就可以对连续时间的量测数据样本进行检测。

3 实 验

3.1 实验数据

本文选择该领域主流的 IEEE 14-bus 和 IEEE 30-bus 节点测试系统作为测试环境,系统网络拓扑、节点数据、支路参数等均从 Matpower 中获得。在每个环境中利用 Matpower 软件仿真生成 150 000 对连续时间的正常量测数据样本和 50 000 对后一时刻量测值被注入攻击的样本,标签分别为 -1 和 1。IEEE 14-bus 中每个样本包括 54 个量测值,IEEE 30-bus 中每个样本包括 112 个量测值。每个测试系统的量测值包括电压幅值、总线相位角、总线注入有功功率和无功功率、各支路注入有功功率和无功功率等,将正常样本和 FDIA 样本进行去均值和归一化处理,分别按照 7∶3 的比例随机抽取样本制作训练集和测试集。

3.2 评测标准

本文采用准确率、漏报率和误报率三个 FDIA 检测领域通用的评测指标验证本文方法的可行性和有效性,首先定义以下变量:

真负类(Ture Negative)表示将正常量测样本正确地识别成正常量测样本的数量,记为 T_n。

假负类(False Negative)表示将正常量测样本误识别成 FDIA 样本的数量,记为 F_n。

真正类(Ture Positve)表示将 FDIA 样本正确地识别成 FDIA 样本的数量,记为 T_p。

假正类(False Positive)表示将 FDIA 样本误识别成正常量测样本的数量,记为 F_p。

(1) 准确率(记为 A_c)计算表达式为:

$$A_c = \frac{T_n + T_p}{T_n + T_p + F_n + F_p} \tag{14}$$

式(14)表示所有被正确判断的样本数量占所有样本的百分比,准确率越高,算法越好。

(2) 正报率计算表达式为:

$$T_r = \frac{T_p}{T_p + F_n} \tag{15}$$

式(15)表示在所有被检测为 FDIA 样本中,被正确预测 FDIA 样本所占的百分比。正报率越高,算法越好。

(3) 误报率计算表达式为:

$$F_r = \frac{F_p}{T_n + F_p} \tag{16}$$

式(16)表示在所有被检测为正常样本中,被错误预测样本所占百分比,误报率越高,算法越差。

3.3 实验设置与分析

本文选取文献[15,18]的方法作为对比方法,文献[15]利用标签数据的监督学习训练分布式支持向量机对 FDIA 样本检测,测试结果记为 SVM;选取文献[18]提出的方法,基于三层双向 LSTM 模型学习单个样本状态量测值序列的特征,测试结果记为 Bi-LSTM。另外,将三层双向 Transformer 编码器作为编码器,测试结果记为 Bi-TRAM。

本文方法首先分别将 IEEE 14-bus 和 IEEE 30-bus 环境中获取的单个样本归一化处理为 60 维和 120 维(54 维和 112 维数据通过补零变为 60 维和 120 维,方便后续处理)的序列向量,则输入为 120 维和 240 维的连续时间序列向量。使用 TensorFlow 深度学习框架构造模型结构。根据模型训练经验,选取多头注意力的头数为 10,在训练 IEEE 14-bus 环境样本时 $d_k = d_v = d_{model}/h = 6$,在训练 IEEE 30-bus 环境样本时,$d_k = d_v = d_{model}/h = 12$,全连接层的隐藏节点数量为 768。优化算法选取 Adam[23],令 $\beta_1 = 0.9$,$\beta_2 = 0.98$,$\varepsilon = 10^{-9}$,epochs 设置为 100,每批数据 batch_size 大小为 256,学习速率为 2e-5,本文连续时间样本训练的方法测试结果记为 CON-TRAM。

实验硬件配置为 Intel Xeon E5-2650,128 GB 内存的服务器、配备 12 GB 的双 GTX 1080Ti 独立显卡进行加速训练。

(1) 综合对比实验。本文方法与各对比方法测试结果如表 1 和表 2 所示。

表 1 IEEE 30-bus 综合实验结果

变量	SVM	Bi-LSTM	Bi-TRAM	CON-TRAM
A_c	0.854	0.894	0.925	0.991
T_r	0.821	0.880	0.936	0.976
F_r	0.138	0.114	0.051	0.023

表 2 IEEE 14-bus 综合实验结果

变量	SVM	Bi-LSTM	Bi-TRAM	CON-TRAM
A_c	0.785	0.867	0.912	0.982
T_r	0.806	0.861	0.927	0.971
F_r	0.238	0.144	0.079	0.026

可以看出,Bi-LSTM 的测试结果优于 SVM,这是因为 RNN 网络在处理高维度序列数据方面比 SVM 更有优势。Bi-LSTM 在计算时刻 t 的隐状态时只利用了量测序列前向 $t-1$ 时刻和后向 $t+1$ 时刻的隐状态,而基于自注意力机制的 Transformer 编码器可以同时利用

所有时刻的隐状态,可以轻松捕获长距离的特征,提取量测序列中电压、电流、功率、有用功、无用功、输入功率、输出功率等多种序列关系特征,经过多头注意力层和位置全连接层的多次迭代训练,最终得到量测序列的向量表示。该向量表示可以更加准确地代表量测样本,因此 Bi-TRAM 三项的评测指标优于 Bi-LSTM。本文 CON-TRAM 不仅关注样本内部特征,还着重考虑了连续时间样本之间的关联特征,利用正常连续内电压、电流、功率、有用功、无用功、输入功率、输出功率等变化的特征判断注入攻击行为。因此 CON-TRAM 的测试结果与对比方法相比有较显著的提升,与次优结果相比,准确率平均提高 7.41%,正报率平均提高 4.51%,误报率平均降低 60.99%。

(2) 多头注意力机制中头数 h 的分析。多头注意力计算中头数 h 是 Transformer 编码器的关键一步,因此本节以 IEEE 30-bus 环境的实验数据分析 h 对 FDIA 检测的影响。令 h 在[0,15]内取值,以 1 为步长训练 FDIA 检测模型,在测试集进行检测任务,以评测指标准确率分析,结果如图 7 所示。

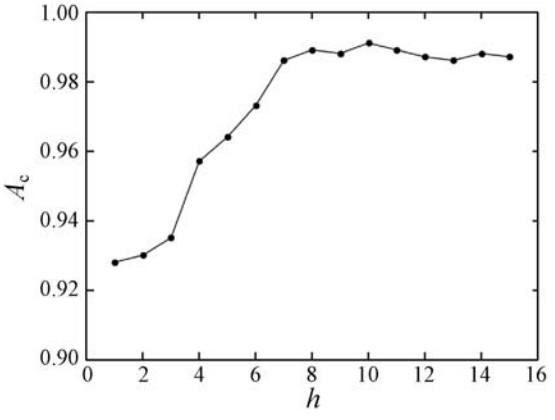

图 7　准确率随着 h 的变化分析

可以看出,在[0,10]的区间内,准确率的总体趋势是随着 h 的增加而增加,从 FDIA 样本提取的特征关系也越来越多样,说明多头注意力机制对提升检测性能有重要作用。当 h 为 10 时达到峰值,随后趋于平稳,可以推测量测样本数据中的电压幅值、总线相位角、总线注入有功功率和无功功率、各支路注入有功功率和无功功率等有 10 种左右的内在关系,符合数据的真实特征。

4　结　语

本文通过引入 Transformer 编码器,解决了当前基于单向多层 RNN 的 FDIA 检测方法中无法同时利用样本序列前后参数信息的问题。另外,本文提出基于连续时间的量测样本训练 FDIA 检测模型,利用连续时间样本之间的关联特征进行检测,提高了 FDIA 检测性能。下一步准备在电网节点规模更大的模拟环境中测试本文方法的有效性。

参　考　文　献

[1] Morello R, Mukhopadhyay S C, Liu Z, et al. Advances on sensing technologies for smart cities and power grids: A review[J]. IEEE Sensors Journal, 2017, 17(23): 7596 – 7610.

[2] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security(TISSEC), 2011, 14(1): 309 – 341.

[3] Bobba R B, Rogers K M, Wang Q, et al. Detecting false data injection attacks on dc state estimation[C]//Preprints of the First Workshop on Secure Control Systems, 2010.

[4] Liang G, Zhao J, Luo F, et al. A review of false data injection attacks against modern power systems[J]. IEEE Transactions on Smart Grid, 2016, 8(4): 1630 – 1638.

[5] Kim T T, Poor H V. Strategic protection against data injection attacks on power grids[J]. IEEE Transactions on Smart Grid, 2011, 2(2): 326 – 333.

[6] Bi S, Zhang Y J. Graphical methods for defense against false-data injection attacks on power system state estimation[J]. IEEE Transactions on Smart Grid, 2014, 5(3): 1216 – 1227.

[7] Liu L, Esmalifalak M, Ding Q, et al. Detecting false data injection attacks on power grid by sparse optimization[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 612 – 621.

[8] Ashok A, Govindarasu M, Ajjarapu V. Online detection of stealthy false data injection attacks in power system state estimation[J]. IEEE Transactions on Smart Grid, 2016, 9(3): 1636 – 1646.

[9] Ozay M, Esnaola I, Vural F T Y, et al. Machine learning methods for attack detection in the smart grid[J]. IEEE Transactions on Neural Networks and Learning Systems, 2015, 27(8): 1773 – 1786.

[10] Esmalifalak M, Liu L, Nguyen N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal, 2014, 11(3): 1644 – 1652.

[11] He Y, Mendis G J, Wei J. 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.

[12] Yan J, Tang B, He H. Detection of false data attacks in smart grid with supervised learning[C]//2016 International Joint Conference on Neural Networks(IJCNN), 2016: 1395 – 1402.

[13] Wang H, Ruan J, Wang G, et al. Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(11):4766 - 4778.

[14] Ozay M, Esnaola I, Vural F T Y, et al. Machine learning methods for attack detection in the smart grid[J]. IEEE Transactions on Neural Networks and Learning Systems, 2015,27(8):1773 - 1786.

[15] Esmalifalak M, Liu L, Nguyen N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal,2014,11(3):1644 - 1652.

[16] Niu X, Sun J. Dynamic detection of false data injection attack in smart grid using deep learning[EB]. arXiv:1808.01094, 2018.

[17] James J Q, Hou Y, Li V O K. Online false data injection attack detection with wavelet transform and deep neural networks[J]. IEEE Transactions on Industrial Informatics, 2018,14(7):3271 - 3280.

[18] Wang Y, Chen D, Zhang C, et al. Wide and recurrent neural networks for detection of false data injection in smart grids [C]//International Conference on Wireless Algorithms, Systems, and Applications,2019:335 - 345.

[19] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[C]//Advances in Neural Information Processing Systems, 2017:5998 - 6008.

[20] Yu Z, 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.

[21] Bahdanau D, Cho K, Bengio Y. Neural machine translation by jointly learning to align and translate[EB]. arXiv:1409.0473,2014.

[22] Devlin J, Chang M W, Lee K, et al. Bert: Pre-training of deep bidirectional transformers for language understanding [EB]. arXiv:1810.04805,2018.

[23] Kingma D P, Ba J. Adam: A method for stochastic optimization[EB]. arXiv:1412.6980,2014.

(上接第 314 页)

[7] 何青,张小琳,贾梦蕾,等.基于可搜索加密的云计算智慧家居系统研究[J].无线互联科技,2017(5):53 - 54,92.

[8] Li J N, Niu X Y, Sun J S. A practical searchable symmetric encryption scheme for smart grid data[C]//ICC 2019 IEEE International Conference on Communications,2019:1 - 6.

[9] Sun W, Wang B, Cao N, et al. Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking[J]. IEEE Parallel and Distributed Technology Systems and Applications, 2013, 25(11):3025 - 3035.

[10] Yu J, Peng L, Zhu Y, et al. Toward secure multikeyword Top-k retrieval over encrypted cloud data[J]. IEEE Transactions on Dependable & Secure Computing, 2013, 10(4): 239 - 250.

[11] Cao N, Wang C, Li M, et al. Privacy-Preserving Multi-Keyword ranked search over encrypted cloud data[J]. IEEE Transactions on Parallel and Distributed Systems,2014, 25(1):222 - 233.

[12] Sun J, Ren L, Wang S, et al. Multi-keyword searchable and data verifiable attribute-based encryption scheme for cloud storage[J]. IEEE Access,2019,7:66655 - 66667.

[13] Krishnamoorthy S. Efficient mining of high utility itemsets with multiple minimum utility thresholds[J]. Engineering Applications of Artificial Intelligence, 2018, 69(1):112 - 126.

[14] Quyen H T L, Tuong L, Bay V, et al. An efficient and effective algorithm for mining top-rank-k frequent patterns[J]. Expert Systems with Applications,2015,42(1):156 - 164.

[15] Tuong L, Bay V, Sung W B. Efficient algorithms for mining top-rank-k erasable patterns using pruning strategies and the subsume concept[J]. Engineering Applications of Artificial Intelligence,2018,68(2):1 - 9.

[16] Zhang C, Wen K, Zheng Y. Maximal frequent itemset mining algorithm based on B-list[J]. Computer Application Research, 2019,36(2):351 - 354.

[17] Deng Z H, Lv S L. PrePost + : An efficient N-lists-based algorithm for mining frequent itemsets via Children—Parent Equivalence pruning[J]. Expert Systems with Applications, 2015,42(13):5424 - 5432.

[18] Dam T L, Li K, Fournierviger P, et al. An efficient algorithm for mining top-rank-k frequent patterns[J]. Applied Intelligence,2016,45(1):96 - 111.

[19] Zhao X, Zhang X, Wang P, et al. A weighted frequent itemset mining algorithm for intelligent decision in smart systems[J]. IEEE Access,2018,6:29271 - 29282.

[20] Lee G, Yun U, Ryu K H. Mining frequent weighted itemsets without storing transaction IDs and generating candidates [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,2017,25(1):111 - 144.

[21] Lan G C, Hong T P, Lee H Y, et al. Tightening upper bounds for mining weighted frequent itemsets[J]. Intelligent Data Analysis,2015,19(2):413 - 429.

[22] Nguyen H, Vo B, Nguyen M, et al. An efficient algorithm for mining frequent weighted itemsets using interval word segments[J]. Applied Intelligence,2016,45(4):1008 - 1020.

[23] Li X, Du T, Liu B. Fast algorithm for mining frequent patterns based on B-list[J]. Computer Application Research, 2017,37(8):2357 - 2361,2367.