DOI: 10.19783/j.cnki.pspc.201130

基于边缘计算的电网假数据攻击分布式检测方法

黄冬梅[1]，何立昂[2]，孙锦中[1]，胡安铎[1]

（1. 上海电力大学电子与信息工程学院，上海 201306；2. 上海电力大学电气工程学院，上海 200090）

摘要：虚假数据注入攻击(FDIA)作为新型的电网攻击手段，严重威胁智能电网的安全运行。爆炸式增长的数据给集中式的 FDIA 检测方法带来了巨大的挑战。基于此，提出了一种基于边缘计算的分布式检测方法。将系统拆分为多个子系统，且在子系统中设置边缘节点检测器进行数据的收集、检测。结合深度学习的方法，构建了 CNN-LSTM 模型检测器，提取数据特征，并将模型的训练过程放置在中心节点上，实现高效、低时延的 FDIA 检测。最后在 IEEE 14 节点和 IEEE39 节点测试系统中，设定不同攻击强度，对所提边缘检测方法进行验证。结果表明，与集中式的检测方法相比，所提边缘检测方法在检测时间和内存消耗两个指标上有明显的下降。

关键词：假数据攻击；边缘计算；分布式检测；深度学习

Distributed detection method for a false data attack in a power grid based on edge computing

HUANG Dongmei[1], HE Li'ang[2], SUN Jinzhong[1], HU Anduo[1]

(1. College of Electronics and Information Engineering, Shanghai University of Electric Power, Shanghai 201306, China;
2. College of Electrical Engineering, Shanghai University of Electric Power, Shanghai 200090, China)

Abstract: A new method of power grid attack, the False Data Injection Attack (FDIA), seriously threatens the safe operation of smart grids. The explosive growth of data has brought huge challenges to centralized FDIA detection methods. This paper proposes a detection method based on edge computing, which divides the system into multiple subsystems, and sets edge node detectors in the subsystems for data collection and detection. Combined with deep learning methods, a CNN-LSTM detecting model is constructed to extract the characteristics of the data, and the training process of the model is placed on the central node to achieve efficient and low-latency FDIA detection. Finally, the proposed edge detection method is verified in the IEEE 14-node and IEEE 39-node test systems for different attack intensities. Compared with the centralized detection method, the results show that the advanced edge detection method can achieve a significant drop in detection time and memory consumption.

This work is supported by the National Natural Science Foundation of China (No. 41671431).

Key words: false data attack; edge computing; distributed detection; deep learning

0 引言

近年来，随着信息通信技术的快速发展，现代电网中信息系统与电力系统不断融合，使得现代电力系统变得“智能化”，发展成智能电网[1]，同时也使其更容易遭受网络攻击。2015 年 12 月，乌兰电网因遭受黑客攻击[2]造成大规模停电事故；2019 年 3 月，委内瑞拉因遭受网络攻击发生最大规模的停电，导致全国 23 个州里 22 个州停电，其结果是灾难性的。虚假数据攻击作为新型的网络攻击手段，严重威胁智能电网的安全运行。

虚假数据注入攻击[3-4](False Data Injection Attack, FDIA)是利用电网状态估计中的漏洞，攻击者有预谋的修改电网收集的量测数据，致使电网控制中心做出错误判断[5]，从而对电网调度和稳定运行造成巨大危害。针对不同的 FDIA，近年来提出了许多检测方法[6]。例如文献[7]提出了一种具有鲁棒性的电网安全框架，在该框架中采用卡尔曼滤波估计，将估计量和系统读数传入卡方检测器和欧式检测器，结果发现欧式距离的度量方式在识别 FDIA 的性能上要优于卡方检测器。文献[8]提出一种框架

基金项目：国家自然科学基金项目资助(41671431)；上海市科委地方院校能力建设项目资助(20020500700)

来检测具有信息物理特性的直流微电网的 FDI 攻击，将物理设备和信息物理系统的控制软件描述为仿真状态流动图(Simulink State Flow, SLSF)，通过对 SLSF 的输入输出进行动态分析推断出候选变量，将候选不变量与实际不变量进行对比，任何不匹配则表明 FDIA 的存在。文献[9]提出了一种检测方法，利用当前数据与历史正常数据的 KL 距离(Kullback-Leibler Distance, KLD)来判断是否存在 FDIA 攻击。上述这些传统方法都是集中式的检测方法，随着智能电网的发展，系统运行速度越来越快，产生的数据越来越多，传统的集中式处理方法无法应对智能电网中爆炸式增长的数据量。分布式的检测方法应运而生，如文献[10]提出了一种自适应采样序列的分布式检测，能够在保证鲁棒性的同时降低能耗，提高检测效率。文献[11]设计了包含中心协调器的双层分布式估计系统，实现结点的内部估计和边界估计。

近年来，随着人工智能的火热发展，将机器学习和深度学习应用于 FDIA 检测成为了一种趋势[12]，这些方法能有效地应对实时的电网数据量的增加，并较传统的检测方法有明显的改进，如文献[13]设计出两种基于机器学习的检测技术，一种是利用带标记数据的监督学习来训练支持向量机，另一种是不需要训练数据的无监督学习算法。文献[14]提出了一种基于深度学习的模型，用于检测智能电表中的 FDIA 攻击。该模型是对历史测量数据的模式进行识别来判断是否遭受了 FDIA 攻击。文献[15]提出了一种基于分布式事件触发机制与机器学习相结合的攻击检测方法。文献[16]提出了一种基于聚类算法与状态预测检测法的 FDIA 检测技术，通过节点和 FDIA 的内部关系，辨识出脆弱节点，采用聚类算法对脆弱节点进行划分并分级，最后通过状态预测检测法完成对 FDIA 的检测。

然而上述方法依赖于云计算技术，所有采集的数据都在电网的数据中心进行处理和应用等工作，有限的通信和存储资源使得电网实时处理数据的能力不足，会导致电网的一些关键性操作不能及时执行。本文提出一种基于边缘计算的分布式检测方法，在电网的边缘侧设置边缘节点检测器，代替原来的中央处理器直接进行数据的收集、存储和检测，将传统集中式的检测变换成分布式的检测方法，并结合深度学习的方法，构建 CNN-LSTM 模型检测器，通过 CNN-LSTM 网络提取数据特征，并将训练过程从边缘节点分离，放置在中心节点完成。最后在测试系统中进行了仿真实验，验证了该方法相较于传统的集中式检测方法，在检测时间和内存消耗上具有较大的优势。

1 问题描述

1.1 状态估计

状态估计是现代电网安全、稳定、效率运行的重要功能之一[6,17]。在电网中，调度中心需要可靠的状态变量来控制和调度发电、输电、配电，调度中心通过数据采集与监控系统(Supervisory Control and Data Acquisition, SCADA)来收集远程智能仪表的量测读数，估计系统运行状态。

正常稳定运行的电力系统，直流状态估计方程为

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

式中：$\boldsymbol{z}$ 为来自数据采集中心的量测值，用于状态估计，被电表采集后上传到能量控制中心；$\boldsymbol{H}$ 为电网拓扑的雅可比矩阵；$\boldsymbol{x}$ 为系统状态变量；$\boldsymbol{e}$ 为量测值误差向量，且服从均值为 0、方差为对角矩阵 $\sum_{\boldsymbol{e}}=\mathrm{diag}\left[\boldsymbol{\sigma}_1^2,\boldsymbol{\sigma}_2^2,\cdots,\boldsymbol{\sigma}_m^2\right]$ 的正态分布。

残差的表达式为

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}} \tag{2}$$

被估计的状态 $\hat{\boldsymbol{x}}$ 可通过最小化式(3)的目标函数得到。

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

通过加权最小二乘估计得到状态变量 $\hat{\boldsymbol{x}}$ 为

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{z} \tag{4}$$

1.2 虚假数据注入攻击原理

传统 FDIA 通常为

$$\boldsymbol{z}_a=\boldsymbol{z}+\boldsymbol{a}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{e} \tag{5}$$

式中：$\boldsymbol{a}$ 为注入的攻击向量；$\boldsymbol{z}_a$ 为被攻击后的量测值向量；$\boldsymbol{x}$ 为原始状态估计值。

要想构建不可观察的 FDIA[16]，只需向量 $\boldsymbol{a}$ 满足式(6)。

$$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c} \tag{6}$$

$$\hat{\boldsymbol{x}}_a=\hat{\boldsymbol{x}}+\boldsymbol{c} \tag{7}$$

式中：$\boldsymbol{c}=[c_1,c_2,\cdots,c_n]^{\mathrm{T}}$ 为一个任意非零向量，其中的非零元素表示该位量测值被攻击；$\hat{\boldsymbol{x}}_a=\hat{\boldsymbol{x}}+\boldsymbol{c}$ 为被攻击后 $\boldsymbol{z}_a$ 的估计值。那么被攻击后的量测值 $\boldsymbol{z}_a$ 向量表达式为

$$\boldsymbol{z}_a=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{H}\boldsymbol{c}+\boldsymbol{e}=\boldsymbol{H}(\boldsymbol{x}+\boldsymbol{c})+\boldsymbol{e}=\boldsymbol{H}\boldsymbol{x}_a+\boldsymbol{e} \tag{8}$$

式(8)中 $\boldsymbol{z}_a$ 形式和式(5)中的相同，此时，被攻击后的残差 r_a 为

$$\begin{aligned}\boldsymbol{r}_a=\boldsymbol{z}_a-\boldsymbol{H}\boldsymbol{x}_a=\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(x+c)=\\ \boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}+(\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c})=\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}\end{aligned} \tag{9}$$

结果同式(2)，由此可以看出只要满足 $\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$，

FDIA 就可以躲过不良数据辨识[18]机制，从而实现“隐形”的电网攻击。

2　基于边缘计算的分布式检测框架

2.1 边缘计算

随着电网规模不断扩大，数据量呈爆炸式增长，云计算瓶颈凸显的同时，边缘计算[4,19]引起了工业界和学术界的重点关注。对于边缘计算有多种定义，但其实质都是将云中心的部分功能下放到靠近数据源的网络边缘侧[20]，以实现数据及相关应用的就地/就近处理。在电力大数据的背景下，边缘计算既能减轻云中心的数据流量压力，又能提高数据处理效率，具有低时延、低宽带、实时性高的特点，是推动电力物联网发展的关键技术之一。

2.2 基于边缘计算的分布式检测模型

本文提出基于边缘计算的分布式检测方法，如图 1 所示。在边缘侧收集数据，模型的训练过程放在中心计算节点上完成，并将训练好的模型下发至边缘节点，实现高效的边缘侧的检测。通过中心节点和边缘节点的协同工作，实现分布式的数据检测。分布式检测系统的基本功能如下。

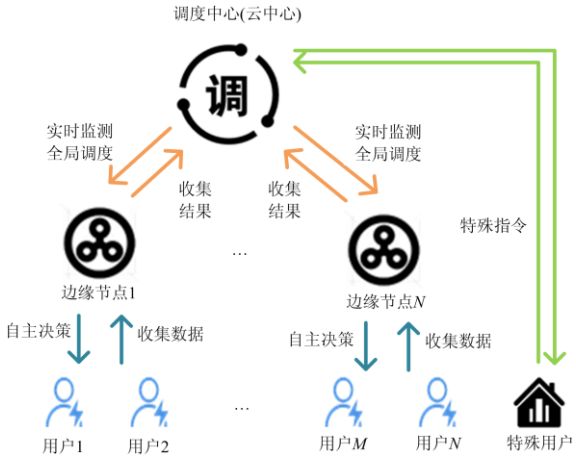


图 1　基于边缘计算的分布式检测框架

Fig. 1 Distributed detection framework based on edge computing

1) 在边缘端，边缘节点负责收集和存储智能电表及周边相关数据，并将处理后的实时数据和已存储的相关历史数据作为输入上传至中心节点，由中心节点完成模型的训练过程。中心节点将训练好的 FDIA 检测模型下发至边缘节点，更新当前边缘节点的检测模型并进行数据检测。边缘节点可以自己实现本区域简单调度工作。相较于传统电网只能通过云中心进行统一调度，边缘节点可看成是云中心在各区域分派了多个“调度员”，承担各自区域的简单区调任务。同时中心节点承担了检测模型的训练任务，该模型训练完成后可下放至相应边缘节点上完成离线检测，实现电网更高效安全的监测，减小了调度中心的压力。

2) 在边云协同中，各边缘节点将检测和决策结果传输至云中心，云中心对边缘节点进行收集和监视，若发现边缘端检测或决策结果出现异常，可进行全局的调度和控制，对异常节点进行隔离、修复、指令的再下发。

3　基于 CNN-LSTM 网络的边缘检测器

3.1 卷积神经网络

卷积神经网络(CNN)是近年在深度学习领域应用广泛的模型之一[21]，其基本结构如图 2 所示。基本的 CNN 模型采用局部连接和共享权值的方式，通过卷积层和池化层的交替使用，获取原始数据中有效的表征，本文采用 CNN 模型将边缘侧采集的量测值的数据特征提取出来。

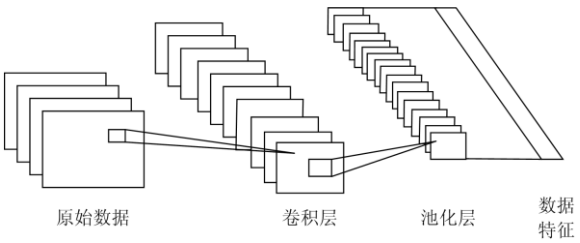


图 2　CNN 基本结构图

Fig. 2 CNN basic structure diagram

3.2 LSTM 网络

长短期记忆神经网络 LSTM[22-25]是从原来的循环神经网络上进行了改进，相较于原来的循环神经网络，有效地解决了训练过程中出现的梯度爆炸以及梯度消失的问题，LSTM 在数据量大的情况下性能更加优越。其网络基本单元如图 3 所示。

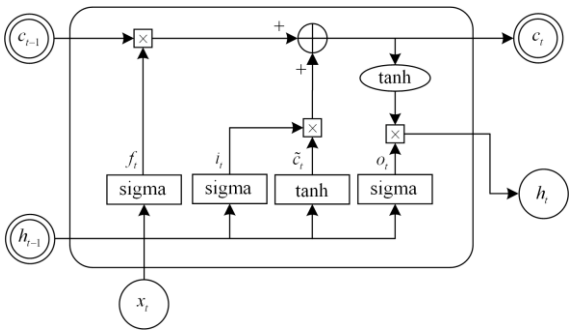


图 3　LSTM 网络基本单元图

Fig. 3 LSTM network basic unit diagram

LSTM 网络的基本单元包括遗忘门、输入门和输出门。本文将提取出的特征向量 $\boldsymbol{x}_t$ 与状态记忆单

元 $\boldsymbol{c}_{t-1}$ 以及中间输出 $\boldsymbol{h}_{t-1}$ 结合输入进遗忘门，从而来决定状态记忆单元中需要遗忘的部分；输入门中的 $\boldsymbol{x}_t$ 分别经过 sigmoid 和 tanh 激活函数变化后共同决定状态记忆单元中需要保留的向量；中间输出的 $\boldsymbol{h}_t$ 由更新后的 $\boldsymbol{c}_t$ 以及输出门的 $\boldsymbol{o}_t$ 共同决定，具体计算公式如式(10)—式(15)所示。

$$i_t=\sigma(x_tW_{xi}+h_{t-1}W_{hi}+b_i) \tag{10}$$

$$f_t=\sigma(x_tW_{xf}+h_{t-1}W_{hf}+b_f) \tag{11}$$

$$o_t=\sigma(x_tW_{xo}+h_{t-1}W_{ho}+b_o) \tag{12}$$

$$\tilde{c}_t=\tanh(x_tW_{xc}+h_{t-1}W_{hc}+b_c) \tag{13}$$

$$c_t=f_t\odot c_{t-1}+i_t\odot \tilde{c}_t \tag{14}$$

$$h_t=o_t\odot \tanh(c_t) \tag{15}$$

式中：i_t、f_t、o_t、$\tilde{c}_t$、c_t、h_t 分别为时间步为 t 时刻的输入门、遗忘门、输出门、候选状态记忆单元、状态记忆单元及中间输出；W_{xi}、W_{hi}、b_i 为输入门的权重和偏置量；W_{xf}、W_{hf}、b_f 为遗忘门的权重和偏置量；W_{xo}、W_{ho}、b_o 为输出门的权重和偏置量；W_{xc}、W_{hc}、b_c 为候选状态记忆单元的权重和偏置量；σ 表示 sigmoid 激活函数；tanh 表示 tanh 激活函数；$\odot$ 为按元素相乘。

3.3 CNN-LSTM 边缘检测器

本文提出的 CNN-LSTM 边缘检测器基本框架如图 4 所示，CNN-LSTM 网络主要由两部分构成，CNN 模块的主要作用是从数据中进行特征地提取和整合，LSTM 模块是将整合出的特征进行记忆与筛选，并进行拟合预测，最后通过 softmax 层进行分类。

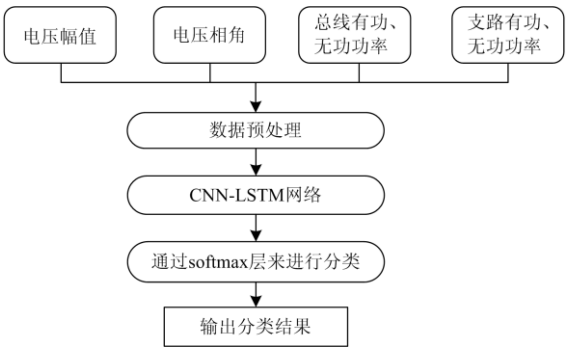


图 4 CNN-LSTM 边缘检测器框图

Fig. 4 CNN-LSTM edge detector block diagram

4 实验结果

考虑到边缘计算的计算能力，本文选择 IEEE14 节点和 IEEE39 节点系统作为测试环境，实验数据即为图 4 中的 4 种输入。随机选择 60 000 组量测样本作为实验数据组成训练和测试集，且使用配置相同的计算机来模拟边缘检测器。

4.1 检测评估指标

本文采用准确度、时间和程序所占内存百分比等 3 个指标，验证所提出的分布式框架检测的有效性和可行性。首先定义如下变量。

1) 真负类(true negative)表示将正常数据识别成正常数据的数量，记为 T_{n}。

2) 假负类(false negative)表示将正常数据识别成错误数据的数量，记为 F_{n}。

3) 真正类(true positive)表示将错误数据识别成错误数据的数量，记为 T_{p}。

4) 假正类(false positive)表示将错误数据识别成正常数据的数量，记为 F_{p}。

用准确率(记为 A_{c})来衡量分布式的检测模型的性能，采用时间和占用内存百分比作为评价指标。

准确率的计算表达式为

$$A_{\mathrm{c}}=\frac{T_{\mathrm{n}}+T_{\mathrm{p}}}{T_{\mathrm{n}}+F_{\mathrm{n}}+T_{\mathrm{p}}+F_{\mathrm{p}}} \tag{16}$$

4.2 IEEE14 节点测试系统的仿真研究

对于 IEEE14 和 IEEE39 节点总线测试系统，如图 5 和图 6 所示，14 个节点被划分为 4 个区域，39 个节点被划分为 5 个区域，一个区域内的电力数据传输给同一个边缘检测器去进行收集、计算和处理，每个边缘检测器都与中心控制器 C 相连。假设系统可以由每个母线的相角幅值、注入功率和各个线路的功率流来完全测量，用 MATPOWER[26]来模拟所有的数据。本次实验主要从平衡[27]的角度去验证检测器在不同强度下的表现情况。

4.3 不同攻击强度下检测实验结果

FDIA 攻击强度的影响因素主要为攻击向量 $\boldsymbol{a}$ 的稀疏性和方差，稀疏度表示量测值中被攻击的数量，方差表示 FDIA 所带来的干扰的大小，本文将受损量测值的稀疏度设置为满秩，即量测值全部被攻击的情况下，攻击强度用 A 表示[24]。本实验将攻击强度分为以下 3 个等级：A=0.05 代表较小强度，A=0.5 代表中等强度，A=5 代表较大强度。

实验结果中出现的两种检测器：中心检测器和边缘检测器，分别放置在中心控制节点和边缘节点上，用这两种检测器模拟集中式和边缘分布式检测的情况。当采用集中式检测方法时，所有的操作过程均在中心节点上完成，用中心检测器模拟集中式方法的检测情况；当采用边缘分布式检测方法时，边缘节点的边缘检测器用来模拟分布式检测情况，将数据进行收集、处理、上传等操作，此时中心控制节点负责完成模型的训练过程和模型的下发。

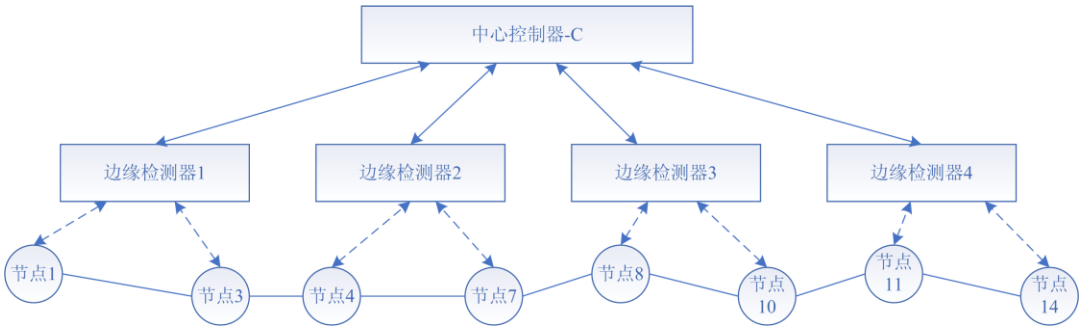


图 5 IEEE14 节点系统的分布式框架检测图

Fig. 5 Diagram of distributed detecting frame for IEEE14 node system

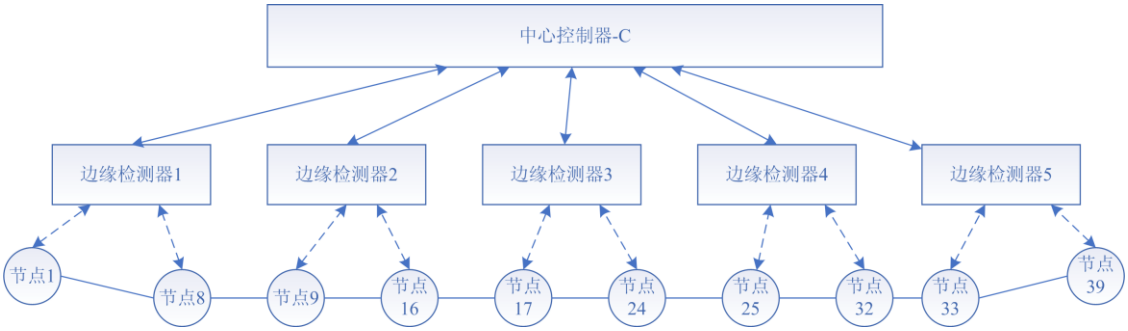
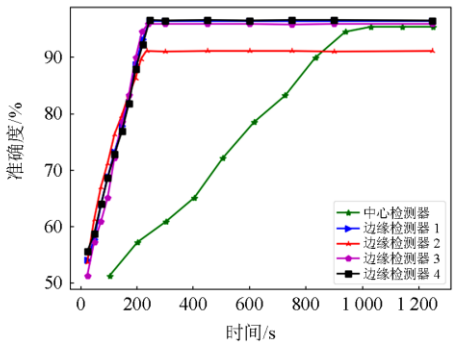


图 6 IEEE39 节点系统的分布式框架检测图

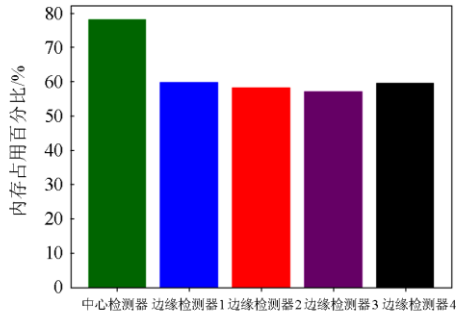
Fig. 6 Diagram of distributed detecting frame for IEEE39 node system

1) IEEE14 节点测试系统的仿真研究

图 7—图 9 及表 1—表 3，给出了 IEEE14 节点系统检测结果，包括中心检测器和边缘检测器。可以清楚地观察到表 1 中除了边缘检测器 2 的检测率略低于中心检测器，边缘检测器 1、3、4 的准确率均高于中心检测器。该情况的发生可能是因为攻击强度较低时(A=0.05)，攻击的特征不明显，导致 2 号边缘检测器的模型拟合的效果不够好，泛化能力稍弱一点；随着攻击强度的增加，攻击的特征愈发明显，边缘检测器检测的准确率呈上升趋势，在中强度和高强度的情况下都比中心检测器的准确率要高。同时，边缘检测器在检测时间和内存消耗上要比中心检测器有明显的降低。在不同的攻击强度下，中心检测器的检测时间明显地大于边缘检测器的检测时间，效果显著，说明本文所提的分布式检测方案能够发挥出边缘计算的优势，有更低的延时性，且随着攻击强度的增加，攻击特征越来越明显，模型识别的速度越快，检测所耗的时间就越少；内存方面，边缘检测器消耗的内存要少于中心检测器，效果同样明显；对于不同的攻击强度，两种检测器消耗内存的百分比随着攻击强度的上升都呈下降趋势，但是变化不大，中心检测器由 78.2%降低至 71.8%；边缘检测器占用内存比下降了 3%左右。



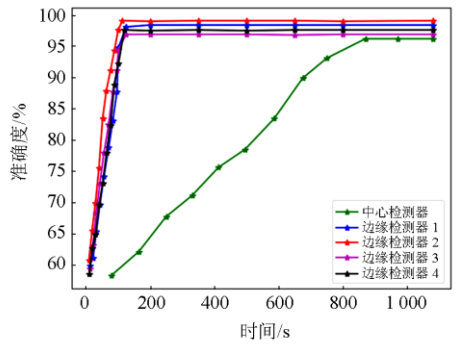
(a) 各检测器所用时间和准确率的对比图



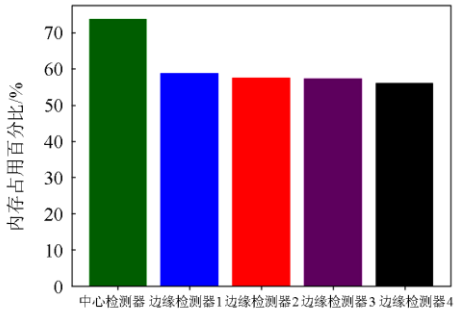
(b) 各检测器所占内存百分比图

图 7 A=0.05(低强度)时中心检测和边缘检测的实验结果

Fig. 7 Experimental results of center detection and edge detection when A=0.05 (low intensity)



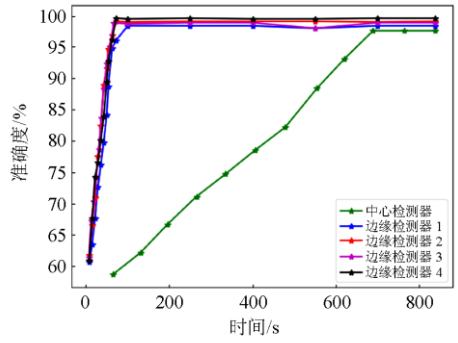
(a) 各检测器所用时间和准确率的对比图



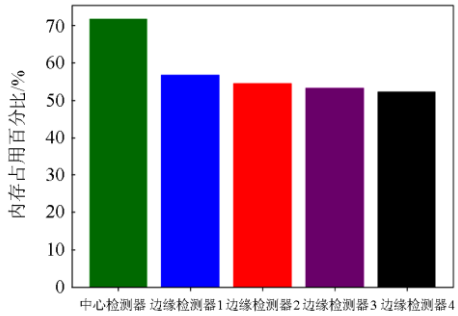
(b) 各检测器所占内存百分比图

图 8　A=0.5（中强度）时中心检测和边缘检测的实验结果

Fig. 8 Experimental results of center detection and edge detection when A=0.5 (medium intensity)



(a) 各检测器所用时间和准确率的对比图



(b) 各检测器所占内存百分比图

图 9　A=5（高强度）时中心检测和边缘检测的实验结果

Fig. 9 Experimental results of center detection and edge detection when A=5 (high intensity)

表 1　A=0.05 时实验数据

Table 1 Experimental data when A=0.05

	中心检测器	边缘检测器 1	边缘检测器 2	边缘检测器 3	边缘检测器 4
准确度/%	95.4	96.4	91.1	95.9	96.6
时间/min	17.2	4.1	3.9	4.0	4.1
内存/%	78.2	59.7	58.3	57.2	59.5

表 2　A=0.5 时实验数据

Table 2 Experimental data when A=0.5

	中心检测器	边缘检测器 1	边缘检测器 2	边缘检测器 3	边缘检测器 4
准确度/%	96.2	98.4	99.1	96.9	97.6
时间/min	14.5	2.1	1.9	2.1	2.0
内存/%	73.8	58.7	57.5	57.2	56.1

表 3　A=5 时实验数据

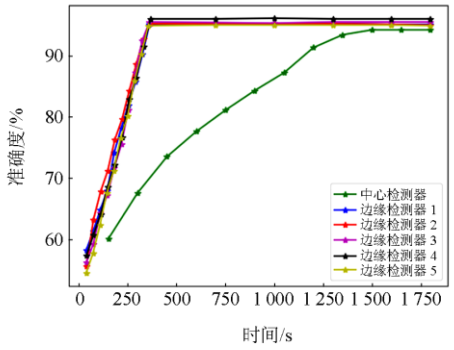
Table 3 Experimental data when A=5

	中心检测器	边缘检测器 1	边缘检测器 2	边缘检测器 3	边缘检测器 4
准确度/%	97.6	98.4	99.1	98.9	99.6
时间/min	11.5	1.2	1.2	1.1	1.2
内存/%	71.8	56.7	54.5	53.2	52.2

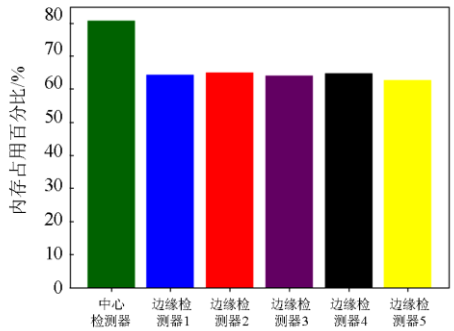
2) IEEE39 节点测试系统的仿真研究

图 10—图 12 及表 4—表 6，给出了 IEEE39 节点系统的检测结果。可以清楚地观察到在 IEEE39 节点测试系统中，边缘检测器的检测准确率均高于

中心节点的检测率。如表 4 所示，在攻击强度 A=0.05 时，中心检测器的检测准确率为 94.2%，边缘检测器的准确率均在 95%以上。这是因为 39 节点相较于 14 节点，边缘节点能获得的数据特征更多，模型拟合效果更好，边缘检测器检测的结果要优于中心检测器的检测结果；随着攻击强度的增加，边缘检测器检测准确率均呈上升趋势，与在 IEEE14 节点实验的趋势相吻合。同时，边缘检测器在检测时间和内存消耗上两个指标上也都呈下降趋势，如表 6 所示，在 A=5 时，中心检测器检测时间需 18.5 min，各个边缘检测器的检测时间均在 2 min 左右，证明了本文所提分布式检测方法在不同的系统和攻击强



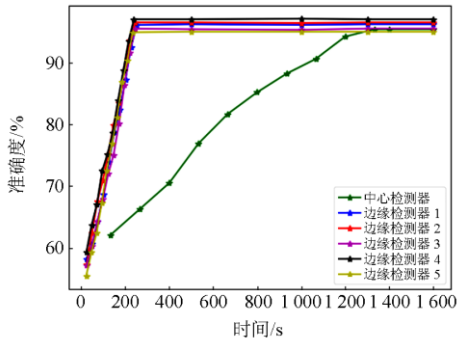
(a) 各检测器所用时间和准确率的对比图



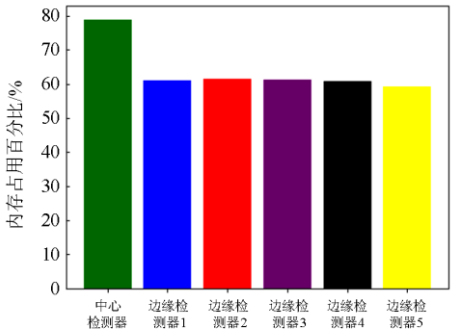
(b) 各检测器所占内存百分比图

图 10　A=0.05（低强度）时中心检测和边缘检测的实验结果

Fig. 10 Experimental results of center detection and edge detection when A=0.05 (low intensity)



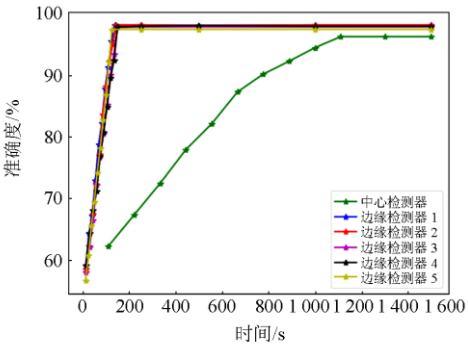
(a) 各检测器所用时间和准确率的对比图



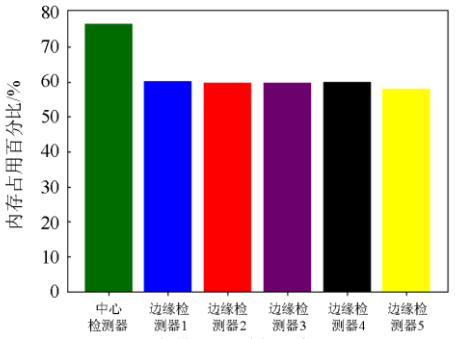
(b) 各检测器所占内存百分比图

图 11　A=0.5（中强度）时中心检测和边缘检测的实验结果

Fig. 11 Experimental results of center detection and edge detection when A=0.5 (medium intensity)



(a) 各检测器所用时间和准确率的对比图



(b) 各检测器所占内存百分比图

图 12　A=5（高强度）时中心检测和边缘检测的实验结果

Fig. 12 Experimental results of center detection and edge detection when A=5 (high intensity)

度下，检测时间和内存占比均低于中心检测器，能够发挥出边缘计算的低延时性。但 39 节点测试的准确率结果整体上要略低于 14 节点的测试结果，这可能是因为 14 节点测试系统的数据要少于 39 节点测试系统，数据的维数在卷积和池化的操作过程中减少的较少，所以 14 节点测试系统的准确率结果要更高一点。除此之外，可能是 39 节点的数据量更多，维度更高更复杂，检测的难度会高于 14 节点系统。

表 4 $A=0.05$ 时实验数据

Table 4 Experimental data when $A=0.05$

	中心检测器	边缘检测器 1	边缘检测器 2	边缘检测器 3	边缘检测器 4	边缘检测器 5
准确度/%	94.2	95.1	95.1	95.5	96.0	95.0
时间/min	25.0	6.0	6.1	6.1	6.2	5.9
内存/%	80.7	64.2	65.0	64.1	64.7	62.6

表 5 $A=0.5$ 时实验数据

Table 5 Experimental data when $A=0.5$

	中心检测器	边缘检测器 1	边缘检测器 2	边缘检测器 3	边缘检测器 4	边缘检测器 5
准确度/%	95.4	96.2	96.6	96.5	97.0	96.1
时间/min	22.2	4.2	4.1	4.1	4.0	3.9
内存/%	78.9	61.0	61.2	61.5	60.8	59.9

表 6 $A=5$ 时实验数据

Table 6 Experimental data when $A=5$

	中心检测器	边缘检测器 1	边缘检测器 2	边缘检测器 3	边缘检测器 4	边缘检测器 5
准确度/%	96.6	98.2	98.2	97.9	98.0	97.5
时间/min	18.5	2.3	2.4	2.5	2.5	2.1
内存/%	76.7	60.1	59.8	59.9	59.9	58.0

5 结语

本文在当下大数据时代背景下，针对电力数据海量增长的情况，结合边缘计算的特点提出了一种全新的分布式检测框架，利用边缘计算的优势来实现轻量级的检测器，并结合深度学习的方法，将繁琐的训练过程放置资源充足的中心节点完成，从而有效地减少了数据的传输时间、检测器的决策时间。仿真结果表明，该框架下的检测方案具有较高的检测精度、较低的时延和较少的内存占有率，能够实现实时高效的检测。未来可以继续探索边缘节点分布对 FDIA 的影响，如何经济、高效的布置边缘节点来检测电网的攻击，以及如何将边缘计算模式应用在电力气象灾害预警等场景中。

参考文献

[1] RAJARAMAN P, SUNDARAVARADAN N A, MALLIKARJUNA B, et al. Robust fault analysis in transmission lines using synchrophasor measurements[J]. Protection and Control of Modern Power Systems, 2018, 3(1): 108-110. DOI: 10.1186/s41601-018-0082-4.

[2] 郭庆来, 辛蜀骏, 王剑辉, 等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化, 2016, 40(5): 145-147.
GUO Qinglai, XIN Shujun, WANG Jianhui, et al. Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout[J]. Automation of Electric Power Systems, 2016, 40(5): 145-147.

[3] LIU Y, REITER M K, NING P. False data injection attacks against state estimation in electric power grids[C] // Proceedings of the 2009 ACM Conference on Computer and Communications Security, November 9-13, 2009, Chicago, Illinois, USA: 23-32.

[4] 钱斌, 蔡梓文, 肖勇, 等. 基于边缘计算的电表计量系统数据协同检测方案[J]. 中国电力, 2019, 52(11): 145-152.
QIAN Bin, CAI Ziwen, XIAO Yong, et al. Data collaborative detection scheme of electric metering system based on edge computing[J]. Electric Power, 2019, 52(11): 145-152.

[5] XU Yan. A review of cyber security risks of power systems: from static to dynamic false data attacks[J]. Protection and Control of Modern Power Systems, 2020, 5(3): 190-201. DOI: 10.1186/s41601-020-00164-w.

[6] 赵丽莉, 刘忠喜, 孙国强, 等. 基于非线性状态估计的虚假数据注入攻击代价分析[J]. 电力系统保护与控制, 2019, 47(19): 38-45.
ZHAO Lili, LIU Zhongxi, SUN Guoqiang, et al. Cost analysis of false data injection attack based on nonlinear state estimation[J]. Power System Protection and Control, 2019, 47(19): 38-45.

[7] MANANDHAR K, CAO X, HU F, et al. Combating false data injection attacks in smart grid using Kalman filter[C] // 2014 International Conference on Computing, Networking and Communications (ICNC), February 3-6, 2014, Honolulu, HI, USA: 16-20.

[8] BEG O A, JOHNSON T T, DAVOUDI A. Detection of false-data injection attacks in cyber-physical DC microgrids[J]. IEEE Transactions on Industrial Informatics, 2017, 13(5): 2693-2703.

[9] CHAOJUN G, JIRUTITIJAROEN P, MOTANI M. Detecting false data injection attacks in AC state estimation[J]. IEEE Transactions on Smart Grid, 2015,

6(5): 2476-2483.

[10] LI S, YILMAZ Y, WANG X. Quickest detection of false data injection attack in wide-area smart grids[J]. IEEE Transactions on Smart Grid, 2017, 6(6): 2725-2735.

[11] KORRES G N. A distributed multiarea state estimation[J]. IEEE Transactions on Power Systems, 2011, 26(1): 73-84.

[12] ASHRAFUZZAMAN M, CHAKHCHOUKH Y, JILLEPALLI A A, et al. Detecting stealthy false data injection attacks in power grids using deep learning[C] // 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), June 25-29, 2018, Limassol, Cyprus: 219-225.

[13] ESMALIFALAK M, LIU L, NGUYEN N, et al. Detecting stealthy false data injection using machine learning in smart grid[J]. IEEE Systems Journal, 2017, 11(3): 1644-1652.

[14] 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.

[15] 陈刘东, 刘念. 面向互动需求响应的虚假数据注入攻击及其检测方法[J]. 电力系统自动化, 2021, 45(3): 15-23.
CHEN Liudong, LIU Nian. False data injection attack and detection method for interactive demand response[J]. Automation of Electric Power Systems, 2021, 45(3): 15-23.

[16] 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 and Instrumentation, 2019(3): 49-52.

[16] 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 & Learning Systems, 2015, 27(8): 1773-1786.

[17] 沈玉兰, 张璞, 李翔宇, 等. 基于多源数据融合的电网抗差状态估计[J]. 广东电力, 2019, 32(9): 146-153.
SHEN Yulan, ZHANG Pu, LI Xiangyu, et al. Grid robust state estimation based on multi-source date fusion[J]. Guangdong Electric Power, 2019, 32(9): 146-153.

[18] 刘雯静, 杨军, 袁文, 等. 一种基于PMU和SCADA单节点互校核的前端数据辨识框架[J]. 电力系统保护与控制, 2020, 48(8): 1-9.
LIU Wenjing, YANG Jun, YUAN Wen, et al. A front-end data identification framework based on single-node mutual checking between PUM and SCADA[J]. Power System Protection and Control, 2020, 48(8): 1- 9.

[19] 曹培, 徐鹏, 高凯, 等. 基于边缘计算的电缆接头运行状态智能传感与监测[J]. 高压电器, 2020, 56(9): 26-32.
CAO Pei, XU Peng, GAO Kai, et al. Intelligent sensing and monitoring of cable joints' state based on edge computing[J]. High Voltage Apparatus, 2020, 56(9): 26-32.

[20] 朱友康, 乐光学, 杨晓慧, 等. 边缘计算迁移研究综述[J]. 电信科学, 2019, 35(4): 74-94.
ZHU Youkang, LE Guangxue, YANG Xiaohui, et al. A survey on edge computing off loading[J]. Telecommunications Science, 2019, 35(4): 74-94.

[21] 刘佳翰, 陈克绪, 马建, 等. 基于卷积神经网络和随机森林的三相电压暂降分类[J]. 电力系统保护与控制, 2019, 47(20): 112-118.
LIU Jiahan, CHEN Kexu, MA Jian, et al. Classification of three-phase voltage dips based on CNN and random forest[J]. Power System Protection and Control, 2019, 47(20): 112-118.

[22] 王激华, 仇钧, 方云辉, 等. 基于深度长短期记忆神经网络的短期负荷预测[J]. 广东电力, 2020, 33(8): 62-68.
WANG Jihua, QIU Jun, FANG Yunhui, et al. Short term load forecasting based on deep LSTM neural network[J]. Guangdong Electric Power, 2020, 33(8): 62-68.

[23] 周秀, 朱洪波, 马云龙, 等. 基于深度学习的变压器局部放电模式识别研究[J]. 高压电器, 2019, 55(12): 98-105.
ZHOU Xiu, ZHU Hongbo, MA Yunlong, et al. Partial discharge pattern recognition of transformer based on deep learning[J]. High Voltage Apparatus, 2019, 55(12): 98-105.

[24] YIN R, LI DX, WANG YF, et al. Forecasting method of monthly wind power generation based on climate model and long short-term memory neural network[J]. Global Energy Interconnection, 2020, 3(6): 571-576.

[25] 陆继翔, 张琪培, 杨志宏, 等. 基于 CNN-LSTM 混合神经网络模型的短期负荷预测方法[J]. 电力系统自动化, 2019, 43(8): 131-137.
LU Jixiang, ZHANG Qipei, YANG Zhihong, et al. Short-term load forecasting method based on CNN-LSTM hybrid neural network model[J]. Automation of Electric Power Systems, 2019, 43(8): 131-137.

[26] ZIMMERMAN R D, MURILLO-SANCHEZ 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.

[27] YAN J, TANG B, HE H. Detection of false data attacks in smart grid with supervised learning[C] // International Joint Conference on Neural Networks (IJCNN), July 24-29, 2016, Vancouver, Canada: 1395-1402.

收稿日期：2020-09-14；　修回日期：2021-02-08

作者简介：

黄冬梅(1964—)，女，教授，研究方向为海洋与电力时空信息技术；

何立昂(1996—)，男，通信作者，硕士研究生，研究方向为智能电网安全；E-mail: 1617104062@qq.com

孙锦中(1981—)，男，讲师，研究方向为电力时空信息技术。E-mail: benima2001@sina.com

（编辑　周金梅）