DOI：10.13334/j.0258-8013.pcsee.221101 文章编号：0258-8013 (2023) 22-8602-20 中图分类号：TM 73；TP 393 文献标识码：A

面向电力 SCADA 系统的 FDIA 检测方法综述

杨玉泽，刘文霞*，李承泽，刘耕铭，张帅，张艺伟

(新能源电力系统国家重点实验室(华北电力大学)，北京市 昌平区 102206)

Review of FDIA Detection Methods for Electric Power SCADA System

YANG Yuze, LIU Wenxia*, LI Chengze, LIU Gengming, ZHANG Shuai, ZHANG Yiwei

(State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources (North China Electric Power University), Changping District, Beijing 102206, China)

ABSTRACT: With the development of information and communication technology and the introduction of intelligent devices, power system has gradually transformed into cyber-physical power system (CPPS), and the deep coupling between cyber layer and physical layer has intensified the risk of power system being subjected to cyber attack. False data injection attack (FDIA) is a kind of cyber attack that is stealthy, flexible and targeted, which poses a great threat to the security and stability of electric power supervisory control and data acquisition (SCADA) system. In order to deal with this challenge, scholars have studied a variety of FDIA detection methods. In this paper, FDIA detection methods for electric power SCADA system are reviewed. Firstly, the attack principle and construction method of FDIA are introduced, the development history of FDIA detection algorithm is summarized, and the algorithms are classified according to model driven and data driven. The mechanism of model-driven detection methods based on state estimation, graph theory and physical characteristics and data-driven detection methods based on supervised learning, unsupervised learning, semi-supervised learning, adversarial game learning and reinforcement learning are analyzed respectively. Then, the detection performance, advantages and disadvantages of relevant algorithms and their application scenarios are compared and analyzed. Finally, the future research direction of FDIA detection defense was prospected.

KEY WORDS: electric power supervisory control and data acquisition (SCADA) system; false data injection attack (FDIA); defense and detection; state estimation; data-driven

摘要：信息通信技术的发展和智能设备的引入使电力系统逐渐演变为电力信息物理系统，而信息层与物理层之间的深度耦合也加剧了电力系统遭受网络攻击的风险。虚假数据注入攻击(false data injection attack，FDIA)作为一种兼具隐蔽性、灵活性和攻击导向性的网络攻击方式，对电力数据采集与监控(supervisory control and data acquisition，SCADA)系统的安全稳定构成很大威胁。为应对这一威胁挑战，学者们研究了各种各样的 FDIA 检测方法。该文对面向电力 SCADA 系统的 FDIA 检测方法进行综述，首先介绍了 FDIA 的攻击原理及构建方法，梳理了 FDIA 检测算法的发展历程，并按照模型驱动和数据驱动对算法进行了分类整理，针对模型驱动中的基于状态估计、图论、物理特性等检测方法和数据驱动中的有监督学习、无监督学习、半监督学习、对抗博弈学习和强化学习等检测方法分别进行了机理分析；然后对比分析了相关算法的检测性能、优缺点及其适用场景；最后，对 FDIA 检测防御的后续研究方向进行了展望。

关键词：电力数据采集与监控系统；虚假数据注入攻击；防御检测；状态估计；数据驱动

0 引言

随着社会生产力发展、科学技术进步以及产业结构调整，城市化率逐年上升，电力占终端用能比例增加，社会的正常运行对电力的依赖程度进一步加深。电力系统是一个规模庞大、结构复杂的自动化系统，为保证其运行的安全性和经济性，需要及时获取系统拓扑和运行状态的变化信息，进行状态估计[1-3](state estimation，SE)，为后续控制和调度奠定基础，该系统称为电力数据采集与监控(supervisory control and data acquisition，SCADA)系统。一旦该系统遭受网络攻击，会导致调度中心做出错误决策，威胁电网的安全稳定，造成经济损失，甚至危害社会功能正常运转与人民生活的安定。如 2003 年的 Slammer 蠕虫病毒[4]和 2010 年 Stuxnet 蠕虫病毒[5]通过恶意病毒注入的方式攻击核电站工业控制系统，威胁核设施的安全运行；2015 年乌克兰的 SCADA 系统遭受网络攻击，黑客通过邮件发送恶意软件、恶意跳闸指令和 DDoS 攻击相结合的

方式造成乌克兰大范围停电长达数小时，影响数百万人的日常生活，是首次由于网络攻击导致物理电网失效继而引发大规模停电事故的案例[6]。可见，网络安全问题不容小觑，针对网络攻击的检测与防御已成为学术研究的焦点之一。

虚假数据注入攻击(false data injection attack，FDIA)作为一种新型的网络攻击，由 Liu 等[7]于 2009 年首次提出。FDIA 属于数据完整性攻击，以破坏数据或信息的精确性和一致性为主要特征[8]，其具体实现方式是通过设计攻击向量篡改量测数据，躲避能量管理系统(energy management system，EMS)中状态估计的不良数据检测器(bad data detection，BDD)，引起调度中心对当前电网状态的误判，从而达到破坏电力系统安全稳定或获取不法收益的目的。随着信息通信技术的迅猛发展和攻击方法的深入研究，FDIA 的涵义已经增广为通过恶意篡改任何系统数据或信息，从而实现破坏、威慑或牟取暴利等非法目的的攻击方式[8]，称为广义 FDIA。广义 FDIA 的直接篡改目标包括电气量测数据、开关量测数据、同步时钟信号和控制指令等；其目标系统也不再局限于电力 SCADA 系统，还包括直流微网[9]、工业控制系统[10]、无人机系统[11]等。其中，以电气量测数据为直接攻击目标的电力 SCADA 系统的 FDIA 最隐蔽且关注度最高，后续无特别说明，FDIA 均指面向电力 SCADA 系统的 FDIA。FDIA 具有隐蔽性好、灵活性高、攻击范围广、破坏力强等特征，研究 FDIA 的攻击机理及检测防范方法具有重要意义。

为更有效地阻断 FDIA，实现 FDIA 的检测防御，首先要掌握 FDIA 的入侵点。如图 1 所示，针对电力 SCADA 系统的 FDIA 入侵点主要有三种[12]，分别为攻击监测、控制和保护设备及远程终端单元(remote terminal unit，RTU)的物理层 FDIA；攻击数据传输通道，截获并篡改量测及控制信息的通信链路 FDIA(也称为中间人攻击)；以及直接渗透到调度中心及 EMS 高级应用程序中进行恶意篡改的信息层 FDIA。由于信息层安全防护措施十分严密，FDIA 不易实施，本文更关注物理层 FDIA 和通信链路 FDIA 的检测和辨识，无特别说明，本文总结的 FDIA 检测方法均适用于这两种攻击方式。

自 Liu 提出 FDIA 的概念以后，许多学者致力于 FDIA 的检测工作。2010 年，Kosut[13]提出一种广义似然比检测器，其检测性能优于传统 L2 范数检测器，是最早提出的 FDIA 检测方法之一。2013—2015 年，Gu[14]和 Wang[15]等对状态估计算法进行改进，提出分布式状态估计算法；Manandhar[16]和 Rawat[17]等提出基于卡尔曼滤波器的 FDIA 检测方法，标志着由 FDIA 单一时间断面检测迈向 FDIA 时序动态检测。与此同时，学者们从不同角度理解并阐释 FDIA 检测原理，相继提出矩阵分解[18]、相对熵[19]、自适应累积和[20]等检测算法，其本质仍属于模型驱动方法。随着大数据与人工智能算法的迅猛发展，FDIA 检测领域也迎来了新的生机。2015 年以后，基于数据驱动的 FDIA 检测算法如雨后春笋般涌现，如支持向量机[21]、K 均值聚类[22]、极限学习机[23]、循环神经网络[24]、自编码器[25]、Q 学习[26]、生成对抗器[27]等等，均在不同程度上取得良好的检测效果。2017 年以后，FDIA 检测方法不再局限于单一场景下检测虚假数据是否存在，相关研究在算法适应性和检测能力等方面进行改进提升，如文献[28]考虑了噪声、负荷波动和拓扑变化的影响，文献[27]提出的算法不仅检测 FDIA 存在，还能辨识 FDIA 位置并进行数据恢复，提升了电网信息安全防御能力。

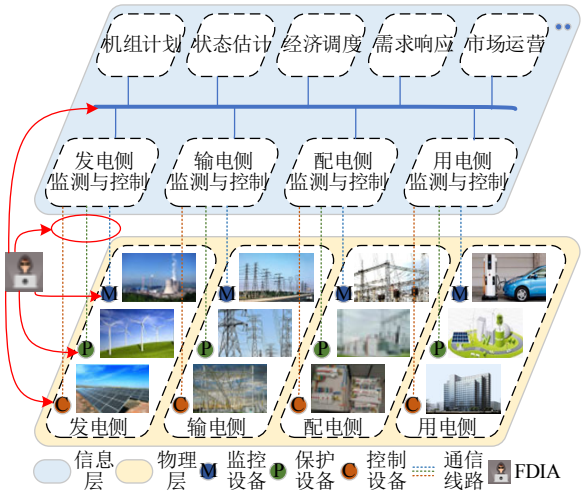

图 1　FDIA 在电力 SCADA 系统中的传播路径

Fig. 1　The propagation path of FDIA in electric power SCADA system

近年来，随着信息物理高度融合和网络安全风险的不断扩大，FDIA 检测方法的研究层出不穷。而 FDIA 综述性文献大多对 FDIA 的攻击构建方法、后果评估及防御配置手段进行总结[29-36]，鲜有针对 FDIA 检测方法的研究综述。为了填补这一缺口，本文重点整理了近些年的 FDIA 检测算法，首先简要介绍了 FDIA 攻击原理及构建方法；其次对 FDIA

检测方法进行分类归纳与机理分析；之后选取影响算法检测性能的典型因素进行对比分析；然后提炼总结了各类方法的优缺点及适应场景；最后，深入分析现今 FDIA 检测研究存在的问题，给出未来电力 SCADA 系统 FDIA 检测的发展方向，为从事相关研究的学者们提供参考和指引。

1 FDIA 攻击原理及构建方法

1.1 FDIA 攻击原理

电力系统通常基于拓扑结构和线路参数等静态数据以及实时量测数据进行建模。系统量测方程常用交流潮流模型表示：

$$\boldsymbol{z}=h(\boldsymbol{x})+\boldsymbol{e} \tag{1}$$

式中：$\boldsymbol{z}\in\mathbf{R}^m$ 为系统测量向量，包括母线电压、母线有功功率和无功功率注入，以及支路有功潮流和无功潮流等；$\boldsymbol{x}\in\mathbf{R}^n$ 为系统状态变量，如节点电压复相量；$h(\cdot)\in\mathbf{R}^m$ 刻画了量测值与系统状态之间的非线性映射，通常取决于系统参数和拓扑结构；$\boldsymbol{e}$ 为均值为 0，方差为 $\sigma^2\in\mathbf{R}^m$ 的量测误差向量；系统量测通常具有一定冗余度，即 $m>n$。

由于高压输电网中母线电压在额定电压附近且支路电阻远小于电抗，为了简化计算、保证收敛性，系统量测方程通常采用线性化的直流潮流模型：

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

式中 $\boldsymbol{H}\in\mathbf{R}^{m\times n}$ 为线性化的量测雅可比矩阵。

由于偶然因素(如随机干扰和设备故障)或者人为因素(如 FDIA)，可能会导致电力 SCADA 系统中采集到的量测数据中存在错误数据。被篡改的量测向量可以表示为 $\boldsymbol{z}^a=\boldsymbol{z}+\boldsymbol{a}$，其中 $\boldsymbol{a}\in\mathbf{R}^m$ 含有非零元素，表示错误数据向量。检测错误数据的传统方法是残差检验，当残差向量的欧式范数 $r=\|\boldsymbol{z}-h(\boldsymbol{x})\|$ 大于系统预定义的阈值 τ 时，系统触发警报，说明检测到错误数据。

然而，对于攻击者精心设计的量测攻击向量，传统的残差检验无能为力。在交流和直流潮流模型下分别构建攻击向量如公式(3)和公式(4)所示：

$$\boldsymbol{a}=h(\hat{\boldsymbol{x}}+\boldsymbol{c})-h(\hat{\boldsymbol{x}}) \tag{3}$$

$$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c} \tag{4}$$

式中：$\hat{\boldsymbol{x}}\in\mathbf{R}^n$ 为状态变量估计值；$\boldsymbol{c}\in\mathbf{R}^n$ 为任意非零向量。

此时系统量测残差欧式范数分别如式(5)、(6)所示：

$$\begin{aligned}r^a=\|\boldsymbol{z}^a-h(\hat{\boldsymbol{x}}^a)\|=\|\boldsymbol{z}+\boldsymbol{a}-h(\hat{\boldsymbol{x}}+\boldsymbol{c})\|=\|\boldsymbol{z}+h(\hat{\boldsymbol{x}}+\boldsymbol{c})-\\ h(\hat{\boldsymbol{x}})-h(\hat{\boldsymbol{x}}+\boldsymbol{c})\|=\|\boldsymbol{z}-h(\hat{\boldsymbol{x}})\|=r<\tau\end{aligned} \tag{5}$$

$$\begin{aligned}r^a=\|\boldsymbol{z}^a-\boldsymbol{H}\hat{\boldsymbol{x}}^a\|=\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|=\\ \|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\|=\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}\|=r<\tau\end{aligned} \tag{6}$$

此时，残差检测无法发现量测数据中掺杂的虚假数据，攻击者能够将量测值和状态变量篡改为任意数值，威胁电力系统安全稳定运行。

为了方便叙述，将能够被传统残差检验发现的 FDIA 称为“随机 FDIA”，将躲避残差检验的 FDIA 称为“隐形 FDIA”，后续无特别说明，FDIA 均指隐形 FDIA。

1.2 FDIA 构建方法

如果攻击者能够获得电力系统所有配置信息(包括电网拓扑信息、线路参数、状态估计算法和坏数据检测方法的细节等)，并且能够获取并篡改所有仪表量测值，那么可以直接通过式(3)、(4)构造攻击向量，成功发动 FDIA，这种攻击方式也被称为完美 FDIA。然而，受制于攻击资源、地域差异和信息保护等因素，攻击者难以完全掌握电力系统的所有信息。因此，构建有约束条件的 FDIA 更具实际意义。本节以直流潮流模型为例，简要总结了 3 种常见的 FDIA 构建方法，详细内容可参阅文献[33-34]。

1）攻击资源受限。

对于攻击者而言，攻击的量测点数越多，表明攻击的成本和代价越高，因此，攻击者期望用最低的攻击成本和代价达到目的。攻击向量的优化模型如式(7)所示：

$$\begin{cases}\alpha_i=\min\limits_{\boldsymbol{c}}\|\boldsymbol{H}\boldsymbol{c}\|_0\\ \text{s.t.}\quad a_i=\boldsymbol{h}_i\boldsymbol{c}=1\end{cases} \tag{7}$$

式中：α_i 为最小稀疏度指标；$\|\cdot\|_0$ 表示非零元素的个数；$\boldsymbol{h}_i$ 为 $\boldsymbol{H}$ 的第 i 行；约束 $a_i=1$ 表示攻击目标为向第 i 个量测仪表注入 1 个单位的虚假数据。

2）部分量测被保护。

当部分量测仪表被防御者保护起来时，意味着攻击者无法对这些仪表注入虚假数据，此时，攻击向量的优化模型如式(8)所示：

$$\begin{cases}\alpha_i=\min\limits_{\boldsymbol{c}}\|\boldsymbol{H}\boldsymbol{c}\|_0\\ \text{s.t.}\quad a_i=\boldsymbol{h}_i\boldsymbol{c}=1\\ \qquad a_k=\boldsymbol{h}_k\boldsymbol{c}=0,\quad \forall k\in\mathbf{P}\end{cases} \tag{8}$$

式中 $\mathbf{P}$ 为被保护的量测仪表集合。

式(7)、(8)描述的优化模型属于 NP 困难问题，

通常采用凸松弛技术、混合整数线性规划、匹配追踪等方法[34]解决。

3）系统信息不完全。

当攻击者掌握的系统拓扑或线路参数信息不完全时，攻击者眼中的量测雅可比矩阵 $\boldsymbol{H}$ 也将不再准确，此时构造的攻击向量如下所示：

$$\boldsymbol{a}=\bar{\boldsymbol{H}}\boldsymbol{c}=\boldsymbol{H}\boldsymbol{c}+\boldsymbol{\delta}\boldsymbol{c} \tag{9}$$

式中：$\bar{\boldsymbol{H}}$ 为攻击者估计的量测雅可比矩阵；$\boldsymbol{\delta}$ 为 $m\times n$ 维的误差矩阵。

被攻击的状态变量估计值为

$$\hat{\boldsymbol{x}}^{a}=\hat{\boldsymbol{x}}+\bar{\boldsymbol{c}}=\hat{\boldsymbol{x}}+\boldsymbol{c}+(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{\delta}\boldsymbol{c} \tag{10}$$

式中：$\bar{\boldsymbol{c}}$ 为攻击者实际引入的状态变量误差向量；$\boldsymbol{W}\in\mathbf{R}^{m\times m}$ 为测量向量的权重矩阵。

系统量测残差的欧式范数如下所示：

$$\begin{aligned}r^{a}&=\|\boldsymbol{z}^{a}-\boldsymbol{H}\hat{\boldsymbol{x}}^{a}\|=\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\bar{\boldsymbol{c}})\|=\\&\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{\delta}\boldsymbol{c}+\boldsymbol{H}(\boldsymbol{c}-\bar{\boldsymbol{c}})\|=\\&\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+(\boldsymbol{I}-\boldsymbol{H}(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W})\boldsymbol{\delta}\boldsymbol{c}\|\end{aligned} \tag{11}$$

当 $r^{a}<\tau$ 时，攻击者成功发动 FDIA。

值得注意的是，本文介绍的绝大多数 FDIA 检测论文的攻击样本仅采用 1.1 节中的 FDIA 攻击模型，不考虑 1.2 节中的 FDIA 构建方法。

2　FDIA 检测方法分类及机理

FDIA 检测旨在对系统中已经发生的攻击行为进行实时的监测和辨识。近年来，随着攻击和检测技术的博弈发展，FDIA 检测方法呈现出多元化发展趋势，但从机理上大致可分为模型驱动和数据驱动两类。FDIA 检测方法分类如图 2 所示。

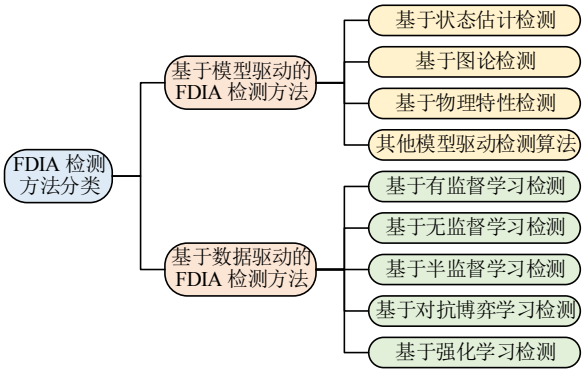

图 2　FDIA 检测方法分类

Fig. 2　Classification of FDIA detection methods

2.1　基于模型驱动的 FDIA 检测方法

基于模型驱动的 FDIA 检测方法通常根据电力系统自身的模型和参数，通过对某一时间断面或连续时间的电力 SCADA 系统数据进行处理分析并与人为设定的检测阈值相比较，从而检测出 FDIA。根据具体检测原理的不同，模型驱动的 FDIA 检测算法可进一步细分为基于状态估计检测、基于图论检测、基于物理特性检测和其他四大类别。

2.1.1　基于状态估计的 FDIA 检测

状态估计也称为滤波，它是利用实时量测系统的冗余度来提高数据精度，自动排除随机干扰引起的错误信息，估计或预报系统的运行状态(或轨迹)，分为静态状态估计和动态状态估计[37]。

为了检出 FDIA，很多学者对状态估计算法进行深入研究，针对静态状态估计，学者们提出了分布式状态估计、计及信息系统影响的状态估计和变换目标防御等方法，使 FDIA 难以躲避改进后的残差检验而被发现；针对动态状态估计，学者们不断改进卡尔曼滤波算法，使遭受 FDIA 的量测值偏离预期轨迹，提高了电力系统对 FDIA 的敏感度和鲁棒性。

1）基于静态状态估计的 FDIA 检测方法。

静态状态估计(static state estimation，SSE)仅利用同一断面的量测信息估计电网的状态，各时间断面上求解出的状态变量相互独立。基于静态状态估计检测 FDIA 的机理是通过分块计算、参数调整或量测变换等手段，使状态估计后的量测偏差难以躲避改进的残差检测或统计假设检验方法而被检出。

静态状态估计最常用的算法是加权最小二乘法(Weighted least squares，WLS)，其中状态变量的估计值可以通过以下优化问题解得：

$$\min J(\boldsymbol{x})=(\boldsymbol{z}-h(\boldsymbol{x}))^{\mathrm{T}}\boldsymbol{W}(\boldsymbol{z}-h(\boldsymbol{x})) \tag{12}$$

式中 $\boldsymbol{W}\in\mathbf{R}^{m\times m}$ 为测量向量的权重矩阵。

针对传统集中式控制容易同时接收协调配合的一组篡改量测值从而导致 FDIA 漏检的缺点，一些学者采用分布式状态估计检测 FDIA。文献[38]采用中值滤波(median filtering，MF)算法，将当前节点量测值与所有相邻节点经基尔霍夫定律得到的该点估计值进行中值滤波，从而实现 FDIA 检测，计算复杂度低，然而存在不确定参数时，其检测率不稳定，适应性和扩展性较差。Gu[14]和 Wang[15]基于图分解理论将电力系统划分为若干子系统，然后分别对每个子系统执行状态估计，由于子系统自由度更低，卡方检验的阈值也更小，相比集中式计算更容易发现 FDIA。Duan[39]提出一种基于分布式直

流最优潮流的 FDIA 弹性控制机制，在所有母线上布置分布式控制器与相邻母线交换信息，通过将接收信息与估计信息之差的 L2 范数与阈值对比，更新相邻母线的信誉指数。当母线信誉值低于门槛值时，认为该母线遭受 FDIA，舍弃该母线传输的信息并用相应估计值代替，一定程度上消除了 FDIA 的影响。与文献[39]类似，Xie[40]提出一种基于信任度的分布式状态估计算法检测 FDIA，通过判断相邻节点估计值之差是否落入置信区间修改信任度并分配权重系数，节点状态由相邻节点估计值加权计算得出。

上述文献的检测方法仅利用了物理系统的量测信息，并未考虑信息系统异常流量的影响。文献[41]首次将信息层中入侵检测系统(intrusion detection system，IDS)的异常流量分析结果与基于 WLS 的状态估计相结合形成异常流量状态估计算法(abnormal traffic-indexed state estimation，ATSE)，算例表明 ATSE 比传统卡方检验平均提高了 20%的检测率。改进后的优化模型为

$$\min J_{\mathrm{ATSE}}(\boldsymbol{x})=(\boldsymbol{z}-h(\boldsymbol{x}))^{\mathrm{T}}\boldsymbol{\Phi}^{-1}\boldsymbol{W}(\boldsymbol{z}-h(\boldsymbol{x})) \quad (13)$$

式中：$\boldsymbol{\Phi}\in\mathbf{R}^{m\times m}$ 为网络影响因子矩阵，是一个对角元素为权重系数的对角矩阵：$\boldsymbol{\Phi}_i$ 的权重越大，则说明该量测遭受 FDIA 的可能性越大。

与大多数被动检测算法不同，一些学者采用主动防御检测思想，通过主动改变电网线路参数或变换量测值，使状态信息与攻击者篡改后的产生差异，提高检出率。根据实现手段可以分为物理特性参数变换和量测信息变换两类。尽管实现手段不同，其检测方案都基于状态估计 WLS 算法。

基于物理特性参数变换的典型方法是变换目标防御(moving target defense，MTD)，其基本思想是通过利用装设在输电线路上的分布式柔性交流输电系统设备(distributed flexible alternative current transmission systems，D-FACTS)主动改变电网特性参数(如电抗)，使攻击者基于错误参数信息构建的 FDIA，在状态估计中表现出更大的残差，从而更容易被检测出来。文献[42]首次提出该思想并对变换目标防御的可行性进行了理论分析。随后，文献[43-45]权衡了电抗参数改变引起的功率损耗成本和检测率，指出 D-FACTS 的执行周期不应大于攻击者通过数据渗透窃取电抗参数的周期，并分析了变换目标防御检测 FDIA 的局限性。

由于变换目标防御通常造成系统偏离最优潮流运行点，引起系统功耗增加或控制性能损失，部分学者寻求运行成本更低廉的方法，采用量测信息变换的思路主动检测 FDIA。Miao[46]提出的编码策略(coding schemes)是该思路的代表性方法，通过在攻击者未知的情况下对量测信息进行编解码操作，干扰攻击者设计的隐形攻击向量，使量测残差增大从而实现检测。Zhao[47]设计了求编解码矩阵可行解的计算思路，然而应用场景限于线性模型；随后 Shi[48]将该方法扩展到非线性模型的智能电网中；Liu[49]结合前人的研究成果，分析了隐形 FDIA 检测与编码通信成本之间的关系，构建并求解了最优编码策略，检测效果很好。编码策略结构简单，只需在量测数据传输前后分别设置编码器和解码器，不需要新增检测装置；然而该方法假设攻击者只能在编码操作之后执行攻击，即仅适用于通信链路 FDIA，对物理层 FDIA 失效。

2）基于动态状态估计的 FDIA 检测方法。

随着可再生能源并网，电力系统状态的随机性增加，传统的静态状态估计难免捉襟见肘。动态状态估计(dynamic state estimation，DSE)利用当前时刻的量测信息和前一时刻的量测信息对当前时刻的状态进行估计，能够准确捕捉系统状态的动态变化，为电力系统运行控制保驾护航。DSE 的核心方法是卡尔曼滤波器(Kalman filter，KF)，KF 的计算主要包含预测步和更新步这两个步骤，基本形式如下所示：

$$\text{预测步}\begin{cases}\hat{\boldsymbol{x}}_t^-=\boldsymbol{A}\hat{\boldsymbol{x}}_{t-1}^-\\ \boldsymbol{P}_t^-=\boldsymbol{A}\boldsymbol{P}_{t-1}\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{Q}\end{cases} \quad (14)$$

$$\text{更新步}\begin{cases}\boldsymbol{K}_t=\boldsymbol{P}_t^-\boldsymbol{C}^{\mathrm{T}}(\boldsymbol{C}\boldsymbol{P}_t^-\boldsymbol{C}^{\mathrm{T}}+\boldsymbol{R})^{-1}\\ \hat{\boldsymbol{x}}_t=\hat{\boldsymbol{x}}_t^-+\boldsymbol{K}_t(\boldsymbol{z}_t-\boldsymbol{C}\hat{\boldsymbol{x}}_t^-)\\ \boldsymbol{P}_t=(\boldsymbol{I}-\boldsymbol{K}_t\boldsymbol{C})\boldsymbol{P}_t^-\end{cases} \quad (15)$$

式中：$\hat{\boldsymbol{x}}_t^-,\hat{\boldsymbol{x}}_t\in\mathbf{R}^n$ 分别为状态变量的先验估计值和后验估计值；$\boldsymbol{A}\in\mathbf{R}^{n\times n}$ 为状态转移矩阵；$\boldsymbol{P}_t^-,\boldsymbol{P}_t\in\mathbf{R}^{n\times n}$ 分别为估计误差的先验和后验协方差矩阵；$\boldsymbol{Q}\in\mathbf{R}^n$ 为过程噪声协方差阵；$\boldsymbol{K}_t\in\mathbf{R}^{n\times m}$ 为卡尔曼增益；$\boldsymbol{C}\in\mathbf{R}^{m\times n}$ 为量测方程的雅可比矩阵，取决于系统参数和拓扑结构；$\boldsymbol{R}\in\mathbf{R}^{m\times m}$ 为量测误差协方差阵；$\boldsymbol{I}$ 为维数为 $\mathbf{R}^{n\times n}$ 的单位矩阵。

基于动态状态估计检测 FDIA 的原理是在系统历史数据不受攻击的假设条件下，遭受 FDIA 的量测估计值会偏离预测轨迹，通过将当前时刻动态状

态估计与静态状态估计的估计偏差值与设定阈值进行比较实现检测。这一类检测算法在思路上大致相同，相关文献通过不断改进 KF 算法，使检测模型更加准确。

文献[16]将 KF 和欧氏距离检测器相结合成功检测出了虚假数据的存在，是最早应用卡尔曼滤波器进行 FDIA 检测的文章之一。随后，文献[17,50]分别引入余弦相似度匹配和在线累积和(cumulative sum，CUSUM)检测器，有效克服了文献[16]中检测效果受系统规模影响和无法处理含有时变不确定性攻击参数的缺陷，提高了检测精度和鲁棒性。文献[51]充分结合历史量测与当前量测，形成了递归 WLS 算法，形式上相当于状态转移矩阵取单位矩阵的 KF 算法，一定程度上克服了静态状态估计无法检测连续 FDIA 或者重放攻击的问题。文献[52-53]将 KF 引入 AGC 系统，拓展了该算法的应用场景。

为了对系统进行更准确的建模从而提高 FDIA 检测精度，部分学者提出扩展卡尔曼滤波器(extended Kalman filter，EKF)，使之适用于非线性的交流模型。EKF 算法核心是通过对非线性方程进行泰勒级数展开并忽略高阶项，得到线性化的雅可比矩阵用于预测和更新系统状态。文献[54-56]通过比较 EKF 估计状态与静态估计值或可信量测估计值的偏差进行 FDIA 检测。由于 EKF 计算雅克比矩阵难度较大，且会引入线性化误差，同时对模型不确定性的鲁棒性较差，Julier 提出了无迹卡尔曼滤波器[57](unscented Kalman filter，UKF)，通过无迹变换来近似状态变量经非线性变换后的统计特性，无需计算雅可比矩阵，具有更高的估计精度。有一些学者[58-60]将 UKF 引入 FDIA 检测，通过比对 UKF 与静态状态估计的偏差，检测辨识 FDIA 的存在。然而，当 UKF 更新步的量测量中存在虚假数据时，容易增大 FDIA 检测的误警率，文献[61]将基于 XGBoost 的日前负荷预测与 UKF 相结合，同时引入中心极限定理，实现对 FDIA 的精确检测和修正。

2.1.2　基于图论的 FDIA 检测

FDIA 为了保证自身隐蔽性，需要满足基尔霍夫定律和潮流平衡约束，具有拓扑连接相关性，即往往需要同时篡改一组彼此相邻相关的母线或支路。因此，可以考虑从图论的角度研究 FDIA 检测问题，将电力系统抽象为以母线为顶点、以支路为边组成的图形网络。近几年，开始有学者尝试运用图论知识检测 FDIA。

文献[62]采用基于图信号处理(graph signal processing，GSP)的检测方案，设计高通滤波器，对电网估计状态进行图傅立叶变换并过滤图的高频分量，将该结果的最大范数与阈值比较，从而检测 FDIA 的存在。随后，Jorjani 等[63]深入分析了 FDIA 的拓扑连接相关性，首先对状态估计结果进行离群点检测，然后利用图论中节点度的概念，当离群点在拓扑上彼此相邻相关时检测并定位 FDIA。该方法有效克服了文献[62]中检测率过低的问题，同时检测速度很快(毫秒级)，适合在线检测；然而该方法的检测阈值是通过枚举手段获得的，当电网拓扑或规模变化时，需重新设定阈值。Sedghi[64]提出一种基于母线相角马尔可夫图的分散式 FDIA 检测方案，当系统存在 FDIA 时，利用条件协方差检验构造的马尔科夫图与电网拓扑图之间的差异触发警报实现检测。文献[65]将 FDIA 检测问题转化为求解每个区域边际马尔科夫图的极大似然估计(maximum likelihood estimate，MLE)问题，实现 FDIA 的快速检测。

上述检测方法均将电网视为一个拓扑不变的有权无向图，边的权重通常与线路导纳有关。由于线路潮流具有方向，文献[66]将电网建模为一个有权双向图，采用基于矢量的胶囊图神经网络(graph neural networks，GNN)算法检测并定位 FDIA。而文献[67]首次考虑网络拓扑改变的情况，通过策略性地轮流切换预选的输电线路子集来检测并消除 FDIA，作者同时给出了拓扑重构消除 FDIA 的充要条件，即所选的线路集合必须包含电网拓扑图的生成树。

2.1.3　基于物理特性的 FDIA 检测

FDIA 造成的影响可以通过一些物理特性指标或固有参数体现出来，一些学者企图从电力系统的物理特性出发，研究如何利用相关物理参数的异常变化反映 FDIA 的存在[68-75]。

文献[68]提出一种基于输电线路参数的 FDIA 检测方法，通过计算线路两端等效阻抗相角差并与已知参数进行对比，从而判断攻击类型及位置，然而该方法要求所有线路两端装设相量测量单元(phasor measurement unit，PMU)，成本昂贵。与文献[68]类似，Ameli[69]针对线路电流差动继电器(line current differential relay，LCDR)的 FDIA，提出利用终端量测与本地量测比较的检测方法。而文献[70-72]利用节点电压稳定性指标(node voltage stability

index，NVSI)结合聚类算法将电网的脆弱节点分类，优先检测脆弱程度高的节点是否遭受 FDIA，但检测率过低是其主要缺点。Kaviani 等[73]从电网物理规律出发，将功率传输分布因子(power transfer distribution factor，PTDF)引入 FDIA 的最优构建和检测中来，应用快速贪婪算法识别输电线路敏感总线，开发安全指标执行检测，该方法检测率很高且无需历史数据，便于实时检测。Li[74]开发了一种两阶段的 FDIA 检测方法，设计了基于 PTDF 和线路过载程度等多种物理指标的检测手段并验证了负荷随机波动和线路中断情况下成功辨识 FDIA 的准确性和鲁棒性。Chakrabarty[75]首次考虑了针对移相器的 FDIA，利用线路电流和节点注入电流与端电压的比值设计检测指标，在量测噪声和负荷波动场景下检测率依然很高。

2.1.4 其他 FDIA 检测算法

除了以上 FDIA 检测方法，其他基于系统模型或参数的检测算法均归于此类。

有些学者利用矩阵论知识，根据量测矩阵的低秩特征和攻击矩阵的稀疏性，将 FDIA 检测问题转化为矩阵分离问题[18,76-78]。自文献[18]首次提出这一思路以后，Gao[76]对矩阵分离问题进行了再表述并提供了理论证明；之后，Li[77]综合考虑了计算效率和精度，用双边随机投影代替奇异值分解提出 Go Decomposition 算法；Huang[78]将攻击矩阵范数小于特定阈值的行置零从而保证解的收敛性，并与上述几种矩阵分离算法对比证明了所提算法的优越性。

为了克服离线检测算法无法应对量测配置或拓扑结构动态变化的缺点，Govindarasu 等[79-80]提出一种在线 FDIA 检测方法，利用实时负荷预测结果与当前时刻状态估计值的偏差进行检测。

由于虚假数据注入前后的量测值通常呈现不同的概率分布，不少学者应用数理统计的方法检测 FDIA。文献[19,81-82]引入相对熵(Kullback-Leibler divergence，KLD)的概念，通过计算不同时刻量测值概率分布之间的差异区分 FDIA 和正常数据，其中文献[20]利用图像增强技术中的对数变换和伽马变换进一步提高了 FDIA 检测率。然而该方法侧重于数据整体检测，对孤立节点的连续小幅度攻击失效。Huang 和 Li 等[20,83]采用基于自适应 CUSUM 的实时检测算法，具有高鲁棒性和低时间复杂度等优点。文献[84]将 WLS 结合残差预白化方法解决残差协方差矩阵不满秩的情况，并利用 CUSUM 实时检测 FDIA。Milano[85]首次将金融领域的本福特定律(Benford's law)应用于电力系统量测数据，通过多种算例系统验证该方法检测 FDIA 的可行性。然而，作者假设 FDIA 服从均匀分布或通过几个量测值互换实现，与常规 FDIA 不同，且方案有效性仍需进一步验证。

本节分 4 个部分详细综述了基于模型驱动的 FDIA 检测算法，下一节将对基于数据驱动的 FDIA 检测方法展开介绍。

2.2 基于数据驱动的 FDIA 检测方法

基于数据驱动的 FDIA 检测方法通常不需要任何系统模型参数信息，而是利用大数据及人工智能算法对电力 SCADA 系统中的量测数据进行训练学习及特征提取，挖掘 FDIA 的离群特性，进而实现检测。

根据学习方式的不同，数据驱动的 FDIA 检测方法可以分为有监督学习检测、无监督学习检测、半监督学习检测、对抗博弈学习检测和强化学习检测 5 类。

2.2.1 基于有监督学习的 FDIA 检测

有监督学习是一种从标签化训练数据集中分析特征、推断模型的机器学习任务。这类检测方法的思路是将 FDIA 的检测问题转化为机器学习中的二分类问题，从而判别新量测数据是否遭受 FDIA。将输入输出的数学关系表征为$\{(x_i, y_i)\}$，其中 x_i 为第 i 个输入样本，$y_i \in \{-1, 1\}$为样本标签(即是否遭受 FDIA)。现有研究中，支持向量机、K 最邻近、决策树、极限学习机、卷积神经网络等几种算法比较具有代表性。

支持向量机(support vector machine，SVM)是一种对数据进行二元分类的广义线性分类器。若给定输入数据 $\boldsymbol{X}=\{X_1, X_2, \cdots, X_N\}$所在特征空间存在一个作为决策边界的超平面将学习目标 $y_i \in \{-1, 1\}$分成正类和负类，且使任意样本的点到平面距离大于等于 1，则称该分类问题具有线性可分性，此时作为决策边界的超平面表示如下：

$$\boldsymbol{\omega}^{\mathrm{T}}\phi(\boldsymbol{X})+\boldsymbol{b}=0 \tag{16}$$

$$y_i(\boldsymbol{\omega}^{\mathrm{T}}\phi(X_i)+\boldsymbol{b})\geq 1 \tag{17}$$

式中：参数 $\boldsymbol{\omega}$、$\boldsymbol{b}$ 分别为超平面的法向量和截距；$\phi(\cdot)$为映射函数，能够将样本映射到线性可分空间，其内积为核函数。满足 $y_i(\boldsymbol{\omega}^{\mathrm{T}}\phi(\cdot)+\boldsymbol{b})=1$ 的正类和负

类样本称为支持向量。

为保证超平面分类的鲁棒性，存在优化问题使间隔边界之间距离最大，变换后可得：

$$\min_{\boldsymbol{\omega},b}\frac{\|\boldsymbol{\omega}\|^2}{2} \tag{18}$$

$$\text{s.t.}\quad y_i(\boldsymbol{\omega}^{\mathrm{T}}\phi(x_i)+\boldsymbol{b})\geq 1,\quad \forall i \tag{19}$$

上述二次规划问题可使用很多成熟的优化包求解。由于 SVM 算法简单、鲁棒性好、泛化能力强，在 FDIA 检测领域中广泛应用。Esmalifalak 设计了一种结合主成分分析(principal component analysis，PCA)的分布式高斯核 SVM 算法，在保证检测精度的同时最大限度降低计算量，是机器学习算法在 FDIA 检测领域的最早应用[21]。随后，一大批学者基于类似思路研究 SVM 的检测性能[86-92]。然而，由于 SVM 时间复杂度较高，当系统规模过大或样本数较多时将消耗大量训练时间和存储空间。

K 最邻近(k-Nearest Neighbor，KNN)分类算法是数据分类技术中最简单的方法之一。该算法的核心思想是每个样本可以用离它最近的 K 个邻近值来代表，并根据多数投票机制得出新样本的标签。判别样本类别的标准是未标记的新样本 x_i 与已标记样本 x_j 之间的欧氏距离：

$$d_{ij}=\|x_i-x_j\|_2 \tag{20}$$

在文献[22,25,86-87,90,93]中，学者们采用 KNN 算法检测 FDIA，对上式求出的欧氏距离升序排列，取前 K 个，并根据少数服从多数的原则，确定新样本为正常样本或 FDIA 样本。

标准 KNN 算法的一个明显不足是当不同样本容量不平衡时，容易出现误判。因此，Yan[87]提出一种扩展近邻算法(extended nearest neighbor，ENN)，利用样本类别的全局分布和局部近邻提升算法性能。然而，无论是 KNN 还是 ENN，都无法避免“维数诅咒”，即随着数据维度的增加，计算量增长显著，分类性能也受到严重影响。

决策树(decision tree，DT)是一类常见的预测模型，表征目标属性与量测值之间的映射关系，通常由根节点、分裂节点和叶节点组成。决策树根据属性值将输入变量逐次分割成子集。CAMANA[94]和 Lu[95]将其应用于 FDIA 检测，根据 FDIA 样本和正常量测样本属性值的差异划分到不同子集。该算法可解释性好、实现简单，但极易出现过拟合问题，一般需要剪枝操作减少过度学习。

人工神经网络(artificial neural networks，ANN)是一种模仿动物神经网络行为特征，进行分布式并行信息处理的数学模型。自 ANN 提出以来，相关算法发展迅速，应用广泛，数据分类是其典型应用之一。反向传播算法(backpropagation，BP)是 ANN 的典型监督学习算法，但是存在计算效率低，梯度消失等问题。极限学习机(extreme learning machine，ELM)作为一种 BP 算法的改进形式，通过随机或人为给定隐含层节点的权重和个数，具有学习速度快、泛化性能好的优点。文献[23,96-98]基于 ELM 实现了 FDIA 检测。其中，Wu[98]不仅检测到 FDIA 存在，还通过负荷预测等方法实现状态恢复，以提高电网弹性。

上述方法通常只涉及一种分类器模型，其性能有好有坏。为了获得更好的分类性能，集成学习(ensemble learning)的思想被引入 FDIA 检测中。集成学习通过构建并结合多个学习器来完成学习任务，相比单一学习器具有更加显著的泛化性能。集成学习通常分为 Boosting 和 Bagging 两大流派，其区别在于各分类器之间是否具有依赖性。Boosting 流派各分类器之间存在依赖关系，必须串行训练，代表性算法如 Adaboost[86]、lightgbm[99]、XGBoost[100]。而 Bagging 流派各分类器之间没有依赖关系，可以并行学习，典型算法是随机森林[101-103](random forest，RF)、集成 ELM 算法[98]。其中，随机森林将多个决策树组合，克服了过拟合的问题。

随着大数据与人工智能的迅猛发展，数据量和计算资源的指数型增长，深度学习算法应运而生。多层感知器(multilayer perceptron，MLP)作为深度学习算法的雏形，在单层神经网络基础上引入一到多个隐藏层，提升了表征学习的能力。文献[86,90-91,96,104]基于 MLP 检测 FDIA，具有较高的准确率。卷积神经网络(convolutional neural networks，CNN)是一类包含卷积计算、具有深度结构的神经网络算法，在图像识别和自然语言处理等方面表现优异。由于该算法出色的特征提取能力，Niu、Wang 等[105-108]应用 CNN 处理 FDIA 检测问题。其中 Wang[106]将 FDIA 检测问题转化为多标签分类问题，弥补了传统二分类问题只能检测 FDIA 是否存在而无法辨识 FDIA 具体位置的缺陷。电网量测数据除了具有空间相关性，还存在时序特征。为了模拟电网动态行为并捕获 FDIA 引起的异常数据特征，文献[24,89,105,108-111]

提出采用循环神经网络(recurrent neural network，RNN)检测 FDIA。RNN 的循环单元对时序数据的处理十分有效，能够检测出持续注入的 FDIA。深度信念网络(deep belief network，DBN)是一种基于深度神经网络的概率生成模型，该模型建立了一个观测数据和标签之间的联合分布，能够捕捉量测数据的高阶特征。He[112]提出一种改进 DBN 模型，能够分析实时量测数据中的时序攻击模式，在 FDIA 检测方面应用效果良好。

2.2.2 基于无监督学习的 FDIA 检测

无监督学习是一种根据未标记样本解决模式识别中各种问题的机器学习方法，适用于对数据缺乏先验知识或人工类别标注成本太高的情况。由于 FDIA 在实际场景中的样例较少难以获取，且注入量和攻击位置等信息具有不确定性，一些学者采用无监督学习的思路，通过挖掘电网量测数据中的隐藏特征，将 FDIA 与正常量测数据划分到不同类别，从而实现智能电网的 FDIA 检测。

K 均值聚类算法(K-means clustering，KMC)是一种很常用的无监督学习算法，广泛应用于聚类问题。文献[22]采用该算法检测 FDIA，通过预先将电网量测数据分为K组并随机选取K个对象作为聚类中心(质心)，然后计算每个对象与各质心之间的欧式距离，将每个对象分配给距离它最近的质心，FDIA 样本与正常样本由于欧氏距离的差异而被划分到不同的类别，进而实现检测。

K 均值算法实现简单、计算复杂度低，但对初始质心的选取和样本噪声具有高度敏感性。为克服上述方法的缺点，提高 FDIA 检测的鲁棒性和准确性，模糊 c-均值聚类算法脱颖而出。该方法通过优化目标函数得到每个样本点对所有类中心的隶属度，从而决定样本点的类属以达到自动对样本数据进行分类的目的。Mohammadpourfard[28,113]假设注入虚假数据后的状态向量的概率分布发生偏离，利用模糊 c-均值聚类算法，在拓扑变化和可再生能源集成的情况下成功辨识出了 FDIA，拓宽了 FDIA 检测的应用场景。

Chakhchoukh[114]从统计学习的角度研究 FDIA 检测问题，提出一种密度比估计(density ratio estimation，DRE)的检测算法，通过将量测数据的概率密度函数之比与设定阈值进行比较来判别是否遭受 FDIA。而 Ashrafuzzaman[102]采用局部离群因子(local outlier factor，LOF)的思路检测 FDIA，不同于传统离群值的二元属性，LOF 给出了每个对象的离群程度，能够适应 FDIA 样本与正常样本密度不同的情况。

隔离林是一种从异常点出发，通过指定规则进行划分，根据划分次数进行判断的异常检测方法。这是一种由若干隔离树组合的集成学习方法，划分次数相当于从根到叶的路径长度，受损的量测值通常被隔离到树的根附近。文献[102,115]采用该算法进行检测，结果表明 FDIA 样本具有最短平均路径长度，符合隔离林中异常值的分布特征。

自编码器(autoencoder，AE)是一种对输入数据进行表征学习的人工神经网络，是典型的无监督学习算法。AE 包含编码器和解码器两部分，在数据降维、特征提取和异常检测等方面应用广泛。文献[25,116-117]应用 AE 进行 FDIA 检测，相比传统机器学习方法获得更优的检测效果。

2.2.3 基于半监督学习的 FDIA 检测

半监督学习是有监督学习和无监督学习相结合的一种学习方法，通过使用大量的未标记数据和少量的标记数据来进行模式识别工作。考虑到实际电力系统中量测数据标记成本昂贵以及可能出现的标记数据丢失问题，半监督学习方法是解决 FDIA 检测问题的一种有效途径。

Ozay[86]最早应用半监督学习检测 FDIA，构造了一种半监督 SVM 算法；随后，Foroutan[118]提出一种基于混合高斯分布的学习算法，通过估计正常量测数据分布来寻找非拟合的攻击点。Zhang[119]提出一种对抗自编码器的算法来检测配电网中的 FDIA，试验结果表明在仅有 2%的含标签样本情况下仍能满足 FDIA 检测精度，证明该方法的鲁棒性。

2.2.4 基于对抗博弈学习的 FDIA 检测

近年来，一种名为生成对抗网络(generative adversarial networks，GAN)的深度学习算法发展迅猛，成为近年来复杂分布上无监督学习最具前景的方法之一。与传统无监督学习算法不同的是，GAN 采用了博弈论的思想，通过生成器(generator)和判别器(discriminator)两个模块之间进行对抗博弈，让机器在博弈中实现自我成长。其中，生成器学习如何生成近似真实数据的样本来欺骗判别器，而判别器学习如何区分正常量测数据和虚假数据，双方的目标均为最小化各自的损失函数，最终实现纳什均衡。

Zhang[119]和 Huang[120]采用 AE 和 GAN 相结合

的方法检测 FDIA，其中 AE 用于特征提取和数据降维，GAN 用于检测量测数据是否遭受 FDIA；为了提高 GAN 的计算效率和保持状态估计的实时运行，Li[27]分别提出改进平滑训练技术和在线自适应窗口思想，提高了 FDIA 检测性能。利用 GAN 的生成器具有近似真实数据样本的性能，Li 和 Huang 还实现了量测值替换和状态恢复，完善了 FDIA 的防御体系。

2.2.5　基于强化学习的 FDIA 检测

强化学习是一种让智能体(agent)在与环境的交互过程中通过学习策略以达成回报最大化或实现特定目标的机器学习算法。不同于监督学习和非监督学习，强化学习不要求预先给定任何数据，而是通过接收环境对动作的奖励(反馈)获得学习信息并更新模型参数。

基于强化学习思想的 FDIA 检测方法研究目前仅有两篇文章，其性能有待进一步研究。Kurt[26]采用部分可观测马尔可夫决策过程(partially observable markov decision process，POMDP)算法，以模拟 agent 与环境之间的关系。POMDP 是一个七元组$(S, A, T, R, O, \Omega, \gamma)$，$S$ 为系统的状态，该场景中为攻击前状态和攻击后状态两种；A 为 agent 的动作集合，该场景中为继续和终止两种；T 为状态之间的一组条件转移概率；R 为奖励函数，该场景中 reward 函数的目标由最大化折扣奖励修改为平均检测延迟和误警率最小；O 为一组观测集合，该场景中指系统量测数据；Ω 为一组条件观测概率；$\gamma \in [0, 1]$为折扣因子。Kurt 通过让 agent 与环境进行交互，学习攻击前后数据特征之间的差异，不断优化动作决策，从而更及时地发现 FDIA 的存在，实现 FDIA 实时检测。Dou[121]在 Kurt 基础上对奖励函数进行修改和优化，并采用深度强化学习算法进一步提高了 FDIA 检测精度和效率。

3　FDIA 检测性能对比分析

为了对 FDIA 检测方法有一个更全面的认识，本章对各类检测算法的性能进行了详细的整理和对比分析，分别从算法检测率、算法鲁棒性、算法与状态估计的逻辑关系、算法适应性和算法识别能力等方面进行总结。

3.1　FDIA 检测性能汇总

FDIA 检测算法性能对比按照模型驱动和数据驱动两类汇总于表 1、2，选取检测率和误警率两项指标进行表征。需要注意的是，不同论文的算例设计差别较大，攻击建模、攻击幅度和检测次数难以统一，表中的检测率和误警率选取同类算法中的最大范围。

表 1　模型驱动算法分类与比较

Table 1　Classification and comparison of model-driven algorithms

类别	算法	参考文献	检测率	误警率
基于状态估计检测	MF	[38]	0.99	0.0459
	DSE	[14-15]	0.76~0.93	—
	DCOPF	[39]	Detected	—
	Trust-SE	[40]	Detected	—
	ATSE	[41]	0.95	0.9~0.99
	MTD	[42-45]	1	0.2
	编码策略	[46-49]	1	—
	KF	[16-17,50]	Detected	—
	递归 WLS	[51]	0.85~0.98	—
	EKF	[54-56]	Detected	—
	UKF	[58-61]	0.9~1	0.1
基于图论检测	GSP	[62]	0.326	0.21
	Graph	[63]	0.99	0.006
	MLE	[64-65]	0.25~1	0.0004
	GNN	[66]	0.96~0.99	0.015~0.04
	拓扑变换	[67]	Detected	—
基于物理特性检测	输电线路	[68]	0.85~1	—
	LCDR	[69]	Detected	—
	NVSI	[70-72]	0.2~0.9	—
	PTDF	[73-74]	0.95~1	0.0125
	Phaseshifter	[75]	0.99	0.003
其他模型驱动算法	矩阵分解	[18,76-78]	0.92~0.95	0.014~0.048
	负荷预测	[79-80]	0.8~1	0.05~0.35
	KLD	[19,81-82]	0.99	—
	CUSUM	[83-84]	0.65~0.98	<0.02
	Benford'slaw	[85]	Detected	—

注：“—”表示文中未提及；Detected 表示检测到 FDIA。

1）模型驱动。

模型驱动算法的检测性能对比如表 1 所示，本文整理的基于模型驱动的 FDIA 检测算法共有 52 篇，其中基于状态估计检测论文共 25 篇，占比 48.1%，是模型驱动算法中的代表性算法。基于状态估计的检测算法普遍具有较高的检测率，其中变换目标防御和编码策略对于有约束的隐形 FDIA 具有 100%的检测率，是近几年的新兴算法，值得进一步拓展研究；基于图论检测论文共 6 篇，占比 11.5%，文献[63]是该类别的代表算法，具有高达 99%的检测率和 0.6%的误警率。文献[64-65]尽管可以达到 100%的检测率，但是需要大量的攻击向量

表 2 数据驱动算法分类与比较

Table 2 Classification and comparison of data-driven algorithms

类别	算法	FS/FE	参考文献	检测率/%	误警率/%
有监督学习	SVM	PCA/GA	[21,25,86-92]	40~99	—
	KNN	PCA/GA	[22,25,86-87,90,93]	80~97	4
	ENN	—	[87]	85~100	—
	DT	KPCA	[94-95]	86~98	—
	ELM	AE	[23,96-98]	95~99	0.1~10
	Boosting	JMIM/AL	[86,99-100]	95~99	2
	RF	RFC	[101-103]	89~95	2~50
	集成 ELM	—	[98]	99	—
	MLP	GA/RFC	[86,90-91,96,104]	90~99	16.9
	CNN	—	[105-108]	90~99	—
	RNN	DWT	[89,105,108-111]	90~99	1.4~4.6
	DBN	—	[112]	96	3.6
无监督学习	KMC	GA	[22]	90	—
	FC	PCA	[28,113]	87~99	0.5~3
	DRE	—	[114]	17~100	—
	隔离林	RFC/PCA	[102,115]	89~94	0.03~53
	AE	WSV	[25,116-117]	97~99	26
半监督学习	SSVM	—	[86]	80~100	—
	混合高斯分布	PCA	[118]	95.6	—
	AAE	AE	[119]	97.8	—
对抗博弈学习	GAN	AE	[27,119-120]	97~99	0.1~0.6
强化学习	POMDP	—	[26,121]	99	0.2

注：“—”表示文中未提及；FS/FE 表示特征选择/特征提取；GA 表示遗传算法；FPCA 表示核主成分分析；JMIM 表示联合交互信息最大化；AL 表示主动学习；RFC 表示随机森林分类器；DWT 表示离散小波变换；WSV 表示小波奇异值变换。

样本；基于物理特性检测论文共 8 篇，占比 15.4%，文献[73-74]选取的功率传输分布因子作为 FDIA 检测指标具有高于 95%的检测率。文献[68]尽管检测率高达 85%以上，但要求所有线路两端装设 PMU 装置，成本过高；其他模型驱动检测论文共 13 篇，占比 25%，其中矩阵分解和相对熵算法均达到 92%以上的检测率。

值得注意的是，表 1 中检测率受攻击建模、攻击幅度、受攻击量测占比、攻击样本个数、检测阈值和各类模型参数等因素影响，比如降低检测阈值可以提高检测率，但同时也增加了误警率，使得电力系统调度误动作的风险相应提高。因此，FDIA 检测阈值的设定是模型驱动检测算法中的一项主要挑战，需仔细斟酌并通过大量算例进行验证。

2）数据驱动。

数据驱动算法的检测性能对比如表 2 所示，与表 1 略有不同，表 2 还统计了数据驱动算法中采用的特征选择/特征提取方法。

本文整理的基于数据驱动的 FDIA 检测算法共有 44 篇，其中有监督学习检测论文共 32 篇，占比 72.7%，是数据驱动算法中的主要算法。支持向量机是该类检测算法中应用最早且最广泛的算法，然而其检测性能不稳定，且计算复杂度较高，通常结合主成分分析进行数据预处理；相比之下，极限学习机在学习速率和泛化能力上更具优势，在相关论文算例中也表现出更高的检测率。无监督学习检测论文共 9 篇，占比 20.5%，模糊 c-均值聚类表现优异，在考虑噪声及可再生能源集成的场景中仍保持很高的检测率，最高可达 99%；而自编码器除了自身优异的检测性能，通常还作为其他算法的特征提取方法。半监督学习检测论文共 3 篇，占比 6.8%，文献[119]将自编码器和 GAN 相结合，提高了 FDIA 检测的鲁棒性并取得 97.8%的检测率；对抗博弈学习检测共 3 篇，占比 6.8%，基于生成对抗网络的 FDIA 检测算法具有很高的检测率和较低的误警率；强化学习检测仅 2 篇，占比 4.5%，在 FDIA 快速实时检测方面表现优异，然而由于文献数量较少，该算法的检测性能有待进一步验证。

表 2 数据驱动算法的检测率同样受许多因素影响，例如神经网络隐藏层数、神经元个数、训练样本数、正负样本比例、测量噪声等等。其中检测率与训练样本数之间存在依赖关系，训练样本数越多，检测率越高；但同时也增加了计算时间和存储成本，不利于 FDIA 的实时快速检测。值得注意的是，很多深度学习算法的优越性能都需要大量的训练样本来支撑。因此，当计算机配置较高时，应构建足够的 FDIA 攻击样本用于模型训练和测试。

3.2 FDIA 检测算法鲁棒性对比

检测率并非评价一个 FDIA 检测算法好坏的唯一指标，计算复杂度、算法适应性和鲁棒性都是衡量检测算法性能的重要依据[122]。本节从算法鲁棒性的角度对 FDIA 检测算法进行对比分析。

算法鲁棒性一般被认为具有三个层面的概念：一是算法具有较高的精度；二是对于模型假设出现的较小偏差，只能对算法性能产生较小的影响；三是对于模型假设出现的较大偏差，不能对算法性能产生“灾难性”的影响。在 FDIA 检测场景下，算法鲁棒性的第一层概念对应算法的检测率和误警

率，第二层概念对应噪声场景，而第三层概念对应考虑负荷波动和拓扑改变的情况。表 3 对 FDIA 检测算法是否考虑量测噪声、负荷波动和拓扑变化进行了整理与比较。

表 3　FDIA 检测算法鲁棒性对比

Table 3　Robustness comparison of FDIA detection algorithms

类别	参考文献	考虑噪声	考虑负荷波动	考虑拓扑改变
模型驱动算法	[38-41,55-56,62-63,70-72,83-84]	×	×	×
	[16-18,42-43,45-51,58-61,66,68,73,76-80,85]	√	×	×
	[44,54,64-65,69,74-75]	√	√	×
	[19,67,81-82]	√	×	√
数据驱动算法	[86,89-92,101,103,105,107-110,117,121]	×	×	×
	[21-23,87-88,100]	×	√	×
	[27,95-97,99,102,104,112,116]	√	×	×
	[24,94,98,106,111,114-115,118-119]	√	√	×
	[26]	√	×	√
	[28,93,113,120]	√	√	√

在模型驱动检测算法中 16 篇没有考虑上述 3 种场景，25 篇仅考虑了噪声存在，7 篇考虑了噪声和负荷波动的场景，4 篇考虑噪声和拓扑变化的场景；而数据驱动检测算法中，15 篇没有考虑上述 3 种场景，9 篇仅考虑了噪声存在，6 篇仅考虑了负荷波动，9 篇考虑了噪声和负荷波动的场景，1 篇考虑噪声和拓扑变化的场景，仅有 4 篇考虑了上述 3 种场景。

根据上述统计结果可知，量测噪声是检验 FDIA 检测算法鲁棒性的首选场景，占比 61.5%；未考虑鲁棒场景或仅考虑一种场景的论文占比 74%，这是由于很多学者制定的检测算法是为某一特定攻击场景或攻击模型而精心设计的；Mohammadpourfard[28,93,113] 和 Huang[120] 提出的检测算法综合考虑噪声、负荷波动和拓扑变化的场景，具有很高的鲁棒性，能够适应复杂多变的检测环境。

3.3　FDIA 检测算法与状态估计的逻辑关系

鉴于面向电力 SCADA 系统的 FDIA 是针对电网状态估计而提出的，不同 FDIA 检测算法与状态估计之间存在一定的逻辑关系，如图 3 所示。本节将检测算法与状态估计算法之间的关系归纳为五类：检测算法在状态估计之前；检测算法与状态估计并行运算；检测算法在状态估计之后；检测算法基于状态估计；检测算法与状态估计无关。相关文献整理详见表 4。为简便起见，图 3 和表 4 小标题中的“状态估计”用其英文简称“SE”代替。

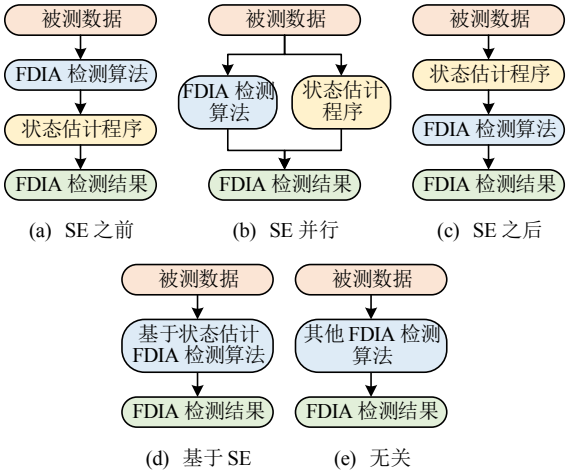

图 3　算法与状态估计逻辑关系

Fig. 3　Logic relation between algorithm and state estimation

表 4　FDIA 检测算法与状态估计的关系

Table 4　Relationship between FDIA detection algorithm and state estimation

算法与 SE 的关系	参考文献
SE 之前	[27,70-72,74,107]
SE 并行	[26,79-80,98,105,121]
SE 之后	[20,24,28,62-66,73,75,83-84,93,96,106,111-113,119-120]
基于 SE	[14-17,38-51,54-61,67]
无关	[18-19,21-23,68-69,76-78,81-82,85-92,94-95,97,99-104,108-110,114-118]

本文整理的 FDIA 检测方法文献中，约 28.1%的论文基于状态估计进行检测，该类方法针对虚假数据躲避残差检测的原理反其道而行之，使特征参数的 2 范数超过检测阈值而检出，是 FDIA 检测领域最先发展起来一类算法，典型算法有 WLS、DSE 等；约 20.8%的论文在状态估计程序之后检测 FDIA，即首先通过状态估计的滤波作用，将误操作或仪表误差导致的量测不良数据剔除，然后针对 FDIA 设计相应算法进行检测，典型算法有基于图论检测和模糊 c-均值聚类等；约 6.3%的论文在状态估计程序执行之前检测，典型算法如 NVSI 和 GAN 等；6 篇论文的检测算法与状态估计程序并行计算，比较两者输出变量的偏差或并行触发警报，典型算法有负荷预测算法和集成 ELM 等；约 40%的论文与状态估计程序无关，仅对量测数据进行处理，单独检测 FDIA，典型算法如矩阵分解、相对熵、SVM 等。

3.4　FDIA 检测算法适应性分析

综合表 1—3 中检测率、考虑场景以及算法计算复杂度，可以确定不同算法适用的系统类型、规

模及场景，对算法进行适应性分析。

面向电力 SCADA 系统的 FDIA 检测场景中，输电网是学者们研究的主要系统类型。在输电网的隐形 FDIA 检测算法中，GAN[27]、图论法[63]、最大似然估计[64-65]、PTDF[73-74]、CUSUM[83-84]以及各种分布式检测算法具有较高的检测率和较低的计算复杂度，适用于大规模系统实时在线检测；集成学习类[98,100]算法检测准确但计算量较大，适用于中小规模系统；模糊 c-均值聚类[28,113]算法在可再生能源集成和拓扑变化场景中表现出良好的鲁棒性；矩阵分解[18,76-78]算法适用于量测冗余度高且攻击向量稀疏的情况，在量测裕度不足或大范围 FDIA 的场景下性能不佳；NVSI[70,72]和相对熵[19,81-82]算法恰恰相反，在攻击量测数占比高时有更好的检测性能，而对于单一节点连续小幅度的 FDIA 失效。

在 AGC 系统中，KF[52-53]算法相比其他算法具有更好的检测性能；LCDR[69]算法是检测继电保护装置中 FDIA 的代表性算法；文献[75]是目前唯一一篇针对移相器 FDIA 检测的文章；针对配电网 FDIA 检测的研究相对较少，基于半监督学习的 AE[119]算法是最近提出的一种高性能检测算法。

需要强调的是，为了实现不同算法检测性能的公平比较，所考虑的算例系统类型、规模及 FDIA 攻击模型应该保持一致。

3.5 FDIA 检测算法识别能力对比

FDIA 检测作为电力系统网络攻击防御体系的重要组成部分，其算法对虚假数据的识别程度和处理能力关系到电力系统网络安全。绝大部分检测文章只关注 FDIA 是否存在，模型驱动算法通常运用二元假设检验进行判别，而数据驱动算法则处理为二元分类问题。不足 20%的检测算法考虑了对量测信息中虚假数据的具体位置进行辨识，其中 F 检验算法[28]、图论算法[63]、DLLD[106]、辨识精准，便于后续的坏量测剔除和保护配置。仅有 7 篇文献([27,39-40,61,97-98,120])不仅辨识出 FDIA 的位置，同时还对系统进行状态恢复，实现 FDIA 弹性控制，对网络攻击风险具有更强的抵御能力。

4 FDIA 检测方法总体评价

4.1 FDIA 检测方法优缺点分析

尽管所有检测算法的目标都是在电力 SCADA 系统中检测出 FDIA，不同类别的算法在实际应用过程中表现出各自不同的优缺点[12]。表 5 总结了模型驱动算法和数据驱动算法的主要优缺点。

表 5 FDIA 检测算法优缺点总结

Table 5 A Summary of the advantages and disadvantages of FDIA detection algorithms

算法	优点	缺点
模型驱动检测算法	•模型依托电力系统运行特性，参数可解释性好 •对特定场景或有约束的 FDIA 具有更好检测效果 •无训练过程的时间成本 •对存储空间要求较少 •对历史数据集需求较小	•需要系统模型和参数 •设定检测阈值 •检测延时大，难以进行实时检测 •可拓展性较差 •计算复杂度较高 •收敛性问题 •部分方法降低系统量测冗余度和供电可靠性
数据驱动检测算法	•不依赖系统模型及参数 •实时快速检测 •可拓展性较好，适应各种约束条件下的 FDIA	•需要耗时的训练过程和大量的训练数据集 •需要额外的存储空间以存储大量历史数据 •训练样本过拟合问题 •对系统通信能力和数据处理能力要求较高 •量测仪表及通信设备投资成本较高

基于模型驱动的 FDIA 检测方法的主要优点是模型建立通常依托于电力系统运行特性，参数可解释性好；对特定场景或有约束条件的 FDIA 具有更好的检测效果；不存在模型训练过程，一旦设计好检测流程可直接投入使用，节省了模型训练阶段的时间成本；同时，大部分模型驱动检测算法仅需要当前时刻量测数据作为输入参数，对历史数据集的需求较小，因此对计算设备存储空间的要求也相对较低。然而，该类方法也存在以下缺点和不足：首先是模型驱动算法强依赖于系统模型及参数，当系统建模不准确或参数不确定时可能产生恶劣的检测性能；其次，设定适合的检测阈值难度较大，阈值较低，会提高误警率，而阈值较高又达不到理想的检测效果；模型驱动算法通常对适用场景及攻击类型作出限定，可拓展性相对较差；部分方法(如基于状态估计检测法和拓扑变换检测法)还会降低系统量测冗余度和供电可靠性，限制电力系统全局输电能力；此外，模型驱动类算法的计算复杂度较高，检测时延较大，同时可能出现计算不收敛的问题。

基于数据驱动的 FDIA 检测方法的主要优点是不依赖于系统的模型及参数，能够从大量输入数据中挖掘特征实现检测，因而算法可拓展性好，能够适应各种场景和约束条件下的 FDIA；同时，数据驱动算法一旦训练完毕，对测试数据集的检测时延很短(单个样本检测时延通常为 ms 级)，适合实时在

线检测。然而，这类方法的缺点也很明显：其一，需要非常耗时的训练过程和大量的训练数据集，数据量不足将严重影响算法检测性能；其二，需要额外的存储空间以存储大量历史数据，对计算机硬件的要求较高；其三，数据驱动类算法往往存在过拟合问题，即对训练样本表现良好而对测试样本表现不佳；其四，为实现 FDIA 的实时快速检测，对系统的通信能力和数据处理能力要求较高；其五，量测仪表及通信设备的投资成本较高。

4.2　存在问题与未来展望

目前，面向电力 SCADA 系统的 FDIA 检测方法普遍存在系统建模简化、不确定性场景下识别能力较差、算法可扩展性较差、适用范围窄等问题。未来随着源网荷储协调互动、信息系统与物理系统耦合程度不断加深以及海量数据的交换共享，电力系统遭受 FDIA 的入侵范围更广、识别难度更大、信息处理时间更短。针对这样的现状问题和未来需求，后续研究需要在检测精度、算法适应性、鲁棒性、时效性等方面进行探索。FDIA 检测方法未来发展方向总结如下：

1）算法适应性。

考虑 FDIA 检测系统的扩展，目前的检测系统大都集中在直流模型下的输电网，随着源网荷储一体化建设，未来可扩展到交流输电网、主动配电网、直流微网、用户储能、综合能源系统及智能电表等系统类型。

2）算法鲁棒性。

从检测场景、攻击建模和自适应性几方面入手。

在 FDIA 检测场景拓展方面，考虑风电光伏等不确定性出力场景下的 FDIA 检测；考虑量测噪声、负荷波动及拓扑变化等鲁棒性场景下的 FDIA 检测；考虑信息物理协同攻击下的异常检测。

在攻击建模方面，考虑更实际的 FDIA 攻击模型。现有的 FDIA 检测文献通常假设攻击者充分了解电网的模型及参数，并且攻击资源不受限制，可以攻击任意数量的量测仪表。然而，更实际的情况是研究攻击资源受限、不完全信息下 FDIA 的检测。

在自适应性方面，研究自适应的 FDIA 检测算法，减少对专家知识的需求。对于模型驱动方法，研究自适应检测阈值的相关算法；对于数据驱动方法，采用更先进更智能的算法。

3）算法时效性。

研究适用于大规模节点系统的实时检测算法。目前大多数论文局限于小规模节点系统，并且往往更关注检测精度而忽略了计算复杂度和检测时间。随着智能电网规模的不断扩展和数据量的指数式增长，研究大规模系统实时快速检测算法具有更高的应用价值。

4）算法检测能力。

由 FDIA 存在性检测过渡到 FDIA 弹性控制。目前大多数文章只能检测 FDIA 是否存在，而 FDIA 弹性控制则要求能够辨识 FDIA 具体位置，并对受损量测进行剔除、预测值替换或应急保护措施，从而实现系统状态恢复。

研究信息系统辅助检测方法。目前的 FDIA 检测方法主要集中于物理系统，随着信息系统与物理系统耦合程度不断加深，未来可深入分析两系统之间的耦合关联关系，借助信息侧异常流量检测弥补单独物理侧检测方法的不足。

研究差异化检测方案。目前没有任何一种算法适用于各种系统和场景，因此需要针对不同攻击类型、攻击后果设计分层检测方案，对电力系统威胁更大的 FDIA 实现优先检测。

5　结论

针对面向电力 SCADA 系统的虚假数据注入攻击，本文从 FDIA 检测方法的发展历程、分类及机理、检测性能等方面对现有研究相关成果进行整理和归纳，总结了 FDIA 检测方法的优缺点，阐述了目前 FDIA 检测研究存在的问题并展望了该领域的未来发展方向。随着源网荷储协调互动、信息系统与物理系统耦合程度不断加深以及海量数据的交换共享，电力系统遭受 FDIA 的风险越来越大，应更加重视电力系统网络安全建设，完善网络攻击检测与保护体系。

参考文献

[1] WU F F. Power system state estimation：a survey[J]. International Journal of Electrical Power & Energy Systems，1990，12(2)：80-87.

[2] 李碧君，薛禹胜，顾锦汶，等. 电力系统状态估计问题的研究现状和展望[J]. 电力系统自动化，1998，22(11)：53-60.
LI Bijun，XUE Yusheng，GU Jinwen，et al. Status Quo and prospect of power system state estimation[J]. Automation of Electric Power Systems，1998，22(11)：53-60(in Chinese).

[3] MONTICELLI A . Electric power system state

estimation[J]. Proceedings of the IEEE，2000，88(2)：262-282.

[4] HARDY T L. Software and system safety：accidents，incidents，and lessons learned[M]. AuthorHouse，2012.

[5] 董朝阳，赵俊华，文福拴，等. 从智能电网到能源互联网：基本概念与研究框架[J]. 电力系统自动化，2014，38(15)：1-11.
DONG Zhaoyang，ZHAO Junhua，WEN Fushuan，et al. From smart grid to Energy Internet：Basic Concept and research framework[J]. Automation of Electric Power Systems，2014，38(15)：1-11(in Chinese).

[6] 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(in Chinese).

[7] LIU Yao，NING Peng，REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security，2011，14(1)：13.

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

[9] 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.

[10] ABOELWAFA M M N，SEDDIK K G，ELDEFRAWY M H，et al. A machine-learning-based technique for false data injection attacks detection in industrial IoT[J]. IEEE Internet of Things Journal，2020，7(9)：8462-8471.

[11] SEDJELMACI H，SENOUCI S M，MESSOUS M A. How to detect cyber-attacks in unmanned aerial vehicles network?[C]//2016 IEEE Global Communications Conference (GLOBECOM). Washington，DC：IEEE，2016：1-6.

[12] MUSLEH A S，CHEN G，DONG Z Y. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid，2020，11(3)：2218-2234.

[13] KOSUT O，JIA Liyan，THOMAS R J，et al. Malicious data attacks on the smart grid[J]. IEEE Transactions on Smart Grid，2011，2(4)：645-658.

[14] GU Yun，LIU Ting，WANG Dai，et al. Bad data detection method for smart grids based on distributed state estimation[C]//2013 IEEE International Conference on Communications (ICC). Budapest：IEEE，2013：4483-4487.

[15] WANG Dai，GUAN Xiaohong，LIU Ting，et al. Extended distributed state estimation：A detection method against tolerable false data injection attacks in smart grids[J]. Energies，2014，7(3)：1517-1538.

[16] MANANDHAR K，CAO Xiaojun，HU Fei，et al. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter[J]. IEEE Transactions on Control of Network Systems，2014，1(4)：370-379.

[17] RAWAT D B，BAJRACHARYA C. Detection of false data injection attacks in smart grid communication systems[J]. IEEE Signal Processing Letters，2015，22(10)：1652-1656.

[18] LIU Lanchao，ESMALIFALAK M，DING Qifeng，et al. Detecting false data injection attacks on power grid by sparse optimization[J]. IEEE Transactions on Smart Grid，2014，5(2)：612-621.

[19] 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.

[20] HUANG Yi，TANG Jin，CHENG Yu，et al. Real-time detection of false data injection in smart grid networks：An adaptive CUSUM method and analysis[J]. IEEE Systems Journal，2016，10(2)：532-543.

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

[22] 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.

[23] YANG Liqun，LI Yuancheng，LI Zhoujun. Improved-ELM method for detecting false data attack in smart grid[J]. International Journal of Electrical Power & Energy Systems，2017，91：183-191.

[24] YU J J Q，HOU Yunhe，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.

[25] PINCETI A，SANKAR L，KOSUT O. Load redistribution attack detection using machine learning：A data-driven approach[C]//2018 IEEE Power & Energy Society

General Meeting (PESGM). Portland：IEEE，2018：1-5.

[26] KURT M N，OGUNDIJO O，LI Chong，et al. Online cyber-attack detection in smart grid：a reinforcement learning approach[J]. IEEE Transactions on Smart Grid，2019，10(5)：5174-5185.

[27] LI Yuancheng，WANG Yuanyuan，HU Shiyan. Online generative adversary network based measurement recovery in false data injection attacks：A cyber-physical approach[J]. IEEE Transactions on Industrial Informatics，2020，16(3)：2031-2043.

[28] MOHAMMADPOURFARD M，SAMI A，WENG Yang. Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations[J]. IEEE Transactions on Sustainable Energy，2018，9(3)：1349-1364.

[29] 王先培，田猛，董政呈，等. 输电网虚假数据攻击研究综述[J]. 电网技术，2016，40(11)：3406-3414.
WANG Xianpei，TIAN Meng，DONG Zhengcheng，et al. A review of research on false data attack in transmission network[J]. Power System Technology，2016，40(11)：3406-3414(in Chinese).

[30] 王琦，郜伟，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(in Chinese).

[31] 汤奕，李梦雅，王琦，等. 电力信息物理系统网络攻击与防御研究综述(二)检测与保护[J]. 电力系统自动化，2019，43(10)：1-9，18.
TANG Yi，LI Mengya，WANG Qi，et al. A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection[J]. Automation of Electric Power Systems，2019，43(10)：1-9，18(in Chinese).

[32] 汤奕，陈倩，李梦雅，等. 电力信息物理融合系统环境中的网络攻击研究综述[J]. 电力系统自动化，2016，40(17)：59-69.
TANG Yi，CHEN Qian，LI Mengya，et al. Overview on cyber-attacks against cyber physical power system[J]. Automation of Electric Power Systems，2016，40(17)：59-69(in Chinese).

[33] DENG Ruilong，XIAO Gaoxi，LU Rongxing，et al. False data injection on state estimation in power systems-attacks，impacts，and defense：a survey[J]. IEEE Transactions on Industrial Informatics，2017，13(2)：411-423.

[34] LIANG Gaoqi，ZHAO Junhua，LUO Fengji，et al. A review of false data injection attacks against modern power systems[J]. IEEE Transactions on Smart Grid，2017，8(4)：1630-1638.

[35] SONG Yufei，LIU Xuan，LI Zhiyi，et al. Intelligent data attacks against power systems using incomplete network information：a review[J]. Journal of Modern Power Systems and Clean Energy，2018，6(4)：630-641.

[36] 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(in Chinese).

[37] 于尔铿. 电力系统状态估计[M]. 北京：水利电力出版社，1985.
YU Erkeng. State estimation of power system[M]. Beijing：Water Resources and Electric Power Press，1985(in Chinese).

[38] LUKICHEVA I，POZO D，KULIKOV A. Cyberattack detection in intelligent grids using non-linear filtering[C]//2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). Sarajevo：IEEE，2018：1-6.

[39] DUAN Jie，ZENG Wente，CHOW M Y. Resilient distributed DC optimal power flow against data integrity attack[J]. IEEE Transactions on Smart Grid，2018，9(4)：3543-3552.

[40] XIE Bin，PENG Chen，YANG Minjing，et al. A novel trust-based false data detection method for power systems under false data injection attacks[J]. Journal of the Franklin Institute，2021，358(1)：56-73.

[41] LIU Ting，SUN Yanan，LIU Yang，et al. Abnormal traffic-indexed state estimation：A cyber-physical fusion approach for smart grid attack detection[J]. Future Generation Computer Systems，2015，49：94-103.

[42] MORROW K L，HEINE E，ROGERS K M，et al. Topology perturbation for detecting malicious data injection[C]//2012 45th Hawaii International Conference on System Sciences. Maui：IEEE，2012：2104-2113.

[43] LIU Chensheng，WU Jing，LONG Chengnian，et al. Reactance perturbation for detecting and identifying FDI attacks in power system state estimation[J]. IEEE Journal of Selected Topics in Signal Processing，2018，12(4)：763-776.

[44] TIAN Jue，TAN Rui，GUAN Xiaohong，et al. Enhanced hidden moving target defense in smart grids[J]. IEEE Transactions on Smart Grid，2019，10(2)：2208-2223.

[45] LI Beibei，XIAO Gaoxi，LU Rongxing，et al. On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS

devices[J]. IEEE Transactions on Industrial Informatics，2020，16(2)：854-864.

[46] MIAO Fei，ZHU Quanyan，PAJIC M，et al. Coding schemes for securing cyber-physical systems against stealthy data injection attacks[J]. IEEE Transactions on Control of Network Systems，2017，4(1)：106-117.

[47] ZHAO Zhengen，HUANG Yimin，ZHEN Ziyang，et al. Data-driven false data-injection attack design and detection in cyber-physical systems[J]. IEEE Transactions on Cybernetics，2021，51(12)：6179-6187.

[48] 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 Linbai，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(in Chinese).

[49] LIU Chensheng，DENG Ruilong，HE Wangli，et al. Optimal coding schemes for detecting false data injection attacks in power system state estimation[J]. IEEE Transactions on Smart Grid，2022，131(1)：738-794.

[50] KURT M N，YILMAZ Y，WANG Xiaodong. Real-time detection of hybrid and stealthy cyber-attacks in smart grid[J]. IEEE Transactions on Information Forensics and Security，2018，14(2)：498-513.

[51] SREENATH J G，MEGHWANI A，CHAKRABARTI S，et al. A recursive state estimation approach to mitigate false data injection attacks in power systems[C]//2017 IEEE Power & Energy Society General Meeting. Chicago：IEEE，2017：1-5.

[52] KHALAF M，YOUSSEF A，EL-SAADANY E. Detection of false data injection in automatic generation control systems using kalman filter[C]//2017 IEEE Electrical Power and Energy Conference (EPEC). Saskatoon：IEEE，2017：1-6.

[53] KHALAF M，YOUSSEF A，EL-SAADANY E. Joint detection and mitigation of false data injection attacks in AGC systems[J]. IEEE Transactions on Smart Grid，2019，10(5)：4985-4995.

[54] 何耀，周聪，郑凌月，等. 基于扩展卡尔曼滤波的虚假数据攻击检测方法[J]. 中国电力，2017，50(10)：35-40.
HE Yao，ZHOU Cong，ZHENG Lingyue，et al. Detection method against false data injection attack based on extended kalman filter[J]. Electric Power，2017，50(10)：35-40(in Chinese).

[55] KARIMIPOUR H，DINAVAHI V. Robust massively parallel dynamic state estimation of power systems against cyber-attack[J]. IEEE Access，2017，6：2984-2995.

[56] KARIMIPOUR H，DINAVAHI V. On false data injection attack against dynamic state estimation on smart power grids[C]//2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE). Oshawa：IEEE，2017：388-393.

[57] JULIER S J，UHLMANN J K，DURRANT-WHYTE H F. A new approach for filtering nonlinear systems[C]// Proceedings of 1995 American Control Conference-ACC'95. Seattle：IEEE，1995：1628-1632.

[58] ŽIVKOVIĆ N，SARIĆ A T. Detection of false data injection attacks using unscented Kalman filter[J]. Journal of Modern Power Systems and Clean Energy，2018，6(5)：847-859.

[59] 罗小元，潘雪扬，王新宇，等. 基于自适应 Kalman 滤波的智能电网假数据注入攻击检测[J/OL]. 自动化学报，2020[2022-06-25]. http://doi.org/10.16383/j.aas.c190636.
LUO Xiaoyuan，PAN Xueyang，WANG Xinyu，et al. Detection of false data injection attack in smart grid via adaptive kalman filtering[J]. Automation，2020[2022-06-25]. http://doi.org/10.16383/j.aas.c190636(in Chinese).

[60] 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)：3226-3234.
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)：3226-3234(in Chinese).

[61] 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)：5462-5475.
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)：5462-5475(in Chinese).

[62] DRAYER E，ROUTTENBERG T. Detection of false data injection attacks in smart grids based on graph signal processing[J]. IEEE Systems Journal，2020，14(2)：1886-1896.

[63] JORJANI M，SEIFI H，VARJANI A Y. A graph theory-based approach to detect false data injection attacks in power system AC state estimation[J]. IEEE Transactions on Industrial Informatics，2021，17(4)：2465-2475.

[64] SEDGHI H，JONCKHEERE E. Statistical structure learning to ensure data integrity in smart grid[J]. IEEE Transactions on Smart Grid，2015，6(4)：1924-1933.

[65] MOSLEMI R，MESBAHI A，VELNI J M. A fast，decentralized covariance selection-based approach to detect cyber attacks in smart grids[J]. IEEE Transactions on Smart Grid，2018，9(5)：4930-4941.

[66] LI Yuancheng，WANG Yuanyuan．Developing graphical detection techniques for maintaining state estimation integrity against false data injection attack in integrated electric cyber-physical system[J]．Journal of Systems Architecture，2020，105：101705．

[67] WANG Shaocheng，REN Wei，AL-SAGGAF U M．Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks[J]．IEEE Systems Journal，2017，11(4)：2640-2651．

[68] PAL S，SIKDAR B，CHOW J H．Classification and detection of PMU data manipulation attacks using transmission line parameters[J]．IEEE Transactions on Smart Grid，2018，9(5)：5057-5066．

[69] AMELI A，HOOSHYAR A，EL-SAADANY E F．Development of a cyber-resilient line current differential relay[J]．IEEE Transactions on Industrial Informatics，2019，15(1)：305-318．

[70] ANWAR A，MAHMOOD A N，TARI Z．Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid[J]．Information Systems，2015，53：201-212．

[71] XU Ruzhi，WANG Rui，GUAN Zhitao，et al．Achieving efficient detection against false data injection attacks in smart grid[J]．IEEE Access，2017，5：13787-13798．

[72] 夏卓群，曾悠优，尹波，等．电力网络中基于物理信息的虚假数据入侵检测方法[J]．信息网络安全，2019，19(4)：29-36．
XIA Zhuoqun，ZENG Youyou，YIN Bo，et al．False data intrusion detection method based on physical information in power network[J]．Netinfo Security，2019，19(4)：29-36(in Chinese)．

[73] KAVIANI R，HEDMAN K W．A detection mechanism against load-redistribution attacks in smart grids[J]．IEEE Transactions on Smart Grid，2021，12(1)：704-714．

[74] LI Xingpeng，HEDMAN K W．Enhancing power system cyber-security with systematic two-stage detection strategy[J]．IEEE Transactions on Power Systems，2020，35(2)：1549-1561．

[75] CHAKRABARTY S，SIKDAR B．Detection of malicious command injection attacks on phase shifter control in power systems[J]．IEEE Transactions on Power Systems，2021，36(1)：271-280．

[76] GAO Pengzhi，WANG Meng，CHOW J H，et al．Identification of successive “unobservable” cyber data attacks in power systems through matrix decomposition [J]．IEEE Transactions on Signal Processing，2016，64(21)：5557-5570．

[77] LI Boda，DING Tao，HUANG Can，et al．Detecting false data injection attacks against power system state estimation with fast go-decomposition approach[J]．IEEE Transactions on Industrial Informatics，2019，15(5)：2892-2904．

[78] HUANG Keke，XIANG Zili，DENG Wenfeng，et al．False data injection attacks detection in smart grid：a structural sparse matrix separation method[J]．IEEE Transactions on Network Science and Engineering，2021，8(3)：2545-2558．

[79] 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，2018，9(3)：1636-1646．

[80] SRIDHAR S，GOVINDARASU M．Model-based attack detection and mitigation for automatic generation control[J]．IEEE Transactions on Smart Grid，2014，5(2)：580-591．

[81] KHANNA K，SINGH S K，PANIGRAHI B K，et al．On detecting false data injection with limited network information using transformation based statistical techniques[C]//2017 IEEE Power & Energy Society General Meeting．Chicago：IEEE，2017：1-5．

[82] SINGH S K，KHANNA K，BOSE R，et al．Joint-transformation-based detection of false data injection attacks in smart grid[J]．IEEE Transactions on Industrial Informatics，2018，14(1)：89-97．

[83] LI Shang，YILMAZ Y，WANG Xiaodong．Quickest detection of false data injection attack in wide-area smart grids[J]．IEEE Transactions on Smart Grid，2015，6(6)：2725-2735．

[84] JIANG Qiaomu，CHEN Huifang，XIE Lei，et al．Real-time detection of false data injection attack using residual prewhitening in smart grid network[C]//2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)．Dresden：IEEE，2017：83-88．

[85] MILANO F，GÓMEZ-EXPÓSITO A．Detection of cyber-attacks of power systems through benford’s law[J]．IEEE Transactions on Smart Grid，2021，12(3)：2741-2744．

[86] 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，2016，27(8)：1773-1786．

[87] YAN Jun，TANG Bo，HE Haibo．Detection of false data attacks in smart grid with supervised learning[C]//2016 International Joint Conference on Neural Networks (IJCNN)．Vancouver：IEEE，2016：1395-1402．

[88] AHMED S，LEE Y，HYUN S H，et al．Feature selection-based detection of covert cyber deception assaults in smart grid communications networks using machine learning[J]．IEEE Access，2018，6：27518-27529．

[89] BINNA S，KUPPANNAGARI S R，ENGEL D，et al. Subset level detection of false data injection attacks in smart grids[C]//2018 IEEE Conference on Technologies for Sustainability (SusTech). Long Beach：IEEE，2018：1-7.

[90] SAKHNINI J，KARIMIPOUR H，DEHGHANTANHA A. Smart grid cyber attacks detection using supervised learning and heuristic feature selection[C]//2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE). Oshawa：IEEE，2019：108-112.

[91] ALIMI O A，OUAHADA K，ABU-MAHFOUZ A M. Real time security assessment of the power system using a hybrid support vector machine and multilayer perceptron neural network algorithms[J]. Sustainability，2019，11(13)：3586.

[92] CHEN Ziyu，ZHU Jizhong，LI Shenglin，et al. Detection of false data injection attack in automatic generation control system with wind energy based on fuzzy support vector machine[C]//IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society. Singapore：IEEE，2020：3523-3528.

[93] MOHAMMADPOURFARD M，WENG Yang，PECHENIZKIY M，et al. Ensuring cybersecurity of smart grid against data integrity attacks under concept drift[J]. International Journal of Electrical Power & Energy Systems，2020，119：105947.

[94] ACOSTA M R C，AHMED S，GARCIA C E，et al. Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks[J]. IEEE Access，2020，8：19921-19933.

[95] LU Xiao，JING Jiangping，WU Yi. False data injection attack location detection based on classification method in smart grid[C]//2020 2nd International Conference on Artificial Intelligence and Advanced Manufacture (AIAM). Manchester：IEEE，2020：133-136.

[96] KHANNA K，PANIGRAHI B K，JOSHI A. AI-based approach to identify compromised meters in data integrity attacks on smart grid[J]. IET Generation，Transmission & Distribution，2018，12(5)：1052-1066.

[97] XUE D，JING X，LIU H. Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework[J]. IEEE Access，2019，7：31762-31773.

[98] WU Ting，XUE Wenli，WANG Huaizhi，et al. Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system[J]. IEEE Transactions on Industrial Informatics，2021，17(3)：1892-1904.

[99] CAO Jie，WANG Da，QU Zhaoyang，et al. A novel false data injection attack detection model of the cyber-physical power system[J]. IEEE Access，2020，8：95109-95125.

[100]XUE Wenli，WU Ting. Active learning-based XGBoost for cyber physical system against generic AC false data injection attacks[J]. IEEE Access，2020，8：144575-144584.

[101]WANG Defu，WANG Xiaojuan，ZHANG Yong，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.

[102]ASHRAFUZZAMAN M，DAS S，CHAKHCHOUKH Y，et al. Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning[J]. Computers & Security，2020，97：101994.

[103]SAKHNINI J，KARIMIPOUR H，DEHGHANTANHA A，et al. Physical layer attack identification and localization in cyber-physical grid：An ensemble deep learning based approach[J]. Physical Communication，2021，47：101394.

[104]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). Limassol：IEEE，2018：219-225.

[105]NIU Xiangyu，LI Jiangnan，SUN Jinyuan，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). Washington，DC：IEEE，2019：1-6.

[106]WANG Shuoyao，BI Suzhi，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.

[107]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(in Chinese).

[108]YIN Xuefei，ZHU Yanming，HU Jiankun. A Subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids[J]. IEEE Transactions on Industrial Informatics，2022，18(3)：1957-1967.

[109]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). Washington，DC：IEEE，2018：1-5.

[110]AYAD A，KHALAF M，EL-SAADANY E．Detection of false data injection attacks in automatic generation control systems considering system nonlinearities[C]//2018 IEEE Electrical Power and Energy Conference (EPEC)．Toronto：IEEE，2018：1-6.

[111]YANG Liqun，ZHANG Xiaoming，LI Zhi，et al．Detecting bi-level false data injection attack based on time series analysis method in smart grid[J]．Computers & Security，2020，96：101899.

[112]HE Youbiao，MENDIS G J，WEI Jin．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.

[113]MOHAMMADPOURFARD M，SAMI A，SEIFI A R．A statistical unsupervised method against false data injection attacks：a visualization-based approach[J]．Expert Systems with Applications，2017，84：242-261.

[114]CHAKHCHOUKH Y，LIU Song，SUGIYAMA M，et al．Statistical outlier detection for diagnosis of cyber attacks in power state estimation[C]//2016 IEEE Power and Energy Society General Meeting (PESGM)．Boston：IEEE，2016：1-5.

[115]AHMED S，LEE Y D，HYUN S H，et al．Unsupervised machine learning-based detection of covert data integrity assault in smart grid networks utilizing isolation forest[J]．IEEE Transactions on Information Forensics and Security，2019，14(10)：2765-2777.

[116]DEHGHANI M，KAVOUSI-FARD A，DABBAGHJAMANESH M，et al．Deep learning based method for false data injection attack detection in AC smart islands[J]．IET Generation，Transmission & Distribution，2020，14(24)：5756-5765.

[117]KUNDU A，SAHU A，SERPEDIN E，et al．A3D：Attention-based auto-encoder anomaly detector for false data injection attacks[J]．Electric Power Systems Research，2020，189：106795.

[118]FOROUTAN S A，SALMASI F R．Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method[J]．IET Cyber-Physical Systems：Theory & Applications，2017，2(4)：161-171.

[119]ZHANG Ying，WANG Jianhui，CHEN Bo．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.

[120]HUANG Xiaoge，QIN Zhijun，XIE Ming，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，2021：1，DOI：10.35833/MPCE.2020.000686.

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

[122]HAMPEL F R，RONCHETTI E M，ROUSSEEUW P J，et al．Robust statistics：the approach based on influence functions[M]．New York：Wiley，1986.

杨玉泽

在线出版日期：2022-11-02。
收稿日期：2022-05-05。

作者简介：
杨玉泽(1998)，男，工学博士，研究方向为电力信息物理系统网络攻击、韧性提升，1835176017@qq.com；
*通信作者：刘文霞(1967)，女，博士，博士生导师，研究方向为电力系统风险评价、智能规划等，liuwenxia001@163.com。

(责任编辑　李泽荣)