文章编号：1674-0629(2025)06-0039-12 中图分类号：TM732 文献标志码：A
DOI：10. 13648/j. cnki. issn1674-0629. 2025. 06. 004

基于状态空间分解的电力系统虚假数据注入攻击检测与防御方法

梁志宏[1,2]，严彬元[3]，洪超[1,2]，陶佳冶[3]，杨祎巍[1,2]，陈霖[1,2]，李攀登[1,2]
（1. 南方电网科学研究院，广州 510663；2. 广东省电力系统网络安全重点实验室，广州 510663；3. 贵州电网有限责任公司信息中心，贵阳 550000）

摘要：在可再生能源高渗透率的背景下，电力系统的负荷频率控制(load frequency control，LFC)面临虚假数据注入攻击(false data injection attack，FDIA)的安全威胁。现有检测方法难以有效区分控制输入攻击和测量数据攻击，影响系统的稳定性和安全性。为此建立了包含可再生能源及储能系统的LFC状态空间模型，并分析了FDIA对系统动态特性的影响。通过状态空间分解方法将攻击信号解耦为控制输入攻击和测量攻击，提高检测精度。基于滑模观测器设计攻击估计方法，实现对攻击信号的实时检测。进一步结合H_∞控制理论，提出了抗攻击控制(attack-resilient control，ARC)策略，以增强系统在攻击环境下的鲁棒性。仿真算例表明：与传统方法相比攻击估计均方误差降低约30 %，系统频率响应稳定性显著提升。结果表明，该方法能够有效检测FDIA并提高电力系统的安全性和抗干扰能力。

关键词：负荷频率控制；虚假数据注入攻击；状态空间分解；滑模观测器；抗攻击控制

Detection and Defense Methods for False Data Injection Attack in Power Systems Based on State-Space Decomposition

LIANG Zhihong[1,2], YAN Binyuan[3], HONG Chao[1,2], TAO Jiaye[3], YANG Yiwei[1,2], CHEN Lin[1,2], LI Pandeng[1,2]
（1. Electric Power Research Institute, CSG, Guangzhou 510663, China；2. Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou 510663, China；3. Information Centre of Guizhou Power Grid Co., Ltd., Guiyang 550000, China）

Abstract: With the growing integration of renewable energy, load frequency control (LFC) in power systems faces security risks from false data injection attack (FDIA). Existing detection methods struggle to differentiate control input attacks from measurement attacks, compromising system stability and security. This paper develops a state-space model for LFC incorporating renewable energy and energy storage systems and analyzes the impact of FDIA on system dynamics. A state-space decomposition method is employed to decouple attack signals into control input and measurement attacks, improving detection accuracy. A sliding mode observer-based attack estimation method is proposed for real-time detection. Additionally, an attack-resilient control (ARC) strategy is designed using H_∞ control theory to enhance system robustness. Simulations show that the proposed method reduces the attack estimation mean squared error by nearly 30% and significantly improves frequency response stability compared to traditional methods. These results demonstrate the method′s effectiveness in detecting FDIA and enhancing power system security.

Key words: load frequency control; false data injection attack; state-space decomposition; sliding mode observer; anti-attack control

基金项目：国家重点研发计划资助项目(2023YFB3106802)；贵州电网有限责任公司科技项目(GZKJXM20222346)。
Foundation item: Supported by National Key Research and Development Program of China (2023YFB3106802); the Science and Technology Project of Guizhou Power Grid Co., Ltd.(GZKJXM20222346).

0 引言

电力系统中负荷频率控制(load frequency control，LFC)作为稳定系统频率的核心调节机制，近年来面临双重挑战：一方面，来自高比例可再生能源接入带来的频率扰动频繁增强了调控难度；另一方面，电力系统信息化程度的提升引发新型网络安全威胁，虚假数据注入攻击(false data injection attack，FDIA)成为干扰状态感知与控制决策的关键风险因素[1-3]。应对FDIA潜在影响迫切要求构建面向动态物理过程的精确检测机制与多维抗干扰能力协同的控制策略。但现有研究在攻击检测精度、模型适应性以及防御机制集成方面仍存在重要不足[4-5]。

围绕FDIA的研究主要聚焦于3个策略路径，即数据层面的检测方法、攻击策略的建模与生成机制以及完整控制系统中的防御机制构建。首先，在虚假数据检测方面，研究主要集中于提升异常信号识别准确率与鲁棒性，应对电力数据的高维性、非线性与标签缺失等挑战。文献[6]提出将图卷积神经网络与重采样策略结合以增强异常电量识别能力。文献[7-8]中利用多标签机器学习与自监督聚类拓展了无监督检测场景下的攻击感知边界。文献[9-12]进一步引入扩散模型、谱图分析与图小波结构，有效提升了检测算法对网架结构与时序分布的敏感性与泛化能力。此外，文献[13-16]将卡尔曼滤波、图注意力机制、信息论指标引入检测流程，展现出通过状态动态关联性增强检测性能的重要趋势。

在检测机制持续演进的同时为深入理解攻击者策略与评估系统脆弱性，关于FDIA建模方法的研究日益聚焦于“高隐蔽性—低可观测性”两难环境下的攻击构造能力。文献[17-20]分别探讨在状态信息部分缺失条件下如何通过稀疏重构、稳健回归或张量因子分解设计可穿透估计模型的攻击向量。文献[21-22]通过引入张量状态估计结构与Kullback-Leibler散度等信息指标量化攻击可检测性，从理论与实用层面提出更具物理适应性的攻击生成策略。该系列方法虽然从攻击角度实现系统脆弱性映射，但尚未构建有效的防护整合机制，难以直接满足实际工程需求。

为突破检测与建模之间存在的机制割裂与响应滞后问题，近年来防御机制构建尝试将物理过程预测、状态估计与控制调整整合入一个闭环调控框架，以实现场景动态适应与攻击反馈响应协同。文献[23-25]分别基于混合自动机、概率预测与滤波融合策略面向配电与广域系统提出多尺度状态稳定机制。文献[26-27]通过引入生成对抗学习、信息物理融合等新型手段提高了异常状态判断的准确性并强化应急策略的收敛效果。这些成果显示未来抗攻击控制的发展趋势是检测与控制逻辑的深度耦合，从而实现对频率扰动与数据攻击的统一响应。

尽管已有研究取得了显著进展，但仍存在以下不足：1)检测方法依赖特定模型参数，难以适应复杂电网结构；2)检测与防御多为分离设计，实时性与精度难兼顾，限制实际应用效果；3)针对高渗透率可再生能源下的多类型攻击应对研究不足，缺乏统一有效的防御框架。本文提出基于状态空间分解的攻击检测与估计一体化抗攻击控制(attack-resilient control，ARC)机制，融合滑模观测器与H_∞控制策略。该方法通过状态空间坐标变换同步识别控制输入与测量攻击，利用滑模观测器估算攻击信号，提升检测鲁棒性；结合H_∞控制动态调整控制指令实现检测与防御的闭环协同优化。与现有方法相比，本方法优势包括：1)状态空间变换增强攻击识别能力，提升检测全面性；2)滑模观测与H_∞控制协同优化，实现检测与防御融合；3)在高比例可再生能源环境下表现出更强稳定性与抗扰能力。通过典型电力系统仿真算例验证了本文方法在攻击检测准确性与系统频率稳定性方面的显著优势。

1 可再生能源渗透下的电力系统FDIA建模

1.1 负荷频率控制系统模型

LFC系统通过调整发电机组输出功率维持系统频率稳定及区域间联络线功率交换在设定范围内。高比例可再生能源并网环境下，LFC必须应对更大的功率波动，否则可能导致频率失稳、机组脱网甚至大规模停电。

本文采用三阶LFC模型描述控制区域动态特性，其状态方程为：

$$\frac{\mathrm{d}\Delta f_i}{\mathrm{d}t}=\frac{1}{2H_i}\left(\Delta P_{\mathrm{g}_i}-D_i\Delta f_i-\Delta P_{\mathrm{tie}_i}-\Delta P_{\mathrm{L}_i}+\Delta P_{\mathrm{RES}_i}\right) \tag{1}$$

$$\frac{\mathrm{d}\Delta P_{g_i}}{\mathrm{d}t}=\frac{1}{T_{t_i}}(\Delta X_i-\Delta P_{g_i}) \tag{2}$$

$$\frac{\mathrm{d}\Delta X_i}{\mathrm{d}t}=\frac{1}{T_{g_i}}(\Delta P_{c_i}-\Delta X_i-\frac{\Delta f_i}{R_i}) \tag{3}$$

式中：H_i为系统惯性常数；D_i为阻尼系数；ΔP_{g_i}为机械出力偏差；ΔP_{L_i}为负荷扰动；ΔP_{RES_i}为可再生能源出力波动；ΔP_{tie_i}为联络线功率偏差；T_{t_i}和T_{g_i}分别为涡轮机和调速器时间常数；ΔX_i为阀门开度偏差；ΔP_{c_i}为控制指令；R_i为调频下垂系数；Δf_i为第i区域频率偏差；下标i表示第i个控制区域。

定义状态变量$\boldsymbol{x}_i=[\Delta f_i,\ \Delta P_{g_i},\ \Delta X_i]^{\mathrm{T}}$，控制输入$u_i=\Delta P_{c_i}$，扰动向量$\boldsymbol{d}_i=[\Delta P_{L_i},\ \Delta P_{RES_i},\ \Delta P_{tie_i}]^{\mathrm{T}}$，则系统状态空间表达为：

$$\frac{\mathrm{d}\boldsymbol{x}_i}{\mathrm{d}t}=\boldsymbol{A}_i\boldsymbol{x}_i+\boldsymbol{B}_iu_i+\boldsymbol{E}_i\boldsymbol{d}_i \tag{4}$$

$$y_i=\boldsymbol{C}_i\boldsymbol{x}_i \tag{5}$$

其中，系统矩阵为：

$$\boldsymbol{A}_i=\begin{bmatrix}-\dfrac{D_i}{2H_i} & \dfrac{1}{2H_i} & 0\\ 0 & -\dfrac{1}{T_{ti}} & \dfrac{1}{T_{ti}}\\ -\dfrac{1}{R_iT_{gi}} & 0 & -\dfrac{1}{T_{gi}}\end{bmatrix} \tag{6}$$

$$\boldsymbol{B}_i=\begin{bmatrix}0\\0\\\dfrac{1}{T_{gi}}\end{bmatrix} \tag{7}$$

$$\boldsymbol{E}_i=\begin{bmatrix}-\dfrac{1}{2H_i} & \dfrac{1}{2H_i} & -\dfrac{1}{2H_i}\\ 0 & 0 & 0\\ 0 & 0 & 0\end{bmatrix} \tag{8}$$

式中y_i为第i个控制区域的测量结果。测量矩阵$\boldsymbol{C}_i$根据实际监测需求设定，例如$\boldsymbol{C}_i=[1,\ 0,\ 0]$表示测量频率偏差，$\boldsymbol{C}_i=[0,\ 1,\ 0]$表示测量功率输出偏差。

1.2　可再生能源模型

1）风机模型

风机输出功率与风速的关系为：

$$P_{\mathrm{W}}=\frac{1}{2}\rho A_{\mathrm{W}}C_{\mathrm{P}}(\lambda,\beta)V_{\mathrm{W}}^3 \tag{9}$$

式中：P_{W}为输出功率；ρ为空气密度；A_{W}为扫掠面积；$C_{\mathrm{P}}(\lambda,\ \beta)$为功率系数；$\lambda$为叶尖速比；$\beta$为桨距角；$V_{\mathrm{W}}$为瞬时风速。风速波动可用Weibull分布描述。

$$f(V_{\mathrm{W}})=\frac{k}{c}\left(\frac{V_{\mathrm{W}}}{c}\right)^{k-1}\mathrm{e}^{-(V_{\mathrm{W}}/c)^k} \tag{10}$$

式中：$f(V_{\mathrm{W}})$为风速的概率密度函数；k和c分别为形状和尺度参数。在本文攻击检测模型中，风电功率波动被视为系统扰动源之一。

2）光伏模型

光伏输出功率计算公式为：

$$P_{\mathrm{PV}}=\eta A_{\mathrm{PV}}G_{\mathrm{T}}(1-\gamma(T-T_{\mathrm{ref}})) \tag{11}$$

式中：P_{PV}为输出功率；η为转换效率；A_{PV}为面板面积；G_{T}为辐照度；γ为温度系数；T和T_{ref}分别为环境温度和参考温度。辐照度通常服从如下Beta分布。

$$f_{\mathrm{G}}(G_{\mathrm{T}})=\frac{G_{\mathrm{T}}^{\alpha-1}(1-G_{\mathrm{T}})^{\beta-1}}{B(\alpha,\beta_1)} \tag{12}$$

式中：$f_{\mathrm{G}}(G_{\mathrm{T}})$为光伏辐照度$G_{\mathrm{T}}$的概率密度函数；$B(\alpha,\ \beta_1)$为Beta函数，$B(\alpha,\ \beta_1)=\int_0^1 t^{\alpha-1}(1-t)^{\beta_1-1}\mathrm{d}t$；$\alpha$和$\beta_1$为形状参数。本文将光伏功率波动作为系统扰动输入，研究其对FDIA检测的影响。

3）储能模型

储能系统可简化为一阶惯性环节如式(13)所示。

$$\frac{\mathrm{d}P_{\mathrm{ESS}}}{\mathrm{d}t}=-\frac{1}{T_{\mathrm{ESS}}}(P_{\mathrm{ESS}}-P_{\mathrm{ref}}) \tag{13}$$

式中：P_{ESS}为实际功率输出；T_{ESS}为时间常数；P_{ref}为参考功率。

将可再生能源与储能系统整合到LFC模型中，统一状态方程为：

$$\frac{\mathrm{d}\boldsymbol{x}}{\mathrm{d}t}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{B}u+\boldsymbol{E}d \tag{14}$$

式中：$\boldsymbol{x}$为总系统状态变量，包括频率偏差Δf、机械出力、储能状态等；u为控制输入变量；d为扰动输入变量，包括负荷扰动、可再生出力扰动与交互联络线扰动项；$\boldsymbol{A}$为系统动态矩阵；$\boldsymbol{B}$为控制输入矩阵；$\boldsymbol{E}$为扰动输入矩阵。

高比例可再生能源接入导致系统惯量减小，特征方程$det(\boldsymbol{A}-\lambda\boldsymbol{I})=0$的解更易接近虚轴，使系统频率响应更敏感，其中$\boldsymbol{I}$为单位矩阵。本文提出的基于状态空间分解的FDIA检测方法可有效识别在此类低惯量系统中的恶意攻击。

为了真实反映可再生能源高渗透率下电力系统动态特性，本文在建模时不仅引入了风电和光伏模

块，并且在总体系统功率扰动中新能源波动作为主导扰动源。不同于简单叠加噪声的方法，本文采用了基于物理特性的Weibull风速建模与Beta辐照度建模，使新能源功率随机变化过程在状态空间动态中占据主导地位，直接影响频率偏移和特征方程根轨迹位置，从而体现出新能源高渗透率对系统频率响应灵敏性提升的作用。

1.3 虚假数据注入攻击模型

1）FDIA基本原理

电力系统状态估计的测量方程为：

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{x} + v \tag{15}$$

式中：$\boldsymbol{z}$为测量向量；$\boldsymbol{H}$为测量矩阵；v为测量噪声。FDIA攻击者构造攻击向量$\boldsymbol{a}$，使被篡改的测量满足式(16)。

$$\boldsymbol{z}' = \boldsymbol{z} + \boldsymbol{a} = \boldsymbol{H}(\boldsymbol{x} + \delta) + v = \boldsymbol{H}\boldsymbol{x}' + v \tag{16}$$

式中：$\boldsymbol{z}'$为攻击后的伪造测量向量；δ为状态偏移量，由攻击者自行设定；$\boldsymbol{x}' = x + \delta$为伪造的系统状态向量。这种攻击可绕过基于残差的检测方法，因为篡改后的测量仍符合系统模型。

FDIA在实际电力系统中可通过多条途径实现，包括前端采集设备渗透、通信链路劫持、主控中心系统感染以及数据共享平台投毒等手段。1)在前端设备层面，攻击者可通过物理接入或远程入侵RTU、PMU等数据采集设备直接篡改频率、潮流等关键原始量测数据，污染数据源。2)在通信链路层，攻击者通过劫持调度数据网络中的中继交换节点或链路加密隧道实行中间人攻击，实时篡改数据报文，隐蔽插入伪造数据。3)在调度主控中心，攻击者通过系统漏洞利用、后门植入等方式感染EMS主站平台或其数据库，批量修改测量数据及调控指令，直接干扰LFC。4)攻击者可通过渗透数据同步与协调平台，伪造新能源功率预测、负荷预测等输入，间接影响区域协同控制与调度决策过程。上述多路径、多层级的攻击机制交互作用，使FDIA能够系统性、隐蔽性地影响电力系统运行状态，增加检测难度和防护挑战。

2）LFC系统中的FDIA类型

针对LFC系统的FDIA主要有3种类型。

(1)量量篡改：通过篡改频率偏差Δf_i和联络线功率$\Delta P_{\mathrm{tie}_i}$的测量值导致控制中心计算错误的调节指令$\Delta P_{\mathrm{c}_i}$，使发电机出力偏离实际需求。

(2)控制量篡改：直接修改发送给调速器的控制指令ΔP_{c_i}，引入偏差$\boldsymbol{a}_{\mathrm{c}}(t)$，可能导致频率持续振荡或超出安全范围。

(3)联络线功率篡改：在多区域系统中，篡改联络线功率数据可引发区域间功率不平衡，特别是在HVDC系统中，这类攻击可快速改变区域功率平衡，导致频率急剧波动。

3）FDIA对系统动态特性的影响

FDIA作用于LFC系统后，修正的状态方程可表示为：

$$\frac{\mathrm{d}\boldsymbol{x}'}{\mathrm{d}t} = \boldsymbol{A}\boldsymbol{x}' + \boldsymbol{B}[u + \boldsymbol{a}_{\mathrm{c}}(t)] + \boldsymbol{E}d \tag{17}$$

式中$\boldsymbol{a}_{\mathrm{c}}$为偏差，即攻击向量。攻击也可等效为系统参数变化，引入修正矩阵$\boldsymbol{A}_{\mathrm{a}}$后，系统特征方程变为：

$$det(\boldsymbol{A} + \boldsymbol{A}_{\mathrm{a}} - \lambda\boldsymbol{I}) = 0 \tag{18}$$

当攻击使特征值实部变为正值时，系统将失稳。本文提出的基于状态空间分解的方法，通过分离攻击影响与正常系统动态有效检测隐蔽性FDIA，防止系统因攻击导致的频率失稳。

2 基于状态空间分解的攻击检测与估计方法

2.1 网络攻击状态空间分解方法

在LFC系统中，状态变量通常包括频率偏差、联络线功率偏差及发电控制状态。当系统遭受FDIA时，传统状态估计方法难以区分系统正常动态与攻击信号的影响，主要原因在于攻击信号与系统状态在同一空间耦合。本文提出的状态空间分解方法通过坐标变换将攻击信号解耦为控制输入攻击和测量攻击两个独立部分，使攻击信号在变换后的坐标系中具有明确的结构特征，从而提高检测精度。这种解耦机制的理论优势在于：1)降低了攻击识别问题的复杂度，将多维耦合问题转化为两个低维子问题；2)消除了不同类型攻击间的相互干扰，避免了传统方法中的虚假检测和漏检；3)为针对性设计观测器提供了理论基础，实现了攻击信号的精确估计。

考虑受攻击的电力系统动态模型，其状态空间表示为：

$$\frac{\mathrm{d}\boldsymbol{x}}{\mathrm{d}t} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{B}\boldsymbol{u} + \boldsymbol{E}\boldsymbol{d} + \boldsymbol{F}\phi(\boldsymbol{x}, t) + \boldsymbol{B}\boldsymbol{a}_{\mathrm{c}}(t) \tag{19}$$

$$\boldsymbol{y} = \boldsymbol{C}\boldsymbol{x} + \boldsymbol{D}\boldsymbol{a}_{\mathrm{m}}(t) \tag{20}$$

式中：$\boldsymbol{x} \in \mathbb{R}^n$ 为系统状态向量；$\boldsymbol{u} \in \mathbb{R}^m$ 为控制输入；$\boldsymbol{y} \in \mathbb{R}^p$ 为测量输出；$\boldsymbol{d} \in \mathbb{R}^q$ 为外部扰动；$\boldsymbol{a}_{\mathrm{c}}(t) \in \mathbb{R}^m$ 和 $\boldsymbol{a}_{\mathrm{m}}(t) \in \mathbb{R}^p$ 分别为作用于控制输入端和测量端的攻击信号；$\phi(\boldsymbol{x},\ t)$ 为系统非线性动态；n、m、p、q 分别为状态、控制输入、测量输出和扰动的维度。这种模型可有效表征 FDIA 对系统的双重影响路径。

本文提出的状态空间分解方法核心在于构造适当的变换矩阵，将攻击信号解耦。定义状态变换矩阵 $\boldsymbol{T} \in \mathbb{R}^{n \times n}$ 和输出变换矩阵 $\boldsymbol{S} \in \mathbb{R}^{p \times p}$，引入新的状态变量和测量输出：

$$\boldsymbol{\zeta} = \boldsymbol{T}\boldsymbol{x} \tag{21}$$

$$\boldsymbol{\omega} = \boldsymbol{S}\boldsymbol{y} \tag{22}$$

式中：$\boldsymbol{\zeta}$ 为变换后的状态变量，包含两部分 $\boldsymbol{\zeta}_1 \in \mathbb{R}^{n_1}$、$\boldsymbol{\zeta}_2 \in \mathbb{R}^{n_2}$，$\boldsymbol{\zeta} = [\boldsymbol{\zeta}_1^{\mathrm{T}}\ \ \boldsymbol{\zeta}_2^{\mathrm{T}}]^{\mathrm{T}}$，$n_1 + n_2 = n$；$\boldsymbol{T}$ 为状态空间解耦变换矩阵；$\boldsymbol{y}$ 为系统测量结果；$\boldsymbol{\omega}$ 为变换后的测量输出，类似地分为 $\boldsymbol{\omega}_1$、$\boldsymbol{\omega}_2$；$\boldsymbol{S}$ 为输出空间解耦矩阵。

将原始系统方程变换至新坐标系：

$$\frac{\mathrm{d}\boldsymbol{\zeta}}{\mathrm{d}t} = \boldsymbol{T}\boldsymbol{A}\boldsymbol{T}^{-1}\boldsymbol{\zeta} + \boldsymbol{T}\boldsymbol{B}\boldsymbol{u} + \boldsymbol{T}\boldsymbol{B}\boldsymbol{a}_{\mathrm{c}}(t) + \boldsymbol{T}\boldsymbol{E}\boldsymbol{d} + \boldsymbol{T}\boldsymbol{F}\phi(\boldsymbol{T}^{-1}\boldsymbol{\zeta}, t) \tag{23}$$

$$\boldsymbol{\omega} = \boldsymbol{S}\boldsymbol{C}\boldsymbol{T}^{-1}\boldsymbol{\zeta} + \boldsymbol{S}\boldsymbol{D}\boldsymbol{a}_{\mathrm{m}}(t) \tag{24}$$

关键在于选择合适的变换矩阵 $\boldsymbol{T}$ 和 $\boldsymbol{S}$，使系统矩阵具有特定的分块结构：

$$\boldsymbol{T}\boldsymbol{A}\boldsymbol{T}^{-1} = \begin{bmatrix} \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{A}_3 & \boldsymbol{A}_4 \end{bmatrix} \tag{25}$$

$$\boldsymbol{T}\boldsymbol{B} = \begin{bmatrix} \boldsymbol{B}_1 \\ 0 \end{bmatrix} \tag{26}$$

$$\boldsymbol{S}\boldsymbol{C}\boldsymbol{T}^{-1} = \begin{bmatrix} \boldsymbol{C}_1 & 0 \\ 0 & \boldsymbol{C}_4 \end{bmatrix} \tag{27}$$

式中：$\boldsymbol{A}_1$ 为模块Ⅰ的状态转移矩阵，描述不含攻击时 $\boldsymbol{\zeta}_1$ 的本地动态；$\boldsymbol{A}_2$ 为模块Ⅰ受模块Ⅱ状态 $\boldsymbol{\zeta}_2$ 影响的耦合项；$\boldsymbol{A}_3$ 为模块Ⅱ受模块Ⅰ状态 $\boldsymbol{\zeta}_1$ 影响的耦合项；$\boldsymbol{A}_4$ 为模块Ⅱ的独立动态部分；$\boldsymbol{B}_1$ 为模块Ⅰ中控制输入的传递矩阵；$\boldsymbol{C}_1$ 为观测模块Ⅰ状态 $\boldsymbol{\zeta}_1$ 的输出变量 $\boldsymbol{\omega}_1$ 对应的观测矩阵；$\boldsymbol{C}_4$ 为观测模块Ⅱ状态 $\boldsymbol{\zeta}_2$ 的测量输出部分。该分块结构确保控制攻击 $\boldsymbol{a}_{\mathrm{c}}(t)$ 与测量攻击 $\boldsymbol{a}_{\mathrm{m}}(t)$ 在两个子系统中分别作用于不同维度，从而实现结构性解耦。

基于上述变换结构，系统可分解为以下两个功能明确的子模块。

1）模块Ⅰ：主要受控制输入攻击 $\boldsymbol{a}_{\mathrm{c}}(t)$ 影响的子系统

$$\frac{\mathrm{d}\boldsymbol{\zeta}_1}{\mathrm{d}t} = \boldsymbol{A}_1\boldsymbol{\zeta}_1 + \boldsymbol{A}_2\boldsymbol{\zeta}_2 + \boldsymbol{B}_1\boldsymbol{u} + \boldsymbol{a}_{\mathrm{c}}(t) + \mathcal{E}_1\boldsymbol{d} + \boldsymbol{F}_1\phi(\boldsymbol{T}^{-1}\boldsymbol{\zeta}, t) \tag{28}$$

$$\boldsymbol{\omega}_1 = \boldsymbol{C}_1\boldsymbol{\zeta}_1 \tag{29}$$

2）模块Ⅱ：主要受测量攻击 $\boldsymbol{a}_{\mathrm{m}}(t)$ 影响的子系统

$$\frac{\mathrm{d}\boldsymbol{\zeta}_2}{\mathrm{d}t} = \boldsymbol{A}_3\boldsymbol{\zeta}_1 + \boldsymbol{A}_4\boldsymbol{\zeta}_2 + \mathcal{E}_2\boldsymbol{d} + \boldsymbol{F}_2\phi(\boldsymbol{T}^{-1}\boldsymbol{\zeta}, t) \tag{30}$$

$$\boldsymbol{\omega}_2 = \boldsymbol{C}_4\boldsymbol{\zeta}_2 + \boldsymbol{D}_2\boldsymbol{a}_{\mathrm{m}}(t) \tag{31}$$

式中 $\boldsymbol{\varepsilon}_1$、$\boldsymbol{\varepsilon}_2$、$\boldsymbol{F}_1$、$\boldsymbol{F}_2$ 和 $\boldsymbol{D}_2$ 为对应的分块矩阵。

这种结构化分解的关键优势在于：1)控制输入攻击 $\boldsymbol{a}_{\mathrm{c}}(t)$ 仅直接影响模块Ⅰ的动态，且可通过 $\boldsymbol{\omega}_1$ 观测；2)测量攻击 $\boldsymbol{a}_{\mathrm{m}}(t)$ 仅直接影响模块Ⅱ的输出方程。这种解耦特性使得攻击检测问题转化为两个更简单的子问题，显著降低了检测算法的复杂度，提高了攻击识别的准确性和鲁棒性。

2.2　基于分解空间的滑模观测器设计

基于状态空间分解结构，本文设计了针对性的滑模观测器以实现对不同类型攻击的精确估计。

针对模块Ⅰ的滑模观测器：假设 $\boldsymbol{\zeta}_2$ 可通过其他方法估计获得，为观测控制输入攻击 $\boldsymbol{a}_{\mathrm{c}}(t)$，设计式(32)所示观测器。

$$\frac{\mathrm{d}\hat{\boldsymbol{\zeta}}_1}{\mathrm{d}t} = \boldsymbol{A}_1\hat{\boldsymbol{\zeta}}_1 + \boldsymbol{A}_2\overline{\boldsymbol{\zeta}}_2 + \boldsymbol{B}_1 u + \boldsymbol{K}_1[\boldsymbol{\omega}_1 - \boldsymbol{C}_1\hat{\boldsymbol{\zeta}}_1] + v_1(t) \tag{32}$$

式中：$\hat{\boldsymbol{\zeta}}_1$ 为状态估计值；$\overline{\boldsymbol{\zeta}}_2$ 为 $\boldsymbol{\zeta}_2$ 的估计值；$\boldsymbol{K}_1$ 为反馈增益矩阵；$v_1(t)$ 为滑模补偿项。定义观测误差 $\boldsymbol{e}_1 = \boldsymbol{\zeta}_1 - \hat{\boldsymbol{\zeta}}_1$，其动态方程为：

$$\frac{\mathrm{d}\boldsymbol{e}_1}{\mathrm{d}t} = [\boldsymbol{A}_1 - \boldsymbol{K}_1\boldsymbol{C}_1]\boldsymbol{e}_1 + \boldsymbol{B}_1\boldsymbol{a}_{\mathrm{c}}(t) + \rho_1(t) - v_1(t) \tag{33}$$

式中 $\rho_1(t)$ 为扰动和非线性项的综合影响。为实现有限时间收敛定义滑模面如式(34)所示。

$$s_1 = \boldsymbol{C}_1\boldsymbol{e}_1 \tag{34}$$

采用滑模控制律如式(35)所示。

$$v_1(t) = -\boldsymbol{K}_{\mathrm{s}}\mathrm{sign}(s_1) \tag{35}$$

式中 $\boldsymbol{K}_{\mathrm{s}} \in \mathbb{R}^{r \times r}$ 为滑模增益矩阵，其选取决定了滑模面的趋近速率和抗扰性能。较大的 $\boldsymbol{K}_{\mathrm{s}}$ 可增强观测误差对攻击突变的响应能力，但可能放大高频噪声。

当系统进入滑模运动后，可通过等效控制方法估计攻击信号，如式(36)所示。

$$\hat{\boldsymbol{a}}_{\mathrm{c}}(t)=\frac{1}{B_1}v_{1,\mathrm{eq}}(t)\approx-\frac{1}{B_1\boldsymbol{K}_{\mathrm{s}}}v_1(t) \tag{36}$$

式中：$\hat{\boldsymbol{a}}_{\mathrm{c}}(t)$为控制通道攻击$\boldsymbol{a}_{\mathrm{c}}(t)$的估计值；$v_{1,\mathrm{eq}}(t)$为等效控制输入，是滑模补偿项$v_1(t)$的低通滤波处理结果，用于提取攻击真实能量分量。

针对模块Ⅱ的滑模观测器：为检测测量攻击$\boldsymbol{a}_{\mathrm{m}}(t)$，设计如式(37)所示观测器。

$$\begin{aligned}\frac{\mathrm{d}\hat{\boldsymbol{\zeta}}_2}{\mathrm{d}t}=&\boldsymbol{A}_4\hat{\boldsymbol{\zeta}}_2+\boldsymbol{A}_3\bar{\boldsymbol{\zeta}}_1+\boldsymbol{L}_2[\omega_2-\\&\boldsymbol{C}_4\hat{\boldsymbol{\zeta}}_2]-\boldsymbol{D}_2\hat{\boldsymbol{a}}_{\mathrm{m}}(t)]+v_2(t)\end{aligned} \tag{37}$$

式中：$\hat{\boldsymbol{\zeta}}_2$为状态估计值；$\bar{\boldsymbol{\zeta}}_1$为$\boldsymbol{\zeta}_1$的估计值；$\boldsymbol{L}_2$为反馈增益矩阵；$v_2(t)$为滑模补偿项；$\hat{\boldsymbol{a}}_{\mathrm{m}}(t)$为测量击估计量。定义观测误差$\boldsymbol{e}_2=\boldsymbol{\zeta}_2-\hat{\boldsymbol{\zeta}}_2$，其动态方程为：

$$\begin{aligned}\frac{\mathrm{d}\boldsymbol{e}_2}{\mathrm{d}t}=&\left[\boldsymbol{A}_4-\boldsymbol{L}_2\boldsymbol{C}_4\right]e_2+\boldsymbol{L}_2\boldsymbol{D}_2\boldsymbol{a}_{\mathrm{m}}(t)+\\&\rho_2(t)-v_2(t)\end{aligned} \tag{38}$$

式中$\rho_2(t)$为扰动和非线性项的综合影响。定义滑模面如式(39)所示。

$$s_2=\boldsymbol{C}_4\boldsymbol{e}_2 \tag{39}$$

采用滑模控制律：

$$v_2(t)=-\boldsymbol{K}_{\mathrm{m}}sign(s_2) \tag{40}$$

式中：$\boldsymbol{K}_{\mathrm{m}}\in\mathbb{R}^{r\times r}$为滑模增益矩阵，决定测量观测误差在滑模面上的趋近速度，其大小结合系统噪声特性与扰动干扰水平，通过线性矩阵不等式方法优化获得，以保证观测误差系统渐近稳定；$sign(\cdot)$为符号函数。

当$(\boldsymbol{A}_4-\boldsymbol{L}_2\boldsymbol{C}_4)$为Hurwitz矩阵且$\boldsymbol{K}_{\mathrm{m}}$取值适当时，系统进入滑模运动后可估计测量攻击信号。

$$\hat{\boldsymbol{a}}_{\mathrm{m}}(t)=\frac{1}{\boldsymbol{L}_2\boldsymbol{D}_2}v_{2,\mathrm{eq}}(t)\approx-\frac{1}{\boldsymbol{L}_2\boldsymbol{D}_2\boldsymbol{K}_{\mathrm{m}}}v_2(t) \tag{41}$$

式中$v_{2,\mathrm{eq}}(t)$为滑模补偿项的等效控制信号，可通过对$v_2(t)$进行低通滤波获得其缓变趋势分量。

观测器参数优化：增益矩阵$\boldsymbol{K}_1$、$\boldsymbol{L}_2$和滑模增益$\boldsymbol{K}_{\mathrm{s}}$、$\boldsymbol{K}_{\mathrm{m}}$可通过求解如下线性矩阵不等式优化。

$$\begin{cases}\boldsymbol{P}_1(\boldsymbol{A}_4-\boldsymbol{K}_1\boldsymbol{C}_1)+(\boldsymbol{A}_4-\boldsymbol{K}_1\boldsymbol{C}_1)^{\mathrm{T}}\boldsymbol{P}_1<-\alpha_1\boldsymbol{I}\\\boldsymbol{P}_2(\boldsymbol{A}_4-\boldsymbol{L}_2\boldsymbol{C}_4)+(\boldsymbol{A}_4-\boldsymbol{L}_2\boldsymbol{C}_4)^{\mathrm{T}}\boldsymbol{P}_2<-\alpha_2\boldsymbol{I}\end{cases} \tag{42}$$

式中：α_1、α_2为正常数，决定收敛速率；$\boldsymbol{P}_1$、$\boldsymbol{P}_2$为对称正定矩阵；$\boldsymbol{I}$为单位矩阵。此优化保证了观测器的稳定性和鲁棒性，同时提高了攻击检测的精度。

3 基于H_∞控制的抗攻击方法

本文提出的防御框架分为两个协同阶段：攻击检测与抗攻击控制。第2节通过状态空间分解实现了控制输入攻击和测量攻击的独立识别，并利用滑模观测器估计攻击信号。本节在此基础上设计H_∞控制器，构建完整的ARC机制，实现电力系统在FDIA环境下的鲁棒运行。

3.1 滑模观测器与H_∞控制协同机制

滑模观测器与H_∞控制协同工作的优势在于滑模观测器能快速精确地估计攻击信号，而H_∞控制器则利用这些信息设计最优控制策略，共同形成“检测-响应”闭环防御系统。两者协同的理论基础是将观测器提供的攻击估计值$\hat{\boldsymbol{a}}_{\mathrm{c}}(t)$和$\hat{\boldsymbol{a}}_{\mathrm{m}}(t)$融入$H_\infty$控制框架，使控制器能针对实时攻击特征调整控制策略。

H_∞控制设计的核心是最小化以下性能指标。

$$J=\int_0^\infty(\boldsymbol{Z}(\boldsymbol{x},\boldsymbol{u})^{\mathrm{T}}\boldsymbol{Z}(\boldsymbol{x},\boldsymbol{u})\gamma^2\boldsymbol{a}^{\mathrm{T}}\boldsymbol{a})\mathrm{d}t \tag{43}$$

式中：J为控制性能指标函数，评价系统在攻击干扰下的整体性能；$\boldsymbol{Z}(\boldsymbol{x},\boldsymbol{u})$为势能输出变量，通常为系统需限制的性能输出(例如频率偏差、电压偏差等状态线性组合)；$\boldsymbol{a}$为统一表示包括$\boldsymbol{a}_{\mathrm{c}}(t)$、$\boldsymbol{a}_{\mathrm{m}}(t)$在内的攻击信号组合向量；$\gamma>0$为攻击抑制水平，表征系统对攻击的容忍度。该性能指标确保闭环系统满足：

$$\|\boldsymbol{z}\|_2^2<\gamma^2\|\boldsymbol{a}\|_2^2 \tag{44}$$

3.2 最优控制器设计与参数选取

为实现最优控制性能，本文通过求解以下代数Riccati方程设计H_∞控制器：

$$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{P}+\boldsymbol{P}\boldsymbol{A}+\boldsymbol{Q}-\boldsymbol{P}(\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}-\gamma^{-2}\boldsymbol{F}_{\mathrm{a}}\boldsymbol{F}_{\mathrm{a}}^{\mathrm{T}})\boldsymbol{P}=0 \tag{45}$$

式中：$\boldsymbol{Q}\in\mathbb{R}^{n\times n}$为权重矩阵，正定，对系统状态偏离的惩罚；$\boldsymbol{R}\in\mathbb{R}^{m\times m}$为控制输入权重矩阵，正定；$\boldsymbol{P}\in\mathbb{R}^{n\times n}$是代数Riccati方程的唯一对称正定解矩阵；$\boldsymbol{F}_{\mathrm{a}}$为攻击入口矩阵，映射攻击信号$a(t)$对状态的影响。

当该方程存在正定解$\boldsymbol{P}>0$时，最优控制律为：

$$u=-\boldsymbol{K}_{\mathrm{c}}x=-\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}Px \tag{46}$$

式中$\boldsymbol{K}_{\mathrm{c}}=\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}P$为$H_\infty$控制器的状态反馈增益矩阵，其结构来源于代数Riccati方程式(45)的最优解

$P>0$。该反馈增益确保系统在最小化性能指标 J 的同时，抑制攻击信号对状态的影响，实现闭环系统的稳定与鲁棒控制。通过调整权重矩阵 $\boldsymbol{Q}$ 与 $\boldsymbol{R}$，可灵活改变 $\boldsymbol{K}_c$ 的数值，从而实现在频率、功率偏差和能量储备等状态指标间的性能权衡。

控制器参数选取依据以下原则。

1）权重矩阵 $\boldsymbol{Q}$ 和 $\boldsymbol{R}$ 基于系统状态和控制输入的相对重要性确定，通常选择 $\boldsymbol{Q}=\mathrm{diag}(q_1, q_2, \cdots, q_n)$ 和 $\boldsymbol{R}=\mathrm{diag}(r_1, r_2, \cdots, r_m)$，其中 $q_i>0$ 和 $r_j>0$。q_i 为系统中第 i 个状态变量对应的权重，r_j 为控制输入中第 j 个控制通道的权重，m 为控制通道数量。

q_i 通常根据各状态变量对系统安全和性能的影响程度进行设定。若需优先抑制频率偏差和联络线功率偏差，可对对应的 q_i 赋予较高权重，以提高该状态的调节能力；而对机械功率或储能状态的波动容忍度相对较高，权重可适当降低。控制输入权重 r_j 用于限制控制作用幅度，防止过激响应。在多源输入系统中，若某类资源成本较高或调节能力有限，应设定较大的 r_j 抑制其控制占比；而对响应快速、代价较低的传统电源控制输入，可设定较小的 r_j。

2）攻击抑制水平 γ 选择需平衡控制性能与鲁棒性，较小的 γ 值提供更强的攻击抑制能力，但可能导致控制增益过大。

3）滑模观测器参数 $\boldsymbol{K}_s$ 和 $\boldsymbol{K}_m$ 选择需确保快速收敛且抑制抖振，典型值为系统最大预期攻击幅值的 1.2~1.5 倍。

本文提出的协同防御机制具有两个关键优势：1）即使在持续性 FDIA 下系统性能仍保持在可控范围内；2）控制器能根据实时估计的攻击特性自适应调整，适应不同类型和强度的攻击场景。

4　算例分析与实验验证

4.1　攻击场景设置

针对本文所提出的 FDIA 检测方法进行仿真测试，验证其有效性和适用性。实验环境基于 MATLAB/Simulink R2022b 进行搭建，硬件平台采用 Intel Core i7−12700K CPU、32 GB RAM。构建的场景如图 1 所示，针对两种不同规模系统拓扑构建了 3 种场景。图中以蓝色实线表示普通交流联络线，以橙色实线表示带可控相移变压器的交流联络线，以绿色实线表示高压直流联络线。

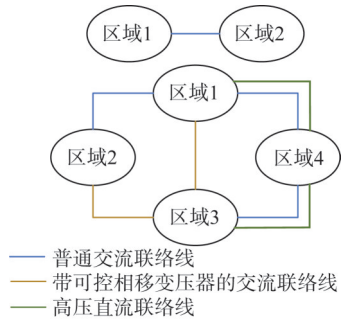
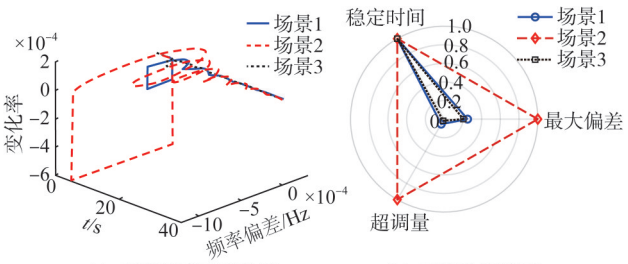


图 1　多区域电力系统拓扑

Fig. 1　Multiregion power system topology

场景 1 使用双区域结构，两区域之间由单条普通交流联络线连接，在 t=5 s 时刻，针对区域 1 施加 1 % p. u. 阶跃负荷扰动，并考虑可再生能源引起的功率波动。由于联络线单一，系统的干扰冗余较低，对于负荷扰动及 FDIA 的抵抗能力相对较弱。场景 2 和场景 3 将系统扩展为四区域结构，并通过多条不同类型的联络线相互连接，更具备复杂电力系统的典型特征。在场景 2 中，t=5 s 时刻，针对区域 1 施加 5 % p. u. 阶跃负荷扰动，同时考虑可再生能源变化影响。在场景 3 中，仅考虑可再生能源变化对系统的影响，不施加额外负荷扰动。



(a) 系统频率响应轨迹　　(b) 系统关键特征

图 2　系统动态响应特性

Fig. 2　System dynamic response characteristics

3 个场景下的动态响应特性如图 2 所示，其中图 2(a)为频率响应轨迹，展现了频率偏差、变化率与时间三者之间的关系。场景 2 的轨迹振荡幅度最大，表明负荷阶跃与新能源波动共同作用时系统瞬态响应最为显著。场景 1 的轨迹振荡幅度最小，围绕原点小幅摆动，说明仅有可再生能源波动时系统的频率响应较平稳。图 2(b)分别从最大偏差、稳定时间和超调量 3 个维度表征 3 个场景的系统特征，场景 2 在最大偏差和超调量等指标上数值最高，表

明5 % p. u. 阶跃负荷扰动对系统稳定性影响极为显著。场景3的指标最小，表明仅有可再生能源变化时对系统整体扰动相对较弱。

4.2 攻击检测方法性能分析

为了测试所提出的FDIA检测与估计方法的有效性，本文构造了4种攻击向量，特征空间如图3(a)所示，能量分布情况如图3(b)所示。

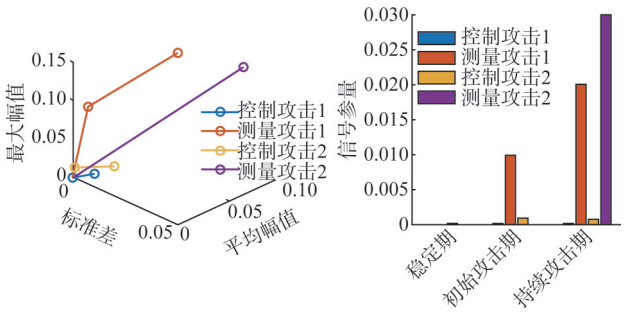


图3 攻击向量特征与能量分布

Fig. 3 Attack vector characteristics and energy distribution

1)控制攻击1：该攻击向量针对控制信号进行攻击，攻击向量的标准差较小，平均幅值处于中等水平，最大幅值较高，其在攻击初始阶段主要呈现周期性正弦特征，但在特定时刻会出现较大的瞬时峰值。

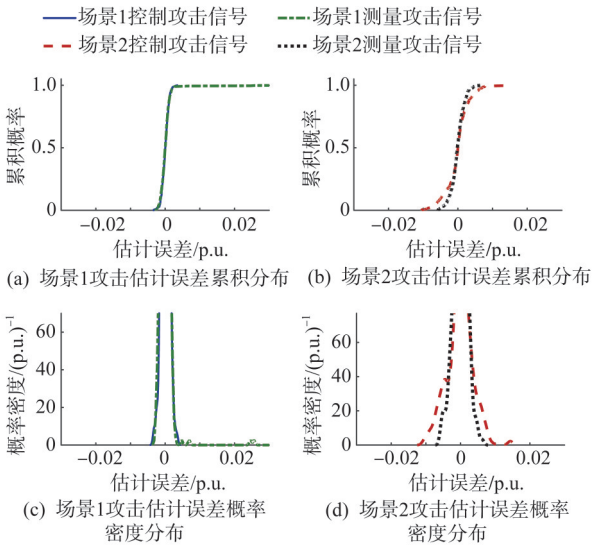
2)测量攻击1：该攻击向量针对量测信号进行攻击，其分布整体较为集中，表明在攻击触发后，幅值围绕某一稳态水平波动。

3)控制攻击2：该攻击向量针对控制信号进行攻击，其标准差和最大幅值较大，具有较强的随机脉冲或噪声特性。

4)测量攻击2：该攻击向量针对量测信号进行攻击，具有线性累积的攻击趋势，影响随着时间的增加而增强。

4种攻击均可分为3个阶段，在稳定期(0~20 s)，所有攻击信号的能量均接近于0，在该阶段系统处于正常状态。初始攻击期(20~40 s)，控制攻击1和控制攻击2的能量值开始显著上升，而测量攻击1和测量攻击2的能量增长相对较缓。持续攻击期(40~60 s)，测量攻击1的能量迅速上升并趋于稳定，测量攻击2的能量为线性渐进式增长，控制攻击2的能量快速波动产生不稳定的动态变化。

针对以上4种攻击向量进行检测和估计，为了量化分析准确性，本文从累积分布函数(cumulative distribution function，CDF)与概率密度函数(probability density function，PDF)两个角度对估计误差的统计特性进行分析。场景1—2在控制攻击信号与测量攻击信号下的估计偏差情况如图4所示，其中图4(a)—(b)表示场景1—2下的攻击估计误差累积分布，图4(c)—(d)为场景1—2的攻击估计误差概率密度分布。



(a) 场景1攻击估计误差累积分布 (b) 场景2攻击估计误差累积分布

(c) 场景1攻击估计误差概率密度分布 (d) 场景2攻击估计误差概率密度分布

图4 攻击估计误差统计特性分析图

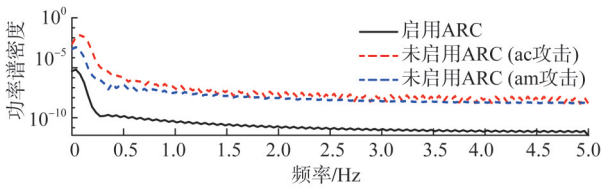
Fig. 4 Analysis diagram of statistical characteristics of errors in attack estimation

攻击估计误差的累积分布分析显示误差曲线在0值附近呈现显著的陡增特性，证明估计误差主要集中于较小的数值区间内。观察场景1数据，控制攻击信号累积分布曲线较测量攻击信号更为陡峭，说明前者具有更高的估计精度；场景2中两种信号的累积分布特性则相对接近。与传统Kalman滤波技术相比，本文提出的估计方法将降低约30 %。场景1中控制攻击信号在±0. 01 p. u. 范围内的累积概率高达95 %，场景2中控制攻击信号在±0. 015 p. u. 范围内的累积概率超过90 %，这些结果有力证实了所提方法在复杂环境中的鲁棒性能。

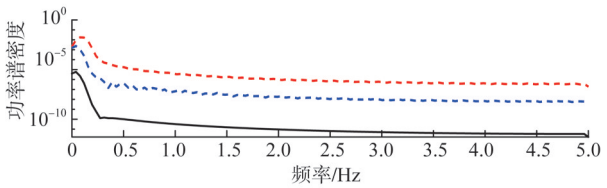
误差的概率密度整体呈现近似正态分布，在峰值附近表现出高度集中性。图4(c)—(d)可以看出控制攻击信号的误差分布相对窄小且集中，其峰值明显高于测量攻击信号，表明其估计波动较小且精度较高。测量攻击信号的分布曲线相对宽广，场景1中概率密度分布显著低于控制攻击信号，说明其估计精度受攻击影响较大。场景2中两种攻击信号

的概率密度分布差异虽有减小，但控制攻击信号的分布仍然表现出更高的集中度。这些分析结果证实了本文方法能够在不同类型攻击信号下保持估计均值接近0，同时维持集中的误差分布和较小的标准差，从而实现高精度的一致性估计效果。

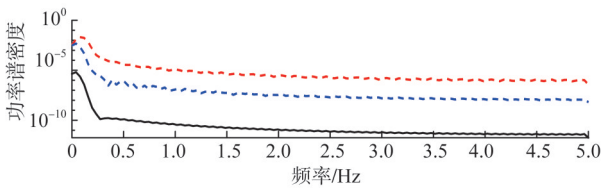
为了分析ARC机制对系统稳定性的影响，同时给出了“启用ARC”、“未启用ARC(控制攻击)”、“未启用ARC(测量攻击)”3种情况下场景1、场景2和场景3的功率谱密度，如图5所示。



(a) 场景1频率响应能量分布特性



(b) 场景2频率响应能量分布特性



(c) 场景3频率响应能量分布特性

图5　电力系统频率响应能量分布特性

Fig. 5　Frequency response energy distribution characteristics of power system

启用ARC的系统表现出较为理想的频谱特性。能量主要分布在0.1~0.3 Hz区间，且幅值维持在10^{-5}量级，表明系统的主要动态响应受到抑制，强化了低频稳定性。此外，低频分量较少，使系统难以产生大幅度的稳态偏差。同时，高频段(>0.5 Hz)的能量明显被抑制，提升了系统的振荡抑制能力和整体动态稳定性。

在未启用ARC且存在控制攻击的情况下系统频谱特性发生显著变化。0.4~0.6 Hz区间出现约10^{-2}量级的能量峰值，这一峰值反映了攻击引入的附加控制信号所造成的高频振荡，可能导致机组与负荷侧的耦合振荡。相较之下，测量攻击对该频率范围的影响相对较弱，但仍可能在中频段引发扰动，使系统面临稳定性下降的风险。

在未启用ARC且存在测量攻击的情况下低频段(<0.1 Hz)的能量持续累积，表明系统长时间偏离平衡点，存在稳态偏差的风险。尽管未出现明显的高频峰值，测量攻击对系统的影响更具持久性，特别是在场景3下测量攻击可能引发渐进式偏差，使得系统频率稳定性进一步下降。如果缺乏额外的控制策略，这种偏差将不断放大，最终影响系统的长期运行可靠性。

综合对比不同工况可见，ARC机制在抑制高频振荡的同时，显著降低了稳态偏差。在所有测试场景中，启用ARC后系统的功率谱密度整体下降1~2个数量级，且能量分布更加集中，体现出较强的频率扰动抑制能力。由此可见，ARC机制有效提升了系统在面对FDIA时的稳定性。

为了进一步验证所提出FDIA检测方法的响应速度和实时性能，本文对不同类型攻击的检测响应延迟进行了统计分析，结果如图6所示。控制攻击1的中位响应延迟约为0.20 s，控制攻击2中位延迟约为0.16 s，测量攻击1的中位延迟约为0.18 s，而测量攻击2的中位延迟为0.15 s。各类攻击下的响应延迟波动范围控制较小，绝大部分样本集中在[0.10，0.25] s范围内，离群点极少，表明检测系统具有良好的稳定性，可满足针对FDIA的实时检测需求。

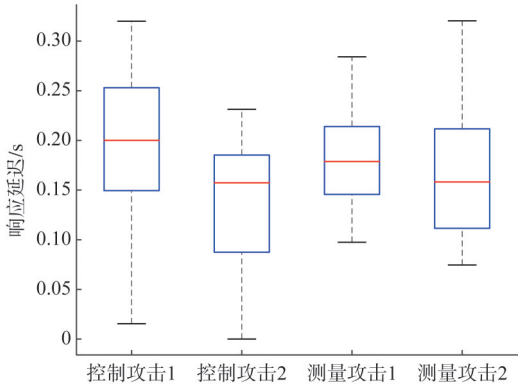


图6　攻击检测延迟统计结果

Fig. 6　Statistical results of attack detection delay

为了系统验证本文所提方法在攻击检测与估计方面的优越性能，本文选取了4种具有代表性的现有方法进行对比分析，分别为标准卡尔曼滤波(Kalman filter，KF)[28]、扩展卡尔曼滤波(extended Kalman filter，EKF)[29]、扩展状态观测器

(extended state observer，ESO)[30]和两阶段去噪扩散模型(two-stage denoising diffusion model，TSDM)[9]。比较内容涵盖攻击检测成功率、攻击估计均方误差(mean squared error，MSE)、最大频率偏差以及系统稳定时间，结果如表1所示。

表1 检测模型性能对比

Tab. 1 Comparison of detection model performance

方法	攻击检测成功率/%	MSE值	最大频率偏差/Hz	稳定时间/s
KF	87.3	1.35×10^{-2}	0.078	23.5
EKF	89.7	1.12×10^{-2}	0.072	21.8
ESO	91.5	9.87×10^{-3}	0.068	20.6
TSDM	92.6	8.70×10^{-3}	0.065	20.1
本文方法	95.2	6.28×10^{-3}	0.053	17.4

从表1数据可以看出，本文方法在各项性能指标上均优于现有其他方法，本文所提方法的攻击检测成功率达到95.2 %，相比标准卡尔曼滤波(87.3 %)、扩展卡尔曼滤波(89.7 %)、扩展状态观测器(91.5 %)和两阶段去噪扩散模型(92.6 %)均有明显提升，特别是在低幅度、隐蔽性攻击场景下仍能保持高检测率，展现了极强的灵敏性和鲁棒性。在估计精度方面，本文方法的攻击估计MSE值为6.28×10^{-3}，显著低于标准卡尔曼滤波(1.35×10^{-2})、扩展卡尔曼滤波(1.12×10^{-2})以及扩展状态观测器(9.87×10^{-3})。即使与性能较优的两阶段去噪扩散模型(8.70×10^{-3})相比，均方误差也降低了27.8%，进一步验证了本文方法在攻击量重构方面的高准确性。在系统动态特性指标方面，本文方案最大频率偏差控制在0.053 Hz，远小于传统方法(标准卡尔曼滤波0.078 Hz，扩展卡尔曼滤波0.072 Hz，扩展状态观测器0.068 Hz)，也明显优于两阶段扩散模型(0.065 Hz)，有效抑制了攻击造成的频率扰动，有助于提升电力系统整体安全性和稳定性。同时，本文方案实现了17.4 s的稳定时间，相比各传统方法普遍超过20 s的情况下缩短了至少14.7 %，具有更快的系统恢复能力。

综合来看，标准卡尔曼滤波在建模误差和微小攻击条件下检测性能低下，扩展卡尔曼滤波虽可处理一定非线性但受攻击隐蔽性制约，扩展状态观测器具备一定鲁棒性但难以区分控制输入与测量攻击，而两阶段扩散模型虽适应多模态数据变化但实时性有所欠缺。相比之下，本文方法能够在保持实时性的同时，准确区分控制输入攻击与测量数据攻击，展现出最优的检测准确性、重构精度与系统稳定性，验证了所提策略的有效性和先进性。

5 结语

本文提出了基于状态空间分解的攻击检测与估计方法，以及结合滑模观测器和H_∞控制策略的ARC机制，以提高系统在FDIA环境下的稳定性和鲁棒性。该方法利用状态空间变换技术，采用滑模观测器模式进行攻击信号估计计算，并使用H_∞控制策略优化控制指令获取最终结果。仿真试验验证了该方法在不同攻击场景下的检测精度和控制效果，结果表明，该方法能够有效识别控制输入攻击和测量攻击，并显著降低系统频率偏差和振荡幅度。

本文主要基于线性状态空间模型进行分析，未来可进一步考虑电力系统的非线性特性，并结合深度学习、强化学习等智能算法提升攻击检测与防御策略的自适应能力。此外，针对更复杂的多区域电力系统，未来研究可探索分布式检测与协同防御机制，以提高系统整体的安全性和鲁棒性。

参考文献

[1] 朱文，江伟，周志烽，等. 基于电网调度系统的网络安全态势感知方法研究[J]. 电测与仪表，2024，61(7)：21－27.
ZHU Wen，JIANG Wei，ZHOU Zhifeng，et al. Network security situation awareness method of power grid dispatching automation system[J]. Electrical Measurement & Instrumentation，2024，61(7)：21－27.

[2] 李卓，谢耀滨，吴茜琼，等. 基于深度学习的电力系统虚假数据注入攻击检测综述[J]. 电力系统保护与控制，2024，52(19)：175－187.
LI Zhuo，XIE Yaobin，WU Qianqiong，et al. Review of deep learning-based false data injection attack detection in power systems[J]. Power System Protection and Control，2024，52(19)：175－187.

[3] 刘增稷，王琦，薛彤. 电力系统中数据驱动算法安全威胁分析及应对方法研究[J]. 中国电机工程学报，2023，43(12)：4538－4554.
LIU Zengji，WANG Qi，XUE Tong. Security threat analysis and countermeasures of data-driven algorithms in power systems[J]. Proceedings of the CSEE，2023，43(12)：4538－4554.

[4] 钱胜，王琦，颜云松. 计及网络攻击影响的安全稳定控制系统风险评估方法[J]. 电力工程技术，2022，41(3)：14－21.
QIAN Sheng，WANG Qi，YAN Yunsong. Risk assessment method for security and stability control system considering the impact of cyber attacks [J]. Electric Power Engineering

Technology，2022，41(3)：14－21.

[5] 李鹏，刘念，胡秦然．“新型电力系统数字化关键技术综述”专辑评述[J]．电力系统自动化，2024，48(6)：1－12.
LI Peng，LIU Nian，HU Qinran. Commentary on special issue of reviews on key technologies for digitalization of new power system[J]. Automation of Electric Power Systems，2024，48(6)：1－12.

[6] 张杰，方浪森，姚立明，等．基于图论及混合卷积神经网络的电力结算电量数据异常检测方法[J/OL]．南方电网技术，2024：1－12[2024－10－30]. https://nfdwjs.csg.cn/gateway-web/zh/debutDetail.html? serialNum=20240527004.
ZHANG Jie，FANG Langsen，YAO Liming，et al. Anomaly detection method for power settlement electricity data based on graph theory and hybrid convolutional neural network[J/OL]. Southern Power System Technology，2024：1－12[2024－10－30]. https://nfdwjs.csg.cn/gateway-web/en/debutDetail.html?serialNum=20240527004.

[7] 席磊，田习龙，余涛，等．基于相关特征-多标签级联提升森林的电网虚假数据注入攻击定位检测[J]．南方电网技术，2024，18(5)：39－50.
XI Lei，TIAN Xilong，YU Tao，et al. Locational detection of false data injection attack in power grid based on relevant features multi-label cascade boosting forest[J]. Southern Power System Technology，2024，18(5)：39－50.

[8] ARNAB Bhattacharjee，ARNAB Kumar Mondal，ASHU Verma，et al. Deep latent space clustering for detection of stealthy false data injection attacks against AC state estimation in power systems[J]. IEEE Transactions on Smart Grid，2022，14(3)：2338－2351.

[9] PEI Jianhua，WANG Jingyu，SHI Dongyuan，et al. Improved efficient two-stage de-noising diffusion power system measurement recovery against false data injection attacks and data losses[EB/OL]. arXiv：2312.04346，https://arxiv. org/abs/2312.04346.

[10] WANG Jun，CHEN Haoran，SI Yifei，et al. FDIA localization and classification detection in smart grids using multi-modal data and deep learning technique[J]. Computers and Electrical Engineering，2024(119)：109572.1－109572.10.

[11] QU Zhaoyang，DONG Yunchang，LI Yang，et al. Localization of dummy data injection attacks in power systems considering incomplete topological information：a spatio-temporal graph wavelet convolutional neural network approach[J]. Applied Energy，2024(360)：122736.1－122736.8.

[12] PENG Sha，ZHANG Zhenyong，DENG Ruilong，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.

[13] ZHANG Guangdou，LI Jian，BAMISILE Olusola，et al. Spatio-temporal correlation-based false data injection attack detection using deep convolutional neural network[J]. IEEE Transactions on Smart Grid，2021，13(1)：750－761.

[14] 席磊，王文卓，白芳岩，等．基于最大信息系数-双层置信极端梯度提升树的电网虚假数据注入攻击定位检测[J]．电网技术，2025，49(2)：824－833.
XI Lei，WANG Wenzhuo，BAI Fangyan，et al. Grid false data injection attack localization detection based on MIC-double-deck confidence XGBoost tree[J]. Power System Technology，2025，49(2)：824－833.

[15] 黄冬梅，王一帆，胡安铎，等．融合无监督和有监督学习的虚假数据注入攻击检测[J]．电力工程技术，2024，43(2)：134－141.
HUANG Dongmei，WANG Yifan，HU Anduo，et al. False data injection attack detection based on the integration of unsupervised and supervised learning[J]. Electric Power Engineering Technology，2024，43(2)：134－141.

[16] 罗小元，耿艺帆，吴莉艳．基于GATv2模型的虚假数据注入攻击检测方法[J]．电气工程学报，2024，19(3)：353－361.
LUO Xiaoyuan，GENG Yifan，WU Liyan. Detection of false data injection attack based on GATv2 model[J]. Journal of Electrical Engineering，2024，19(3)：353－361.

[17] 郭天德，罗萍萍，林济铿．考虑状态量未知情况的电力系统杠杆量测攻击[J]．南方电网技术，2023，17(3)：56－64.
GUO Tiande，LUO Pingping，LIN Jikeng. Leverage measurement attack of power system considering unknown state variates[J]. Southern Power System Technology，2023，17(3)：56－64.

[18] YANG H，ZHANG W，CHUNG C Y，et al. AC false data injection attack based on robust tensor principle component analysis[J]. IEEE Transactions on Industrial Informatics，2024，20(8)：9887－9897.

[19] YANG Haosen，HE Xing，WANG Ziqiang，et al. Blind false data injection attacks against state estimation based on matrix reconstruction[J]. IEEE Transactions on Smart Grid，2022，13(4)：3174－3187.

[20] TIAN Jiwei，WANG Buhong，LI Jing，et al. Data-driven false data injection attacks against cyber-physical power systems[J]. Computers & Security，2022(121)：102836.1－102836.12.

[21] YANG Haosen，ZHANG Wenjie，LIANG Zipeng，et al. Parameter-free false data injection attack against AC state estimation：a canonical polyadic decomposition based approach[J]. IEEE Transactions on Power Systems，2025，40(3)：2153－2164.

[22] 金增旺，刘茵，刁靖东．针对信息物理系统远程状态估计的隐蔽虚假数据注入攻击[J]．自动化学报，2025，51(2)：356－365.
JIN Zengwang，LIU Yin，DIAO Jingdong. Stealthy false data injection attacks on remote state estimation of cyber-physical systems[J]. Acta Automatica Sinica，2025，51(2)：356－365.

[23] 陈炎森，王鹏宇，杨义．基于混合自动机的综合能源系统状态转移空间建模[J]．南方电网技术，2023，17(1)：103－113.
CHEN Yansen，WANG Pengyu，YANG Yi. State transition space modeling of integrated energy systems based on hybrid automata[J]. Southern Power System Technology，2023，17(1)：103－113.

[24] WEI Shuheng，WU Zaijun，XU Junjun，et al. Multi-area probabilistic forecasting-aided interval state estimation for FDIA identification in power distribution networks[J]. IEEE Transactions on Industrial Informatics，2023，20(3)：4271－4282.

[25] 庞清乐，韩松易，周泰．基于ASRUKF和IMC算法的电力信息物理系统虚假数据注入攻击检测[J]．智慧电力，2024，52(7)：111－118.
PANG Qingle，HAN Songyi，ZHOU Tai. False data injection attack detection of cyber-physical power system based on ASRUKF and IMC algorithms[J]. Smart Power，2024，52(7)：111－118.

[26] 王新宇，王相杰，罗小元．基于自适应生成对抗网络的智能电网状态重构的虚假数据攻击检测[J]．电力信息与通信技

术，2024，22(9)：1－7.
WANG Xinyu，WANG Xiangjie，LUO Xiaoyuan. False data injection attack detection for smart grid state reconstruction based on adaptive generative adversarial networks[J]. Electric Power Information and Communication Technology，2024，22(9)：1－7.
[27] 吴在军，徐东亮，徐俊俊. 信息物理多重攻击下配电网状态估计关键技术评述[J]. 电力系统自动化，2024，48(6)：127－138.
WU Zaijun，XU Dongliang，XU Junjun. Review on key technologies for distribution network state estimation under cyber-physical multiple attacks [J]. Automation of Electric Power Systems，2024，48(6)：127－138.
[28] ZHANG Zhixun，HU Jianqiang，LU Jianquan，et al. Preventing false data injection attacks in LFC system via the attack-detection evolutionary game model and KF algorithm[J]. IEEE Transactions on Network Science and Engineering，2022，9(6)：4349－4362.
[29] LI Xue，WANG Ziyi，ZHANG Changda，et al. A novel dynamic watermarking-based EKF detection method for FDIAs in smart grid[J]. IEEE/CAA Journal of Automatica Sinica，2022，9(7)：1319－1322.
[30] AHMAD S，AHMED H. Robust intrusion detection for resilience enhancement of industrial control systems：an extended state observer approach[J]. IEEE Transactions on Industry Applications，2023，59(6)：7735－7743.

收稿日期：2025-03-26；网络首发日期：2025-06-05
作者简介：
梁志宏(1984)，男，高级工程师(教授级)，硕士，研究方向为网络安全；
严彬元(1989)，男，高级工程师，硕士，研究方向为网络安全；
洪超(1987)，男，通信作者，高级工程师，硕士，研究方向为网络安全，chao_hong_004@163.com。

(上接第 13 页 Continued from Page 13)

[26] TAGAWA Y，MASKELIŪNAS R，DAMAŠEVIČIUS R. Acoustic anomaly detection of mechanical failures in noisy real-life factory environments[J]. Electronics，2021，10(19)：2329.1－2329.12.
[27] 吴海荣，李振华，程紫熠，等. 基于注意力机制和LSTM-LightGBM的特高压直流输电线路可听噪声无效数据清洗方法[J].南方电网技术，2024，18(8)：115－123，140.
WU Hairong，LI Zhenhua，CHENG Ziyi，et al. Invalid data cleaning method of audible noise for UHV HVDC transmission lines based on attention mechanism and LSTM-LightGBM[J]. Southern Power System Technology，2024，18(8)：115－123，140.
[28] SALA G，DE BONIS G，COSTABEBER A，et al. Development and validation of a smart architecture for thyristor valves [J]. IEEE Journal of Emerging and Selected Topics in Power Electronics，2023，11(4)：4068－4076.
[29] 刘云鹏，来庭煜，刘嘉硕，等. 特高压直流换流阀饱和电抗器振动声纹特性与松动程度声纹检测方法[J]. 电工技术学报，2023，38(5)：1375－1389.
LIU Yunpeng，LAI Tingyu，LIU Jiashuo，et al. Vibration and voiceprint characteristics of saturable reactors in UHVDC converter valves and voiceprint detection method for loosening degree [J]. Transactions of China Electrotechnical Society，2023，38(5)：1375－1389.
[30] HAN S，WANG B W，LIAO S Z，et al. Defect identification method for transformer end pad falling based on acoustic stability feature analysis [J]. Sensors，2023，23(6)：3258.1－3258.11.
[31] WANG J X，ZHAO Z S，ZHU J，et al. Improved support vector machine for voiceprint diagnosis of typical faults in power transformers [J]. Machines，2023，11(5)：11050539.1－11050539.14.
[32] WU H，HU T，LIU Y，et al. Timesnet：temporal 2d-variation modeling for general time series analysis[EB/OL]. arxiv：2210.02186，https://arxiv.org/abs/2010.02186.
[33] ZUO C，WANG J，LIU M，et al. An ensemble framework for short-term load forecasting based on TimesNet and TCN[J]. Energies，2023，16(14)：5330.1－5330.8.
[34] ZHAO H，HUANG X，XIAO Z，et al. Week-ahead hourly solar irradiation forecasting method based on ICEEMDAN and TimesNet networks [J]. Renewable Energy，2024(220)：119706.1－119706.10.
[35] ZHANG C，ZHANG Y，LI Z，et al. Enhancing state of charge and state of energy estimation in Lithium-ion batteries based on a TimesNet model with Gaussian data augmentation and error correction [J]. Applied Energy，2024(359)：122669.1－122669.12.

收稿日期：2024-09-04；网络首发日期：2025-06-10
作者简介：
唐明珠(1983)，男，教授，博士，研究方向为超特高压换流阀、电力变压器等状态监测与智能评估，tmz@csust.edu.cn；
俞昱(2000)，男，硕士研究生，研究方向为换流阀声纹异常检测与诊断，748685102@qq.com；
吴华伟(1979)，通信作者，男，教授，博士，研究方向为机电故障诊断与健康管理，whw_xy@163.com。