DOI: 10.19783/j.cnki.pspc.231632

基于深度学习的电力系统虚假数据注入攻击检测综述

李 卓[1]，谢耀滨[1]，吴茜琼[1]，张有为[2]

(1. 信息工程大学，河南 郑州 450000；2. 郑州信大先进技术研究院，河南 郑州 450000)

摘要：虚假数据注入攻击(false data injection attack, FDIA)是针对电力系统的一种常见网络攻击，可以通过终端链路或设备注入异常数据，绕过不良数据检测机制，进而引发电力系统的异常运行，造成严重的经济损失。近年来深度学习技术在 FDIA 检测方面取得诸多进展，通过大量的数据训练和强大的模型学习能力，能够自动学习和提取攻击数据特征，相对于传统方法具有更高的准确率和鲁棒性。总结了近年来基于深度学习的电力系统 FDIA 检测研究进展，涵盖卷积神经网络、循环神经网络、图神经网络、生成对抗网络和深度强化学习等典型深度学习模型。首先分析各类深度学习模型的 FDIA 检测原理，并介绍相关技术方法。然后从鲁棒性、评估指标和可扩展性等方面对上述技术进行对比分析，总结其应用范围及存在不足。最后探讨了当前研究中存在的挑战和未来的研究发展方向。

关键词：虚假数据注入；攻击检测；深度学习；电力系统安全

Review of deep learning-based false data injection attack detection in power systems

LI Zhuo[1], XIE Yaobin[1], WU Qianqiong[1], ZHANG Youwei[2]

(1. Information Engineering University, Zhengzhou 450000, China; 2. Zhengzhou Xinda Advanced Technology Research Institute, Zhengzhou 450000, China)

Abstract: False data injection attack (FDIA) is a common network attack targeting power systems. These attacks can cause abnormal operation of the power system and result in serious economic losses by injecting abnormal data through terminal links and devices which can bypass bad data detection mechanisms. In recent years, deep learning technology has made significant progress in FDIA detection. Deep learning methods can automatically learn and extract attack features with a large amount of data training and powerful learning capabilities. These methods have higher accuracy and robustness than traditional methods. The paper summarizes the research on deep-learning-based power systems FDIA detection technologies in recent years, and covers typical deep learning models such as convolutional, recurrent and graph neural networks, generative adversarial networks, and deep reinforcement learning. First, the FDIA detection principles of various deep learning models and relevant technical methods are analyzed and introduced. Then, a comparative analysis of the above-mentioned technologies in terms of robustness, evaluation indicators, and scalability is proposed to summarize their application scope and shortcomings. Finally, the challenges in current and future research directions are discussed.

This work is supported by the National Youth Science Foundation of China “Research on Intelligent Mobile Terminal Data Safety based on File Operation Characteristic Analysis” (No. 62372465).

Key words: false data injection; attack detection; deep learning; power system security

0 引言

现代电力系统依托信息技术的发展，融合了智能化、大数据、云/边缘计算等互联网技术，为电力行业带来了许多便利和机遇。十四五规划中指出“加快电网基础设施智能化改造和智能微电网建设”[1]，为电力系统智能化指明了方向。信息技术同样为电力系统引入网络安全风险，信息系统故障与网络攻击不仅会破坏信息系统的功能，还可能进一步危害到物理系统，威胁物理系统的安全运行[2]。电力系统是国家的重要基础设施，一旦电力系统遭受网络

基金项目：国家青年科学基金项目资助“基于文件操作特征分析的智能移动终端数据安全研究”(62372465)

攻击，不仅会影响电力系统的运行，同时也会造成经济损失[3]，甚至影响社会功能的正常运转和危及人身安全。

近年来，针对电力系统的网络攻击事件频繁发生，对电力系统造成了巨大的破坏。2015 年的乌克兰大规模停电事件，攻击者通过使用针对监控和数据采集(supervisory control and data acquisition, SCADA)系统的“BlackEnergy”病毒，干扰电力系统 SCADA 的正常运行，造成乌克兰大范围停电数小时，影响数百万人的日常生活[4]。2019 年的委内瑞拉停电事件，攻击者通过对水电站的攻击，使得委内瑞拉 18 个州的电力中断，持续超过 24 h[5]。

虚假数据注入攻击(false data injection attack, FDIA)是电力系统中常见的网络攻击之一，由 Liu 等人于 2009 年首次提出[6]。攻击者构造可以绕过不良数据检测的虚假测量值，通过篡改、删除或伪造测量数据，误导系统的状态估计，达到破坏系统控制、干扰正常运行等目的。例如，攻击者可以调低某条线路负载数据，系统可能会基于错误的信息将更多的潮流调度到该线路，导致线路过载或设备损坏。这些恶意篡改的数据可能会产生严重的后果，给电力系统的可靠性和稳定运行带来严重的危害。此外，由于电力系统具有高度复杂性和规模大等特性，虚假数据注入攻击隐藏在大量真实数据中，具有较高的隐蔽性，使得系统操作员难以及时发现[7]。电力系统部署了远程终端，其通信链路和软件系统可能存在安全漏洞，攻击者可以利用这些漏洞实现数据的篡改[8-9]。因此虚假数据注入攻击具有较高的危害性与可行性，对电力系统的安全保护问题提出了更高的要求。

自提出 FDIA 的概念以来，研究人员提出了许多 FDIA 检测方法，主要分为基于模型的检测方法和基于数据驱动的检测方法。基于模型的检测方法如加权最小二乘法和卡尔曼滤波方法等，基于数据驱动的检测方法包括支持向量机(support vector machines, SVM)、K 近邻(k-nearest neighbor, KNN)、决策树(decision tree, DT)和随机森林(random forest, RF)等传统的机器学习方法和各种深度学习方法。最近几年，深度学习技术在电力系统中的 FDIA 检测方面展现出了较大的潜力。深度学习在图像识别[10]、文本生成[11]、安全检测[12]等领域得到广泛应用，具备了成熟的软硬件平台，在智能电网大规模应用的背景下研究深度学习与 FDIA 检测的结合，可以为提高电力系统的安全性与稳定性提供一种可行的安全防护方法。

目前，已有大量文献对电力系统中 FDIA 的构建方法和防御检测等问题进行了总结[13-19]，但现有的综述文章并未针对使用深度学习方法检测电力系统中的 FDIA 这一方面进行总结。本文首先介绍了电力系统中 FDIA 的原理，然后对近年来所提出的使用深度学习方法对电力系统中的 FDIA 进行检测的研究内容进行了全面总结与概述。最后，对该研究领域存在的挑战以及未来的研究方向进行了分析与展望。

1 虚假数据注入攻击原理

FDIA 是一种复杂的数据篡改攻击，其原理如图 1 所示。在电力系统正常运行的情况下，SCADA 系统从现场设备收集测量数据，考虑测量误差，用状态估计器根据测量值估计电力系统的真实状态。而攻击者在了解电力系统的拓扑结构和工作原理的前提下，对系统测量值进行修改，并绕过现有的不良数据检测(bad data detection, BDD)机制。FDIA 会误导状态估计器，使其根据修改后的虚假测量值估计出错误的系统状态，进而执行潮流计算和电力调度，影响系统的安全稳定运行。FDIA 可以通过远程终端设备或通信链路发起，由于数据格式与正常数据一致，具有很强的隐蔽性，现有防火墙和入侵检测系统难以发现。

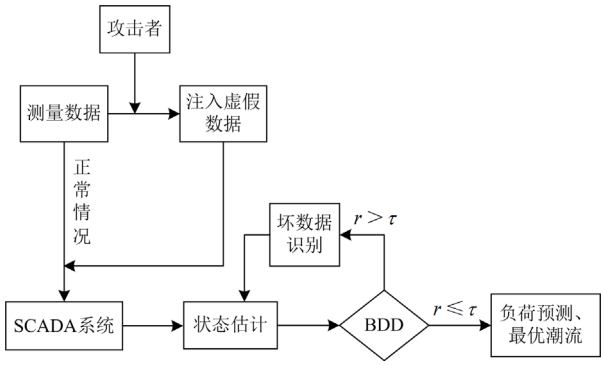

图 1 FDIA 原理

Fig. 1 FDIA principle

2 基于深度学习的虚假数据注入攻击检测方法

已有大量的文献研究了使用传统的机器学习方法检测电力系统中的 FDIA，如支持向量机[20-24]、K 近邻[25]、决策树[26-27]和随机森林[28]等监督学习方法，半监督支持向量机[29]等半监督学习方法，K 均值聚类[30-31]和主成分分析[32-33]等无监督学习方法。然而，传统的机器学习方法通常需要手动设计和选择特征，并且在大规模和复杂的系统中泛化能力较

弱，难以高效的实现 FIDA 检测。

随着深度学习的发展，基于深度学习的 FDIA 检测方法得到越来越多的关注。本文整理的基于深度学习的电力系统虚假数据注入攻击检测文献共有 47 篇，包括卷积神经网络(convolutional neural networks, CNN) 14 篇、循环神经网络(recurrent neural networks, RNN)8 篇、图神经网络(graph neural networks, GNN)9 篇、生成对抗网络(generative adversarial networks, GAN)4 篇、深度强化学习(deep reinforcement learning, DRL)6 篇以及其他文献 6 篇，各模型文献数量分布如图 2 所示。其中，近 5 年的文献共 43 篇，占比 91.5%，文献年份分布如图 3 所示。

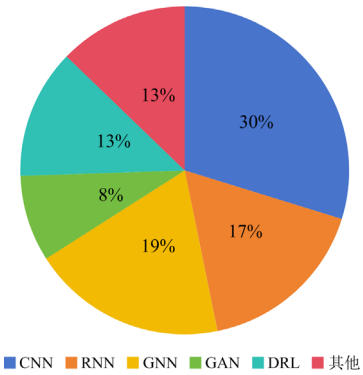

图 2 不同深度学习模型的文献数量分布

Fig. 2 Distribution of the number of publications for different deep learning models

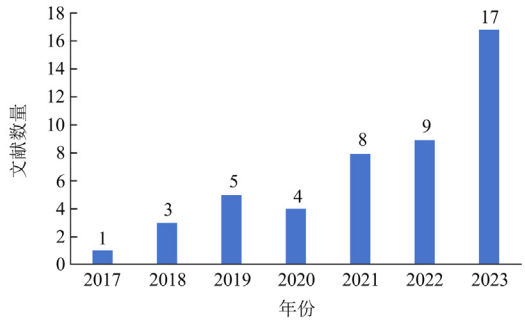

图 3 基于深度学习模型的文献年份分布

Fig. 3 Distribution of publication years for deep learning models

2.1 问题描述

FDIA 检测问题可以描述为：给定电力系统运行时的测量值数据，其中包含正常样本与 FDIA 样本，设计一种算法，可以检测单个样本是否受攻击，或辨识样本中受攻击的测量点位。

对于检测问题，可以用深度学习的二分类算法，而辨识问题，则可以用多标签分类算法，基本流程如下所述。

1) 数据收集：收集包含正常和受攻击状态的电力系统样本数据，并标记它们的状态。

2) 模型构建：选择适合的深度学习模型，该模型应具备提取有用特征并准确识别正常和受攻击状态的能力。

3) 数据划分：将数据分为训练集和验证集，用于模型的训练和评估。

4) 模型训练：使用样本数据对深度学习模型进行训练，并调整权重参数。

5) 模型验证：利用验证集评估训练完成的模型，通过计算评估指标来评估模型性能。

2.2 卷积神经网络

卷积神经网络(CNN)是一种广泛应用于图像识别和计算机视觉任务的深度学习模型[34]，在大规模数据分类任务上具有很强的优势。

CNN 用于检测电力系统中的 FDIA 时，将待检测的数据视为一组向量，利用 CNN 在图像识别上的优势，对向量进行分类，结构如图 4 所示，包括一个输入层、多个卷积层和池化层、一个全连接层和一个输出层。输入层接收电力系统的测量数据作为输入，卷积层自动识别和提取与虚假数据注入攻击相关的特征，池化层实现特征的降维，全连接层将各层的输出结果整合起来，进行最终的分类，最后由输出层输出检测结果。通过训练大量正常数据和受攻击数据，CNN 模型能够学习电力系统的正常和受攻击特征，从而判断是否存在 FDIA。

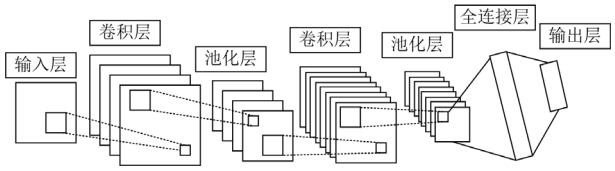

图 4 CNN 结构

Fig. 4 CNN structure

文献[35-41]研究了使用 CNN 检测电力系统中的 FDIA。然而，这些研究着重于检测电力系统中是否受到 FDIA，未能识别受到攻击的具体位置。针对这个问题，文献[42-46]采用 CNN 作为分类器，将 FDIA 位置检测问题表述为多标签分类的问题，通过多标签分类的方法来确定 FDIA 的位置。这些方法提高了 FDIA 位置检测的准确性，对于更好更快地部署有效解决方案至关重要。

此外，CNN 在检测电力系统故障位置时面临着如卷积核大小、卷积层数等超参数选择困难的问题，相关研究人员为了解决这一问题，提出了多种优化算法与卷积神经网络相结合的方法。如文献[47]

引入粒子群优化算法，通过利用粒子群算法对 CNN 模型的超参数空间进行优化，解决了最优超参数选择的问题。文献[48]引入了麻雀搜索算法，提出了一种基于 CNN 并采用麻雀搜索算法进行优化的方法，解决了 CNN 超参数选择困难的问题，提高了检测的准确率。

2.3 循环神经网络

循环神经网络(RNN)是一种能够对输入序列中的依赖关系进行建模和记忆的机器学习模型[49]，能够捕捉序列数据中的上下文信息，在处理具有序列结构的数据时具有高效性。

使用 RNN 检测电力系统中的 FDIA，将待检测数据视为一组时间相关的序列，通过网络中的循环结构提取相邻时间上的数据关联特征，进而预测并识别异常点，结构如图 5 所示，由输入层、隐藏层和输出层组成。输入层接收电力系统的测量数据作为输入；隐藏层由多个循环单元组成，每个循环单元都有内部的记忆状态，可以捕捉到测量数据之间的时间依赖关系，能够对当前的测量数据进行预测和判断；输出层根据隐藏层的输出结果进行分类。电力系统中的数据主要是时间序列数据，涉及连续变化的电流、电压等参数。RNN 通过捕捉电力系统测量数据的时序关系和异常模式，可以有效地检测 FDIA。

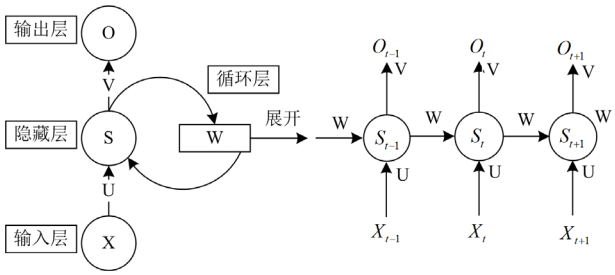

图 5 RNN 结构

Fig. 5 RNN structure

文献[50-52]研究了使用 RNN 检测电力系统中的 FDIA。通过观察测量数据的动态变化，捕捉测量数据之间的时序相关性，并利用先前的输出状态进行预测，有效地检测出 FDIA。

在电力系统中，多变量时间序列状态数据经常包含线性和非线性成分。线性成分是由于电力系统元件参数的变化所导致的，而非线性成分通常是由异常事件引起的，如开关故障、短路等故障事件。以往的研究主要关注线性数据，但为了同时考虑到数据中的线性和非线性成分，相关文献已提出了一些方法。其中，文献[53]提出了一种基于残差递归神经网络预测模型和自适应判断阈值的故障检测方法。该方法将预测过程分为两部分：首先使用线性模型拟合状态数据，然后通过预测线性模型残差的非线性来提高预测精度。此外，文献[54]提出了一种基于卡尔曼滤波和循环神经网络的故障检测方案。该方案利用卡尔曼滤波进行状态预测以适应线性数据，并利用循环神经网络来捕捉非线性数据特征。这些方法的提出为电力系统中的故障检测提供了新的途径，能够更准确地捕捉数据中的复杂特征，提高检测效果。

尽管 RNN 在考虑历史数据对当前状态的影响方面具有优势，但其存在梯度消失或爆炸的问题，难以有效学习长期依赖关系。为了克服这一问题，长短期记忆网络(long short term memory, LSTM)作为一种特殊类型的 RNN 被引入，它引入了记忆单元，有助于网络对长序列进行建模[55]。此外，LSTM 通过门控单元的设计，能够选择性地更新、遗忘和输出信息，成功地解决了梯度消失或爆炸的问题，更好地捕捉了长期依赖。因此，相关文献研究了将 LSTM 代替 RNN 应用于 FDIA 检测。例如，文献[56]设计了一个基于 LSTM 的 RNN 框架来检测电力系统中的 FDIA，该框架能够更好地捕捉电力系统的动态行为，并提高检测准确率。另外，文献[57]提出了一种使用 LSTM 自动编码器来检测智能电网中交流 FDIA 的方法，通过训练 LSTM 自动编码器使用从正常状态估计中提取的特征向量，并学习这些特征向量之间的时间相关性，实现了有效的 FDIA 检测。

2.4 图神经网络

图神经网络(GNN)是一种用于处理图结构数据的机器学习方法[58]，能够直接处理具有复杂拓扑结构的数据，有效地捕捉节点之间的依赖关系。

使用 GNN 检测电力系统中的 FDIA，结构如图 6 所示，其中包括一个输入层、多个隐藏层和一个输出层。输入层接收电力系统的测量数据作为输入，多个隐藏层用于提取电力系统拓扑图中节点之间的空间特征，输出层预测输入的测量数据被攻击的概率。GNN 通过迭代、聚合节点的邻居信息，能够学习每个节点在电力系统拓扑图中的特征表示。利用 GNN 获得各节点的特征表示后，可以预测节点的实际测量值，并与真实测量值进行对比。通过分析预测值与实际值之间的差异，可以判断是否受到 FDIA。

目前已有大量文献研究采用 GNN 来检测电力系统中的 FDIA[59-67]。例如，文献[60]提出了一种基于 GNN 的实时 FDIA 检测器，该模型通过整合智能电网底层拓扑和空间相关的测量数据，利用 GNN 图邻接矩阵将系统拓扑结构融入模型，并利用 GNN

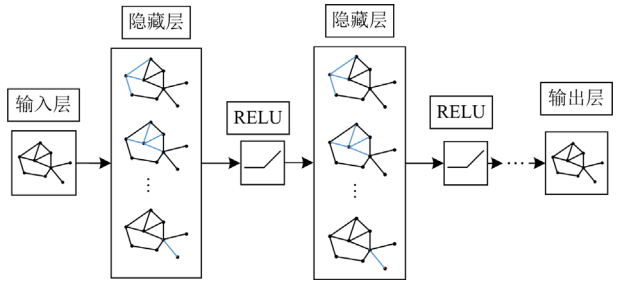

图 6 GNN 结构

Fig. 6 GNN structure

空间层建模历史测量数据，以有效地结合模型驱动和数据驱动的方法，实现更准确的 FDIA 检测。类似地，文献[61-62]也利用电力系统固有的拓扑结构和测量数据相关性，提出了基于 GNN 的检测方法，用于检测 FDIA 的存在并确定受攻击位置。文献[63]针对电力系统测量的空间相关性，提出了一种基于切比雪夫图卷积网络的大型电网攻击检测深度学习模型，在一个具有 2848 个母线的大型电网系统中验证了其高效性。文献[64-65]提出了一种基于广义图神经网络的异常检测器，采用图自编码器进行训练，只需要使用正常数据集，克服了大多数研究方法依赖标记的测量数据的问题。

然而，上述方法大多数都基于固定的拓扑结构进行验证，没有考虑到电力系统故障或运行方式的调整可能导致电网拓扑结构的变化。这样的检测方法会降低检测精度。为了解决这个问题，文献[66]结合了运行数据和电力系统拓扑信息的空间特征，提出了一种基于图神经网络的检测方法，能够在拓扑发生变化时提高 FDIA 检测性能。同时，该方法还可以定位系统中多个被攻击节点的位置，有效解决了数据驱动方法在不考虑电力系统拓扑变化时检测精度低的问题。

2.5 生成对抗网络

生成对抗网络(GAN)是一种包含生成器和判别器两个组件[68]的神经网络结构，在大量无标签数据的场景下具有很强的优势。GAN 最初用于从文本生成图像，是一种无监督学习方法。在应用到数据分析时，GAN 可以有效地解决标记数据不足的问题。GAN 结构如图 7 所示。

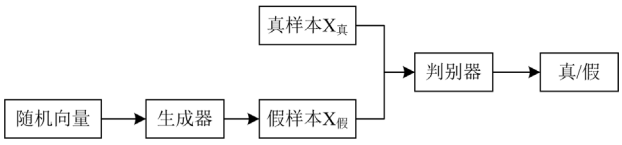

图 7 GAN 结构

Fig. 7 GAN structure

具体而言，首先利用少量已标记的测量数据作为训练集，通过训练生成器生成与真实测量数据相似的样本。然后，将已有的标记测量数据与生成的数据组合构建训练集，并通过训练判别器来区分真实数据和生成数据。通过不断地训练生成器和判别器，提高生成器生成近似真实数据的能力，使判别器更准确地区分真实数据和生成数据。对于训练完成的 GAN 模型，输入测量数据，生成器生成一个匹配的数据，并通过判别器评估输入的测量数据与生成数据之间的差异。若差异较小，则可能是正常数据；反之，若差异较大，则可能存在 FDIA。

文献[69-71]提出了一种全新的数据驱动 FDIA 检测方法，利用 GAN 从历史测量数据中提取物理模型，并结合了注意力机制以进一步捕捉数据中的潮流规律。该方法只需利用易获取的测量数据，便能高效地实现 FDIA 检测，从而显著降低对电力系统信息的需求。文献[72]将 GAN 与自编码器相结合，提出了一种半监督深度学习方法，仅需要少量已标注和未标注的数据即可进行训练，具备较高的检测精度与鲁棒性。

2.6 深度强化学习

深度强化学习(DRL)是一种结合了深度学习和强化学习的方法，可以自适应地处理高维、非线性的状态和动作空间，用于解决具有连续状态和动作空间的复杂决策问题[73]，在处理大规模、高维度数据方面具有很强的优势。采用深度强化学习的方法来检测电力系统中的 FDIA，可以适应 FDIA 的多样性和不确定性。DRL 结构如图 8 所示。

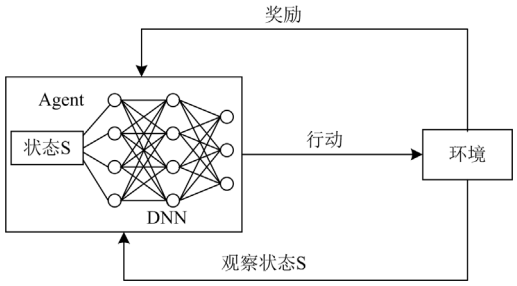

图 8 DRL 结构

Fig. 8 DRL structure

具体而言，将电力系统建模为强化学习环境，利用深度强化学习算法训练智能体进行决策。智能体观察当前状态选择动作并根据环境反馈进行判断是否存在 FDIA。在训练过程中，设计奖励函数来指导智能体学习正确识别正常数据和虚假数据，优化决策过程。经过充分训练的智能体能够应用于未知数据的测试场景，为电力系统提供准确的 FDIA 检

测结果。随着智能体逐步探索并学习系统中的各种攻击和故障模式，其强化学习模型能更好地适应系统的各种变化。

文献[74]是第一篇研究使用强化学习技术在智能电网中进行在线网络攻击检测的文章，作者将强化学习异常检测问题表述为部分可观测马尔可夫决策过程。将强化学习检测 FDIA 建模为马尔可夫决策过程，可以通过学习最优策略来引导电力系统的决策和操作，提高检测效率。利用强化学习算法，系统可以获取环境反馈并根据奖励信号进行策略持续优化，能够有效应对攻击的多样性，提高检测的效率。

然而，传统强化学习方法的学习效率相对较低，不适用于状态空间较大的问题。为了克服这个问题，研究人员将深度学习技术与强化学习相结合，以提高学习效率并避免维度灾难的困扰。文献[75-79]提出了使用深度强化学习进行攻击检测的方法，其中文献[75]在无模型深度强化学习算法中引入了注意力机制，以提取更具代表性和可区分性的状态特征，进一步提高了检测的准确性和效率。

2.7 其他

除了上述方法之外，还有其他深度学习技术用于检测电力系统中的 FDIA，如深度置信网络(Deep neural network, DBN)、变换器(Transformer)、深度迁移学习等。

DBN 由 Geoffrey Hinton 于 2006 年提出[80]，是一种由多个受限波尔兹曼机堆叠而成的生成模型。在检测电力系统中的 FDIA 方面，DBN 是早期应用的深度学习算法之一。相比人工神经网络和支持向量机，DBN 能够自动从数据中学习到更高级、更抽象的特征表示，并且具有更高的准确性[81-83]。

Transformer 是一种基于自注意力机制的神经网络架构[84]，在自然语言处理领域得到广泛应用，同时在机器翻译、文本生成和文本分类等任务中发挥着重要作用。在电力系统中，数据通常以时间序列的形式呈现，其中包含多种类型的信号，例如电流、电压和频率等。使用 Transformer 来检测电力系统中的 FDIA 有许多优势[85-86]。首先，Transformer 能够自适应地学习输入序列之间的关系，从而更好地捕捉到潜在的故障特征。其次，Transformer 还能够处理变长的序列数据，适用于具有不同长度的历史数据和故障时间。

迁移学习是指通过将已在一个任务上学习到的知识和经验迁移到另一个相关任务中的过程，可以解决数据稀缺的问题[87]。大多数已有的 FDIA 检测方法假设电力系统可以被准确建模。然而，在实际情况中，电力系统的许多参数是动态的，无法在运行过程中准确获取。为了解决这个问题，文献[88]提出了一种基于深度迁移学习的 FDIA 检测方法。将模拟的电力系统作为源域，利用丰富的模拟攻击和正常数据训练基于深度神经网络(deep neural networks, DNN)的 FDIA 检测器。同时，真实世界的运行系统被视为目标域，从中收集足够的真实正常数据来微调 DNN。通过这种方式，在无法准确知道系统参数的情况下，实现了对 FDIA 的高精度检测。

3 检测方法的对比分析

3.1 基于机器学习与基于深度学习的检测方法对比

在实际的检测中，基于传统的机器学习和基于深度学习的检测方法存在着不同的优缺点，如表 1 所示。其中，基于机器学习的检测方法通常需要较少的标注数据，可以在数据有限的情况下进行有效的监督学习，同时，相比于深度学习，经典的机器学习技术训练时间较短。但是基于机器学习的检测方法存在着对非线性关系建模能力较弱的缺点，在电力系统中可能无法有效地挖掘出数据中的特征，从而检测性能较低。基于深度学习技术的检测方法能够捕捉到电力系统中复杂的非线性关系，对非线性的虚假数据注入攻击有较强的检测能力。然而，基于深度学习的方法需要大量的标注数据进行训练，并且在复杂的电力系统数据中需要较长的时间训练数据。

表 1 机器学习与深度学习的检测方法对比

Table 1 Comparison of detection methods between machine learning and deep learning

	优点	缺点
机器学习	1.模型解释性较强 2.训练时间相对较短 3.使用较少的标注数据	1.手动特征工程 2.对非线性关系建模能力较弱 3.对噪声和异常值敏感
深度学习	1.自动特征学习 2.高度非线性建模能力 3.数据预处理要求低	1.需要大量标注数据 2.训练时间长 3.模型解释性较弱

3.2 基于深度学习不同模型的检测方法对比

使用不同的深度学习方法检测电力系统中的 FDIA 具有不同的特点，如表 2 所示。其中，卷积神经网络 CNN 在处理数据时具有局部感知能力，能够更好地捕捉数据中的局部模式和关联关系。在电力系统中，虚假数据注入攻击可能会导致局部数据的异常变化，而 CNN 可以通过对局部数据进行卷积操作，更好地检测出这些异常情况。但是卷积神经网络并不擅长处理具有时间关联性的数据，而

电力系统中的数据通常具有高度的时间相关性。

表 2 不同深度学习模型的检测方法对比

Table 2 Comparison of detection methods for different deep learning models

	文献	优点	缺点
CNN	[35-48]	1.对时空数据处理效果好 2.自动学习空间特征 3.模型参数共享	对时间序列数据关系的建模能力弱
RNN	[50-57]	1.处理时序数据能力强 2.能够处理可变长度的输入序列	1.训练效率较低 2.存在消息传递的局限性
GNN	[59-67]	1.能够捕捉节点之间的关系 2.适用于灵活的图结构	1.可能存在信息传递局限性 2. 对大规模图结构计算复杂度高
GAN	[69-72]	1.能够生成虚假数据 2.强大的学习能力	1.训练过程不稳定 2.生成的虚假样本缺乏可解释性
DRL	[74-79]	1.无需标注数据 2.适应不确定性的环境 3.模型具有自我优化的能力	1.训练时间较长 2.需要设计合适的奖励机制

循环神经网络 RNN 在处理序列数据时具有较好的时序建模能力。在电力系统中，测量数据通常是按时间顺序产生的，而虚假数据注入攻击可能会导致数据的时序变化。RNN 可以通过记忆先前的状态和信息，对序列数据进行建模，从而更好地检测出虚假数据注入攻击。但是 RNN 在反向传播过程中采用连续乘积方式来计算梯度，在学习长期依赖关系时，数值不稳定，可能会导致梯度消失或爆炸。

图神经网络 GNN 可以对图结构数据进行建模和分析，通过节点之间的信息传递和聚合，可以捕捉到节点之间的相互影响和传播。在电力系统中，虚假数据注入攻击可能会导致节点之间的数据异常变化，而 GNN 可以通过跨节点的信息传递，更好地检测出这种异常变化。然而，GNN 存在大规模图结构计算复杂度高和信息传递局限性等问题。

生成对抗网络 GAN 能够通过学习真实数据分布，生成与真实数据类似但具有差异的虚假数据，用于模拟攻击情景。同时，GAN 可以进行无监督学习，不需要标注的真实数据和虚假数据进行训练，解决了在实际中难以获得大量标记数据的问题。然而，GAN 存在着训练不稳定的问题，可能导致检测的准确率降低。

深度强化学习使用强化学习框架，智能体通过与环境的交互来学习最优的行为策略。在电力系统中，可以将虚假数据注入攻击视为环境，智能体通过与环境的交互来学习检测虚假数据注入攻击的最佳策略。通过不断地与环境交互，使得深度强化学习在面对未知或新型的虚假数据注入攻击时具有较强的适应性和泛化能力。然而，电力系统数据具有复杂和巨量等特点，使用深度强化学习检测电力系统中的 FDIA 存在着训练时间长等问题。

总之，不同的深度学习算法具有不同的优缺点，而这与算法本身的特性相关，在实际使用中，需要结合具体的情况选择合适的方法，从而提高检测的准确率和效率。

4 检测性能的对比分析

本节从鲁棒性、评估指标和可扩展性对上述文献提出的方法进行了对比，结果见表 3。

表 3 检测性能对比分析

Table 3 Comparison and analysis of detection performance

	文献	测试系统	噪声	攻击强度	评价指标	多标签	交流
CNN	[35]	IEEE 118		√	False positive, Correct		
	[36]	—		√	Accuracy, Time		
	[37]	IEEE 39		√	Accuracy		
	[38]	IEEE 14 IEEE 118		√	False positive, False negative, Accuracy		
	[39]	IEEE 39	√		Accuracy, Time, Loss		
	[40]	IEEE 14			Accuracy, Precision, Recall, F1- score, Specificity		
	[41]	IEEE 14 IEEE 39		√	Accuracy, Time		
	[42]	IEEE 14 IEEE 118	√		Precision, Recall, F1- score	√	
	[43]	IEEE 118	√	√	Precision, Recall	√	
	[44]	IEEE 14 IEEE 118	√	√	Precision, Recall, F1- score	√	
	[45]	IEEE 14	√	√	Precision, Recall, F1- score, Racc	√	
	[46]	IEEE 14 IEEE 118	√	√	Precision, Recall, F1- score, Racc	√	
	[47]	—			Accuracy, Precision, Recall, F1- score	√	
	[48]	IEEE 14 IEEE 118	√		Precision, Recall, F1- score	√	
RNN	[50]	IEEE 30			Accuracy, Precision, Specificity, Sensibility		
	[51]	IEEE 30			Accuracy, Precision, Specificity, Sensibility		
	[52]	IEEE 39			Accuracy		
	[53]	IEEE 14			MRSE, RE		
	[54]	IEEE 14 IEEE 57		√	Accuracy, F1- score		
	[56]	IEEE 14	√		F1- score, FP, Time		
	[57]	IEEE 14 IEEE 118	√		Accuracy, F1- score, Recall		√

续表 3

	文献	测试系统	噪声	攻击强度	评价指标	多标签	交流
GNN	[59]	IEEE 9 IEEE 39 IEEE 118	√		Accuracy, Precision, Recall, F1- score	√	
	[60]	IEEE 14 IEEE 118 IEEE 300	√	√	Accuracy, Recall, False alarm rate		√
	[61]	IEEE 57 IEEE 118 IEEE 300	√		Accuracy, F1- score	√	
	[62]	IEEE 14 IEEE 39 IEEE 118			Accuracy, Recall, False alarm rate		
	[63]	2848-bus system	√		Recall, False alarm rate		
	[64]	IEEE 14 IEEE 39 IEEE 118		√	Accuracy, Recall, False alarm rate		
	[65]	IEEE 14 IEEE 39 IEEE 118			Accuracy, Recall, False alarm rate		
	[66]	IEEE 14 IEEE 118		√	Accuracy, Missing alarm rate		
	[67]	IEEE 118		√	Accuracy		
GAN	[69]	IEEE 30 IEEE 118	√	√	Voltage amplitude, phase		
	[70]	IEEE 14 IEEE 118	√		Residual, Time		
	[71]	IEEE 118 IEEE 300	√	√	Accuracy	√	
	[72]	IEEE 13 IEEE 123	√	√	Accuracy, Precision, Recall		
DRL	[74]	IEEE 14	√		Precision, Recall, F1- score		
	[75]	IEEE 14 IEEE 118			Accuracy, Delay False Positive		
	[76]	IEEE 9 IEEE 14 IEEE 30		√	Delay-alarm error rate, False-alarm error rate, Detect-failure rate		√
	[77]	IEEE 9 IEEE 14 IEEE 30 IEEE 57		√	Detection rate		
	[78]	IEEE 14	√		Precision, Recall, F1- score		
	[79]	Pecan Street		√	Precision, Recall, F1- score		
其他	[81]	IEEE 118 IEEE 300	√		Accuracy		
	[82]	IEEE 14 IEEE 30 IEEE 118 IEEE 300		√	F1-score		
	[83]	IEEE 14	√		Accuracy		
	[85]	IEEE 14 IEEE 30			Accuracy, Precision, Recall		
	[86]	IEEE 14 IEEE 118	√	√	Accuracy, Precision, Recall, F1-score		
	[88]	IEEE 14 IEEE 118	√		Accuracy, Missing Alarm Rate		

4.1 鲁棒性对比

为了确保对电力系统 FDIA 的高效检测，必须考虑算法的鲁棒性，特别是考虑到电力系统中噪声和攻击强度的影响。噪声是电力系统中普遍存在的非攻击性数据波动，可能源于传感器误差、测量噪声以及通信干扰等。这些噪声可能干扰正常数据的分布，从而对虚假数据注入攻击检测造成挑战。攻击强度是指攻击者注入虚假数据的程度，即改变数据大小的程度。通过对噪声和攻击强度的考虑，在实验中进行对比分析，可以评估算法在不同噪声和攻击强度下的性能。

在基于深度学习的检测算法中，共 23 篇文章中考虑了在不同噪声下算法的检测性能，22 篇文章中考虑了在不同攻击强度下算法的检测性能，9 篇文章中既在不同噪声下，也在不同攻击强度下测试了所提出算法的检测性能。

4.2 评估指标对比

不同的文章采用不同的评估指标来测试所提出的检测机制的有效性，大多数文章采用了精确度、召回率和 F1 分数(F1-score)作为评估指标，以评估检测机制的性能。精确度的高值表示虚假数据注入攻击检测机制能够准确地找出真正的攻击样本，降低了误报率。召回率的高值意味着虚假数据注入攻击检测机制能够有效地捕获到大部分攻击样本，降低了漏报率。F1-score 的高值说明虚假数据注入攻击检测机制在精确度和召回率之间取得了较好的平衡。除了精确度、召回率和 F1-score 之外，一些研究也采用了其他指标，例如敏感性(sensibility)、误报率(false alarm rate)和漏报率(missing alarm rate)等。这些指标提供了对算法在不同方面性能的更详细评估，帮助研究人员可靠地比较和评估不同检测机制的性能。

4.3 可扩展性对比

检测机制的可扩展性是 FDIA 检测问题中一个重要的考虑因素。电力系统是一个复杂大型的网络，包括多个节点和大量的测量设备，数据量庞大。因此，在设计检测方法时需要考虑如何处理大规模数据，提高检测的效率和准确性。

在基于深度学习的检测算法中，大部分文章在 IEEE 14 和 IEEE 118 系统中测试所提出的检测机制的性能，然而也存在少数文章，如文献[40,45,53,56,74,78]对所提出的方法仅在 IEEE 14 等较小规模的测试系统中进行测试。小型系统的数据集相对较小，便于进行训练和验证，然而在大型系统中可能并不具有有效性。

总之，对于虚假数据注入检测算法，可扩展性

是一个关键指标。算法必须能够适应不同电力系统拓扑、参数和配置的变化，并保持良好的检测性能。

4.4 识别能力对比

检测算法对 FDIA 的识别能力关系到电力系统的安全稳定运行。大多数 FDIA 的检测方法都集中于检测 FDIA 的存在，将检测问题处理为二元分类问题，而无法获得准确的受攻击的位置。仅有 10 篇文献将 FDIA 位置检测问题表述为多标签分类问题，不仅能够检测攻击是否存在，同时能够精确定位系统中受攻击的母线和线路。

准确定位受攻击的位置，能够在电力系统受到攻击之后，快速采取适当的措施来应对攻击，有效地提高了电力系统的安全稳定性。

4.5 检测范围对比

电力系统中除了正常和受 FDIA 两种情形外，还存在突发事件等故障情况。然而，大多数研究中仅考虑了前两种情况，而未考虑电力系统的突发事件等故障情况。仅文献[27, 33, 47, 56]从更全面的角度出发，在检测 FDIA 时考虑了正常电网的突发事件，并且能够将 FDIA 与故障区分开来。

对于电力系统运营商来说，在检测 FDIA 时，能够将故障区分开来至关重要。因为 FDIA 误报会导致不必要的损失，而漏报则会导致严重的后果。在关键时刻做出正确的反应，需要准确地识别 FDIA 和其他类型的故障，并及时采取措施进行处理，以进一步保证电力系统的安全稳定运行。

5 未来展望

虽然深度学习在检测电力系统 FDIA 方面呈现出许多优势，但该领域仍然面临着多项挑战。未来随着信息与物理系统的进一步融合，以及人工智能等技术的快速发展，使得电力系统中面临的虚假数据注入攻击更加难以识别。因此，使用深度学习检测 FDIA 的未来发展方向可以包括以下几个方面。

1) 提高检测算法的扩展性：通常，直流和交流状态估计都可能受到 FDIA。由于交流系统非线性的特征，目前大部分 FDIA 检测系统都集中在直流模型下的输电网上，然而，与直流状态估计模型相比，交流状态估计模型更常用于现实世界的公用事业，检测交流 FDIA 更具有现实意义。且未来电力系统将呈现出更加复杂和多样化的形态，FDIA 检测系统需要进一步的扩展和改进，以应对更多的系统类型。

2) 多种检测方法相结合：目前大多数研究中的检测机制仅使用一种深度学习方法，然而，一种单独的检测算法可能无法全面地捕获虚假数据注入攻击，未来的研究可以尝试将多个深度学习算法结合起来，也可以尝试将深度学习算法与传统的检测方法相结合，从而构建更加全面可靠的检测机制。

3) 跨领域合作：电力系统安全是一个复杂的领域，涉及多个领域的知识和数据。未来的研究可以促进跨领域的合作与交流，从而在深度学习与电力系统安全领域之间建立起有效的桥梁。例如，可以结合密码学和物联网等技术来设计更安全的数据传输和验证机制。

4) 提高实时监测能力：虚假数据注入攻击是一个动态变化的过程，攻击者可能会不断改变攻击策略。因此，未来的研究可以致力于提高模型在实时监测和响应方面的能力，能够及时发现并应对新的攻击。

6 结语

本文介绍了 FDIA 的原理，对比分析了基于机器学习和基于深度学习的 FDIA 检测方法。此外，详细介绍了基于不同深度学习模型的检测方法。最后，讨论了使用深度学习检测 FDIA 的未来研究方向。

与基于机器学习的方法相比，基于深度学习的方法能够更好地处理 FDIA 的复杂特征，从而提高检测的准确性和鲁棒性。然而，不同的检测算法都有其优点和缺点，在实际应用中，需要结合实际情况，根据具体的需求和约束条件选择适合的检测方法。

深度学习在大量领域已经实现落地应用，凭借强大的数据学习能力与成熟的软硬件平台，逐渐取代了这些领域原有的技术。FDIA 本质上属于数据分析，是深度学习的强项之一，目前基于深度学习的 FDIA 检测虽然还存在不足，但是在网络对抗日趋复杂的当下，其强大的特征学习能力与海量数据处理能力，使其具有广泛的应用前景。通过持续的研究和创新，深度学习将为 FDIA 检测和防范提供更强大和更可靠的解决方案。

参考文献

[1] 中华人民共和国中央政府. 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要[EB/OL]. https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm

[2] 杨杰, 郭逸豪, 郭创新, 等. 考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述[J]. 电力系统保护与控制, 2022, 50(7): 176-187.
YANG Jie, GUO Yihao, GUO Chuangxin, et al. A review of dynamic security protection on a cyber physical power system considering model and data driving[J]. Power System Protection and Control, 2022, 50(7): 176-187.

[3] 田继伟, 王布宏, 李夏. 智能电网状态维持拓扑攻击及其对经济运行的影响[J]. 电力系统保护与控制, 2018, 46(1): 50-56.
TIAN Jiwei, WANG Buhong, LI Xia. State-preserving topology attacks and its impact on economic operation of smart grid[J]. Power System Protection and Control, 2018, 46(1): 50-56.

[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] 龚郁安. 关于委内瑞拉大停电事故的情况分析和关键基础设施的安全防护建议[J]. 信息技术与网络安全, 2019, 38(4): 1-2.
GONG Xi'an. Analysis of Venezuela's blackouts and suggestions on network security of critical infrastructure[J]. Information Technology and Network Security, 2019, 38(4): 1-2.

[6] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[C] // Proceeding of the 16th ACM conference on Computer and Communications Security, November 9-13, 2009, Chicago, USA: 21-32.

[7] ZHANG T, YE D. False data injection attacks with complete stealthiness in cyber-physical systems: a self-generated approach[J]. Automatica, 2020, 120.

[8] 龚立, 王先培, 田猛, 等. 电力信息物理系统韧性的概念与提升策略研究进展[J]. 电力系统保护与控制, 2023, 51(14): 169-187.
GONG Li, WANG Xianpei, TIAN Meng, et al. Concepts and research progress on enhancement strategies for cyber physical power system resilience[J]. Power System Protection and Control, 2023, 51(14): 169-187.

[9] KONSTANTINOU C, MANIATAK M. Impact of firmware modification attacks on power systems field devices[C] // 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), November 2-5, 2015, Miami, FL, USA: 283-288.

[10] WU M, CHEN L. Image recognition based on deep learning[C] // 2015 Chinese Automation Congress (CAC), November 27-29, 2015, Wuhan, China: 542-546.

[11] ABDELWAHAB O, ELMAGHARVY A. Deep learning based vs. Markov chain based text generation for cross domain adaptation for sentiment classification[C] // 2018 IEEE International Conference on Information Reuse and Integration (IRI), July 6-9, 2018, Salt Lake City, UT, USA: 252-255.

[12] 武雾阳, 李强, 陈潜, 等. 知识图谱框架下基于深度学习的 HVDC 系统故障辨识[J]. 电力系统保护与控制, 2023, 51(20): 160-169.
WU Jiyang, LI Qiang, CHEN Qian, et al. Fault identification of an HVDC system based on deep learning in the framework of a knowledge graph[J]. Power System Protection and Control, 2023, 51(20): 160-169.

[13] MUSLEH A S, CHEN G, DONG Z. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2019, 11(3): 2218-2234.

[14] REDA H T, ANWAR A, MAHMOOD A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts[J]. Renewable and Sustainable Energy Reviews, 2022, 163: 112423.

[15] SAYGHE A, HU Y, ZOGRAFOPOULOS I, et al. Survey of machine learning methods for detecting false data injection attacks in power systems[J]. IET Smart Grid, 2020, 3(5): 581-595.

[16] 朱炳铨, 郭逸豪, 郭创新, 等. 信息失效威胁下的电力信息物理系统安全评估与防御研究综述[J]. 电力系统保护与控制, 2021, 49(1): 178-187.
ZHU Bingquan, GUO Yihao, GUO Chuangxin, et al. A survey of the security assessment and security defense of a cyber physical power system under cyber failure threat[J]. Power System Protection and Control, 2021, 49(1): 178-187.

[17] WANG Q, TAI W, TANG Y, et al. Review of the false data injection attack against the cyber-physical power system[J]. IET Cyber-Physical Systems: Theory & Applications, 2019, 4(2): 101-107.

[18] 杨玉泽, 刘文霞, 李承泽, 等. 面向电力 SCADA 系统的 FDIA 检测方法综述[J]. 中国电机工程学报, 2023, 43(22): 8602-8622.
YANG Yuze, LIU Wenxia, LI Chengze, et al. Review of FDIA detection methods for electric power SCADA system[J]. Proceedings of the CSEE, 2023, 43(22): 8602-8622.

[19] 王琦, 郃伟, 汤奕, 等. 面向电力信息物理系统的虚假数据注入攻击研究综述[J]. 自动化学报, 2019, 45(1): 72-83.
WANG Qi, TAI Wei, TANG Yi, et al. A review on false data injection attack toward cyber-physical power system[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.

[20] 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.

[21] DENG Y, ZHU K, WANG R, et al. Real-time detection of false data injection attacks based on load forecasting in smart grid[C] // 2019 IEEE International Conference on

Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), October 21-23, 2019, Beijing, China: 1-6.

[22] ALWAGEED H S. Detection of cyber attacks in smart grids using SVM-boosted machine learning models[J]. Service Oriented Computing and Applications, 2022, 16(4): 313-326.

[23] KUMAR A, SAXENA N, CHOI B J. Machine learning algorithm for detection of false data injection attack in power system[C] // 2021 International Conference on Information Networking (ICOIN), January 13-16, 2021, Jeju Island, Korea (South): 385-390.

[24] ALWAGEED H S. Detection of cyber attacks in smart grids using SVM-boosted machine learning models[J]. Service Oriented Computing and Applications, 2022, 16(4): 313-326.

[25] 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), July 24-29, 2016, Vancouver, BC, Canada: 1395-1402.

[26] LU X, JING J, WU Y. False data injection attack location detection based on classification method in smart grid[C] // International Conference on Artificial Intelligence and Advanced Manufacture (AIAM), October 15-17, 2020, Manchester, United Kingdom: 133-136.

[27] JENA P K, GHOSH S, KOLEY E, et al. An ensemble classifier based scheme for detection of false data attacks aiming at disruption of electricity market operation[J]. Journal of Network and Systems Management, 2021, 29(4): 43.

[28] WANG D, WANG X, ZHANG Y, et al. Detection of power grid disturbances and cyber-attacks based on machine learning[J]. Journal of Information Security and Applications, 2019, 46: 42-52.

[29] 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.

[30] AHMED S, LEE Y D, HYUN S H, et al. Covert cyber assault detection in smart grid networks utilizing feature selection and Euclidean distance-based machine learning[J]. Applied Sciences, 2018, 8(5): 772.

[31] PARIZAD A, HATZIADONIU C J. Cyber-attack detection using principal component analysis and noisy clustering algorithms: a collaborative machine learning-based framework[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4848-4861.

[32] CUI J, GAO B, GUO B. A novel detection and defense mechanism against false data injection attack in smart grids[J]. IET Generation, Transmission & Distribution, 2023, 17(20): 4514-4524.

[33] MUSLEH A S, CHEN G, DONG Z Y, et al. Online characterization and detection of false data injection attacks in wide-area monitoring systems[J]. IEEE Transactions on Power Systems, 2021, 37(4): 2549-2562.

[34] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998, 86(11): 2278-2324.

[35] LU M, WANG L, CAO Z, et al. False data injection attacks detection on power systems with convolutional neural network[C] // Journal of Physics: Conference Series, May 23-25, 2020, Kunming, China: 1-10.

[36] HE Y, LI L, QIAN H, et al. CNN-GRU based fake data injection attack detection method for power grid[C] // 2022 2nd International Conference on Electrical Engineering and Control Science (IC2ECS), December 16-18, 2022, Nanjing, China: 408-411.

[37] NIU X, LI J, SUN J, et al. Dynamic detection of false data injection attack in smart grid using deep learning[C] // 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), February 18-21, 2019, Washington, DC, USA: 1-6.

[38] 李元诚, 曾婧. 基于改进卷积神经网络的电网假数据注入攻击检测方法[J]. 电力系统自动化, 2019, 43(20): 97-104.
LI Yuancheng, ZENG Jing. Detection method of false data injection attack on power grid based on improved convolutional neural network[J]. Automation of Electric Power Systems, 2019, 43(20): 97-104.

[39] ZHANG G, LI J, BAMISILE O, et al. Identification and classification for multiple cyber attacks in power grids based on the deep capsule CNN[J]. Engineering Applications of Artificial Intelligence, 2023, 126.

[40] KHAN A. Detection of false data injection cyber-attack in smart grid by convolutional neural network-based deep learning technique[M] // Security, Privacy and Data Analytics: Select Proceedings of ISPDA 2021, Singapore: Springer Singapore, 2022: 33-48.

[41] 黄冬梅, 何立昂, 孙锦中, 等. 基于边缘计算的电网假数据攻击分布式检测方法[J]. 电力系统保护与控制, 2021, 49(13): 1-9.
HUANG Dongmei, HE Li'ang, SUN Jinzhong, et al. Distributed detection method for a false data attack in a power grid based on edge computing[J]. Power System Protection and Control, 2021, 49(13): 1-9.

[42] MUKHERJEE D, CHAKRABORTY S, GHOSH S. Deep learning-based multilabel classification for locational detection of false data injection attack in smart grids[J]. Electrical Engineering, 2022, 104(1): 259-282.

[43] MUKHERJEE D. A novel strategy for locational

detection of false data injection attack[J]. Sustainable Energy, Grids and Networks, 2022, 31.

[44] HEGAZY H I, TAG ELDIEN A S, TANTAWY M M, et al. Real-time locational detection of stealthy false data injection attack in smart grid: using multivariate-based multi-label classification approach[J]. Energies, 2022, 15(14): 5312.

[45] ZIA M F, INAYAT U, NOOR W, et al. Locational detection of false data injection attack in smart grid based on multilabel machine learning classification methods[C] // 2023 IEEE IAS Global Conference on Renewable Energy and Hydrogen Technologies (GlobConHT), March 11-12, 2023, Male, Maldives: 1-5.

[46] WANG S, BI S, ZHANG Y J A. Locational detection of the false data injection attack in a smart grid: a multilabel classification approach[J]. IEEE Internet of Things Journal, 2020, 7(9): 8218-8227.

[47] BITIRGEN K, FILIK Ü B. A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid[J]. International Journal of Critical Infrastructure Protection, 2023, 40.

[48] SHEN K, YAN W, NI H, et al. Localization of false data injection attack in smart grids based on SSA-CNN[J]. Information, 2023, 14(3): 180.

[49] ELMAN J L. Finding structure in time[J]. Cognitive Science, 1990, 14(2): 179-211.

[50] 王海吉, 胡健坤, 田元. 基于 RNN 的智能电网拓扑变异型 FDI 攻击检测方法[J]. 沈阳工业大学学报, 2023, 45(2): 139-144.
WANG Hanji, HU Jiankun, TIAN Yuan. Detection method based on RNN for topology variation FDI attacks in smart grid[J]. Journal of Shenyang University of Technology, 2023, 45(2): 139-144.

[51] AYAD A, FARAG H E Z, YOUSSEF A, et al. Detection of false data injection attacks in smart grids using recurrent neural networks[C] // 2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), February 19-22, 2018, Washington, DC, USA: 1-5.

[52] WANG Y, CHEN D, ZHANG C, et al. Wide and recurrent neural networks for detection of false data injection in smart grids[C] // Wireless Algorithms, Systems, and Applications: 14th International Conference, WASA 2019, June 24-26, 2019, Honolulu, HI, USA: 335-345.

[53] WANG Y, SHI W, JIN Q, et al. An accurate false data detection in smart grid based on residual recurrent neural network and adaptive threshold[C] // 2019 IEEE International Conference on Energy Internet (ICEI), May 27-31, 2019, Nanjing, China: 499-504.

[54] WANG Y, ZHANG Z, MA J, et al. KFRNN: an effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network[J]. IEEE Internet of Things Journal, 2021, 9(9): 6893-6904.

[55] HOCHREITER S, SCHMIDUBER J. Long short-term memory[J]. Neural Computation, 1997, 9(8):1735-1780.

[56] MOHAMMADPOURFARD M, KHALILI A, GENC I, et al. Cyber-resilient smart cities: detection of malicious attacks in smart grids[J]. Sustainable Cities and Society, 2021, 75.

[57] 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.

[58] SCARSELLI F, GORI M, TSOI A C, et al. The graph neural network model[J]. IEEE Transactions on Neural Networks, 2008, 20(1): 61-80.

[59] PENG S, ZHANG Z, DENG R, et al. Localizing false data injection attacks in smart grid: a spectrum-based neural network approach[J]. IEEE Transactions on Smart Grid, 2023, 14(6): 4827 - 4838.

[60] BOYACI O, UMUNNAKWE A, SAHU A, et al. Graph neural networks based detection of stealth false data injection attacks in smart grids[J]. IEEE Systems Journal, 2021, 16(2): 2946-2957.

[61] BOYACI O, NARIMANI M R, DAVIS K R, et al. Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks[J]. IEEE Transactions on Smart Grid, 2021, 13(1): 807-819.

[62] TAKIDDIN A, ATAT R, ISMAIL M, et al. A graph neural network multi-task learning-based approach for detection and localization of cyber attacks in smart grids[C] // ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), June 4-10, 2023, Rhodes Island, Greece: 1-5.

[63] BOYACI O, NARIMANI M R, DAVIS K, et al. Cyber attack detection in large-scale smart grids using Chebyshev graph convolutional networks[C] // 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE), March 29-31, 2022, Alanya, Turkey: 217-221.

[64] TAKIDDIN A, ISMAIL M, ATAT R, et al. Robust graph autoencoder-based detection of false data injection attacks against data poisoning in smart grids[J]. IEEE Transactions on Artificial Intelligence, 2024, 5(3): 1287-1301.

[65] TAKIDDIN A, ATAT R, ISMAIL M, et al. Generalized graph neural network-based detection of false data injection attacks in smart grids[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2023, 7(3): 618-630.

[66] LI X, WANG Y, LU Z. Graph-based detection for false data injection attacks in power grid[J]. Energy, 2023, 263.

[67] HAGHSHENAS S H, HASNAT M A, NAEINI M. A

temporal graph neural network for cyber attack detection and localization in smart grids[C] // 2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), January 16-19, 2023, Washington, DC, USA: 1-5.

[68] GOODFOLLEW I, POUGET-ABADIE J, MIEZA M, et al. Generative adversarial nets[J]. Advances in Neural Information Processing systems, 2014, 27.

[69] LI Y, WANG Y, HU S. Online generative adversary network based measurement recovery in false data injection attacks: a cyber-physical approach[J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 2031-2043.

[70] JIAO R, XUN G, LIU X, et al. A new AC false data injection attack method without network information[J]. IEEE Transactions on Smart Grid, 2021, 12(6): 5280-5289.

[71] HUANG X, QIN Z, XIE M, et al. Defense of massive false data injection attack via sparse attack points considering uncertain topological changes[J]. Journal of Modern Power Systems and Clean Energy, 2021, 10(6): 1588-1598.

[72] ZHANG Y, WANG J, CHEN B. Detecting false data injection attacks in smart grids: a semi-supervised deep learning approach[J]. IEEE Transactions on Smart Grid, 2020, 12(1): 623-634.

[73] MNIK V, KAVUKCUOGLU K, SILVER D, et al. Human-level control through deep reinforcement learning[J]. Nature, 2015, 518: 529-533.

[74] KURT M N, OGUNDIJO O, LI C, et al. Online cyber-attack detection in smart grid: a reinforcement learning approach[J]. IEEE Transactions on Smart Grid, 2018, 10(5): 5174-5185.

[75] HUANG R, LI Y, WANG X. Attention-aware deep reinforcement learning for detecting false data injection attacks in smart grids[J]. International Journal of Electrical Power & Energy Systems, 2023, 147.

[76] AN D, YANG Q, LIU W, et al. Defending against data integrity attacks in smart grid: a deep reinforcement learning-based approach[J]. IEEE Access, 2019, 7: 110835-110845.

[77] LIN X, AN D, CUI F, et al. False data injection attack in smart grid: attack model and reinforcement learning-based detection method[J]. Frontiers in Energy Research, 2023, 10.

[78] RAN X, TAY W P, LEE C H T. A robust deep Q-network based attack detection approach in power systems[C] // 2022 4th International Conference on Smart Power & Internet Energy Systems (SPIES), December 9-12, 2022, Beijing, China: 995-1000.

[79] ROUZBAHANI H M, KARIMIPOUR H, LEI L. Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids[J]. International Journal of Electrical Power & Energy Systems, 2023, 146.

[80] HINTON G E, SALAKHUTDINOV R R. Reducing the dimensionality of data with neural networks[J]. Science, 2006, 313: 504-507.

[81] 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.

[82] WEI L, GAO D, LUO C. False data injection attacks detection with deep belief networks in smart grid[C] // 2018 Chinese Automation Congress (CAC), November 30, 2018, Xi'an, China: 2621-2625.

[83] 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.

[84] VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need[J]. Advances in Neural Information Processing Systems, 2017, 30.

[85] 陈冰, 唐永旺. 基于 Transformer 编码器的智能电网虚假数据注入攻击检测[J]. 计算机应用与软件, 2022, 39(7): 336-342.
CHEN Bing, TANG Yongwang. False data injection attacks detecting based on Transformer encoder in smart grid[J]. Computer Applications and Software, 2022, 39(7): 336-342.

[86] LI Y, WEI X, LI Y, et al. Detection of false data injection attacks in smart grid: a secure federated deep learning approach[J]. IEEE Transactions on Smart Grid, 2022, 13(6): 4862-4872.

[87] PAN S J, YANG Q. A survey on transfer learning[J]. IEEE Transactions on knowledge and data engineering, 2009, 22(10): 1345-1359.

[88] XU B, GUO F, WEN C, et al. Detecting false data injection attacks in smart grids with modeling errors: a deep transfer learning based approach[J]. arXiv preprint arXiv: 2104.06307, 2021.

收稿日期：2023-12-21；　修回日期：2024-01-25

作者简介：

李　卓(2000—)，男，硕士研究生，研究方向为信息物理系统安全；E-mail: 18737171322@163.com

谢耀滨(1981—)，男，通信作者，博士，副教授，研究方向为工业控制系统安全；E-mail: yb_xie@163.com

吴茜琼(1981—)，女，硕士，副教授，研究方向为电力系统控制与优化；E-mail: 40913436@qq.com

张有为(1976—)，男，硕士，副教授，研究方向为嵌入式系统安全。E-mail: zhangyouwei@zxiat.com

(编辑　魏小丽)