DOI:10.19651/j.cnki.emt.2417593

基于检测约束的微电网虚假数据注入攻击策略*

林鼎杰 夏候凯顺
(华南理工大学电力学院 广州 510641)

摘 要:当前微电网频率控制系统的安全研究缺乏对强攻击场景的深入分析,尤其是在攻击者利用内部信息发起的高隐蔽性攻击下,系统脆弱性及其影响程度尚未得到充分评估。针对传统虚假数据注入攻击易被检测的问题,构建一种基于检测约束的微电网最优攻击策略,实现高隐蔽性强攻击。首先搭建了一个包含风光储的微电网频率控制模型,并对其通信层进行脆弱性分析,明确潜在的攻击路径。为考虑隐蔽性约束,通过引入松弛变量构建了可优化的攻击模型,将非线性优化问题转化为线性规划形式,实现快速求解并构建特定的攻击序列。最后在孤岛运行状态下的微电网中进行多次攻击测试,相比传统随机攻击方法,所提出的优化攻击序列在保持 95%以上隐蔽性的同时,使攻击有效性提升了约 40%。此外,分析了微电网关键系统参数、不同运行模式和可再生能源渗透率对最优攻击的影响。结果表明所提出的基于优化的攻击序列能够在保持攻击隐蔽性的同时,显著提升攻击的成功率和有效性,微电网系统面对精心设计的攻击时仍具有潜在脆弱性。

关键词:微电网;频率控制;攻击策略;优化模型;安全性分析
中图分类号:TM73;TN91 **文献标识码**:A **国家标准学科分类代码**:470.4

False data injection attacks strategy for microgrids based on detection constraints

Lin Dingjie Xiahou Kaishun
(School of Electric Power Engineering, South China University of Technology, Guangzhou 510641, China)

Abstract: Existing security research on microgrid frequency control systems lacks a comprehensive analysis of severe attack scenarios, particularly high-concealment attacks executed by adversaries using internal information. The system vulnerabilities and the extent of their potential impact remain insufficiently assessed. This paper develops a load frequency control model of microgrid that incorporates wind, solar, and storage, and performs a vulnerability analysis of its communication layer to identify potential attack vectors. To address concealment constraints, an optimized attack model is formulated by introducing slack variables, which transforms the nonlinear optimization problem into a linear programming problem, enabling faster solutions and the generation of specific attack sequences. Finally, multiple attack tests are conducted on microgrids in islanded operation mode. Compared to traditional random attack methods, the proposed optimized attack sequence achieves approximately 40% improvement in attack effectiveness while maintaining over 95% stealth. The effects of key microgrid system parameters, different operation modes, and various renewable energy penetration rates on optimal attacks are analyzed. Results show that the proposed optimization-based attack can significantly improve attack success rate and effectiveness while maintaining stealthy, indicating that microgrid systems remain potentially vulnerable to well-designed attacks.

Keywords: microgrid; frequency control; attack strategy; optimization model; security analysis

0 引 言

随着清洁能源与分布式发电技术的快速发展,微电网将会成为分布式新能源就地消纳的主要形式[1-3]。作为典型的信息物理融合系统(cyber-physical systems, CPS)应用场景[4],现代微电网系统通过将信息通信技术、传感器网络与物理电力设备深度融合,实现了能源的智能调度与协同控制。然而随着微电网中对信息物理依赖性不断提高,

收稿日期:2024-12-10
* 基金项目:国家自然科学基金(52207106)、华南理工大学 2024 年“百步梯攀登计划”(j2tw202402115)项目资助

其面临的网络安全威胁也日益严峻。特别是微电网的频率控制系统，作为确保系统稳定运行的关键环节，一旦遭受恶意攻击将可能导致系统失稳甚至崩溃，造成严重的经济损失和社会影响[5-6]。

近年来，对微电网频率控制系统的安全性研究主要集中在系统脆弱性分析[7]、攻击检测[8-9]和防御策略[10-11]等方面。其中，虚假数据注入攻击(false data injection attack，FDIA)因其较强的隐蔽性和破坏性，已成为威胁微电网频率控制系统的主要攻击手段之一[6]。然而，现有研究多针对简单的随机 FDIA 场景进行分析，缺乏对具有高度隐蔽性的强攻击场景的深入研究[9,12-13]。特别是在攻击者能够获取系统内部信息的情况下，如何评估系统面临的安全风险，以及如何量化攻击对系统造成的影响，这些问题尚未得到充分解答。

在确定攻击目标情况下，构建攻击向量需要确定要修改的量测对象和修改的目标值。文献[14]以负荷数据作为虚假数据攻击的目标，提出一种物理攻击和信息攻击的混合攻击方法。这种方法以不良数据检测为基础，以物理攻击资源和信息攻击资源为约束。文献[15]提出了一种结合稀疏优化、平行因子分解和凸优化的数据驱动攻击方法，通过系统信息矩阵的构建实现了有效的虚假数据注入。文献[16]从控制系统安全的角度研究了伪数据注入攻击，设计了伪数据攻击序列，以避免在控制系统性能受损时被检测器检测到。文献[17]提出了一种基于多目标部分可观马尔可夫决策过程的自动发电控制攻击方法，通过强化学习的近端策略优化算法生成难以被传统基于区域控制误差分析的检测方法和未知输入观测器检测的虚假数据注入攻击。然而，目前多数研究为简化问题的复杂度，通常基于静态状态估计算法与完全信息情形。在掌握部分信息与攻击资源的情形下，如何构造攻击向量，对电网造成最严重后果，属于多项式复杂程度的非确定性问题，需要进一步研究平衡计算资源和时间的攻击算法优化策略。另外，传统的攻击分析方法往往忽视了攻击隐蔽性这一重要特征，仅通过固定的阈值降低攻击被发现的概率[18]，导致所得结论可能低估系统面临的实际安全风险。而高隐蔽性的 FDIA 往往更具危害性，因为这类攻击更难被现有的安全防护机制发现和阻止。因此，有必要深入研究考虑隐蔽性约束的攻击策略。

本文针对上述问题，提出了一种基于优化的 FDIA 序列构建方法。通过引入松弛变量，将包含隐蔽性约束的非线性优化问题转化为线性规划形式，实现了最优 FDIA 序列的快速求解。该方法不仅考虑了攻击的隐蔽性要求，还能够在保证攻击效果的前提下最大化攻击的成功概率。研究结果表明，相比传统的随机攻击方法，本文提出的优化攻击策略能够显著提升攻击的成功率，同时保持较高的隐蔽性，为微电网频率控制系统的安全性评估提供了新的研究思路。

1　含风光储的微电网建模

微电网系统通常由多个分布式电源(distributed generation，DG)构成[19]，主要包括光伏发电单元(photovoltaic array，PV)、风力发电机组(wind turbine，WT)、微型燃气轮机(micro turbine，MT)以及储能系统(energy storage system，ESS)。其中储能系统包括燃料电池(fuel cell，FC)、蓄电池(battery energy storage system，BESS)和飞轮储能系统(flywheel energy storage system，FESS)。各 DG 通过电力电子装置与微电网相连。这些接口装置既可以实现交流电源的同步，也可以完成直流电源的逆变。每个 DG 都配备有断路器，可在系统受到严重干扰时断开与微电网的连接，或在设备维护时使用。

为实现交流及混合型微电网的频率合成控制，系统的频率响应特性至关重要[20]。为此，考虑一个包含多种可再生能源的微电网，如图 1 所示。每种 DG 都配备相应的等效模型，用于描述其动态特性。系统中各发电机组均引入相应的标幺发电系数 K_{DG}，定义为单个机组装机容量与系统总装机容量之比[21]。可再生能源机组的发电系数 K 值越高，表明系统中可再生能源的渗透率越大。

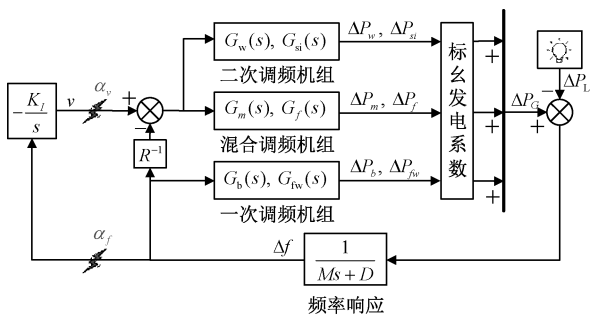


图 1　微电网频率响应框图

Fig. 1　Block diagram of microgrid frequency response

针对 WT 和 PV，由于包含接口元件的高阶动态影响相对较小，被忽略而不会显著影响整体系统的分析结果，因此仅考虑或 DC/DC 变流器或 DC/AC 逆变器的动态过程[22]：

$$G_w(s)=\frac{1}{T_w s+1};\ G_s(s)=\frac{1}{T_{si}s+1} \tag{1}$$

式中：$G_w(s)$、$G_{si}(s)$分别代表风机、光伏的动态响应过程，T_w 是风力发电机时间常数，T_{si} 是光伏逆变器时间常数。

储能系统的动态模型取决于储能系统的类型。由于储能的快速注入，BESS 和 FESS 可以用具有相对较小时间常数的一阶传递函数建模：

$$G_b(s)=\frac{1}{T_b s+1};\ G_{fw}(s)=\frac{1}{T_{fw}s+1} \tag{2}$$

式中：$G_b(s)$、$G_{fw}(s)$分别代表 BESS、FESS 的动态响应过程。T_b 是电池的时间常数，反映电池充放电过程的动态特性。T_{fw} 是飞轮系统时间常数，反映飞轮储能系统的机电

耦合动态特性。

FC具有高阶特性[23],具有时间常数 T_f、T_i 和 T_c 的三阶模型,主要包含燃料模块、用于将直流电压转换为交流电压的逆变器和互连装置,其传递函数如下:

$$G_f(s)=\frac{1}{T_f s+1}\cdot\frac{1}{T_i s+1}\cdot\frac{1}{T_c s+1} \tag{3}$$

式中:T_f 代表FC调速器的时间常数,反映燃料供应的动态特性;T_i 是FC逆变器时间常数,反映电力电子接口的响应速度;T_c 是FC滤波器时间常数,用于抑制高频干扰。

MT的动态响应通常可以用一个两阶传递函数来表示,包括涡轮机械系统和发电机电气系统[9]。一个典型MT传递函数可以表示为:

$$G_m(s)=\frac{1}{T_g s+1}\cdot\frac{1}{T_t s+1} \tag{4}$$

式中:T_g 是调速器时间常数,T_t 是涡轮机械系统时间常数。

负荷和系统频率响应用一阶惯性环节来表示,则微电网的频率偏差可以表示为各DG功率变化的函数:

$$\Delta f=\frac{1}{Ms+D}\cdot(\Delta P_G-P_L) \tag{5}$$

式中:M 是系统的等效惯性常数;D 是等效阻尼。ΔP_G 各分布式电源功率变化的总和;ΔP_L 表示负荷功率变化。

分布式负荷频率控系统通过传感器网络实时采集微电网频率偏差 Δf,并将采集数据传输至控制中心进行处理[24]。基于获取的频率偏差,控制中心生成相应的调节信号 v,从而实现对系统频率的动态调节。在任意时刻 t,控制调节量 v 可表示为:

$$v=K_I\int\Delta f\,\mathrm{d}t \tag{6}$$

式中:K_I 是控制器的积分增益。

根据式(1)~(6),可以构建一个完整的微电网状态空间模型:

$$\dot{\boldsymbol{x}}(t)=\begin{bmatrix}\boldsymbol{A}_{11}&\boldsymbol{A}_{12}\\ \boldsymbol{A}_{21}&\boldsymbol{A}_{22}\end{bmatrix}\boldsymbol{x}(t)+\boldsymbol{E}\mathrm{d}(t) \tag{7}$$

式中:$\boldsymbol{x}=[\Delta f,\ \Delta P_g,\ \Delta P_t,\ \Delta P_f,\ \Delta P_i,\ \Delta P_c,\ \Delta P_b,\ \Delta P_{fw},\ \Delta P_{si},\ \Delta P_w,\ v]^T$,$\boldsymbol{d}=[\Delta P_L]^T$,$\boldsymbol{y}=[\Delta f,\ v]^T$,

$$\boldsymbol{A}_{11}=\begin{bmatrix}-\frac{D}{M}&0&\frac{1}{M}&0&0&\frac{1}{M}\\ -\frac{1}{RT_g}&-\frac{1}{T_g}&0&0&0&0\\ 0&\frac{1}{T_t}&-\frac{1}{T_t}&0&0&0\\ 0&0&0&-\frac{1}{T_f}&0&0\\ 0&0&0&\frac{1}{T_i}&-\frac{1}{T_i}&0\\ 0&0&0&0&\frac{1}{T_c}&-\frac{1}{T_c}\end{bmatrix},$$

$$\boldsymbol{A}_{12}=\begin{bmatrix}\frac{1}{M}\mathbf{1}_{1\times5}&0\\ \mathbf{0}_{1\times5}&\frac{1}{T_g}\\ \mathbf{0}_{1\times5}&0\\ \mathbf{0}_{1\times5}&\frac{1}{T_f}\\ \mathbf{0}_{1\times5}&0\\ \mathbf{0}_{1\times5}&0\end{bmatrix},\quad \boldsymbol{A}_{21}=\begin{bmatrix}-\frac{1}{T_b}&\mathbf{0}_{1\times5}\\ -\frac{1}{T_{fw}}&\mathbf{0}_{1\times5}\\ 0&\mathbf{0}_{1\times5}\\ 0&\mathbf{0}_{1\times5}\\ -K_I\beta&\mathbf{0}_{1\times5}\end{bmatrix},$$

$$\boldsymbol{A}_{22}=\begin{bmatrix}-\frac{1}{T_b}&0&0&0&0\\ 0&-\frac{1}{T_{fw}}&0&0&0\\ 0&0&-\frac{1}{T_{si}}&0&\frac{1}{T_{si}}\\ 0&0&0&-\frac{1}{T_w}&\frac{1}{T_w}\\ 0&0&0&0&0\end{bmatrix},$$

$$\boldsymbol{E}=\begin{bmatrix}-\frac{1}{M}&0&0&0&0&0&0&0&0&0&0\end{bmatrix}^T,$$

$$\boldsymbol{C}=\begin{bmatrix}1&0&0&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&1\end{bmatrix}。$$

2 最优攻击序列

在微电网遭受攻击的过程中,攻击者首先向频率测量通道和控制信号测量通道中分别注入虚假数据,使得控制中心收到的频率测量值变为错误量测,各DG收到的控制信号也并非真实的控制信号。DG收到错误的信号后做出响应,导致系统实际负载与发电之间出现不平衡,造成系统频率偏离额定值。如果这种情况持续存在且未被及时发现,系统将偏离预期工作点,频率调节能力受损,最终可能引发连锁稳定性问题[9,25]。

为了确保FDIA对测量值 $\boldsymbol{z}$ 的攻击不被检测,攻击者需要绕过状态估计器的坏数据检测(bad data detection,BDD)。此外,控制中心还会对 $\boldsymbol{z}$ 应用其他检测方法,比如要求 $\boldsymbol{z}$ 在短时间内不会发生显著变化。如果FDIA攻击向量 α 的每个元素都接近于0,将不太可能触发警报[26]。若攻击信号过于明显,容易引发系统的警报机制,导致隔离措施的启动,从而使攻击无法达到预期效果。

若将原始测量值记为 $\boldsymbol{z}$,攻击向量记为 $\boldsymbol{\alpha}$,则注入攻击后的测量值为 $\boldsymbol{z}+\boldsymbol{\alpha}$。攻击者需要确保 $\boldsymbol{z}+\boldsymbol{\alpha}$ 能通过状态估计的残差测试,同时保持攻击向量 $\boldsymbol{\alpha}$ 的各分量足够小。

$$\min\|\boldsymbol{\alpha}\| \tag{8}$$

$$s.t.\ h(\boldsymbol{x}+\boldsymbol{c})=\boldsymbol{z}+\boldsymbol{\alpha} \tag{9}$$

$$\|\boldsymbol{z}+\boldsymbol{\alpha}-h(\hat{\boldsymbol{x}})\|\leqslant\tau \tag{10}$$

式中:$\boldsymbol{x}$ 为系统状态向量,$\hat{\boldsymbol{x}}$ 为状态估计向量,$\boldsymbol{c}$ 为期望状

态偏移量，$h(\boldsymbol{x})$为测量方程，τ 为 BDD 检测阈值。保证攻击最小化不仅能够规避 BDD 检测，还能保证攻击信号的平滑性，避免触发时间序列异常检测等其他防护机制。

除了最小化攻击向量范数外，攻击者还需考虑物理可实现性约束：

1)DG 机械输出功率约束：

$$\Delta \underline{P}^{\mathrm{m}} \leqslant \Delta P^{\mathrm{m}} \leqslant \Delta \bar{P}^{\mathrm{m}} \tag{11}$$

式中：ΔP^{m} 表示 DG 的机械输出功率，$\Delta \underline{P}^{\mathrm{m}}$ 表示输出功率增量的下限，$\Delta \bar{P}^{\mathrm{m}}$ 输出功率增量的上限。

2)控制信号幅值约束：

$$\underline{v} \leqslant v \leqslant \bar{v} \tag{12}$$

式中：v 表示发送给第 DG 的控制信号，$\underline{v}$ 为控制信号的最小值，$\bar{v}$ 为控制信号的最大值。

3)频率变化连续性约束：

$$\left|(\Delta f[k+1]+\Delta \widetilde{f}[k+1])-(\Delta f[k]+\Delta \widetilde{f}[k])\right| \leqslant \sigma^{f} \tag{13}$$

式中：$\Delta f[k]$代表微电网第 k 个时刻的频率偏移，$\Delta \widetilde{f}[k]$ 代表在第 k 个时刻的攻击频率偏移，σ^{f} 表示两个连续时刻频率变化的允许限值。

为了量化攻击对系统影响的有效性，引入平均频率偏差超出安全阈值(ε_L，ε_U)的威胁关键时间(critical time to threat，CTT)，即从攻击开始到系统达到危险状态的时间间隔。如图 2 所示。

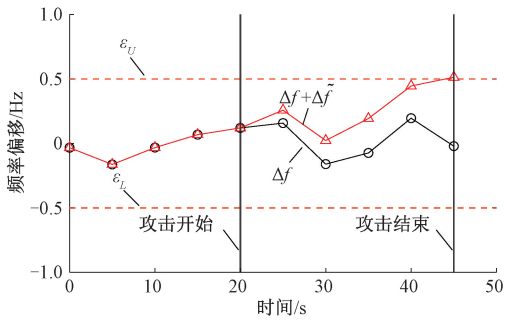


图 2　威胁关键时间示意图

Fig. 2　Diagram of the critical time to threat

式(8)～(13)这些约束条件共同构成了 FDIA 攻击的隐蔽性要求，确保攻击行为不会导致测量数据出现明显的异常。通过满足这些约束，攻击者可以降低被传统检测机制发现的风险。同时又由于这些隐蔽性约束的存在，单次数据注入攻击难以直接导致系统频率发生显著偏移[17]。因此，攻击者需要设计一个精心构造的攻击序列，通过持续的小幅攻击逐步实现预期目标。假设当前微电网控制周期的时间索引为 k，攻击者在后续 h 个周期内实施持续性攻击，则攻击序列表示为：

$$\mathcal{A}=\{\boldsymbol{\alpha}_{k+1},\boldsymbol{\alpha}_{k+2},\ldots,\boldsymbol{\alpha}_{k+h}\} \tag{14}$$

式中：k 为初始周期索引，h 为攻击持续的周期数，α_{k+i} 为第 $k+i$ 个周期的攻击向量。

一旦系统的频率偏差超出安全阈值，将触发紧急控制措施以维持系统稳定。然而，这些紧急措施有时可能反而导致系统失稳。这是因为快速的干预和调整可能无法充分考虑系统的动态特性，进而引发不必要的振荡或过冲，从而加剧频率波动[6]。基于上述要求，为了同时满足隐蔽性和有效性约束条件，构建如下优化目标函数：

$$\min\ \eta_1\sum\varepsilon_f[k]+\eta_2\sum\varepsilon_v[k]+\eta_3\varepsilon_{CTT} \tag{15}$$

$$s.t.\begin{cases}\varepsilon_f[k]\geqslant\left|\Delta\widetilde{f}[k+1]-\Delta\widetilde{f}[k]\right|,k\in\mathcal{A}\\ \varepsilon_v[k]\geqslant\left|\widetilde{v}[k+1]-\widetilde{v}[k]\right|,k\in\mathcal{A}\\ \varepsilon_{CTT}\geqslant 0\\ \text{式(8)}\sim\text{(13)}\end{cases} \tag{16}$$

式中：η 为加权因子，用于平衡各个部分在目标函数中的重要性；ε_f 和 ε_v 代表频率攻击和控制信号攻击的松弛项，用于衡量攻击的影响程度；ε_{CTT} 代表攻击发起到频率超限的 CTT 时间。确保攻击行为在隐蔽性约束内进行的同时，最小化攻击所持续的时间。将攻击问题转化为线性规划的优化形式，以便于求解。

3　仿真分析

为验证所提出的最优虚假数据注入攻击策略的有效性，使用 Matlab/Simulink 平台构建如图 1 所示的微电网模型，包含风电机组、光伏机组、储能系统以及负载等关键单元。通过仿真分析研究该攻击方法对微电网系统稳定性和安全性的影响，并与随机攻击情景进行对比，从而验证攻击策略的可行性。同时开展关键参数敏感性分析以及不同运行模式、不同可再生能源渗透率下的适应性研究，从而全面验证攻击策略的有效性。

微电网安全阈值参数根据系统运行标准确定，其中频率、控制信号等关键指标的变化范围参考微电网运行规程，功率波动等指标则基于微电网正常运行时的波动特性设定。为确保实验结果的可靠性，选择典型微电网相关参数[27]。系统负荷波动设置为基准负荷的标准差 0.02 的高斯分布，以模拟实际负荷的随机性特征。攻击隐蔽性约束的相关参数基于正常运行工况进行选择，以确保攻击行为不被传统检测机制发现。具体参数值如表 1 所示。

在微电网控制系统中，频率和控制信号是两个关键变量。因此，本节在仿真中重点关注 FDIA 对这些重要变量的影响。首先对无攻击场景下的微电网正常运行进行仿真，其波形如图 3 所示。

在正常运行状态下，微电网根据负载波动和可再生能源发电的变化自动进行频率调节，维持系统稳定。系统的频率波动保持在正常范围[49.95 Hz，50.05 Hz]之间。

表 1　微电网及攻击优化参数

Table 1　Microgrid and attack optimization parameters

变量	参数值	变量	参数值	变量	参数值
M	0.1677	T_b	0.1	ε_L	−0.5
D	0.0015	T_{fw}	0.2	ε_U	0.5
R	0.05	T_f	0.26	$\underline{v}$	−0.01
K_I	1.4	T_i	0.04	$\bar{v}$	0.01
β	5	T_c	0.004	σ^f	0.001
T_w	1.5	T_g	0.4	$\Delta\underline{P}^m$	−0.15
T_{si}	0.04	T_t	0.08	$\Delta\bar{P}^m$	0.15

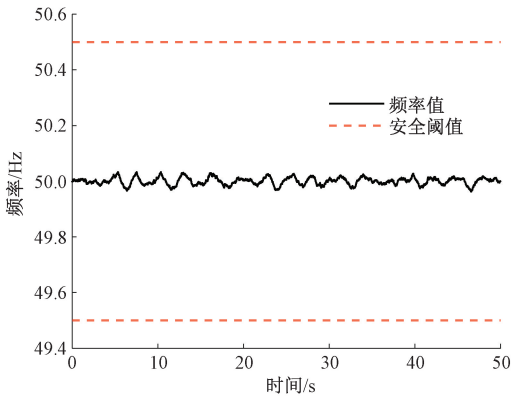


图 3　未受攻击下微电网频率波动

Fig. 3　Microgrid frequency fluctuation under non-attack conditions

3.1　最优攻击序列生成

基于前文所述的攻击模型,本文利用式(7)、(15)和(16)求解生成最优攻击序列。首先针对单次攻击进行仿真分析,如图 4 所示。攻击从 $t=20$ s 开始发起,攻击开始后,微电网实际频率开始快速上升,并在 $t=20.76$ s 突破预设阈值,$CTT=0.76$ s。这表明所设计的攻击策略能够有效导致系统频率偏离安全运行区间。

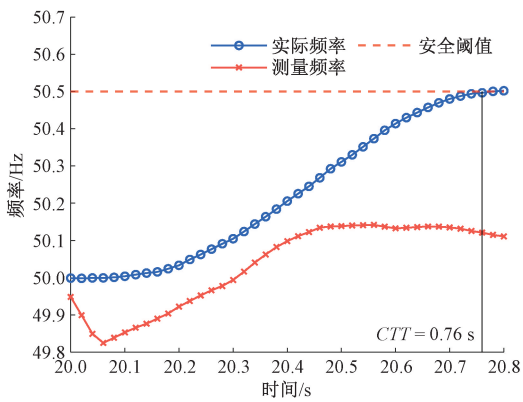


图 4　在最优攻击序列下的频率偏移

Fig. 4　Waveform of the generated optimal FDIA sequence

在攻击发生后,频率测量值从接近零的正常状态急剧降低至负值区域,随后快速上升并超过系统正常运行水平。这种异常的频率测量值误导了控制系统对系统状态的判断,进而引发不当的调节操作。攻击通过降低频率测量值,使系统误判区域负载增加,继而向 DG 发出增加出力的控制指令。随后,攻击序列利用机组调节的滞后特性,叠加攻击与系统的双重响应,最终导致系统频率快速突破安全阈值。

图 5 展示了算法生成的最优攻击序列特征,其结果表明在攻击过程中,FDIA 的强度并非越大越有效。相反,为实现最优攻击效果,需要在不同攻击之间实现平衡与协调。

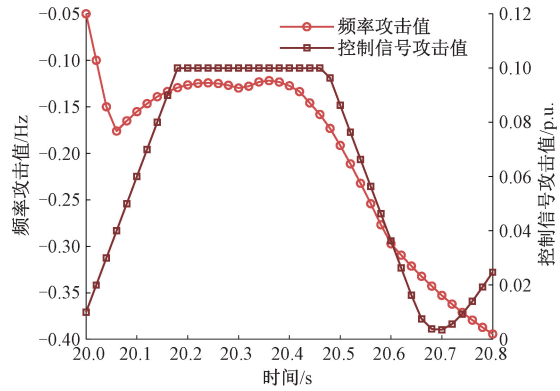


图 5　生成的最优攻击序列特征图

Fig. 5　Frequency diagram under optimal FDIAs sequence

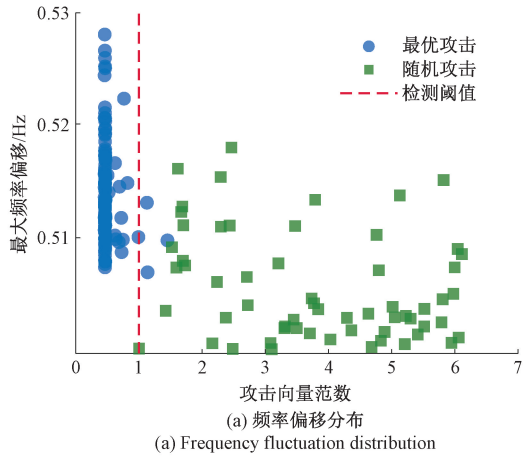
单一的递增或递减趋势容易触发系统检测机制,反而降低攻击的隐蔽性和效果。通过不同攻击的协同配合,可以在躲过 BDD 的同时持续扰动系统关键变量。渐进式的影响累积既提高了攻击的隐蔽性,也增强了对系统的持续干扰能力。综上所述,所设计的最优攻击序列能够在保持隐蔽性的同时,短时间内使系统频率突破安全阈值,验证了该攻击的有效性。

3.2　理想性能评估

为进一步验证所提出算法的有效性,使用所提算法生成的 100 组最优攻击序列,并与随机攻击序列进行对比分析。图 6 展示了最优攻击序列和随机攻击序列在最大频率偏移与攻击向量范数关系上的对比,以及各攻击生成的 CTT 分布情况。

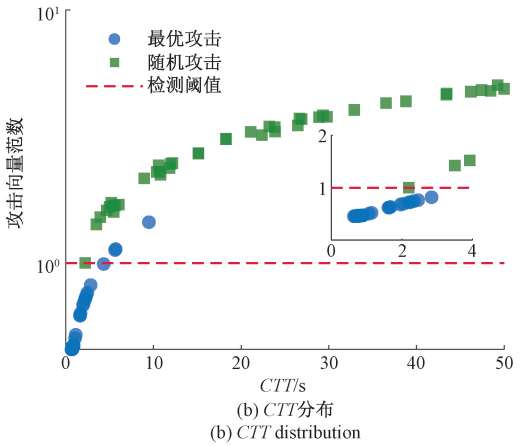
通过对比最优攻击与随机攻击在隐蔽性、有效性和 CTT 等多个维度的表现,最优攻击策略在各项指标上均显著优于随机攻击,展现微电网系统面对精心设计的攻击时所具有的潜在脆弱性。图 6(a)表明,本文提出的算法生成的最优攻击序列能够产生更大的频率偏移,且很好的将攻击向量范数保持在检测阈值之内,而随机攻击序列并不能够保持其隐蔽性。图 6(b)展示了所生成攻击的 CTT 分布。这表明本文所提算法能够更有效地利用有限的攻击资源。

其统计结果如表 2 所示。从攻击成功率来看,所设计算法达到了 92.1%的成功率,而随机攻击虽然有效性能达到 60%,但其隐蔽性并不能绕过 BDD 检测机制。较低的



(a) 频率偏移分布

(a) Frequency fluctuation distribution



(b) *CTT*分布

(b) *CTT* distribution

图 6　不同类型攻击散点分布图

Fig. 6　Scatterplot of different types of attacks

攻击成功率更容易触发系统的安全预警机制，进而导致系统管理员开展安全排查。一旦系统漏洞被发现，防御机制将被升级加固，这不仅会降低当前攻击的效果，还会增加后续攻击的难度。

表 2　不同类型攻击序列统计结果

Table 2　Statistical results of different attack sequences

性能指标	最优攻击	随机攻击
隐蔽性/%	**97.0**	0
有效性/%	**95.0**	60
CTT/s	**1.138±1.233**	33.467±23.504
攻击向量范数	**0.519±0.162**	3.787±1.538
成功率/%	**92.1**	0

在威胁关键时间 CTT 方面，最优攻击的平均耗时为 1.13 s，标准差为 1.233，明显优于随机攻击的 33.467 s，标准差为 23.504。较短的 CTT 表示从攻击发起到系统频率越限的时间更短，这能够快速触发系统切机、切负荷等紧急控制措施。这些应急措施虽然能在短期内使频率回归稳定，却可能被攻击者作为系统脆弱性加以利用，引发更大幅度的频率震荡，最终导致整个系统失去稳定性[6]。此外，从攻击范数来看，所设计算法的范数为 0.519，显著低于随机攻击的 3.787，说明所设计算法能够以更小的扰动幅度实现成功攻击，具有更好的隐蔽性。综上所述，实验结果充分证明了所设计攻击序列在攻击成功率、威胁关键时间和攻击范数 3 个关键指标上均优于随机攻击序列。

3.3　关键参数敏感性分析

上述评估建立在理想条件下，验证了所提方法的可行性和性能。然而，测量噪声和传感器漂移等因素不可避免地会影响攻击的隐蔽性，增加的误报率也会降低攻击效果。为了全面评估所提方法的实用性，本节将针对非理想因素进行鲁棒性分析。

通过对微电网中的关键参数进行系统性调整和扰动，深入研究了所提优化方法在面对不同参数时的性能，包括等效惯性常数、等效阻尼常数、控制增益和负荷波动等参数。具体结果如表 3 所示。

表 3　关键参数敏感性分析

Table 3　Sensitivity analysis of key parameters

关键参数	变化/%	隐蔽性/%	有效性/%	平均 CTT/s	成功率/%
基准	**0**	**97.0**	**95.0**	**1.138**	**92.1**
测量噪声参数	0.01	95.0	98.0	1.023	93.1
	0.05	93.0	98.0	1.128	91.1
	+20	85.0	92.0	3.577	78.2
M 参数	−20	100.0	100.0	0.678	100
	+20	96.0	100.0	1.143	96.0
D 参数	−20	97.0	100.0	1.116	97.0
	+20	97.0	100.0	1.113	97.0
K_1 负荷波动	−20	95.0	100.0	1.179	95.0
	5	100.0	100.0	0.906	100.0
	1	98.0	96.0	1.194	94.1

基准结果反映了理想条件下的攻击性能。考虑到实际系统中存在测量误差，分析了噪声对攻击性能的影响。测量噪声通常来自传感器的随机扰动，可建模为均值为零的高斯白噪声。随着噪声强度的增加，攻击的隐蔽性和有效性会逐渐降低。当噪声水平为 0.01%时，隐蔽性和有效性分别为 95% 和 98%，成功率为 93.1%。当噪声增至 0.05%时，隐蔽性降至 93%，有效性维持在 98%，成功率降至 91.1%。这表明尽管测量噪声会在一定程度上影响攻击效果，但所提方法仍具有较强的抗噪声能力。

敏感性分析结果表明，等效惯性常数和负荷波动率的变化对最优攻击的影响最为显著。当 M 增加 20%时，方法的隐蔽性从基准的 97% 降至 83.7%，有效性降至 92.0%，CTT 显著增加至 3.577 s，成功率也降低至 77%。相反，当 M 减少 20%时，各项攻击性能指标反而得到提

升,表明较小的等效惯性常数有利于攻击的实施。负荷波动分析表明,较大的波动幅度显示出更好的性能表现,表明微电网对攻击的敏感度随负荷波动的增加而提高。等效阻尼常数和控制增益的影响相对较小,在±20%的变化范围内仅导致性能指标的微小波动,隐蔽性维持在 95%～97%之间,CTT 的变化不超过 0.1 s,所提方法对上述参数具有良好的鲁棒性。

微电网系统普遍具有较小的等效惯性常数,这种特性虽然有利于系统灵活性,但也使其更易受到攻击。其次,微电网负荷波动幅度通常较大,这种动态特性反而为攻击者提供了更好的隐蔽环境。这些固有缺陷的叠加效应,使微电网系统在面对精心设计的攻击时表现出明显的脆弱性,为攻击者创造了有利条件。

3.4 运行模式与可再生能源渗透率适应性分析

为全面评估微电网系统在不同运行条件下的安全性能,本节从运行模式和可再生能源渗透率两方面开展研究。在运行模式方面,考虑了微电网三种典型工作状态:孤岛运行、并网运行以及微电网群运行。同时,设置了 3 种不同 MT 装机比例的工况:正常渗透率工况(K_m=48%)、高渗透率工况(K_m=25%)和低渗透率工况(K_m=90%)。在各工况中,MT 标幺发电系数 K_m 的差值由风电 K_w 和光伏发电机组 K_{si} 按照相同比例分摊补充,以保证系统总发电容量保持恒定。并网模式下,主电网选择典型火电参数[9]为:M=10 s,D=1。微电网群采用三区微电网互联的结构,相邻微电网 2 和微电网 3 的参数在微电网 1 的基础上进行适度调整。通过对不同运行模式及工况下系统性模拟分析,攻击效果的评估结果如图 7 和表 4 所示。

针对孤岛、并网和微电网群 3 种运行模式的性能对比分析表明,运行模式对攻击效果具有显著影响。在孤岛运行模式下,系统表现出较大的性能波动:CTT 值在 0.897 s 至 1.755 s 之间变化,且标准差较大,表明攻击响应时间不稳定。攻击向量范数在 0.480～0.598 之间波动,成功率在 92%～100%之间,其中工况 2 表现最佳,而工况 3 的性能相对较差。

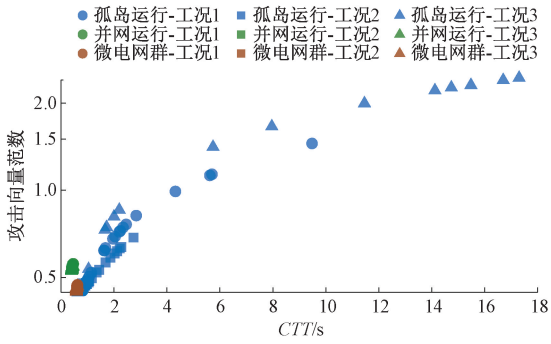


图 7 不同场景下攻击散点分布图

Fig. 7 Scatter plot of attacks in different scenarios

表 4 运行模式与可再生能源渗透率适应性分析

Table 4 Adaptability analysis of operation modes and renewable energy penetration rates

运行场景	工况	CTT/s	攻击向量范数	成功率/%
孤岛运行	1	1.138±1.233	0.519±0.162	97
	2	0.897±0.372	0.480±0.041	100
	3	1.755±3.505	0.598±0.457	92
并网运行	1	0.430±0.011	0.547±0.003	100
	2	0.426±0.009	0.545±0.002	100
	3	0.417±0.014	0.537±0.006	100
微电网群	1	0.602±0.007	0.954±0.005	100
	2	0.586±0.009	0.944±0.003	100
	3	0.590±0.012	0.945±0.007	100

并网运行模式展现出最稳定的攻击效果。CTT 均值维持在约 0.42 s 的较低水平,且标准差仅为 0.009～0.014 s,表明响应迅速且稳定。攻击向量范数保持在 0.54 左右,波动极小,3 种工况下均达到 100%的成功率,显示出优异的攻击性能。微电网群模式下的性能介于前两者之间。CTT 值稳定在 0.59 s 左右,标准差较小(约 0.01 s),表明响应时间适中且稳定。另外,由于该种运行模式下是假设同时对 3 个微电网进行攻击,攻击向量的维度增加导致其范数显著增大,但这并未影响攻击效果。

基于上述结果,并网运行模式为攻击提供了最有利的条件,表现出最优且最稳定的攻击性能。相比之下,孤岛运行模式受外部因素影响较大,性能波动明显。微电网群虽然需要较大的攻击向量,但仍能保持稳定的高成功率。这一结果揭示了不同运行模式下系统的脆弱性特征,为防御策略的制定提供了重要参考。

4 结 论

本文针对微电网频率控制系统在强攻击场景下的安全性问题,提出了一种基于检测约束的最优攻击建模方法。通过引入松弛变量将非线性优化问题转化为线性规划形式,实现了在保持高隐蔽性的同时提升攻击效果。实验验证表明,该方法在保持 95%以上隐蔽性的同时,使攻击有效性提升约 40%。通过系统分析关键参数、运行模式和可再生能源渗透率的影响,证明了微电网频率控制系统在面对精心设计攻击时存在潜在脆弱性,为系统安全防护提供了重要参考。研究结果表明,传统的微电网频率控制系统在高隐蔽性攻击场景下仍面临显著安全风险,为微电网频率安全性分析提供了新的思路。后续研究将着重于提升微电网的主动防御能力,推进方法在实际工程中的应用。

参考文献

[1] 葛磊蛟,范延赫,来金钢,等. 面向低碳经济的人工智

能赋能微电网优化运行技术[J]. 高电压技术，2023，49(6)：2219-2238.
GE L J，FAN Y H，LAI J G，et al. Artificial intelligence enabled microgrid optimization technology for low carbon economy [J]. High Voltage Engineering，2023，49(6)：2219-2238.

[2] FENG F，ZHANG P，ZHOU Y F，et al. Distributed networked microgrids power flow [J]. IEEE Transactions on Power Systems，2023，38(2)：1405-1419.

[3] 李瑜，张占强，孟克其劳，等. 基于改进深度确定性策略梯度算法的微电网能量优化调度[J]. 电子测量技术，2023，46(2)：73-80.
LI Y，ZHANG ZH Q，MENG K Q L，et al. Energy optimal dispatch of microgrid based on improved depth deterministic strategy gradient algorithm [J]. Electronic Measurement Technology，2023，46(2)：73-80.

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

[5] CHEN Y L，QI D L，DONG H N，et al. A FDI attack-resilient distributed secondary control strategy for islanded microgrids [J]. IEEE Transactions on Smart Grid，2021，12(3)：1929-1938.

[6] JAFARI M，ASHIQUR RAHMAN M，PAUDYAL S. Optimal false data injection attacks against power system frequency stability[J]. IEEE Transactions on Smart Grid，2023，14(2)：1276-1288.

[7] JIANG Z M，TANG Z F，ZHANG P，et al. Programmable adaptive security scanning for networked microgrids[J]. Engineering，2021，7(8)：1087-1100.

[8] CHEN B R，WU Q H，LI M S，et al. Detection of false data injection attacks on power systems using graph edge-conditioned convolutional networks [J]. Protection and Control of Modern Power Systems，2023，8(2)：1-12.

[9] XIAHOU K S，LIU Y，WU Q H. Decentralized detection and mitigation of multiple false data injection attacks in multiarea power systems[J]. IEEE Journal of Emerging and Selected Topics in Industrial Electronics，2022，3(1)：101-112.

[10] XIAHOU K S，LIU Y，WU Q H. Robust load frequency control of power systems against random time-delay attacks[J]. IEEE Transactions on Smart Grid，2021，12(1)：909-911.

[11] XIAHOU K S，XU X Y，HUANG D Y，et al. Sliding-mode perturbation observer-based delay-independent active mitigation for AGC systems against false data injection and random time-delay attacks[J]. IEEE Transactions on Industrial Cyber-Physical Systems，2024，2：446-458.

[12] LIU M X，ZHAO CH CH，DENG R L，et al. False data injection attacks and the distributed countermeasure in DC microgrids [J]. IEEE Transactions on Control of Network Systems，2022，9(4)：1962-1974.

[13] KHALGHANI M R，SOLANKI J，SOLANKI S K，et al. Resilient frequency control design for microgrids under false data injection[J]. IEEE Transactions on Industrial Electronics，2021，68(3)：2151-2162.

[14] LI F F，TANG Y. False data injection attack for cyber-physical systems with resource constraint [J]. IEEE Transactions on Cybernetics，2020，50(2)：729-738.

[15] HU L，WANG Z D，HAN Q L，et al. State estimation under false data injection attacks：Security analysis and system protection[J]. Automatica，2018，87：176-183.

[16] REN X X，YANG G H. Adaptive control for nonlinear cyber-physical systems under false data injection attacks through sensor networks [J]. International Journal of Robust and Nonlinear Control，2020，30(1)：65-79.

[17] SHEREEN E，KAZARI K，DÁN G. A reinforcement learning approach to undetectable attacks against automatic generation control[J]. IEEE Transactions on Smart Grid，2024，15(1)：959-972.

[18] AMELI A，HOOSHYAR A，EL-SAADANY E F，et al. Attack detection and identification for automatic generation control systems[J]. IEEE Transactions on Power Systems，2018，33(5)：4760-4774.

[19] 张国澎，郑钰麒，郑征，等. 含混合储能直流微电网混合势函数建模及稳定性分析[J]. 国外电子测量技术，2023，42(4)：38-48.
ZHANG G P，ZHENG Y Q，ZHENG ZH，et al. Hybrid potential function modeling and stability analysis of DC microgrid with hybrid energy storage[J]. Foreign Electronic Measurement Technology，2023，42(4)：38-48.

[20] 文云峰，杨伟峰，林晓煌. 低惯量电力系统频率稳定

分析与控制研究综述及展望[J]. 电力自动化设备，2020，40(9)：211-222.
WEN Y F，YANG W F，LIN X H. Review and prospect of frequency stability analysis and control of low-inertia power systems [J]. Electric Power Automation Equipment，2020，40(9)：211-222.

[21] 张剑云，李明节. 新能源高渗透的电力系统频率特性分析[J]. 中国电机工程学报，2020，40(11)：3498-3507.
ZHANG J Y，LI M J. Analysis of the frequency characteristic of the power systems highly penetrated by new energy generation[J]. Proceedings of the CSEE，2020，40(11):3498-3507.

[22] 魏玮，吕游，齐欣宇，等. 基于CNN-LSTM-AM动态集成模型的电站风机状态预测方法[J]. 仪器仪表学报，2023，44(4)：19-27.
WEI W，LYU Y，QI X Y，et al. State prediction method for power plant fans based on the CNN-LSTM-AM dynamic integrated model[J]. Chinese Journal of Scientific Instrument，2023，44(4)：19-27.

[23] 龚浩岳，周勤勇，郭强，等. 高比例新能源接入场景电力系统频率分析模型改进与应用[J]. 电网技术，2021，45(12)：4603-4612.
GONG H Y，ZHOU Q Y，GUO Q，et al. Improvement and application of frequency analysis modules for power system in high proportion of renewable energy situation [J]. Power System Technology，2021，45(12)：4603-4612.

[24] 刘鹏辉，郑克影，朱军，等. 考虑负荷动态变化的孤岛微电网二次频率控制[J]. 电子测量与仪器学报，2024，38(6)：213-224.
LIU P H，ZHENG K Y，ZHU J，et al. Secondary frequency control of isolated microgrid with consideration of dynamic varying loads[J]. Journal of Electronic Measurement and Instrumentation，2024，38(6)：213-224.

[25] ZHOU T L，XIAHOU K S，ZHANG L L，et al. Real-time detection of cyber-physical false data injection attacks on power systems [J]. IEEE Transactions on Industrial Informatics，2021，17(10)：6810-6819.

[26] DENG R L，ZHUANG P，LIANG H. False data injection attacks against state estimation in power distribution systems[J]. IEEE Transactions on Smart Grid，2019，10(3)：2871-2881.

[27] 吴振龙，刘艳红，薛亚丽，等. 基于预期动态方程的含高比例可再生能源孤岛运行微电网负荷频率控制[J]. 上海交通大学学报，2024，58(6):954-964.
WU ZH L，LIU Y H，XUE Y L，et al. Load frequency control of lslanding micro-grid with high-proportiona renewable energy based on desired dynamics equation[J]. Journal of Shanghai Jiao Tong University，2024，58(6)：954-964.

作者简介

林鼎杰，硕士研究生，主要研究方向为新能源电力系统信息物理安全。
E-mail:eplindj@mail.scut.edu.cn

夏候凯顺(通信作者)，博士，副教授，主要研究方向为新能源电力系统信息物理安全与控制。
E-mail：xiahouks@scut.edu.cn