

信息物理协同攻击在新型电力系统中的分析、 建模与防御策略综述

黄辉辉, 魏强, 耿洋洋, 吴茜琼, 陈昊文

(信息工程大学网络空间安全学院, 河南 郑州, 450001)

摘要: 新型电力系统信息物理深度融合加剧了网络安全风险, 信息物理协同攻击 (cyber-physical coordinated attack, CCPA) 通过跨域路径对系统的稳定性构成重大威胁。针对新型电力系统信息物理深度融合的特点, 对CCPA建立了“攻击特征-建模方法-防御策略”三位一体的研究体系。首先, 识别新型电力系统面临的攻击类型, 构建“感-传-决-控”闭环威胁分析模型, 解构CCPA过程的多阶段协同特征与级联失效机理; 其次, 基于信息-物理域耦合接口威胁分析, 构建多维度建模技术分类体系, 探讨CCPA在复杂建模中面临的挑战和不同实际场景下的差异性; 最后, 融合博弈论与多目标优化理论, 综述了跨学科、多层次的防御策略框架, 并指出其在实际应用中面临的挑战。研究结果可为提升新型电力系统的安全性和韧性提供理论依据和实践指导。

关键词: 信息物理协同攻击; 感-传-决-控; 耦合威胁; 攻击建模; 防御策略; 新型电力系统安全

中国分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2025042

Cyber-physical coordinated attack: a review of analysis, modeling and defense strategies in next-generation power systems

HUANG Huihui, WEI Qiang, GENG Yangyang, WU Qianqiong, CHEN Haowen

School of Cyberspace Security, Information Engineering University, Zhengzhou 450001, China

Abstract: The deep cyber-physical integration in next-generation power systems was found to exacerbate cybersecurity risks, among which cyber-physical coordinated attacks (CCPA) were identified as significant threats to system stability through cross-domain pathways. To address the characteristics of deep cyber-physical integration in modern power systems, a tripartite research framework focusing on “attack characteristics – modeling methods –

收稿日期: 2025-03-05; 修回日期: 2025-06-24

通信作者: 黄辉辉, huanghui2015@whu.edu.cn

基金项目: 国家自然科学基金 (61833015); 中原科技创新领军人才计划项目 (224200510002)

Foundation Items: The National Natural Science Foundation of China (61833015), Zhongyuan Leading Talents in Science and Technology Innovation Program (224200510002)

引用格式: 黄辉辉, 魏强, 耿洋洋, 等. 信息物理协同攻击在新型电力系统中的分析、建模与防御策略综述[J]. 网络与信息安全学报, 2025, 11(4): 50-72.

Citation Format: HUANG H H, WEI Q, GENG Y Y, et al. Cyber-physical coordinated attack: a review of analysis, modeling and defense strategies in next-generation power systems[J]. Chinese Journal of Network and Information Security, 2025, 11(4): 50-72.

defense strategies” was established. Attack types faced by emerging power grids were systematically identified, and a closed-loop “sense – transmit – decide – control” (STDC) threat analysis model was developed to dissect the multi-stage coordinated features and cascading failure mechanisms of CCPA. Through threat analysis conducted at the coupling interfaces between the information and physical domains, a multi-dimensional modeling taxonomy was constructed to explore the complex modeling challenges and differences present in actual scenarios during the evolution of CCPA. By integrating game theory and multi-objective optimization theory, a cross-disciplinary defense framework with hierarchical coordination was proposed, while practical implementation challenges were highlighted. The research findings provide theoretical foundations and actionable insights for enhancing the security and resilience of next-generation power systems.

Keywords: cyber-physical coordinated attack, sense-transmit-decide-control, coupled threat, attack modeling, defense strategy, new-type power system security

0 引言

随着全球能源转型的加速推进，电力系统正经历从传统机电一体化向信息物理深度融合的新型范式变革。然而，这种深度融合导致网络安全边界日益模糊，催生出信息物理协同攻击（cyber-physical coordinated attack, CCPA）这一新的威胁形态。CCPA通过跨域协同的攻击路径，能够对电力系统实施多阶段、多维度的级联破坏，其危害程度从设备级、系统级逐步升级至全域级^[1]。2015年乌克兰电网遭遇网络攻击导致23万用户断电，以及2022年俄乌冲突期间持续升级的电网网络战^[2]等典型案例，充分证明了此类攻击的现实威胁。在此背景下，开展新型电力系统CCPA防御机制研究，对于实现电力基础设施安全保障具有重要的理论意义。

（1）新型电力系统的安全挑战

当前，国际网络安全格局正经历深刻变革，电力系统的安全防护要求持续升级。在政策层面，美国国家标准与技术研究院（national institute of standards and technology, NIST）发布的《网络安全框架》（CSF）2.0将能源系统列为最高优先级防护对象，强调信息物理系统（cyber physical system, CPS）的纵深防御体系建设；欧盟《数字市场法案》（DMA）则要求电网运营部署具备实时威胁感知能力的防御系统。在技术标准方面，工业自动化和控制系统安全标准（IEC 62443-4-1: 2021）新增对多域协同攻击的防护要求，而ISO/IEC 27032:2012首次将电力信息物理系统纳入网络空间安全防护范畴，为CCPA防御提供了标准依据。攻击手段也在不断

演进，MITRE ATT&CK框架2023版新增了9项针对电力系统的攻击战术（T1560-T1568），其中基于物联网设备的CCPA占比高达37%^[3]。

新型电力系统呈现出三大特征。①能源结构加速转型：风电、光伏装机突破12亿千瓦，新能源发电占比超35%^[4]。②系统形态深度重构：虚拟电厂、微电网等新型市场主体超2 000个，电力市场交易向实时化方向发展^[5]。③控制模式革新升级：省级以上电网实现全景监控全覆盖，控制指令与数据流交互达到毫秒级。这些变革带来了双重安全挑战：在物理层，新能源设备通信接口数量激增4~6倍，导致攻击面扩大40%；在信息层，毫秒级实时交互需求，导致传统边界防护机制面临失效风险^[6]。针对这些挑战，学术界已展开深入研究。蔡晔等^[7]于2021年率先构建了基于线路攻击代价指标的CCPA识别框架，通过量化信息-物理耦合强度来辨识电网薄弱环节，揭示了多阶段攻击的代价敏感特性。刘依晗等^[8]于2022年开发了跨域连锁故障演化模型，通过信息域扰动注入实验验证了CCPA对电力域的级联放大效应。这些研究揭示了CCPA对新型电力系统“感-传-决-控”闭环的全链条威胁，凸显了构建适应性防御体系的紧迫性。

（2）研究现状与不足

近年来，国内外学者围绕CCPA问题开展了系统性研究，研究视角已从传统电力系统的防御架构逐步拓展至新型电力系统的场景适配，具体研究进展如表1所示。

结合表1对研究进展的系统梳理，可从以下维度总结其演进路径。

表 1 信息物理电力系统（CCPS）协同攻击研究进展

Table 1 Research progress on cooperative attacks in cyber-physical power systems (CCPS)

文献及其提出年份	研究内容	核心方法	主要贡献	存在的不足
文献[9], 2019 年	综述 CPPS 建模与评估方法	提出分层防御架构模型	梳理传统电力系统攻击路径框架; 构建基础防御体系架构	未分析跨域攻击的传播时序特征; 缺乏对“信息-物理-信息”循环攻击模式的系统性描述
文献[10], 2021 年	分析信息失效威胁下的安全评估方法	构建多维度的风险评估指标体系	完善风险量化评估维度; 提出多指标综合评估框架	未充分考虑新型电力系统的通信时延敏感性; 未建立时延敏感设备(如保护继电器)的攻击阈值模型
文献[11], 2022 年	研究模型与数据双驱动的动态防护策略	提出联邦学习框架, 用于实现知识共享	融合数据驱动与控制模型; 设计分布式协同防御机制	未建立攻击行为与物理响应的定量映射关系; 缺乏对控制指令物理语义的攻击影响量化分析
文献[12], 2022 年	CCPS 测试床分类研究	提出标准化测试环境构建方法	完善测试床验证体系; 推动标准化测试环境建设	未验证数字孪生体在新型电力系统中的应用场景; 测试床未包含高比例可再生能源场景
文献[13], 2024 年	智能检测技术研究	基于 LSTM 网络的攻击行为预测模型	建立时序攻击行为预测模型; 提出智能检测技术优化路径	未充分适配新型电力系统通信协议的多样性; 未考虑 IEC 61850 与 Modbus 协议的攻击面差异
文献[14], 2025 年	协同攻击防御方法综述	提出博弈论框架下的防御策略优化	构建基于博弈论的防御分析框架; 提出差异化的防御资源配置方案	未区分传统电网与新型电力系统的防御需求差异

1) 攻击分析层面。早期研究（2019 年前）聚焦于传统电力系统攻击路径框架构建。王琦等^[9]提出分层防御架构模型，系统梳理了物理层设备攻击、网络层通信渗透等典型威胁路径。随着新型电力系统的发展（2020 年后），研究重点转向新能源接入带来的异构性挑战。Yohanandhan 等^[12]构建了多物理场耦合仿真模型，该模型支持储能系统、SiC/GaN 器件等新型设备特性的分析。Feng 等^[14]提出基于博弈论的防御框架，尝试区分传统电网与虚拟电厂等新兴场景的防御需求差异。

2) 建模方法层面。建模技术演进呈现两大方向，具体如下。①数据驱动与物理机理融合方面：朱炳铨等^[10]分析了信息失效威胁下的安全评估方法，构建了多维度的风险评估指标体系，为跨域风险的量化评估提供了基础框架。杨杰等^[11]提出的联邦学习框架，实现了控制指令物理语义与数据驱动异常检测的协同分析，提升了攻击识别的准确性。②多域耦合仿真技术方面：Yohanandhan 等^[12]提出的多物理场耦合模型首次将电力电子器件的动态特性纳入仿真体系，显著提升了建模精度。

3) 防御策略创新层面。研究主要从检测技术优化、资源动态分配和标准化体系建设 3 个方面展开。Tooki^[13]提出基于 LSTM 网络的时序预测模型，有

效增强了攻击行为识别的时效性。Feng 等^[14]通过博弈论框架优化防御资源配置，理论上可使响应效率提升 22%。Yohanandhan 等^[12]推动 CPPS 测试床的标准化建设，为新型电力系统场景下的防御策略验证提供了标准化的实验平台与技术支撑。

尽管已有研究取得了一定进展，但仍存在以下局限性。

1) 跨域攻击机理揭示不足：现有研究多聚焦单一攻击路径（如文献[9]），缺乏对“信息渗透→物理效应放大→信息反馈增强”闭环机制的系统分析。

2) 建模方法适配性受限：新型电力系统拓扑结构和运行状态具有时变性，使得系统本身和攻击行为的建模难度显著提升，现有模型（如文献[10-11]的联邦学习框架）未建立攻击行为特征与物理系统响应之间的定量映射关系。

3) 新型场景防御策略缺失：CCPA 的本质是利用信息空间与物理空间的深度耦合特性，通过跨信息-物理域的协同攻击路径形成闭环攻击链，实施多阶段、递进式破坏。然而，现有防御机制（如文献[12-14]）多采用孤立防护策略，缺乏对攻击路径动态演化的全局感知能力，导致防御响应的时效性与整体性不足。

上述不足表明，在新型电力系统深度融合的背景下，现有研究对 CCPA 的威胁认知仍停留在

单一域分析层面，跨域耦合建模精度难以匹配系统时变特性，防御策略缺乏对攻击链动态演化的适应性响应，存在显著提升空间。针对上述问题，本文将从构建“感-传-决-控”闭环的威胁分析框架、创新跨域耦合建模方法和构建弹性防御体系3个维度展开深入研究，旨在为新型电力系统应对CCPA威胁提供系统性的理论支撑与可落地的实践指导。

1 信息物理协同攻击分析

本节围绕新型电力系统中CCPA的演化机理与防御需求开展递进式分析。首先，对典型CCPA进行分类，明确不同攻击的载体类型与作用对象；然后，以新型电力系统的“感-传-决-控”闭环结构为切入点，逐一剖析感知层、传输层、决策层和控制层的具体攻击形式；最后，提炼出CCPA的多阶段协同与动态博弈特征。该分析框架不仅为

后续跨学科威胁模型的搭建提供了理论支撑，还为分层防御策略的制定奠定了逻辑基础。

1.1 电力系统面临的攻击分类

基于Hahn等学者提出的针对CPPS的攻击模型^[15-16]，CPPS主要面临以下5类威胁，如图1所示。

1) 传感器设备攻击：通过虚假数据注入、传感器致盲（如GPS欺骗）或电磁信号干扰，破坏数据采集的可靠性，导致物理过程感知偏差^[17-18]。

2) 执行器攻击：对断路器等物理执行设备实施有限能量攻击（如数据包丢失、控制信号抑制），或通过信号屏蔽实施有界攻击，直接导致设备响应延迟、拒动或误动，破坏物理层的正常操作流程^[19]。

3) 计算机系统攻击：利用恶意代码（如木马、病毒）或拒绝服务（DoS）攻击侵入数据采集与监控系统（SCADA）、电网调度系统（EMS）等核心控制系统，破坏系统数据的完整性与可用

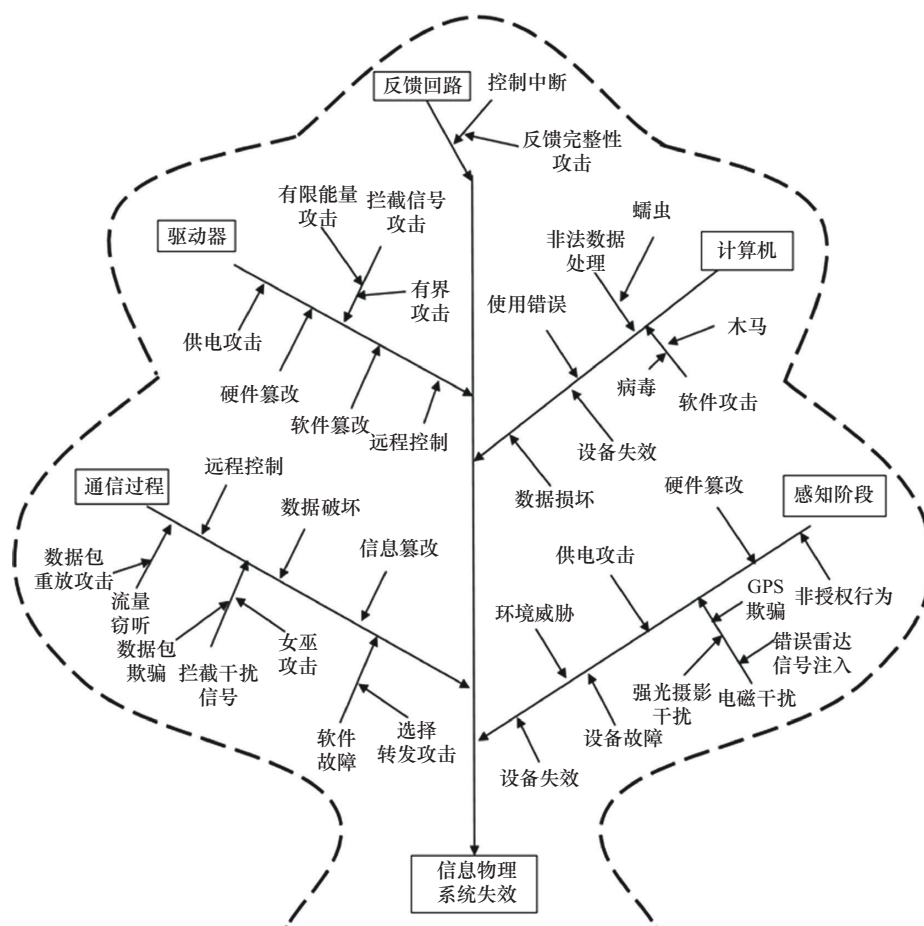


图1 CPPS面临的威胁树状图

Figure 1 Threat tree diagram of CPPS

性；部分攻击通过伪造测量误差掩盖恶意操作，增加攻击检测难度^[20-21]。

4) 通信过程攻击：针对电力专用通信网实施数据包欺骗、重放攻击或 Sybil 攻击（伪造节点身份），干扰信息传输信道，导致控制指令等关键数据失真或丢失^[18,22]。

5) 反馈回路攻击：通过篡改电压、电流等反馈信号的测量值，破坏闭环控制精度，可能引发发电机功角振荡、电压失稳等连锁反应，对系统的稳定性造成威胁^[15,23]。

上述攻击类型系统阐明了 CPPS 的固有脆弱性，为解析新型电力系统面临的复合型安全威胁提供了理论框架。然而，电力系统安全风险的本质并非仅源于单一组件或环节的脆弱性，更在于信息层与物理层之间深度耦合的动态交互过程。

1.2 “感-传-决-控”广义闭环中的安全风险

CPPS 在“感-传-决-控”广义闭环中的安全

风险如图 2 所示^[24]。

1) 感应阶段：攻击者通过数据完整性攻击伪造传感器测量数据，干扰调度决策^[25]；或利用重放攻击篡改控制指令时序，破坏“测量-控制”的时序协同性^[26]。

2) 传输过程：在测量数据与控制命令传输过程中，极光攻击可通过远程操控断路器开关状态，破坏电网功率平衡，引发低频振荡^[27]；虚假数据注入与负载再分配攻击相结合，会误导潮流计算，导致线路过载风险提升^[28-29]；而 DoS 攻击通过掩盖攻击痕迹，延长防御响应窗口期，造成损害扩大化^[30]。

3) DoS 攻击通过流量淹没目标网络，可直接导致光伏 SCADA 系统瘫痪^[31]；隐形攻击、摆渡攻击、水坑攻击、SQL 注入、缓冲区溢出、命令注入等手段，可突破安全边界，实现对调度指令、执行器控制信号的恶意篡改^[32-34]。

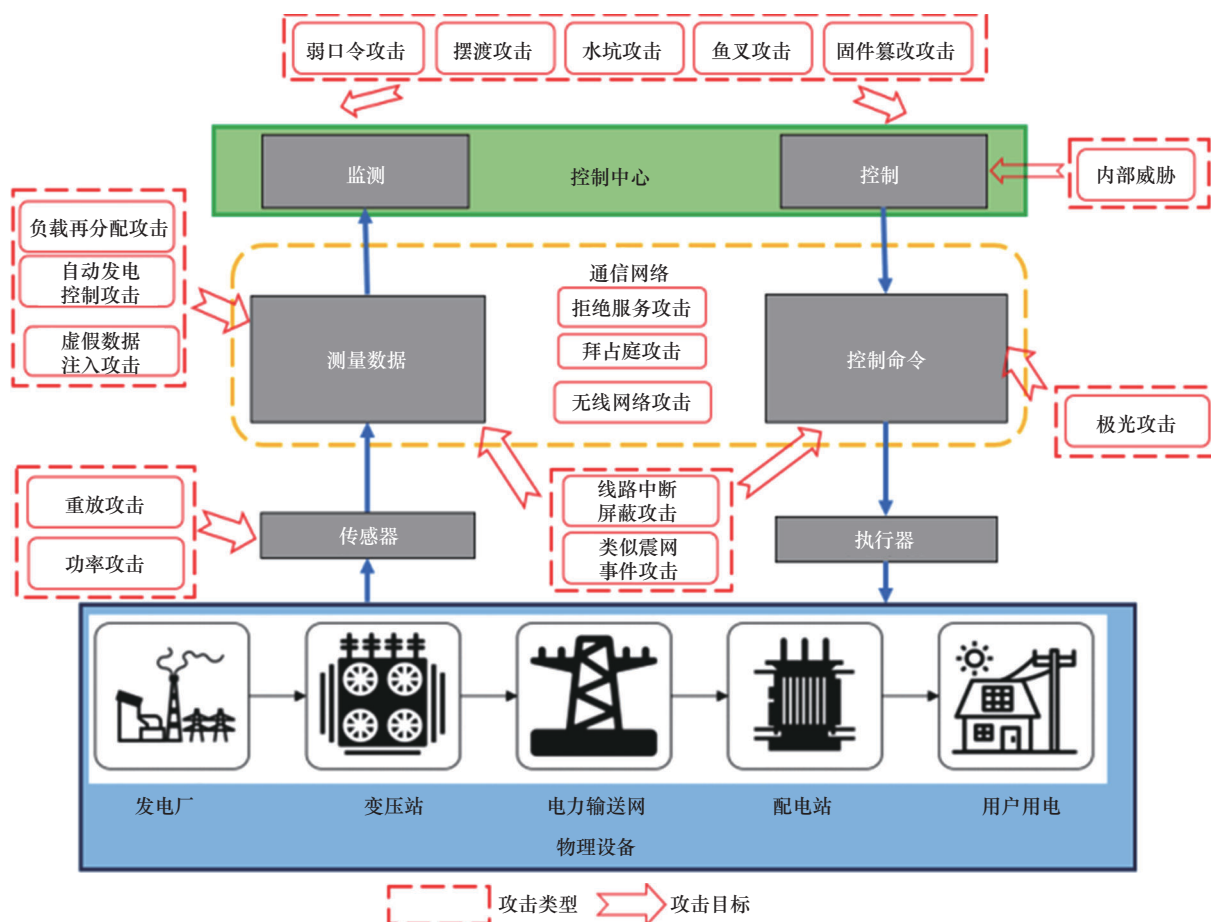


图 2 CPPS 在“感-传-决-控”广义闭环中的安全风险

Figure 2 Security risks in the broad sense closed loop of “sensing-transmission-decision-control”

这些攻击不仅暴露了电力系统在“感-传-决-控”各环节的固有脆弱性，更揭示了系统内部信息组件与物理组件之间耦合交互的复杂性。尤其在新能源高比例接入的场景下，这种复杂性被进一步放大，单一环节的攻击可能触发多阶段协同破坏，最终引发系统级的连锁故障，造成更大的损害。

1.3 电力信息物理协同攻击过程及特征

在电力系统的“感-传-决-控”闭环中，信息域与物理域的双向耦合是协同攻击的核心诱因，其通过跨域攻击路径形成级联失效链，直接威胁系统的安全稳定运行。下述典型案例清晰印证了这一特征^[35]。2010年，Stuxnet病毒通过篡改离心机传感器的转速数据（信息层欺骗），诱导物理设备偏离正常运行参数，最终引发核设施离心机异常振动并停机；2015年，BlackEnergy

恶意软件利用SCADA协议漏洞伪造电网拓扑数据（控制层篡改），导致乌克兰电网调度决策误判，触发物理层断路器批量跳闸，造成大范围停电；2017年，ARP（Address Resolution Protocol）缓存投毒攻击通过局域网协议欺骗劫持风电场控制指令（网络层渗透），致使频率调节失效；2019年，委内瑞拉水电站攻击则通过篡改水轮机保护逻辑（决策层逻辑注入），导致物理层设备保护误动，引发全网级联跳闸。这些攻击均呈现信息-物理域闭环破坏特征：攻击者利用信息层漏洞（如协议欺骗、数据篡改）触发物理层故障（如设备过载、保护误动），而物理层失效又通过状态估计偏差、控制指令失真等反馈机制放大信息层攻击效果，形成跨域协同的级联失效链。图3所示的CCPA攻击链，攻击者通过信息-物理域的协同作用，破坏电网状态估计功能，形成闭环

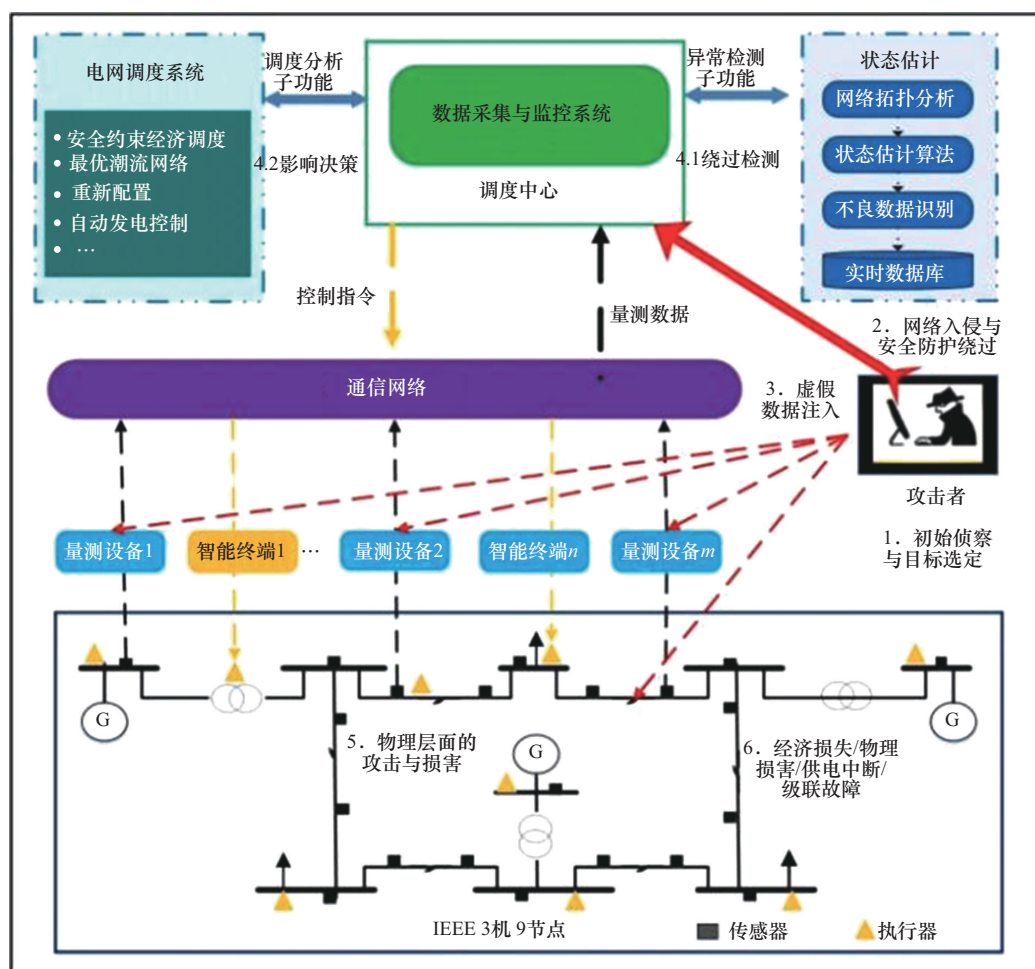


图3 针对状态估计的CCPA攻击过程

Figure 3 CCPA attack process for state estimation

破坏效应，具体演化路径如下。

1) 跨域渗透阶段（步骤1和2）：攻击者首先对调度中心的网络拓扑、状态估计算法原理及量测设备分布进行智能侦察，识别SCADA/EMS中的协议漏洞、防护薄弱点及量测盲区。

2) 双向攻击实施（步骤3和5）：信息层与物理层攻击同步推进。信息层通过伪造电压/功率量测数据（如虚报线路负荷）、注入虚假拓扑信息等手段，诱导状态估计结果偏离真实工况；物理层则同步触发断路器误动、负荷恶意投切等操作，人为制造物理扰动，进一步扩大状态估计误差的传播范围。

3) 闭环放大效应（步骤3、4和5）：状态估计偏差直接导致调度决策失真（如误判线路过载），继而触发自动保护装置动作或下发人工干预指令，形成“信息误判→物理响应失当→新攻击窗口暴露”的级联失效链。

4) 级联故障终结（步骤6）：最终引发电网频率崩溃、区域停电等灾难性后果，造成经济损失与社会影响的双重损害。

CCPA通过信息层漏洞与物理层失效的动态耦合，构建起“攻击-反馈-再攻击”的增强链路，从而突破传统单层防御的边界。其核心威胁在于攻击路径的跨域协同性与闭环自增强特性。国际信息安全组织将CCPA定义为“由信息域发起，在物理域产生实质影响”的跨域协同攻击模式^[36]。为系统解析CCPA攻击路径的跨域耦合特性，本文提出图4所示的基于网络域（C）与物理域（P）的攻击分类框架，其攻击路径可分为以下两类。

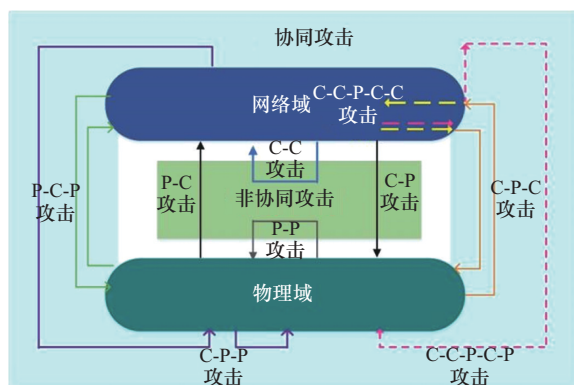


图4 CPPS中跨域攻击路径示意图

Figure 4 Diagram of cross-domain attack paths in CPPS

1) 非协同跨域攻击：该类攻击包含单向跨域路径（ $C \rightarrow P$ 、 $P \rightarrow C$ ）攻击和同域攻击（ $C \rightarrow C$ 、 $P \rightarrow P$ ），其特点是攻击行为局限于单一方向或域内。文献[34]中仅通过 $C \rightarrow P$ 路径实施的虚假数据注入攻击便是典型的非协同攻击案例。该攻击仅通过篡改信息层的量测数据影响物理层决策，并未利用物理层的状态反馈来优化攻击手段。

2) 协同跨域攻击：该类攻击涵盖双向渗透路径（如 $P \rightarrow C \rightarrow P$ 、 $C \rightarrow P \rightarrow C$ ）及复杂多阶段路径（如 $C \rightarrow C \rightarrow P \rightarrow C \rightarrow P$ ），其核心特征在于信息域与物理域的动态闭环耦合。图3所示的 $C \rightarrow C \rightarrow C \rightarrow C \rightarrow P \rightarrow P$ 攻击链（即智能侦察→网络渗透→数据篡改→决策干扰→物理破坏→级联失效”的6阶段闭环流程）便是典型的协同跨域攻击。

基于CCPA的攻击链特征分析，其核心威胁可归纳为以下3点。

1) 跨域闭环破坏机制：CCPA具有明显的跨域交互特性，攻击者通过信息域与物理域的双向耦合作用形成级联破坏效应。

2) 多阶段复合攻击手段：CCPA是攻击者精心策划的多阶段协同攻击，通过组合信息域与物理域的攻击技术（如网络入侵、虚假数据注入攻击、物理攻击等），实现对电网监控与控制系统的误导。

3) 动态博弈对抗本质：CCPA过程是一个动态且复杂的策略竞争过程，攻防双方遵循“探测-响应-演化”的实时对抗模式，攻击者持续挖掘系统的脆弱性，而防御者则依赖监测机制进行快速响应。

相较于传统网络攻击（如信息窃取或物理功能破坏），CCPA具有以下4个核心差异特征。

1) 跨域交互性（空间维度）：突破传统攻击的域内限制，形成“信息扰动→物理效应→信息反馈”的跨域破坏路径。

2) 多阶段协同性（时间维度）：攻击行为包含侦察、入侵、数据操纵、物理破坏等多阶段时序配合，攻击时序涵盖毫秒级数据篡改（ $C \rightarrow C$ ）至分钟级设备损毁（ $P \rightarrow P$ ）的多尺度叠加。

3) 隐蔽性与级联放大效应（效果维度）：信息攻击掩盖物理攻击痕迹，物理故障通过信息反馈加剧系统崩溃，形成“信息渗透→物理效应放

大→信息反馈增强”的闭环。

4) 动态博弈性（行为维度）：攻击者能够实时感知防御措施并动态调整攻击策略，形成“攻击试探→防御响应→攻击演化”的闭环博弈过程。传统攻击模型（如MITRE ATT&CK框架）难以刻画这种跨域动态耦合特征，需要构建分层交互式建模框架来揭示CCPA双向反馈机制的演化规律。

2 信息物理协同攻击建模

威胁建模作为CCPA防御体系的认知基石，本文通过构建跨学科分析框架阐明其多域耦合机制，为防御策略的数学建模提供理论支撑。本文从耦合接口的威胁分析切入，系统梳理建模技术分类，深入探讨CCPA建模面临的挑战，并基于实际应用场景验证不同建模方法的性能差异。本文构建的方法体系为量化分析CCPA威胁传播规律提供了结构化分析范式。

2.1 新型电力系统耦合接口威胁分析

CPPS的核心特征表现为物理系统与网络系

统在多层次时空尺度上的深度融合。物理系统由发电机、变压器、输电线路和动态负载等组成，直接参与能量流的传输与转换。网络系统则通过通信网络实现各组件间的信息流交互。两类系统在拓扑结构上的差异性，使得其交互接口成为系统脆弱性的关键所在。基于文献[37]的3层架构划分耦合接口（组件级→通信基础设施→广域网络），每个层级涉及特定组件与交互接口，具体结构如图5所示。

第1层耦合交互发生在电力系统核心组件（如发电机、变压器、输电线路和动态负载）与控制器之间，依赖精确的信息反馈优化电网运行。攻击者可通过篡改传感器数据（如GPS欺骗）或控制器指令（如DoS攻击），直接破坏能量流传输的稳定性^[38-41]。

第2层耦合交互聚焦于电力系统控制与通信基础设施的互动，通信基础设施负责协调电网CPS中各子系统（包括传感器、执行器、接口、控制、计算和通信单元）间的通信传输。其脆弱性主要体现在两方面：一是传输时延，尽管5G

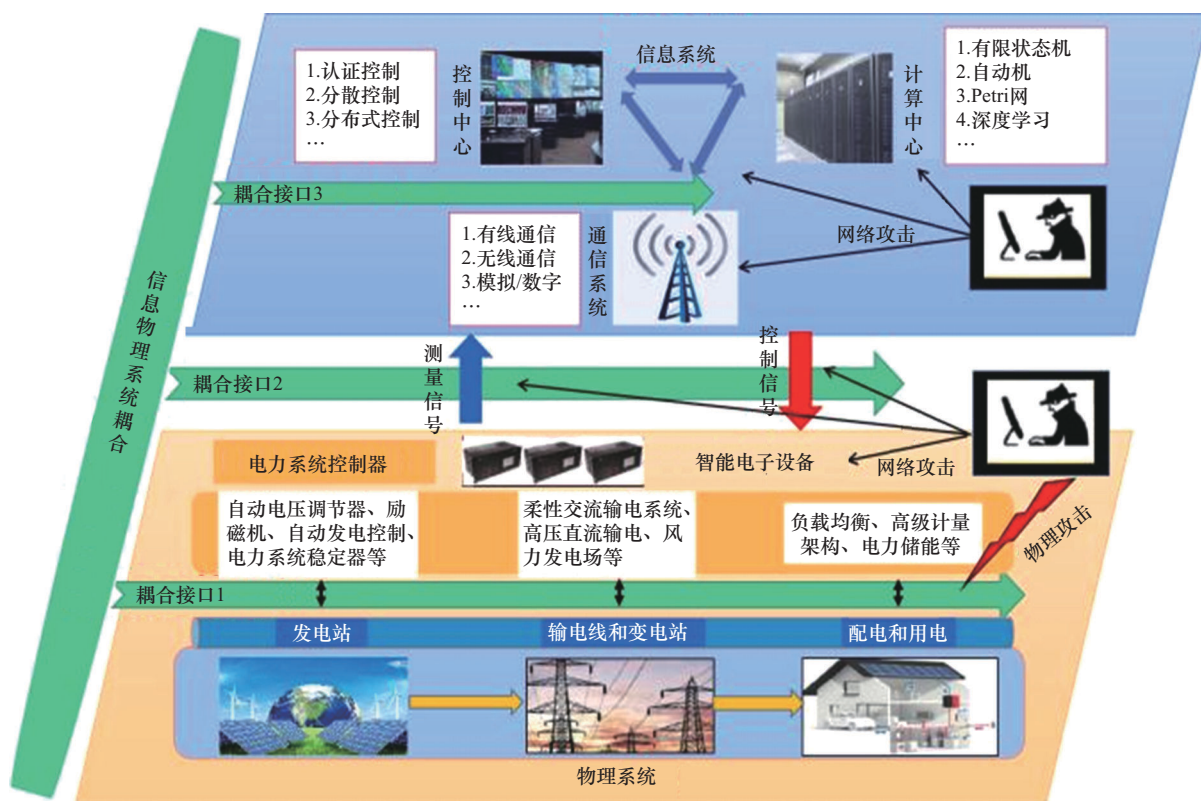


图5 CPPS结构

Figure 5 Structure of CPPS

通信时延小于 1 ms, 但攻击者通过流量压制可使同步相量测量单元 (phasor measurement unit, PMU) 的数据更新周期延长至 50 ms, 导致状态估计误差率上升^[42-43]; 二是协议漏洞, IEC 61850 协议栈的 MMS (manufacturing message specification) 服务存在未加密传输缺陷, 攻击者可借此伪造 GOOSE (generic object oriented substation event) 报文触发保护误动^[44-45]。

第 3 层耦合交互发生在通信基础设施与更广泛的网络系统之间, 涉及主从系统、通信服务器、双向通信结构、高性能计算站、智能控制应用软件和安全防护设备等关键网络系统组件。该层次的风险不仅涵盖数据传输, 还包括负载预测、状态估计、无功优化、电压控制、振荡监测、广域监测与控制、运营规划、模型验证和稳定性分析等高级操作的安全性^[46-51]。

表 2 阐释了新型电力系统中 10 类核心功能组件 (包括自动电压调节、负载均衡、高级计量等关键模块) 的跨域耦合特征与安全风险等级, 揭示了组件间的交互漏洞对系统稳定性的级联影响。深度解析这些耦合交互机制不仅能够构建攻击路径的拓扑映射关系, 还能为防御策略设计提供跨组件交互风险的量化评估依据。

2.2 新型电力系统威胁建模方法

本节提出 3 类建模范式, 从物理机理、交互行为到系统依赖性构建多维度分析框架, 覆盖从底层设备交互到高层策略博弈的完整威胁链路。

表 3 归纳了 CPPS 的建模方法。可将这些建

模方法归为以下 3 种类型。

1) 耦合建模 (信息-物理接口的动态交互分析): 该方法聚焦物理组件与网络系统的接口特性, 采用混合系统理论构建数学模型。例如, 通过结合微分方程 (描述发电机、变压器等连续动态过程) 与差分方程 (描述通信协议、控制指令等离散事件), 借助 ADC/DAC 接口实现对信号转换的精确建模^[58-61]。在实际场景中, 可用于分析 GPS 欺骗对同步 PMU 的影响, 进而揭示数据采集频率与控制指令时延的耦合关系。

2) 交互建模 (跨域行为的动态博弈分析): 通过图形化与仿真手段刻画物理层-信息层的交互影响。例如, 图形模型基于图论构建电网拓扑与通信网络的关联图谱, 识别关键节点 (如控制中心) 的级联失效路径^[62-65]; Petri 网模型模拟分布式能源并网场景下的多状态切换过程, 量化攻击者对虚拟电厂调度策略的干扰效果^[66-69]; 攻击图模型结合网络漏洞 (如 IEC 61850 协议缺陷) 与物理脆弱性 (如断路器误动阈值), 生成多阶段攻击路径^[70-75]。

3) 依赖建模 (系统级风险传播机制): 从全局视角分析物理层与网络层的强耦合依赖关系。例如, 机制模型通过能量流-信息流混合仿真, 评估新能源高渗透率场景下频率调节与通信带宽的动态平衡^[78-84]; 概率模型引入博弈论框架, 量化攻击者与防御者的策略互动 (如攻击成本与防御资源分配的纳什均衡)^[85-87]; 仿真验证基于 OpenDSS 与 NS-3 联合仿真平台, 复现 2015 年乌

表 2 新型电力系统中核心功能组件耦合关系

Table 2 Coupling relationships among core functional components in new type power systems

组件	耦合方式	耦合频率	脆弱等级	典型攻击场景
传感器	数据采集与传输	高频	高危	GPS 欺骗导致量测值失真
执行器	指令执行与反馈	高频	高危	断路器拒动引发级联跳闸
控制中心	控制策略生成与下发	中频	高危	恶意代码篡改调度计划
通信网络	数据交互与传输时延	高频	极高危	DDoS 攻击导致通信中断
数据管理系统	数据存储与处理	中频	高危	模型篡改引发频率崩溃
设备状态监测	状态更新与故障诊断	高频	高危	伪造传感器数据诱导误诊
负荷控制系统	负荷分配与调节	中频	高危	负荷分配指令篡改
电网拓扑监控	拓扑更新与网络重构	中频	中危	虚假拓扑数据注入
安全防护系统	安全更新与修复	低频	高危	安全设备供应链投毒
能量管理系统	能量调度与优化	中频	中危	经济调度数据篡改

表3 CPPS的建模方法
Table 3 Modeling methods for CPPS

序号	建模类别	描述	索引文献
1	物理组件	采用微分方程对电力系统的物理组件（包括发电机、变压器、输电线路等）进行建模，这些组件的状态通过时间参数化的变量加以表征，且其状态与输入值可能受到特定约束的限制	[52-53]
2	网络组件	网络组件的建模聚焦于离散状态变量，这类变量负责执行算法、开展计算及通过数字网络传输数据。它们在离散事件的驱动下完成更新，其更新过程可能受条件结构控制，以实现特定的转换功能	[54-55]
3	接口系统	涉及物理系统与网络系统之间的接口（如模数转换器和数模转换器），以及它们如何实现物理系统输出与网络系统输入之间的转换	[56-57]
4	耦合模型整合	将物理组件和网络组件的模型通过接口整合，形成一个完整的CPPS数学模型。该模型融合了连续动态与离散动态，其表达形式可采用微分方程与差分方程，或两者的混合形式	[58-61]
5	图形模型	采用图形模型对物理系统与网络系统之间的关系进行可视化呈现，包括基于图论的模型和有限状态机（FSM）模型。这类模型不仅有助于构建电网结构，还支持对各类攻击场景下的系统运行状态展开分析	[62-65]
6	Petri网模型	Petri网是一种数学建模语言，适用于描述分布式与并行系统中的状态变化及转换过程，尤其适合研究CPPS中物理系统的连续性质与网络系统的离散性质之间的交互机制	[66-69]
7	网络攻击模型	这类模型包括攻击树和攻击图，它们可展示网络攻击中可能存在的攻击路径及攻击者可能利用的系统漏洞。其中，攻击树方法适用于对受限类型攻击进行建模，而攻击图模型则用于探究攻击者如何利用系统漏洞达成目标状态	[70-75]
8	状态转换图	采用马尔可夫决策过程模拟攻击行为，以预测系统在不同攻击行为作用下的脆弱性表现	[76-78]
9	机制模型	机制模型结合了连续事件动态行为系统与离散事件静态行为系统，可用于分析CPPS中能量流与信息流的混合特性，以及物理系统与网络系统之间的相互作用机制	[79-84]
10	概率模型	这类模型包括不确定性模型和博弈论模型，可用于描述CPPS中物理系统和网络系统事件的不确定性。这些模型适用于刻画不确定条件下多个决策者之间的互动过程	[85-87]
11	仿真模型	仿真模型能够支持电力系统运营商对连续系统的动态行为与离散系统的静态行为进行集成建模。OpenDSS、OMNeT++、NS-2及NS-3等仿真工具可用于构建电力系统的仿真模型	[88-92]

克兰电网遭攻击场景，验证攻击路径从C→P→C的跨域演化过程（文献[88]重现攻击耗时缩短至实际事件的1/3）。

本节提出的3类建模范式，涵盖了从物理机理到博弈行为的多维度分析框架，不仅揭示了电力系统与网络信息系统间的动态耦合机制，还为快速构建CCPA模型提供了方法论支撑。

2.3 电力信息物理协同攻击建模方法

CCPA建模是揭示攻击机理、评估系统脆弱性与优化防御策略的核心环节。本节梳理CCPA建模方法，从攻击者与防御者的博弈对抗、多阶段攻击演化到数据驱动的动态分析，构建覆盖全攻击链的建模框架，并分析不同模型的复杂性特征。

表4归纳了CCPA的建模方法，覆盖单域攻击到跨域协同攻击的全谱系建模需求。由于CCPA建模须兼顾物理动态特性与信息博弈策略，本文采用“博弈对抗建模→时序演化仿真→

数据驱动优化→资源协同配置”的技术路线进行分析，具体如下。

1) 攻防博弈建模：策略对抗的数学刻画。通过构建攻防双方的策略竞争模型，量化攻击效果与防御成本的权衡关系。以隐蔽的物理攻击（表4序号1）为例，可采用动态电力网络中的信息物理攻击的全面建模框架（如双层优化模型或三重优化模型）。在典型应用场景中，攻击者通过伪造传感器数据（如虚报电压）掩盖断路器物理攻击，并在电网动态约束下实现攻击效果最大化。

2) 多阶段建模：攻击链的时序演化分析。该模型采用分层框架描述CCPA的动态演化过程，覆盖初始侦察、目标选择、安全防护绕过、虚假数据注入、系统决策影响到潜在物理层面攻击的全流程，每个阶段的建模均须考虑攻击者可能采用的技术和策略，并量化这些行动对电力系统的具体影响。此类模型适用于分析多阶段信息物理协同拓扑攻击（表4序号3），其中基于深度Q网

表 4 CCPA 的建模方法
Table 4 Modeling methods for CCPA

序号	攻击类型	攻击目标	攻击手段	影响范围	建模方法
1	隐蔽的物理攻击 ^[93-95]	破坏电力系统组件	网络攻击掩盖物理攻击	级联效应, 广泛停电	动态电力网络中信息物理攻击的建模框架 (如双层优化模型、三重优化模型)
2	信息物理攻击 ^[95]	实现比单独行动更显著的效果	重放攻击和优化攻击	可能导致比单一攻击更严重的后果	利用分布式柔性交流输电系统设备和主动扰动电网传输线阻抗
3	多阶段信息物理协同拓扑攻击 ^[96]	最大化物理攻击效果, 最小化攻击代价	单阶段物理攻击使线路中断, 双阶段网络攻击掩盖物理攻击	较单一攻击更加隐蔽且有效, 对电网的破坏程度更大	基于深度 Q 网络的最小攻击资源确定方法
4	考虑电压控制的信息物理协同攻击 ^[97]	最大化物理攻击效果, 最小化攻击代价	虚假数据注入攻击, 双层优化模型	协同攻击较单一攻击更加有效、隐蔽	基于 KKT 条件和 FAM 方法的单层混合整数线性规划模型
5	考虑虚假数据注入的智能电网信息物理协同攻击 ^[98]	最大化负荷损失	重放型和优化型信息物理协同攻击模型	对电力系统造成有效的负荷损失, 影响电力系统的运行状态	基于双重网络攻击下的信息物理协同攻击策略
6	面向电力信息物理系统的虚假数据注入攻击研究 ^[44]	破坏电力系统的安全性和稳定性	虚假数据注入	严重影响电力系统的运行状态	基于状态估计、轨迹预测等检测方法, 基于博弈论的攻防过程建模等
7	面向信息物理协同的电力系统攻击/防御策略 ^[99]	最大化物理攻击效果, 最小化攻击代价	蠕虫传播模型, 虚假数据注入攻击	病毒通过信息网络层的扩散对物理系统造成的破坏更大	基于邻接节点感染度的检测概率定性分析模型
8	网络攻击下电力信息-物理融合系统的风险传播及防控策略 ^[100]	最大化风险传播	网络攻击病毒在信息侧的作用过程	信息侧风险穿透边界引发物理侧风险	基于入侵容忍技术的信息-物理风险防控框架
9	电力系统网络攻击信息物理协同防御方法 ^[101]	最大化物理攻击效果, 最小化攻击代价	基于信息物理关联状态挖掘的动态权重集成孤立森林模型	潜伏的信息侧攻击活动	基于信息物理双侧信息的网络攻击协同识别方法
10	提升电力信息物理系统韧性的蓄意攻击防御及故障恢复策略 ^[102]	最大化物理攻击效果, 最小化攻击代价	基于跨域连锁故障分析和非合作零和博弈理论的防御资源分配方法	如何识别协同攻击是系统的薄弱环节	基于耦合风险均衡的主备通信路由优化方法

络的最小攻击资源确定方法可以用来优化攻击资源的最优分配。常用的建模工具包括: Petri 网, 用于刻画离散事件 (如攻击步骤切换) 与连续过程 (如潮流变化) 的交互机制; 马尔可夫决策过程, 用于量化攻击各阶段的状态转移概率与策略收益, 支撑攻击者在动态环境中实现阶段目标的最优决策。

3) 数据驱动建模: 历史经验的量化复现。基于历史攻击数据与系统运行记录构建预测分析模型。例如, 通过关联规则挖掘算法 (如 GPS 欺骗与频率波动的时序关联) 识别攻击特征; 利用 LSTM 网络预测攻击路径演化趋势。该模型的优势在于无须依赖先验知识, 适用于新型攻击模式的快速识别; 但数据获取难度较大, 且可能需要结合数字孪生等技术实现攻击场景的动态复现。

4) 综合防御优化建模: 资源分配的策略求解。基于上述模型, 在综合考虑成本、效率和系统稳定性的基础上, 通过多目标优化实现防御资源的动态调配。该建模还须进一步纳入风险评估内容, 包括评估攻击可能造成的损害、确定关键基础设施的保护优先级, 以及开发有效的防御措施以减小攻击影响。例如, 基于主动割集的电力信息物理系统饱和防御策略 (表 4 序号 4), 通过改进赋权 GN 分裂法搜索信息割面可行域, 并结合机组同调约束、功率平衡约束进行优化求解。

2.4 验证案例综述与建模差异分析

本节从微电网、虚拟电厂等典型场景切入, 分析仿真环境与实际场景的建模差异, 并通过典型案例揭示这种差异对防御策略设计的潜在影响。

表 5 展示了微电网与虚拟电厂两类场景的代表

表5 实际电力系统的验证案例综述

Table 5 Review of verification cases in actual power systems

序号	类型	标题	核心内容	关键方法/模型	验证场景/案例
1	微电网	微电网信息物理系统脆弱性分析与防御策略研究 ^[103]	微电网CPS脆弱性分析、虚假数据注入攻击检测、半实物仿真平台开发	攻击方法-对象关联矩阵、信息攻击双层规划模型、区间估计锥优化模型、卡尔曼滤波算法、RT-LAB 仿真平台	基于RT-LAB的半实物仿真平台验证攻击检测与防御策略的有效性
2		信息物理融合的孤岛微电网安全稳定运行控制研究 ^[104]	孤岛微电网在通信丢包和攻击下的协同控制策略设计	改进虚拟领航者-跟随算法、预测补偿策略、滑模控制、攻防演化博弈理论	仿真算例验证丢包与DoS攻击下控制策略的有效性
3		信息物理融合下微电网运行评估及控制研究 ^[105]	微电网CPS运行风险评估、分布式鲁棒控制、网络攻击检测与弹性控制	蒙特卡罗模拟、分布式鲁棒H ∞ 控制、动态时间弯曲距离反馈函数	IEEE标准节点系统，对微电网的安全运行进行评估和协同控制验证
4		信息物理融合环境下网络攻击的微电网弹性控制策略 ^[106]	网络攻击下微电网弹性控制策略设计，涵盖量测异常、控制信号异常、通信中断等场景	滑模观测器融合变论域模糊控制、分布式自适应滑模控制、信誉机制、自触发通信机制	仿真算例，验证弹性控制策略在攻击下的有效性
5	虚拟电厂	面向虚拟电厂的协同网络攻击模型及跨空间故障传播机理 ^[107]	虚拟电厂网络攻击跨空间传播机理分析	事件驱动-融合流模型、虚假数据注入攻击与DoS攻击建模	改进的IEEE 30节点系统仿真，验证攻击传播路径与危害量化
6		虚拟电厂网络安全研究综述及展望 ^[5]	虚拟电厂网络安全研究现状与未来方向综述	未涉及具体模型	未涉及具体案例
7		双反馈(C-P/P-C)耦合模型(本文模型)	信息层负载重新分配攻击(LRA)和物理层线路过载之间的动态反馈机制量化	双层规划、LAR与物理攻击结合、KKT转化、C-P模型与P-C模型动态交互捕捉、攻击资源约束	IEEE 14节点多场景测试，量化攻击序列对系统影响的差异化

性研究进展。在微电网场景中，研究主要聚焦于网络攻击下的微电网弹性控制策略设计。文献[103]利用RT-LAB仿真平台开展了半实物仿真，验证了攻击检测与防御策略的有效性。文献[105]结合某海岛微电网实际运行数据（含风光出力曲线、负荷波动特性），提出蒙特卡罗风险评估方法。在虚拟电厂场景中，研究着重于网络攻击的传播机理分析与跨空间故障传播机理。例如，基于事件驱动-融合流模型的网络攻击建模^[107]，构建含风电、储能单元的虚拟电厂模型，通过改进IEEE 30节点系统模拟“云平台数据篡改→本地逆变器误动作”的攻击链。

然而，现有仿真环境与实际场景在信息物理建模方面存在明显差异，具体体现在以下4个方面。

1) 动态实时性差异。现有仿真大多数采用离线批处理方式，难以准确模拟实际系统中毫秒级乃至更高速的动态交互过程^[103]。具体而言，传统实时仿真平台受限于固定的时间分辨率，往往无法精确反映电力电子器件的纳秒级开关特性，而实际CPS中CCPA的攻击窗口可能极为短暂。为提升动态实时性，建议从两个方面进行改进：

其一，采用更先进的实时仿真平台（如混合仿真架构RT-LAB+OPAL-RT），实现物理层200 μ s级与信息层10 ms级的多时间尺度协同仿真；其二，开发轻量化数字孪生模型，通过算法优化将IEEE 118节点系统等大型电网的仿真时长从小时级显著压缩至分钟级。

2) 模型复杂度差异。现有仿真系统为减轻计算负担，通常会对物理层细节进行简化处理，如在IEEE 118节点系统仿真中忽略变压器励磁涌流等复杂物理特性^[106]。然而，这些被忽略的特性可能对CCPA的传播路径产生显著影响，导致实际攻击效果与仿真预测结果存在显著偏差。为提升模型精度，建议在仿真模型中增加关键物理层细节（重点考虑变压器励磁涌流、线路分布电容效应等对系统动态特性影响显著的因素）。具体措施包括引入基于有限元分析的高保真电力设备模型、采用多物理场耦合仿真技术，实现电力系统电磁暂态与机械暂态特性的协同仿真。

3) 数据异构性与实时性差异。实际电力系统中的数据环境具有高度复杂性，多源异构数据流（如PMU毫秒级量测数据、SCADA秒级遥信数

据、IED 事件驱动型告警信息等) 并存, 且这些数据在采样频率、数据格式等方面存在显著差异。而传统仿真环境通常仅能处理单一数据源, 且多源数据的频率差异会引发攻击检测的时空不一致性 (如 PMU 与 SCADA 数据的时间失配可能使攻击隐蔽期延长)。为解决数据异构性与实时性问题, 建议从 3 个方面进行改进。①开发多源异构数据融合技术, 统一数据频率和格式; ②设计多源数据同步中间件, 利用时间戳对齐算法解决 PMU (200 Hz) 与 SCADA (1 Hz) 数据的频率失配问题; ③构建基于联邦学习的边缘计算框架, 在保护数据隐私的前提下实现多源数据的有效融合。

4) 攻击反馈机制差异: 仿真环境常将“攻击-防御”过程假设为静态模式, 实际场景中这一过程却呈现出动态反馈特性。“信息攻击→物理故障→保护动作→信息失真”这种闭环反馈机制会产生显著的攻击放大效应。然而, 现有仿真模型难以有效刻画攻击传播过程中的非线性累积效应, 这导致在模拟实际攻击过程和评估攻击后果时存在较大局限性。为提升仿真真实性, 建议构建动态反馈仿真体系, 以模拟实际的“信息攻击→物理故障→保护动作→信息失真”闭环反馈过程, 实时更新攻击和防御策略, 开发基于模型预测控制 (MPC) 的动态防御算法。

为量化分析 CCPA 中信息层与物理层的跨层耦合效应, 本文提出双反馈耦合模型 (dual-feedback coupling model)。该模型通过双层规划方法, 建立了信息层负载重新分配攻击 (LRA) 和物理层线路过载之间的动态反馈机制, 为 CCPA 机理研究和防御策略设计提供了新的视角。

双反馈耦合模型的构成如下。

上层攻击模型 (信息层): 目标最大化物理层线路过载数量。

$$\max \|\mathbf{v}\|_0$$

$$\text{s.t.} \begin{cases} \text{攻击约束 } (\mathbf{1}^T \cdot \delta_D + 2 \cdot \mathbf{1}^T \cdot \delta_{PL} \leq R_c), \\ \text{检测规避约束 } (-\tau \cdot D_0 \leq \Delta D \leq \tau \cdot D_0), \\ \text{功率平衡修正 } (\mathbf{1}^T \cdot (D + \Delta D - S) = \mathbf{1}^T \cdot P) \end{cases}$$

创新点: 通过引入功率平衡修正项 ($\mathbf{1}^T \cdot (D + \Delta D - S) = \mathbf{1}^T \cdot P$) 解决传统 LRA 模型的功率失衡问题^[29]。

下层防御模型 (物理层): 目标最小化安全

约束经济调度 (SCED) 的经济损失。

$$\begin{aligned} & \min \sum_{j \in J} (c_j P_j + c_{sj} S_j) \\ & \text{s.t.} \begin{cases} \text{潮流约束 } (-PL_l^{\min} \leq PL_l \leq PL_l^{\max}), \\ \text{电压约束 } (V_n^{\min} \leq V_n \leq V_n^{\max}), \\ \text{恢复机制1 } (\mu_l \cdot (PF_l - PF_l^{\max}) \leq \Delta PF_l), \\ \text{恢复机制2 } (\Delta PF_l \leq \mu_l \cdot (PF_l^{\max} - PF_l)) \end{cases} \end{aligned}$$

其中, μ_l 为分段线性费用系数。

关键改进: 嵌入动态恢复机制, 模拟实际电网的分级保护策略。

该模型的双反馈机制具体实现原理如下。

1) 信息→物理反馈: 在信息层, 攻击者注入虚假数据, 改变 SCED 的决策变量 (P_j, S_j), 导致其输出的潮流 PL_l 偏离估计值 (图 4 中 C-P 攻击路径), 具体流程如图 6 所示。

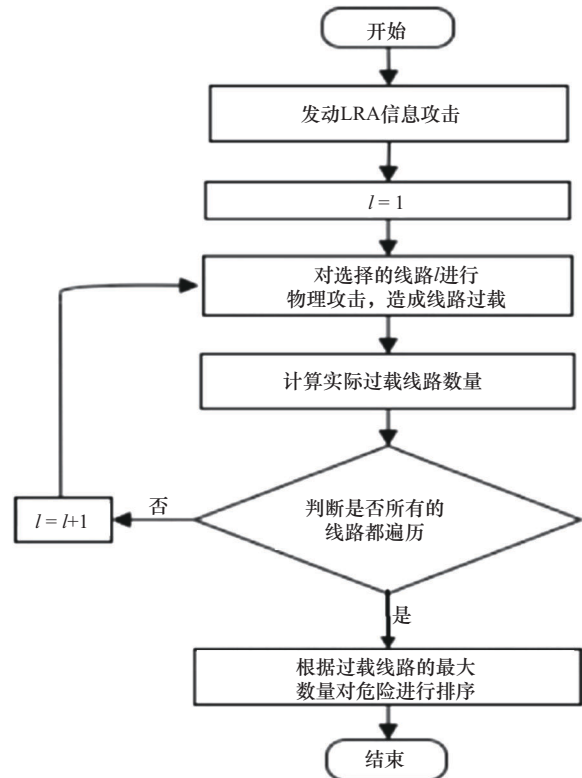


图 6 C-P 攻击流程: 信息攻击先于物理攻击

Figure 6 C-P attack workflow: cyber attacks precedes physical attacks

2) 物理→信息反馈: 物理层线路出现过载状态, 保护装置依据预设逻辑启动动作, 这种物理层的动作会反作用于信息层的测量拓扑线路 (图 4 中 P-C 攻击路径), 具体流程如图 7 所示。

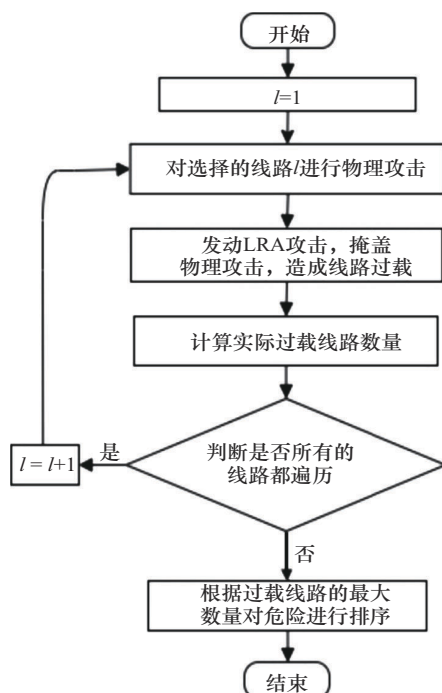


图7 P-C攻击流程:物理攻击先于信息攻击
Figure 7 P-C attack workflow: physical attacks precedes cyber attacks

表6展示了在IEEE 14节点系统上开展的多场景测试的结果。结果表明,与传统的单向攻击模型相比,双反馈耦合模型能够更准确地反映CCPA的实际影响。在相同攻击资源条件下,该模型对线路过载数量和系统运行成本增幅的预测更贴近实际场景。实验还揭示了不同攻击序列(C-P和P-C)对系统稳定性的影响差异,为制定针对性防御措施提供了依据。例如,图8显示在C-P攻击场景下,随着攻击资源的增加,第2、3、10号线路会持续过载,当攻击强度达到一定程度时,这3条线路均达到最大过载数量4。基于此

本文提出基于攻击模式的空间漏洞热点防御策略,具体包括优先保护易受篡改的总线和线路、升级关键传输路径等。如图9所示,由于第2号和第3号线路在多个攻击实例中频繁超载,因此提高这些线路的热极限或在附近部署冗余路径可有效缓解攻击导致的过载问题。

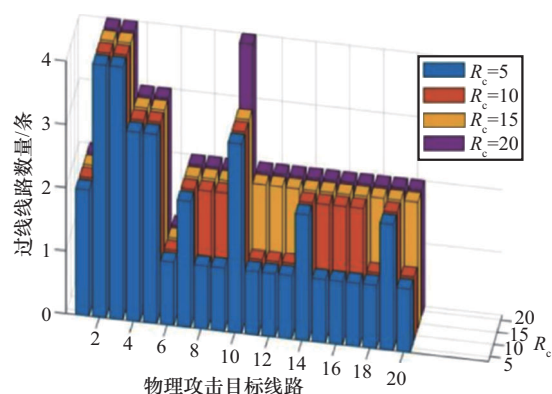


图8 C-P模型在不同攻击资源下的过载线路数
Figure 8 Number of overloaded lines under different attack resources for C-P model

(1) 复杂性分析

双反馈耦合模型的求解涉及双层规划问题,其时间复杂度主要取决于上层和下层问题的求解时间。上层问题的时间复杂度为 $o(n^3)$,其中 n 表示系统中节点的数量。这是由于在求解过程中需要计算Moore-Penrose伪逆矩阵,而该矩阵的计算复杂度较高。下层问题的时间复杂度为 $o(m^2)$,其中 m 表示系统中线路的数量。这是因为下层问题需要反复调整发电输出和负荷削减量,以满足相关约束条件。在IEEE 14节点系统上开展的实验中,该模型的求解时间约为2.5 min,计算资源消耗处于适中水平。为进一步验证模型在更大规

表6 不同模型在不同攻击资源下的结果

Table 6 Summary of results for different models under varying attack resource

攻击资源阈值	攻击模型	物理攻击线路列表	平均SCED值 (\$/h)	平均线路负荷率	平均过载线路数量/条
5	C-P	1-20	6 203.27	8.428 2	1.8
	P-C	19	6 202.99	8.240 1	2
10	C-P	1-20	6 196.74	8.460 9	2.05
	P-C	12, 18-20	6 119.32	8.276 3	1.5
15	C-P	1-20	6 182.87	8.480 9	2.3
	P-C	11-13, 16, 18-19	6 192.61	8.357 4	1.57
20	C-P	1-20	6 166.33	8.508	2.35
	P-C	9, 11-13, 16-20	6 198.17	8.387 7	1.56

模系统中的适用性,本文在 IEEE 118 节点系统上开展了初步实验。实验结果表明,模型在该系统中的求解时间约为 20 min。这一结果说明模型在更大规模的系统中依然能够有效运行,具备一定的可行性,但需要进一步优化以提高计算效率。

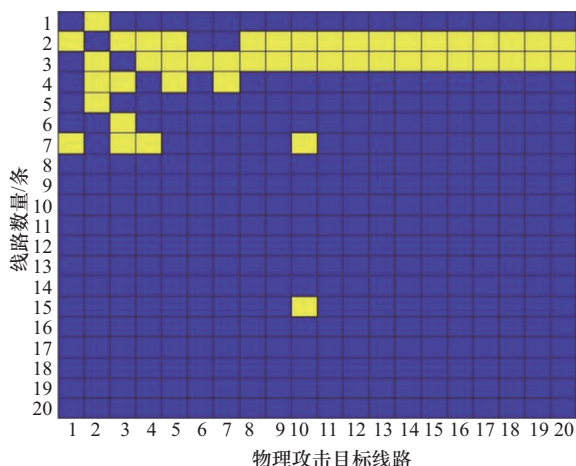


图9 在 $R_c=20$ 时 C-P 模型的过载线路分布

Figure 9 Overload line distribution under $R_c=20$ for C-P model

(2) 与 Petri 网和强化学习模型对比分析

为更全面地评估双反馈耦合模型的性能,本文还在相同攻击场景下,将其与 Petri 网模型和强化学习模型展开了对比分析。

Petri 网模型在描述电力系统中的并发事件及状态转换方面颇具优势^[57-59],但在处理大规模电网拓扑数据时,其计算复杂度会显著上升,且难以精准捕捉电力系统的动态特性与非线性关系。

强化学习模型在动态环境中展现出较强的自适应能力,能够通过与环境的交互学习最优防御策略^[96,108-109]。不过,该模型在实时攻击响应过程中,存在数据需求量大、训练时间长以及泛化能力不足等问题。

相比之下,双反馈耦合模型在检测效率与计算复杂度之间实现了良好平衡,不仅能更准确地预测攻击影响,还能为防御策略的设计提供更可靠的依据。

(3) 高比例新能源场景的适配性分析

高比例新能源接入使得电力系统的间歇性与不确定性显著增强,这对模型的鲁棒性和适应性提出了更高的要求。双反馈耦合模型凭借其双层规划结构与动态反馈机制,能够在一定程度上应

对新能源场景带来的挑战。其中,动态反馈机制可实时捕捉信息层与物理层的交互过程,并依据新能源发电的波动性及时调整攻击与防御策略,从而维持系统的稳定运行。然而,新能源场景下的大规模数据会导致模型计算复杂度上升。未来研究将围绕模型简化与优化展开,例如采用分布式计算方法和近似算法,以减轻计算负担并提高实时性。此外,引入机器学习技术对新能源发电的不确定性进行预测,同时强化关键线路的监测与保护也是提高模型适应性的有效手段。

3 信息物理协同攻击防御策略的制定

本节聚焦博弈论与多层规划模型,系统阐述新型防御策略的理论框架与实施路径,以应对复杂攻击场景下的电力系统安全挑战。

3.1 新型防御策略框架

传统电力系统安全标准(如 NERC N-1/N-2)虽保障供电连续性,但难以抵御 CCPA。为此,亟需开发融合先进检测技术、区块链技术、分布式能源管理及防御资源重构的新型策略。Deng 等^[95]提出了基于 PMU 测量验证与等效阻抗在线跟踪的检测方法。Sikorski 等^[110]探索了区块链技术在工业 M2M 交互中的安全应用。Costa 等^[111]设计了两阶段优化模型以实现防御资源的动态部署。在众多研究方法中,博弈论与多层规划模型因兼具理论完备性与决策可解释性,已成为防御策略创新的核心方向。

3.2 博弈论在防御策略中的深化应用

博弈论通过建模攻防双方的策略互动,揭示了电力系统防御的动态演化规律。Holmgren 等^[112]构建的攻击-防御-博弈综合模型首次量化了防御措施对系统安全性的边际效益。Bompard 等^[113]引入混合策略分析攻击可能性空间,并建立了风险评估矩阵;Chen 等^[114]通过博弈模型解析目标攻击的传播路径,提出了更具普适性的风险量化指标。在复杂场景建模方面,Ma 等^[115]采用马尔可夫博弈处理 N-K 攻击中的信息缺失问题。Wei 等^[87]设计了多阶段随机博弈模型,通过状态转移矩阵刻画攻防行为的动态演化过程。Sanjab 等^[116]构建了斯塔克尔伯格博弈框架,分析了主导防御方与多攻击方之间的非对称博弈均衡。在此基础上,Ranjbar 等^[117]基于纳什均衡优化了旋转备用资源分

配策略，以有效应对智能物理攻击。这些研究共同构成了覆盖多维度防御场景的博弈论方法体系，为电力系统安全防御提供了系统的理论支撑。

3.3 多层规划模型的优化设计

针对博弈论模型中假设“攻击者完全信息”的局限性，多层规划模型通过分层决策架构显著提升了防御策略的现实适用性。

双层混合整数线性规划（bilevel mixed-integer linear programming, BMILP）模型借助分层决策架构，能够精准刻画攻击者与防御者之间的策略互动。其中，上层模型聚焦于攻击者的目标函数优化，以最小化线路负载偏差或最大化系统失稳概率等目标，优化虚假数据注入策略，实现攻击效果最大化；下层模型则负责求解含虚假数据注入约束的最优潮流（optimal power flow, OPF）问题，在满足功率平衡、线路容量等物理约束条件的前提下，生成系统的最优运行状态^[118-119]。在图10所示的典型双层规划框架中：在上层问题中，攻击者选择目标母线及虚假数据注入强度，以规避不良数据检测机制；而在下层问题中，通过嵌入OPF的直流潮流方程与虚假数据注入误差限值，确保计算结果符合电力系统物理规律。文献^[118]验证了该模型的有效性，通过优化注入母线-线路组合的虚假数据，成功诱导目标输电线路过载。文献^[120]进一步扩展了模型容量，提出多线路协同攻击优化算法，并在IEEE 118节点系统中实现了多回路过载攻击的快速求解，验证了该模型在大规模电网中的实用性。

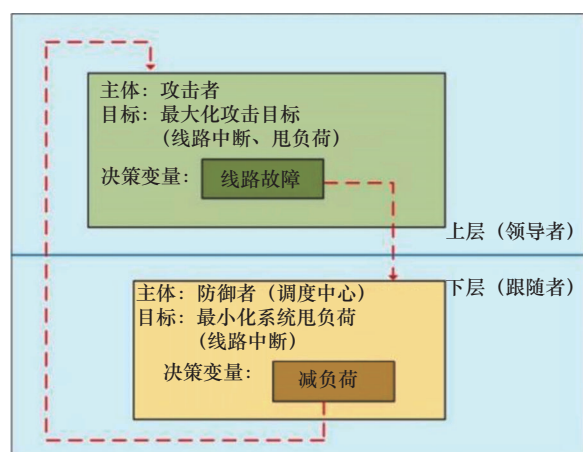


图10 攻击者视角下的双层规划模型

Figure 10 Bilevel programming model from the attacker's perspective

在3层优化模型研究领域，Yao等^[121]首次将3层规划问题引入电力网络防御领域，构建了“攻击者-防御者-系统运营商”协同优化框架。该模型采用迭代求解方法，将复杂问题分解为较小的嵌套双层问题逐步求解，最终找到最优解，显著提升了电力网络抵御潜在恐怖袭击的能力，展现了3层优化在电力系统安全防御中的显著优势。

为增强配电系统在自然灾害中的韧性，Du等^[122]提出了多阶段多区域的防御者-攻击者-分配者（DAD）模型。该模型通过优化线路加固和能源存储系统部署策略，能够有效最小化最坏情况下的加权负荷削减，并采用列与约束生成算法实现高效求解。在此基础上发展的混合鲁棒3层DAD模型^[123]创新性地结合N-K准则和攻击场景不确定性分析，实现了对多周期不确定攻击风险的精准防控，显著降低了电力系统的预期负荷损失。近年来，3层优化模型在CCPA防御中得到了广泛应用^[93,124-125]。Huang等^[124]提出了图11所示的针对CCPA的3层规划模型。该模型通过优化PMU部署策略，不仅有效预防了CCPA引发的停电事故，还大幅减少了所需的安全PMU数量，为电力系统安全防御提供了创新性解决方案。

多层线性规划模型凭借其对电网规划者、攻击者和操作者之间复杂互动的准确模拟，以及对多阶段攻防策略的综合考量，已成为现代电网防御规划的核心方法。通过优化防御资源配置，这些模型能够显著降低潜在的风险、减少损失，从而全面提升电网的安全性和韧性。

3.4 模型求解优化与工程适配

尽管多层规划模型在理论上为电网防御提供了有效的策略，但在实际应用中，求解这些模型往往非常困难。这主要源于电力系统规模庞大、约束条件复杂等特点。针对双层规划问题，常用的求解方法有混合整数线性规划^[126]、KKT条件转换、对偶理论、分层求解^[127]、增强引力搜索算法（EGSA）^[128-129]、二阶锥规划（SOCP）和归一化法向约束法（NNC）^[130]等。

相较于双层规划，3层规划问题的求解难度更高。其常见的求解方法是下层问题重构为混

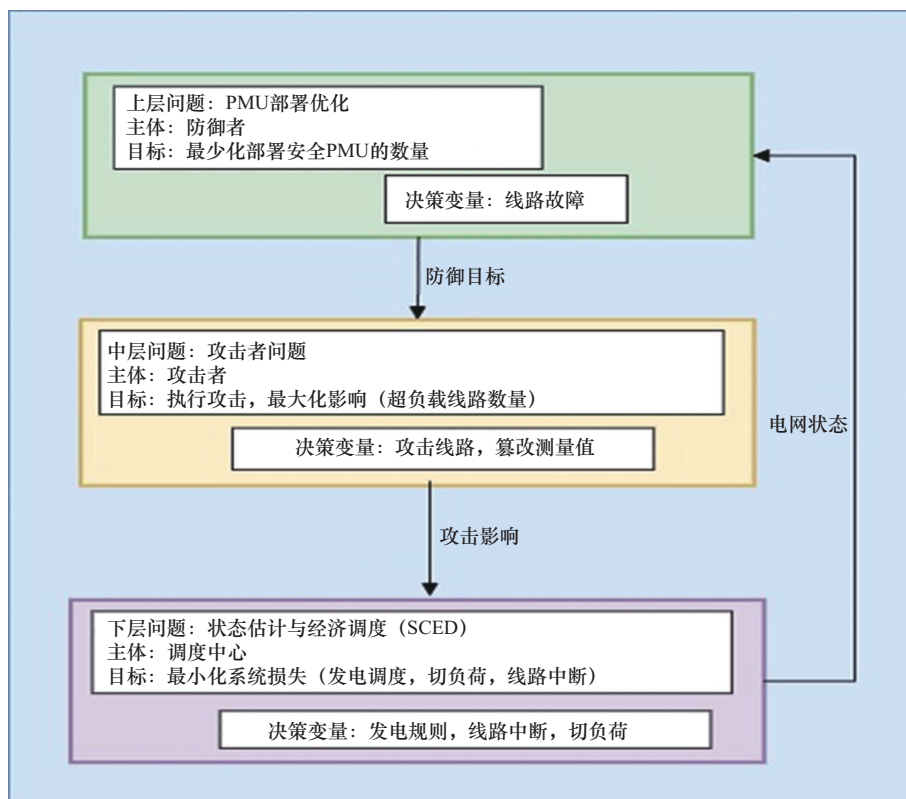


图 11 针对 CCPA 的 3 层规划模型
Figure11 Trilevel planning model for CCPA

合整数线性规划形式，并使用嵌套列与约束生成算法（C&CG）进行求解^[131]。此外，Benders 分解技术^[128,132-133]和列与约束生成算法（C&CG）^[134-135]也是求解 3 层规划问题的常用方法。文献[124]在求解 3 层规划问题时，首先将其转换为 BMILP 问题，然后采用交替优化框架，通过迭代添加约束条件来逐步逼近最优解。同时，针对大规模电网，该文献还开发了启发式算法以获取次优解，整个过程借助现有的优化求解器实现。这种方法有效处理了攻击者与防御者之间的策略互动，为电力系统协同攻击防御提供了切实可行的 PMU 部署策略。

3.5 新兴技术在防御策略中的融合

随着电力系统数字化进程的加速，基于电力系统多模态数据（如 PMU 时序量测、设备日志、拓扑变更记录）的攻击预测技术已成为研究热点^[136]。在异常检测领域，深度学习模型展现出显著优势。LSTM 网络通过捕捉电力潮流的时序相关性，可将攻击检测时延缩短至秒级；Transformer 架构凭借自注意力机制，能有效建模线路

拓扑与潮流分布的非线性关系；图神经网络（GNN）在处理大规模电网拓扑数据时表现出色。然而，数据质量、标注成本和模型可解释性仍是制约其工程应用的关键瓶颈，尤其是需要解决计算复杂度随节点数呈指数增长的问题。

从动态博弈视角来看，防御策略需要兼顾攻击者的策略演变与系统物理约束。通过将 AI 预测结果嵌入博弈论模型，可构建攻击-防御动态均衡分析框架。一方面，利用 LSTM-Transformer 混合模型实时预测攻击概率分布，作为博弈参与方的策略空间输入；另一方面，设计基于分级防御动作库的马尔可夫决策过程，通过 Q-learning 算法优化防御资源配置。此外，多层规划模型能对物理层潮流约束与信息层攻防博弈进行解耦-耦合迭代优化，实现跨层协同决策。具体而言，可将 AI 预测的攻击概率分布作为博弈论模型的输入参数，动态优化防御策略的博弈均衡点；同时，借助多层规划模型将实时攻击检测结果与物理层防御动作进行协同优化，实现攻击响应的闭环控制。将 AI 预测与传统博弈论、多层规划防

御策略相结合, 能够构建全方位防御体系, 提升防御策略的精准性和实效性。

综上所述, 电网防御策略研究是一个多学科交叉的领域, 涉及电气工程、控制理论、信息技术、优化算法及AI技术等。通过实施这些策略, 可显著提升电网抵御威胁的能力, 保障电网的安全稳定运行。

4 结束语

电力系统向新型电力系统的转型, 带来了结构、运行机制及市场模式的深刻变革, 同时也给网络安全领域带来了新的挑战。在信息物理系统深度融合的背景下, CCPA呈现出日益复杂的特征, 使得电力系统面临的安全风险更加严峻。本文通过剖析协同攻击的过程与特征, 揭示了信息空间与物理系统耦合交互过程中存在的安全隐患, 着重强调了这种耦合交互对电力系统安全性的影响。基于对攻击者行为模式的深入解析, 本文的研究为前瞻性防御措施的设计提供了科学依据, 有助于提升系统抵御复杂攻击的能力。

未来的研究将致力于构建一个全面的防御策略框架, 以助力CPPS抵御协同攻击。该框架以攻防博弈和协同攻击建模为基础, 旨在评估并增强电力系统在复杂攻击场景下的防御能力。其核心在于综合考量攻击者的行为模式与策略选择, 优化有限防御资源的部署方案, 并设计高效的应急响应与恢复策略。通过这种综合性方法, 研究者能够更精准地预测攻击造成的影响, 为电力系统安全管理提供科学支撑, 进而构建起完善的综合防御体系。

参考文献:

- [1] ZHANG Z Y, DENG R L, TIAN Y L, et al. SPMA: stealthy physics-manipulated attack and countermeasures in cyber-physical smart grid[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 581-596.
- [2] SALAZAR L, CASTRO S R, LOZANO J, et al. A tale of two industrial trojans: it was the season of darkness[C]//Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 312-330.
- [3] 樊伟, 刘永艳. 美国多措并举构建网络安全战略体系[J]. 军事文摘, 2024(1): 34-37.
FAN W, LIU Y Y. The United States has taken many measures to build a network security strategic system[J]. Military Digest, 2024(1): 34-37.
- [4] 乐健, 郎红科, 谭甜源, 等. 新型配电系统分布式经济调度信息安全问题研究综述[J]. 电力系统自动化, 2024, 48(12): 177-191.
LE J, LANG H K, TAN T Y, et al. Review of research on information security problems in distributed economic dispatch for new distribution system[J]. Automation of Electric Power Systems, 2024, 48(12): 177-191.
- [5] 胡金炜, 张玉健, 蔡莹, 等. 虚拟电厂网络安全研究综述及展望[J]. 中国电机工程学报, 2025, 45(8): 2876-2899.
HU J W, ZHANG Y J, CAI Y, et al. Review and prospect on cyber security of virtual power plant[J]. Proceedings of the CSEE, 2025, 45(8): 2876-2899.
- [6] 程鹏, 张镇勇, 邓瑞龙, 等. 新型电力系统主动防御技术体系白皮书(2023)[R]. 浙江大学, 2023.
CHENG P, ZHANG Z Y, DENG R L, et al. White paper on active defense technology system for new power systems (2023)[R]. Zhejiang University, 2023.
- [7] 蔡晔, 刘放, 曹一家, 等. 电力信息物理系统低代价多阶段高危攻击策略研究[J]. 电力系统自动化, 2021, 45(20): 1-8.
CAI Y, LIU F, CAO Y J, et al. Research on low-cost multi-stage high-risk attack strategy for power cyber-physical system[J]. Automation of Electric Power Systems, 2021, 45(20): 1-8.
- [8] 刘依晗, 王宇飞. 新型电力系统中跨域连锁故障的演化机理与主动防御探索[J]. 中国电力, 2022, 55(2): 62-72, 81.
LIU Y H, WANG Y F. Exploring the evolution mechanism and active defense of cross-domain cascading failures in new type power system[J]. Electric Power, 2022, 55(2): 62-72, 81.
- [9] 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 Q, LI M Y, TANG Y, et al. A review on research of cyber-attacks and defense in cyber physical power systems part one modeling and evaluation[J]. Automation of Electric Power Systems, 2019, 43(9): 9-21.
- [10] 朱炳钰, 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 C 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.
- [11] 杨杰, 郭逸豪, 郭创新, 等. 考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述[J]. 电力系统保护与控制, 2022, 50(7): 176-187.
YANG J, GUO Y H, GUO C X, et al. A review of dynamic security protection on a cyber physical power system considering model and data driving[J]. Power System Protection and Control, 2022, 50(7): 176-187.
- [12] YOHANANDHAN R V, ELAVARASAN R M, PUGAZHENDHI R, et al. A holistic review on cyber-physical power system (CPPS) testbeds for secure and sustainable electric power grid-Part-II: classification, overview and assessment of CPPS testbeds[J]. International Journal of Electrical Power & Energy Systems, 2022, 137: 107721.

- [13] TOOKI O O, POPOOLA O M. A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems[J]. *Renewable Energy Focus*, 2024, 51: 100628.
- [14] FENG Y X, HUANG R, ZHAO W J, et al. A survey on coordinated attacks against cyber-physical power systems: attack, detection, and defense methods[J]. *Electric Power Systems Research*, 2025, 241: 111286.
- [15] HAHN A, THOMAS R K, LOZANO I, et al. A multi-layered and kill-chain based security analysis framework for cyber-physical systems[J]. *International Journal of Critical Infrastructure Protection*, 2015, 11: 39-50.
- [16] ALGULIYEV R, IMAMVERDIYEV Y, SUKHOSTAT L. Cyber-physical systems and their security issues[J]. *Computers in Industry*, 2018, 100: 212-223.
- [17] BROOKS Z. Hacking driverless vehicles [C]//DEFCON. 2016.
- [18] KROTOFIL M, LARSEN J, GOLLMANN D. The process matters: ensuring data veracity in cyber-physical systems[C]//Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2015: 133-144.
- [19] DJOUADI S M, MELIN A M, FERRAGUT E M, et al. Finite energy and bounded actuator attacks on cyber-physical systems[C]//Proceedings of the 2015 European Control Conference (ECC). Piscataway: IEEE Press, 2015: 3659-3664.
- [20] SINGHAL A. Data warehousing and data mining techniques for cyber security[M]. Cham: Springer, 2007.
- [21] MITCHELL R, CHEN I R. Effect of intrusion detection and response on reliability of cyber physical systems[J]. *IEEE Transactions on Reliability*, 2013, 62(1): 199-210.
- [22] YU H F, KAMINSKY M, GIBBONS P B, et al. SybilGuard: defending against sybil attacks via social networks[J]. *IEEE/ACM Transactions on Networking*, 2008, 16(3): 576-589.
- [23] NAIR V J, SRIVASTAVA P, ANNASWAMY A. Enhancing power grid resilience to cyber-physical attacks using distributed retail electricity markets[C]//Proceedings of the 15th ACM/IEEE International Conference on Cyber-Physical Systems. Piscataway: IEEE Press, 2024:55-66.
- [24] ZHANG H, LIU B, WU H Y. Smart grid cyber-physical attack and defense: a review[J]. *IEEE Access*, 2021, 9: 29641-29659.
- [25] ZHANG J N, LI Q, YE J, et al. Cyber-physical security framework for photovoltaic farms[C]//Proceedings of the 2020 IEEE CyberPELS (CyberPELS). Piscataway: IEEE Press, 2020: 1-7.
- [26] LI H W, LU R X, ZHOU L, et al. An efficient merkle-tree-based authentication scheme for smart grid[J]. *IEEE Systems Journal*, 2013, 8(2): 655-663.
- [27] ZELLER M. Common questions and answers addressing the aurora vulnerability[R]. Schweitzer Engineering Laboratories, 2011.
- [28] LIANG J W, SANKAR L, KOSUT O. Vulnerability analysis and consequences of false data injection attack on power system state estimation[J]. *IEEE Transactions on Power Systems*, 2016, 31(5): 3864-3872.
- [29] YUAN Y L, LI Z Y, REN K. Modeling load redistribution attacks in power systems[J]. *IEEE Transactions on Smart Grid*, 2011, 2(2): 382-390.
- [30] SOLTAN S, ZUSSMAN G. EXPOSE the line failures following a cyber-physical attack on the power grid[J]. *IEEE Transactions on Control of Network Systems*, 2018, 6(1): 451-461.
- [31] CHA S T, WU Q W, NIELSEN A H, et al. Real-time hardware-In-the-loop (HIL) testing for power electronics controllers[C]//Proceedings of the 2012 Asia-Pacific Power and Energy Engineering Conference. Piscataway: IEEE Press, 2012: 1-6.
- [32] ZHAO C C, HE J P, CHENG P, et al. Analysis of consensus-based distributed economic dispatch under stealthy attacks[J]. *IEEE Transactions on Industrial Electronics*, 2017, 64(6): 5107-5117.
- [33] PLIATSIOS D, SARIGIANNIDIS P, LAGKAS T, et al. A survey on SCADA systems: secure protocols, incidents, threats and tactics[J]. *IEEE Communications Surveys & Tutorials*, 2020, 22(3): 1942-1976.
- [34] UPADHYAY D, SAMPALLI S. SCADA (supervisory control and data acquisition) systems: vulnerability assessment and security recommendations[J]. *Computers & Security*, 2020, 89: 101666.
- [35] WAN Y, CAO J D. A brief survey of recent advances and methodologies for the security control of complex cyber-physical networks[J]. *Sensors*, 2023, 23(8): 4013.
- [36] KANG W J, LIU Q, ZHU P D, et al. Coordinated cyber-physical attacks based on different attack strategies for cascading failure analysis in smart grids[J]. *Wireless Networks*, 2024, 30(5): 3821-3836.
- [37] YOHANANDHAN R V, ELAVARASAN R M, MANOHARAN P, et al. Cyber-physical power system (CPPS): a review on modeling, simulation, and analysis with cyber security applications[J]. *IEEE Access*, 2020, 8: 151019-151064.
- [38] KHALID H M, MUYEEN S M, PENG J C H. Cyber-attacks in a looped energy-water nexus: an inoculated sub-observer-based approach[J]. *IEEE Systems Journal*, 2020, 14(2): 2054-2065.
- [39] YU L, SUN X M, SUI T J. False-data injection attack in electricity generation system subject to actuator saturation: analysis and design[J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, 49(8): 1712-1719.
- [40] PATEL A, PURWAR S. Switching attacks on smart grid using non-linear sliding surface[J]. *IET Cyber-Physical Systems: Theory & Applications*, 2019, 4(4): 382-392.
- [41] WU G Y, WANG G, SUN J, et al. Optimal partial feedback attacks in cyber-physical power systems[J]. *IEEE Transactions on Automatic Control*, 2020, 65(9): 3919-3926.
- [42] QI J J, HAHN A, LU X N, et al. Cybersecurity for distributed energy resources and smart inverters[J]. *IET Cyber-Physical Systems: Theory & Applications*, 2016, 1(1): 28-39.
- [43] CARDENAS D J S, HAHN A, LIU C C. Assessing cyber-physical risks of IoT-based energy devices in grid operations[J]. *IEEE Access*, 2020, 8: 61161-61173.
- [44] 王琦, 郁伟, 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 Q, TAI W, TANG Y, et al. A review on false data injection attack toward cyber-physical power system[J]. *Acta Automatica Sinica*, 2019, 45(1): 72-83.
- [45] JAHROMI A A, KEMMEUGNE A, KUNDUR D, et al. Cyber-

- physical attacks targeting communication-assisted protection schemes[J]. *IEEE Transactions on Power Systems*, 2020, 35(1): 440-450.
- [46] ASHOK A, GOVINDARASU M, WANG J H. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid[J]. *Proceedings of the IEEE*, 2017, 105(7): 1389-1407.
- [47] HUANG X G, QIN Z J, LIU H. A survey on power grid cyber security: from component-wise vulnerability assessment to system-wide impact analysis[J]. *IEEE Access*, 2018, 6: 69023-69035.
- [48] CHEN K R, WEN F S, PALU I. Cyber contingencies impacts analysis in cyber physical power system[C]//*Proceedings of the 2019 IEEE International Conference on Energy Internet (ICEI)*. Piscataway: IEEE Press, 2019: 37-41.
- [49] AHMADIAN S, TANG X, MALKI H A, et al. Modelling cyber attacks on electricity market using mathematical programming with equilibrium constraints[J]. *IEEE Access*, 2019, 7: 27376-27388.
- [50] ZHANG Y, KRISHNAN V V G, PI J, et al. Cyber physical security analytics for transactive energy systems[J]. *IEEE Transactions on Smart Grid*, 2019, 11(2): 931-941.
- [51] CAO G, GU W, LI P X, et al. Operational risk evaluation of active distribution networks considering cyber contingencies[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(6): 3849-3861.
- [52] RAWAT D B, RODRIGUES J, STOJMENOVIC I. Cyber - physical systems: from theory to practice [M]. Boca Raton: CRC Press, 2015.
- [53] SANFELICE G R. Control of hybrid systems: an overview of recent advances[M]//*Hybrid Systems with Constraints*. Hoboken: Wiley, 2013.
- [54] GOEBEL R, SANFELICE R G, TEEL A R. Hybrid dynamical systems[J]. *IEEE Control Systems Magazine*, 2009, 29(2): 28-93.
- [55] SANFELICE R G. On the existence of control Lyapunov functions and state-feedback laws for hybrid systems[J]. *IEEE Transactions on Automatic Control*, 2013, 58(12): 3242-3248.
- [56] SANFELICE R G. Interconnections of hybrid systems: some challenges and recent results[J]. *Journal of Nonlinear Systems and Applications*, 2011, 2: 111-121.
- [57] SANFELICE R G, GOEBEL R, TEEL A R. Generalized solutions to hybrid dynamical systems[J]. *ESAIM: Control, Optimisation and Calculus of Variations*, 2008, 14(4): 699-724.
- [58] SANFELICE R, COPP D, NANEZ P. A toolbox for simulation of hybrid systems in Matlab/Simulink: hybrid equations (HyEQ) toolbox[C]//*Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control*. New York: ACM, 2013: 101-106.
- [59] GOEBEL R, SANFELICE R G, TEEL A R. Hybrid dynamical systems: modeling, stability, and robustness[M]. New Jersey: Princeton University Press, 2012.
- [60] WANG Y N, LIN Z Y, LIANG X, et al. On modeling of electrical cyber-physical systems considering cyber security[J]. *Frontiers of Information Technology & Electronic Engineering*, 2016, 17(5): 465-478.
- [61] PARANDEHGHEIBI M, MODIANO E, HAY D. Mitigating cascading failures in interdependent power grids and communication networks[C]//*Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Piscataway: IEEE Press, 2014: 242-247.
- [62] KIM J, TONG L. On topology attack of a smart grid: undetectable attacks and countermeasures[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(7): 1294-1305.
- [63] LOU X, YAU D K Y, NGUYEN H H, et al. Profit-optimal and stability-aware load curtailment in smart grids[J]. *IEEE Transactions on Smart Grid*, 2013, 4(3): 1411-1420.
- [64] WILLIAMS M A, KOELN J P, PANGBORN H C, et al. Dynamical graph models of aircraft electrical, thermal, and turbomachinery components[J]. *Journal of Dynamic Systems, Measurement, and Control*, 2018, 140(4): 041013.
- [65] LI W Z, XIE L, DENG Z L, et al. False sequential logic attack on SCADA system and its physical impact analysis[J]. *Computers & Security*, 2016, 58: 149-159.
- [66] GURSESLI O, DESROCHERS A A. Modeling infrastructure interdependencies using Petri nets [C]//*Proceedings of the 2003 IEEE International Conference on Systems, Man & Cybernetics*. Piscataway: IEEE Press, 2003: 1506-1512.
- [67] LAPRIE J C, KANOUN K, KAËNICHE M. Modelling interdependencies between the electricity and information infrastructures[M]//*Computer Safety, Reliability, and Security*. Heidelberg: Springer, 2007: 54-67.
- [68] LIU X X, ZHANG J X, ZHU P D. Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory[J]. *International Journal of Critical Infrastructure Protection*, 2017, 16: 13-25.
- [69] CHEN T M, SANCHEZ-AARNOUTSE J C, BUFORD J. Petri net modeling of cyber-physical attacks on smart grid[J]. *IEEE Transactions on Smart Grid*, 2011, 2(4): 741-749.
- [70] DAVIS K R, DAVIS C M, ZONOUZ S A, et al. A cyber-physical modeling and assessment framework for power grid infrastructures[J]. *IEEE Transactions on Smart Grid*, 2015, 6(5): 2464-2475.
- [71] KHAND P A. System level security modeling using attack trees[C]//*Proceedings of the 2009 2nd International Conference on Computer, Control and Communication*. Piscataway: IEEE Press, 2009: 1-6.
- [72] WADHAWAN Y, ALMAJALI A, NEUMAN C. A comprehensive analysis of smart grid systems against cyber-physical attacks[J]. *Electronics*, 2018, 7(10): 249.
- [73] LIU N, ZHANG J H, ZHANG H, et al. Security assessment for communication networks of power control systems using attack graph and MCDM[J]. *IEEE Transactions on Power Delivery*, 2010, 25(3): 1492-1500.
- [74] WANG Y F, GAO K L, ZHAO T, et al. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J]. *Proceedings of the Chinese Society of Electrical Engineering*, 2016, 36(6): 1490-1499.
- [75] ZHANG Y C, WANG L F, XIANG Y M, et al. Power system reliability evaluation with SCADA cybersecurity considerations[J]. *IEEE Transactions on Smart Grid*, 2015, 6(4): 1707-1721.

- [76] ZONOUZ S, DAVIS C M, DAVIS K R, et al. SOCCA: a security-oriented cyber-physical contingency analysis in power infrastructures[J]. *IEEE Transactions on Smart Grid*, 2013, 5(1): 3-13.
- [77] ZHANG Y C, WANG L F, XIANG Y M, et al. Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation[J]. *IEEE Transactions on Power Systems*, 2016, 31(6): 4379-4394.
- [78] BOZZELLI L, MOLINARI A, MONTANARI A, et al. Interval vs. point temporal logic model checking[J]. *ACM Transactions on Computational Logic*, 2019, 20(1): 1-31.
- [79] ZHANG Z H, GONG S P, DIMITROVSKI A D, et al. Time synchronization attack in smart grid: impact and analysis[J]. *IEEE Transactions on Smart Grid*, 2013, 4(1): 87-98.
- [80] 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.
- [81] SRIDHAR S, GOVINDARASU M. Model-based attack detection and mitigation for automatic generation control[J]. *IEEE Transactions on Smart Grid*, 2017, 5(2): 580-591.
- [82] ZHANG X L, YANG X Y, LIN J, et al. On data integrity attacks against real-time pricing in energy-based cyber-physical systems[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2016, 28(1): 170-187.
- [83] YANG Q Y, YANG J, YU W, et al. On false data-injection attacks against power system state estimation: modeling and countermeasures[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2014, 25(3): 717-729.
- [84] LIU S, MASHAYEKH S, KUNDUR D, et al. A framework for modeling cyber-physical switching attacks in smart grid[J]. *IEEE Transactions on Emerging Topics in Computing*, 2013, 1(2): 273-285.
- [85] ELIASSI M, KHOSHKOLGH DASHTAKI A, SEIFI H, et al. Application of Bayesian networks in composite power system reliability assessment and reliability-based analysis[J]. *IET Generation, Transmission & Distribution*, 2015, 9(13): 1755-1764.
- [86] FARRAJ A, HAMMAD E, AL DAOUD A, et al. A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems[J]. *IEEE Transactions on Smart Grid*, 2016, 7(4): 1846-1855.
- [87] WEI L F, SARWAT A I, SAAD W, et al. Stochastic games for power grid protection against coordinated cyber-physical attacks[J]. *IEEE Transactions on Smart Grid*, 2018, 9(2): 684-694.
- [88] BHOR D, ANGAPPAN K, SIVALINGAM K M. Network and power-grid co-simulation framework for smart grid wide-area monitoring networks[J]. *Journal of Network and Computer Applications*, 2016, 59: 274-284.
- [89] CELLI G, PEGORARO P A, PILO F, et al. DMS cyber-physical simulation for assessing the impact of state estimation and communication media in smart grid operation[J]. *IEEE Transactions on Power Systems*, 2014, 29(5): 2436-2446.
- [90] CAO Y J, SHI X Y, LI Y, et al. A simplified co-simulation model for investigating impacts of cyber-contingency on power system operations[J]. *IEEE Transactions on Smart Grid*, 2018, 9(5): 4893-4905.
- [91] KAZMI J H, LATIF A, AHMAD I, et al. A flexible smart grid co-simulation environment for cyber-physical interdependence analysis[C]// *Proceedings of the 2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. Piscataway: IEEE Press, 2016: 1-6.
- [92] LI W, MONTI A, LUO M, et al. VPNET: a co-simulation framework for analyzing communication channel effects on power systems[C]// *Proceedings of the 2011 IEEE Electric Ship Technologies Symposium*. Piscataway: IEEE Press, 2011: 143-149.
- [93] LI S H, SHI L B. A tri-level optimization strategy incorporating wind power against coordinated cyber-physical attacks[J]. *IET Generation, Transmission & Distribution*, 2023, 17(10): 2228-2248.
- [94] LI Z Y, SHAHIDEHPUR M, ALABDULWAHAB A, et al. Bi-level model for analyzing coordinated cyber-physical attacks on power systems[J]. *IEEE Transactions on Smart Grid*, 2016, 7(5): 2260-2272.
- [95] DENG R L, ZHUANG P, LIANG H. CCPA: coordinated cyber-physical attacks and countermeasures in smart grid[J]. *IEEE Transactions on Smart Grid*, 2017, 8(5): 2420-2430.
- [96] 伊娜, 徐建军, 陈月, 等. 基于深度强化学习的多阶段信息物理协同拓扑攻击方法[J]. *电力工程技术*, 2023, 42(4): 149-158.
- YI N, XU J J, CHEN Y, et al. A multi-stage coordinated cyber-physical topology attack method based on deep reinforcement learning[J]. *Electric Power Engineering Technology*, 2023, 42(4): 149-158.
- [97] 刘耕铭, 刘文霞, 张艺伟, 等. 考虑电压控制的信息物理协同攻击模型[J]. *华北电力大学学报(自然科学版)*, 2023, 50(3): 46-56, 66, 128-130.
- LIU G M, LIU W X, ZHANG Y W, et al. Coordinated cyber-physical attacks model considering voltage control[J]. *Journal of North China Electric Power University (Natural Science Edition)*, 2023, 50(3): 46-56, 66, 128-130.
- [98] 魏玉玺. 考虑虚假数据注入的智能电网信息物理协同攻击策略与影响分析[D]. 沈阳: 东北大学, 2021.
- WEI Y X. Analysis of cyber-Physical coordinated attack strategy and impact considering false data injection in smart grid[D]. Shenyang: Northeastern University, 2021.
- [99] 冯晓萌. 面向信息物理协同的电力系统攻击/防御策略研究[D]. 沈阳: 东北大学, 2019.
- FENG X M. Research on attack/defense strategies for power systems under cyber-physical cooperation[D]. Shenyang: Northeastern University, 2019.
- [100] 原欣. 网络攻击下电力信息-物理融合系统的风险传播及防控策略研究[D]. 沈阳: 东北大学, 2018.
- YUAN X. Research on risk propagation and prevention and control strategies of power information - physical fusion systems under cyber attacks[D]. Shenyang: Northeastern University, 2018.
- [101] 蔡星浦. 电力系统网络攻击信息物理协同防御方法研究[D]. 南京: 东南大学, 2021.
- CAI X P. Research on cyber - physical cooperative defense methods for power system network attacks[D]. Nanjing: Southeast University, 2021.
- [102] 施宝中. 提升电力信息物理系统韧性的蓄意攻击防御及故障

- 恢复策略研究[D]. 北京: 华北电力大学, 2022.
- TI B Z. Research on intentional attack defense and fault recovery strategies to enhance the resilience of power information physical systems[D]. Beijing: North China Electric Power University, 2022.
- [103] 闫旻睿. 微电网信息物理系统脆弱性分析与防御策略研究[D]. 杭州: 浙江大学, 2024.
- YAN M R. Research on vulnerability analysis and defense strategies of microgrid cyber-physical systems[D]. Hangzhou: Zhejiang University, 2024.
- [104] 张博. 信息物理融合的孤岛微电网安全稳定运行控制研究[D]. 秦皇岛: 燕山大学, 2021.
- ZHANG B. Research on secure and stable operation control of islanded microgrids with cyber-physical convergence[D]. Qinhuangdao: Yanshan University, 2021.
- [105] 曹戈. 信息物理融合下微电网运行评估及控制研究[D]. 南京: 东南大学, 2021.
- CAO G. Research on operation evaluation and control of microgrids with cyber-physical convergence[D]. Nanjing: Southeast University, 2021.
- [106] 马良. 信息物理融合环境下网络攻击的微电网弹性控制策略[D]. 北京: 华北电力大学, 2021.
- MA L. Resilient control strategies for microgrids against network attacks in cyber-physical converged environments[D]. Beijing: North China Electric Power University, 2021.
- [107] 殷浩洋, 刘东, 陈冠宏, 等. 面向虚拟电厂的协同网络攻击模型及跨空间故障传播机理[J]. 电力系统自动化, 2023, 47(8): 34-43.
- YIN H Y, LIU D, CHEN G H, et al. Coordinated cyber attack model and cross-space fault propagation mechanism for virtual power plant[J]. Automation of Electric Power Systems, 2023, 47(8): 34-43.
- [108] WANG Z H, HE H B, WAN Z Q, et al. Coordinated topology attacks in smart grid using deep reinforcement learning[J]. IEEE Transactions on Industrial Informatics, 2021, 17(2): 1407-1415.
- [109] LEI J Y, GAO S B, SHI J, et al. A reinforcement learning approach for defending against multisenario load redistribution attacks[J]. IEEE Transactions on Smart Grid, 2022, 13(5): 3711-3722.
- [110] SIKORSKI J J, HAUGHTON J, KRAFT M. Blockchain technology in the chemical industry: machine-to-machine electricity market[J]. Applied Energy, 2017, 195: 234-246.
- [111] COSTA A, GEORGIAIDIS D, NG T S, et al. An optimization model for power grid fortification to maximize attack immunity[J]. International Journal of Electrical Power & Energy Systems, 2018, 99: 594-602.
- [112] HOLMGREN A J, JENELIUS E, WESTIN J. Evaluating strategies for defending electric power networks against antagonistic attacks[J]. IEEE Transactions on Power Systems, 2007, 22(1): 76-84.
- [113] BOMPARD E, GAO C W, NAPOLI R, et al. Risk assessment of malicious attacks against power systems[J]. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 2009, 39(5): 1074-1085.
- [114] CHEN G, DONG Z Y, HILL D J, et al. Exploring reliable strategies for defending power systems against targeted attacks[J]. IEEE Transactions on Power Systems, 2011, 26(3): 1000-1009.
- [115] MA C Y T, YAU D K Y, LOU X, et al. Markov game analysis for attack-defense of power networks under possible misinformation[J]. IEEE Transactions on Power Systems, 2012, 28(2): 1676-1686.
- [116] SANJAB A, SAAD W. Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2038-2049.
- [117] RANJBAR M H, KHERADMANDI M, PIRAYESH A. Game framework for optimal allocation of spinning reserve to confront intelligent physical attacks on power system[J]. IET Generation, Transmission & Distribution, 2019, 13(1): 92-98.
- [118] KHEZRIMOTLAGH D, KHAZAEI J, ASRARI A. MILP modeling of targeted false load data injection cyberattacks to overflow transmission lines in smart grids[C]//Proceedings of the 2019 North American Power Symposium (NAPS). Piscataway: IEEE Press, 2019: 1-7.
- [119] ALKAF M, KHAZAEI J, HADI AMINI M, et al. Optimal attack strategy for multi-transmission line congestion in cyber-physical smart grids[C]//Proceedings of the 2019 tenth International Green and Sustainable Computing Conference (IGSC). Piscataway: IEEE Press, 2019: 1-6.
- [120] TAN Y, LI Y, CAO Y J, et al. Cyber-attack on overloading multiple lines: a bilevel mixed-integer linear programming model[J]. IEEE Transactions on Smart Grid, 2017, 9(2): 1534-1536.
- [121] YAO Y M, EDMUNDS T, PAPAGEORGIOU D, et al. Trilevel optimization in power network defense[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2007, 37(4): 712-718.
- [122] ZHANG H B, MA S T, DING T, et al. Multi-stage multi-zone defender-attacker-defender model for optimal resilience strategy with distribution line hardening and energy storage system deployment[J]. IEEE Transactions on Smart Grid, 2021, 12(2): 1194-1205.
- [123] DU M, LIU X, ZHOU Q, et al. Hybrid robust tri-level defense model against multiperiod uncertain attacks[J]. IEEE Transactions on Smart Grid, 2022, 13(4): 3255-3265.
- [124] HUANG Y D, HE T, CHAUDHURI N R, et al. Preventing outages under coordinated cyber-physical attack with secured PMUs[J]. IEEE Transactions on Smart Grid, 2022, 13(4): 3160-3173.
- [125] HE H H, HUANG S J, LIU Y J, et al. A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks[J]. International Journal of Electrical Power & Energy Systems, 2021, 130: 106903.
- [126] MOTTO A L, ARROYO J M, GALIANA F D. A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat[J]. IEEE Transactions on Power Systems, 2005, 20(3): 1357-1365.
- [127] 江钧, 成乐祥, 孙国强, 等. 考虑安全域的配电网重构二阶锥双层规划模型[J]. 电力系统保护与控制, 2019, 47(4): 9-16.
- JIANG J, CHENG L X, SUN G Q, et al. Distribution network reconfiguration based on second order cone bi-level programming considering security distance[J]. Power System Protection and

Control, 2019, 47(4): 9-16.

- [128] JAHAN M S, AMJADY N. Solution of large-scale security constrained optimal power flow by a new bi-level optimisation approach based on enhanced gravitational search algorithm[J]. IET Generation, Transmission & Distribution, 2013, 7(12): 1481-1491.
- [129] WEI L, TIAN Q L. Multi-objective optimal load distribution based on improved gravitational search algorithm in power plants[C]// Proceedings of the 2018 Chinese Control and Decision Conference (CCDC). Piscataway: IEEE Press, 2018: 3910-3915.
- [130] 张忠会, 雷大勇, 蒋昌辉, 等. 基于二阶锥规划和NNC法的交直流混合配电网双层规划模型及其求解方法[J]. 中国电机工程学报, 2023, 43(1): 70-85.
- ZHANG Z H, LEI D Y, JIANG C H, et al. A bi-level planning model and its solution method of AC/DC hybrid distribution network based on second-order cone programming and NNC method[J]. Proceedings of the CSEE, 2023, 43(1): 70-85.
- [131] WANG C, WEI W, WANG J H, et al. Robust defense strategy for gas-electric systems against malicious attacks[J]. IEEE Transactions on Power Systems, 2016, 32(4): 2953-2965.
- [132] STREET A, MOREIRA A, ARROYO J M. Energy and reserve scheduling under a joint generation and transmission security criterion: an adjustable robust optimization approach[J]. IEEE Transactions on Power Systems, 2014, 29(1): 3-14.
- [133] 荆朝霞, 王宏益, 吴青华. 220 kV 电网供电能力计算的改进 Benders 分解法[J]. 中国电机工程学报, 2017, 37(17): 4893-4900.
- JING Z X, WANG H Y, WU Q H. Modified Benders decomposition method for total supplying capability calculation of 220kV power grid[J]. Proceedings of the CSEE, 2017, 37(17): 4893-4900.
- [134] XIANG Y M, WANG L F. An improved defender-attacker-defender model for transmission line defense considering offensive resource uncertainties[J]. IEEE Transactions on Smart Grid, 2019, 10(3): 2534-2546.
- [135] GAN W, SHAHIDEHPOUR M, GUO J B, et al. A tri-level planning approach to resilient expansion and hardening of coupled power distribution and transportation systems[J]. IEEE Transactions on Power Systems, 2022, 37(2): 1495-1507.
- [136] 马钰锡, 张全新, 谭毓安, 等. 面向智能攻击的行为预测研究[J]. 软件学报, 2021, 32(5): 1526-1546.
- MA Y X, ZHANG Q X, TAN Y A, et al. Research on behavior-prediction for intelligent attacks[J]. Journal of Software, 2021, 32(5): 1526-1546.

[作者简介]



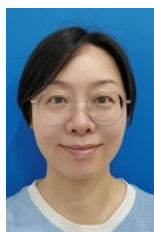
黄辉辉 (1988-), 男, 河南洛阳人, 信息工程大学副教授, 主要研究方向为电力信息物理系统安全。



魏强 (1979-), 男, 江西南昌人, 信息工程大学博士生导师, 主要研究方向为网络空间安全。



耿洋洋 (1993-), 男, 新疆伊犁人, 信息工程大学讲师, 主要研究方向为工业控制系统安全。



吴茜琼 (1981-), 女, 江西萍乡人, 信息工程大学副教授, 主要研究方向为电力系统安全。



陈昊文 (1990-), 男, 河南新乡人, 信息工程大学讲师, 主要研究方向为软件安全。