DOI: 10.19783/j.cnki.pspc.210899

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

杨 杰[1]，郭逸豪[1]，郭创新[1]，陈 哲[2]，王胜寒[1]

(1. 浙江大学电气工程学院，浙江 杭州 310027；2. 国网浙江省电力有限公司电力科学研究院，浙江 杭州 310014)

摘要：数字革命的到来使智能电网运行安全防护问题从单一的物理层面防护扩展至信息物理协同防护，先进的网络安全威胁将会对电网物理侧造成严重影响。高效、可靠、实时的电网协同安全防护方法是智能电网发展的核心基础支撑。回顾了国内外相关研究。针对电力信息物理系统的内涵特征，提出了模型与数据双重驱动下的智能电网动态安全防护闭环控制思想，具体包括未知攻击快速入侵检测、信息物理穿透式风险评估及协同安全决策等三个科学问题。总结分析了智能电网安全防护现有的研究成果和缺陷并提出其未来研究方向，为建设本质安全的智能电网奠定理论和工程基础。

关键词：智能电网；入侵检测；风险评估；协同安全；动态防护

A review of dynamic security protection on a cyber physical power system considering model and data driving

YANG Jie[1], GUO Yihao[1], GUO Chuangxin[1], CHEN Zhe[2], WANG Shenghan[1]

(1. College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China;
2. Electric Power Research Institute of State Grid Zhejiang Electric Power Co., Ltd., Hangzhou 310014, China)

Abstract: The digital revolution has expanded the security protection of smart grid operation from the pure physical level protection to cyber physical synergistic protection. Advanced cyber threats can have a serious impact on the physical side of the grid. Efficient, reliable, and real-time synergistic protection methods are the core foundation support for the development of the smart grid. This paper reviews relevant research at home and abroad. In view of the connotative characteristics of the cyber physical power system, both a model and data-driven closed-loop control idea with three scientific issues is proposed, i.e., rapid intrusion detection of unknown attacks, penetration risk assessment of the cyber physical system and synergistic security decision making. Then, current research results and problems are summarized and analyzed, and future research directions are proposed to lay the theoretical and engineering foundation for building an intrinsically safe smart grid.

This work is supported by the National Natural Science Foundation of China (No. U1866209).

Key words: smart grid; intrusion detection; risk assessment; synergistic security; dynamic protection

0 引言

信息领域的技术革新与进步是工业发展的基石，随着计算机技术、物联网技术和大数据技术的快速发展，以“精准控制、智能生产”为目的的第三次工业革命[1]呼之欲出，工业控制系统将逐步实现从“黑色”到“透明”，从“封闭”到“开放”的转变。

电力系统作为一种典型的工控系统，随着信息技术的发展已经从单一的物理系统发展为信息物理融合系统(Cyber Physical System, CPS)[2]。所谓电力信息物理系统(Cyber Physical Power System, CPPS)是指通过现代信息技术与电力系统的有机融合而形成的多维异构复杂系统，其本质是要借助先进传感、通信、计算、物联技术[3]，实现电力产消过程中信息单元和物理实体的高度集成和广泛交互，构建从数据采集到分析处理自下而上的感知流和从正确决策到精准执行自上而下的控制流。现代电力系统信

基金项目：国家自然科学基金项目资助(U1866209)

息物理深度交互，智能终端、云计算平台的接入[4]使传统的封闭的电力系统变得开放，导致其安全边界日趋模糊、高级安全威胁不断增多，信息安全事故频频发生[5]。2010 年伊朗核电站震网病毒事件[6]打破了信息物理系统封闭且无法实施网络攻击的观念，在全球范围内引起广泛关注。2015 年乌克兰电力系统遭受定向网络攻击[7]，三分之一的地区持续断电。二次系统遭受恶意攻击后将对物理世界造成严重影响，因此对电力系统信息物理协同安全防护问题的研究具有重大现实意义，已经受到各国政府的高度重视。2011 年，美国国家标准技术研究院(National Institute of Standards and Technology, NIST)首先发布的《工业控制系统安全指南》[8]，是对工业领域信息安全防护的第一份全面指导方案。2013 年，德国也将网络安全作为重要发展方向之一[9]。2014 年，我国颁布《电力监控系统安全防护规定》，正式将电力信息安全提高到国家安全层面[10]。

传统的信息安全要素由 NIST 提出[11]，具体包括：保密性(confidentiality)、完整性(integrity)和可用性(availability)。通常，信息系统最关注信息的保密性，即仅允许有权限用户获取相关关键信息，且实时性要求不高，生命周期较短，软件升级方便快捷。而 CPPS 作为国民生产生活的重要基础，具有相当严苛的运行要求，具体包括：1) 必须保证电力系统 7×24 h 的可用性；2) 必须保证电力系统被控过程的操作可持续且确定；3) 必须保证电力系统运行性能；4) 必须保证电力系统全生命周期安全。因此，电力信息物理系统的可用性具有最高优先级，需要在遭受网络攻击的情况下依然保证功能安全和运行安全。

随着智能电网数字化建设进程的加快，传统的 CPPS 安防体系受到强烈冲击，具体来讲：1) 海量异构数据源接入可能产生误导性信息，现阶段缺乏规范的数据驱动框架，由此将导致过量连接或不必要阻断，前者引发安全性和保密性问题，后者降低数字化效益；2) 大规模终端涌入必然导致互换性、互操作性下降和调控难度上升；3) 开放的市场化交互行为对有效的控制访问机制需求更迫切。

综上所述，电力系统的信息安全防护更偏向于动态在线防御。本文从技术层面研究现代电力系统信息安全问题，针对模型与数据双重驱动下的智能电网信息物理动态协同安全防护存在的相关问题，基于闭环控制思想总结形成以下 3 个主要研究方向并逐一进行详细阐述，具体包括：1) 数据驱动的快速入侵检测；2) 信息物理系统的穿透式风险评估；3) 信息物理系统协同安全防御决策。

1　电力信息物理系统结构特征

本节首先针对 CPPS 的具体结构进行了建模，并描述了电力系统和信息系统的耦合关系，同时展示了在电力物联网背景下我国电力信息物理系统的特点。

新一代电力系统的主要特点是“广泛互联、智能互动、灵活柔性、安全可控”，本质上强调了物理系统与信息系统的深度耦合，通过信息侧数据下沉，以可观性的提升促进可控性的提高。电力信息物理系统是一种特殊的工业控制系统，与一般的工控系统类似，也具有明显的层级结构，本文依据设备和功能的不同，将电力信息物理系统自上而下划分成三个层级，具体包括信息层、接入层及物理层，其模型如图 1 所示。信息层是一个纯粹的信息系统，主要包括数据采集与监视控制系统(Supervisory Control and Data Acquisition, SCADA)、能量管理系统(Energy Management System, EMS)及信息管理系统(Management Information System, MIS)等。相应的，终端层是一个纯粹的物理系统，主要包括断路器、分段开关、变压器等一系列一次设备。而接入层则是整个系统的信息枢纽，同时也是信息流与能量流互动的核心环节，可以实现故障诊断、隔离、恢复等功能，包含了保护、监视、控制设备以及远程数据终端(Remote Terminal Unit, RTU)和合并单元(Merging Unit, MU)等。在接入层内，通过大量的交换机可以实现数据纵向传输和横向共享。

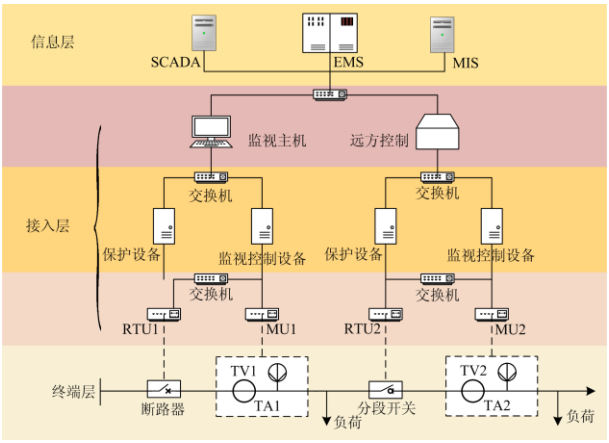

图 1 电力信息物理系统层次模型

Fig. 1 Hierarchical model of cyber-physical power system

根据本文提出的模型，攻击者可以从两个角度发起攻击。对于从模型顶层发起的攻击，一般通过修改断路器或分段开关配置文件的关键参数来构造虚假指令，导致上述设备的误动和拒动，进而影响

电网正常运行。这种类型的攻击通常可以分为三个步骤：1) 利用监控主机和远程接口的安全漏洞，获取相应的控制权限；2) 利用协议或消息漏洞不断渗透并到达相关设备；3) 干扰或破坏相关设备的正常功能，使受控物理设备运行在不良状态，扰乱电网的正常运行。另一方面，如果攻击从位于模型底部的互感器等开始，则通常通过篡改和中断传感器数据使控制中心无法看到真实的电网状态。因此，下达的控制命令必然会偏离实际需求，从而导致电网故障。

基于上述分析，可以发现两种角度的攻击目标都聚焦在执行器(开关等)和传感器(互感器等)，而这两类设备也是信息系统和物理系统互动的关键节点。因此，上述模型可以进一步简化，如图 2 所示。

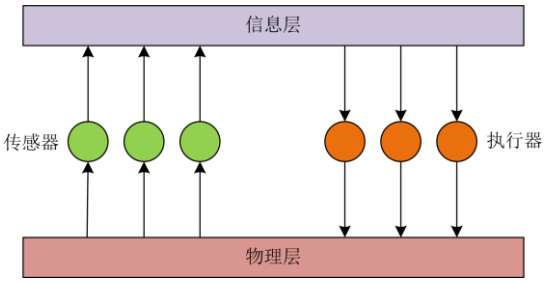

图 2 电力信息物理系统简化模型

Fig. 2 Simplified model of cyber-physical power system

中国的电力基础设施一直走在世界的前列，物联网、大数据、云计算等技术在电网上的应用十分广泛。尽管电力系统在全球范围内尤其是在中国正经历着重大的升级，但同时也面临着一些重大的挑战，具体来说：1) 近年来，主网的传感设备部署程度已经较高，但配网侧的传感器数量少，可观性和智能化程度都较低，数据下沉不足，无法对高级数据分析形成有效支撑。尽管电力物联网正在持续推进，但离终态尚有距离。2) 对目前已经部署的物联、传感设备，其通信协议、组件、应用均呈现异构特点，数据壁垒依旧存在，难以实现广泛集成。既能保证安全性，又具备充分开放性的协议标准有待进一步研究和推广。3) 随着数据的下沉，末端计算存储资源和大数据分析实时性之间的矛盾日益加深，需要包括边缘计算、雾计算、云计算在内的多元化的数据分析平台。

在上述发展背景下，考虑模型和数据双重驱动的电力信息物理系统动态安全防护的本质就是基于历史数据的离线学习和基于量测数据的在线分析有机结合。一方面，基于数据挖掘、机器学习和专家知识的安全知识模型库和数据库能够在难以建立精确的电力信息物理系统动态安全防护模型的情况下提供高准确率的分析结果。另一方面，电力信息物理系统的模型能够弥补数据驱动方法在可解释性上的不足，同时在线分析结果又能不断丰富历史数据库，使得系统具备自趋优特性。

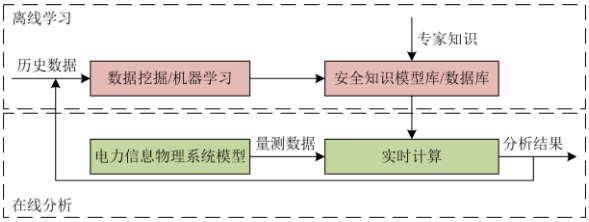

图 3 模型与数据双驱动的电力信息物理系统动态安全防护

Fig. 3 Dynamic security protection on cyber physical power system considering model and data driving

2 数据驱动的快速入侵检测

入侵检测是智能电网动态协同安全防护的基础，在工业及信息领域都受到广泛关注，其主要任务是实时监测系统行为并发现网络攻击。

2.1 智能电网网络安全威胁

伴随着信息领域新技术、新设备的大量涌现，智能电网面临的高级威胁日益增多，种类繁杂。本文依据信息安全要素，即 CIA 目标，将网络攻击分为四类，包括：中断、截取、篡改及伪造[12]。

2.1.1 中断攻击

中断攻击以系统可用性为目标，损害相关资源，致使信息系统无法提供正常服务。DoS 攻击是一种典型的中断攻击，包括带宽攻击和连通性攻击，前者消耗网络资源，后者消耗操作系统资源。文献[3]指出通过对 PMU 或智能量测单元施加 DoS 攻击使其数据丢失或产生延时，将会导致电力系统状态估计偏差或电网量测设备故障。文献[13]证明即使仅对电力通信网络节点子集实施 DoS 攻击，也可能破坏整个网络，从而对电力系统稳定性和可靠性造成严重损坏。当攻击者联合控制多台主机并同时向目标发起 DoS 攻击时，就形成了 DDoS 攻击。由于此种攻击模式是分布式的，难以溯源，并且攻击规模和强度都远胜 DoS，已经成为最主要的中断攻击方法。文献[14]指出在过去的十年里，DDoS 攻击的规模和数量一直在增长，现有的解决方案效率较低，通过数据包检测很难有效识别。

2.1.2 截取攻击

截取攻击是指未经授权的实体对资源的非法访问，即保密性攻击。例如在 PMU 和相量数据集中器(PCD)之间的信道中获取电网功角量测信息。典

型的截取攻击包括数据包探嗅和边信道攻击。文献[15]指出在没有加密的情况下，攻击者可以使用Wireshark等软件程序访问PMU或智能量测单元发送的所有数据包内容。文献[16]研究表明强大的加密算法虽然可以保证其在数学层面上的安全，但是算法所依赖的物理平台却仍然会将功率损耗、电磁辐射、加密时间等形式的边信道信息泄露，攻击者可以利用上述信息提取加密设备密钥。

2.1.3 篡改攻击

篡改攻击是指攻击者在未经授权的情况下，非法获取数据并进行修改。攻击者通常利用智能电网中的安全漏洞对其数据库或信道进行劫持，进而修改相关数据，其目的是破坏信息完整性。中间人攻击(Man-in-the-middle, MITM)和结构化查询语言(Structured Query Language, SQL)注入是较为常见的篡改攻击方式。

文献[17]指出MITM攻击是指恶意的第三方即攻击者秘密控制两台或多台主机之间的通信信道，攻击者可以控制并修改传输数据，但主机并不知道攻击者的存在。文献[18]基于SCADA系统专用的网络安全测试平台研究了MITM攻击问题并指出有效的入侵检测技术是解决SCADA系统网络安全的重要支撑。SQL注入攻击可以通过软件漏洞在目标数据库中插入恶意脚本命令，使攻击者能够绕过身份验证和授权等安全措施，检索整个数据库，也可以通过SQL注入来添加、修改或删除相关数据[19-20]，目前主要有5种类型的SQL注入攻击，具体来讲：1) Boolean注入攻击，即根据注入后回显的布尔变量获取数据库相关信息；2) 报错注入攻击，即从回显的错误消息中获取相关信息；3) 堆叠查询注入攻击，即利用相关漏洞，同时执行多条任意的SQL语句；4) Union注入攻击，原理类似于堆叠查询注入攻击，但仅允许使用SELECT语句；5) 时间注入攻击，攻击者利用SLEEP、WAITFOR和BENCHMARK等典型关键字检索敏感信息或根据目标数据库响应时间判断假设条件的真伪。当电网遭受SQL注入攻击时，会使电网运行的非正常态无法被察觉，造成系统崩溃[3]。文献[21]对SQL注入攻击展开研究，优化深度森林结构，有效检测SQL注入攻击。

2.1.4 伪造攻击

如前文所述，篡改攻击是指对既有数据的修改，而伪造攻击则是虚构不存在的数据。攻击者通过在电力信息网络中创建一个虚拟实体设备并发送虚拟数据。如果系统缺乏有效的身份验证机制，上述伪造数据很可能被其他实体设备接收，导致真实的电网运行态势无法被感知，电网运行风险剧增。数据欺骗是一种典型的伪造攻击。文献[22]列举了若干向智能电网注入虚假信息的案例如电压、电流、频率及GPS授时等，研究表明伪造攻击将造成电网稳定性、安全性及可靠性的严重降级。电力系统中的故障检测、事故定位等功能都依赖于GPS的精准授时，时间戳攻击(Time Stamp Attack, TSA)通过欺骗GPS影响电网同步测量。文献[23]在3机9节点测试系统中进行蒙特卡罗模拟，证明此类攻击对具有PMU的智能电网状态估计具有严重影响。文献[24-25]研究了电力信息物理融合背景下的虚假数据注入攻击，并分别提出了代价分析方法和安全防御策略。

上述网络攻击分类涵盖了各种攻击的特点，但不足以准确描述现阶段以及未来的智能电网网络攻击。随着现代电力系统的数字化建设逐步完善，电力信息发生了时间、空间和形态上的多维度转变，在提升电网可观性的同时，也为各种高级威胁提供了入侵机会。针对智能电网的网络协同攻击是经过精心策划和精准执行的，发生于信息系统却精准作用于物理系统，具体来讲：1) 从渗入手段上看，此类协同攻击具有很强的漏洞利用能力，尤其是末端物联设备，并能充分利用电力信息在时间、空间上大尺度转移的特点进行广泛传播；2) 从攻击手段上看，网络攻击具有多元化和智能化发展趋势，攻击具备自学习能力，可以根据攻击资源、对象特征自主选择攻击组合方式和目标；3) 从潜伏手段上看，高级协同攻击样本很难获取，难以短时间内形成有效检测方法。

2.2 智能电网入侵检测

目前的信息安全防护系统在入侵检测方面提出了不同的实现手段，总体可以分为以下三个方面：1) 误用检测(misuse-based detection)；2) 规程检测(specification-based detection)；3) 异常检测(anomaly-based detection)[26]。

2.2.1 误用检测

误用检测通过描述攻击行为特征，指定完善检测规则来辨识已知威胁，因此又称为基于知识的入侵检测。文献[27]通过对智能电子设备(Intelligent Electronic Device, IED)发起数据包嗅探模拟攻击并收集数据开发了一种变电站入侵检测系统(Intrusion Detection Systems, IDS)。但是该方法仅限于使用IEC61850通信标准的变电站且无法应对未知攻击。此外，文献[28-30]还指出，此类入侵检测方法的缺陷还包括：1) 维护已知攻击的特征和规则数据库要求巨大的存储空间；2) 高度依赖人为操作来更新安全规则数据库；3) 很难应对当前层出不穷的先进网

络攻击。

2.2.2 规程检测

规程检测根据通信协议、业务流程、运行方式等系统自身特征，制定检测规则，识别明显系统偏差以辨识网络攻击。文献[31]设计了一种基于多模型的入侵检测系统，在实际攻击与故障的判别中采用了隐马尔可夫模型分类器，具备相当的智能与弹性协调能力。但规程检测同样无法应对未知攻击。

2.2.3 异常检测

异常检测很大程度上可以视作人工智能(Artificial Intelligence, AI)方法在工控系统安全防护领域的具体应用。因此该方法的性能与训练数据集和测试数据集的数量、质量密切相关。异常检测系统从经验和数据中获取系统正常态运行特征，并在线计算系统当前状态与正常态的距离，实现异常检测。早期成功的 AI 技术是基于完全形式化的规则列表来完成相应任务的，文献[32]通过建立完善的控制逻辑行为规则先验知识库，对 SCADA 系统实现复杂攻击的检测。该方法与误用检测的区别在于前者建立的规则数据库更完备[33]。

电力信息物理系统是一个极其庞大而复杂的系统，充满不确定性和随机性，精准而确定的规则很难应用、维护并且脆弱。因此，统计分析方法在入侵检测中应用广泛。文献[34]基于多变量统计分析开发了一种可监控潮流结果和检测网络攻击的算法，利用主成分分析法对潮流变化不规则子空间中的信息进行分析，并确认电网数据是否被泄露或修改。

电力大数据的完善促使机器学习方法成为异常检测的重要手段。不少研究采用支持向量机[35]、Adaboost[36]、循环神经网络[37]以及各种组合算法[38]等监督算法对网络攻击进行检测，但电力系统数据分布极不平衡，标注样本数量远小于未标注样本数量，导致监督算法受到较多局限。在此背景下，半监督学习和无监督学习成为基于表示学习的未知攻击检测方法的重要研究方向。文献[39]设计了一种无监督聚类算法用于自动识别给定系统 SCADA 数据的一致性状态并从中自动提取接近度检测规则。文献[40]针对完整性攻击，开发了一种融合线性时不变模型和神经网络模型的完整性攻击检测方法，并在 IEEE30 节点系统上进行仿真，结果表明该方法可以检测不同强度的完整性攻击。文献[41]针对错误数据注入攻击提出了一种基于条件深度信念网络架构的实时检测机制，利用历史数据学习攻击行为特征进行在线检测，实验结果表明该方法具有良好的检测效果和扩展性。

异常检测无需先验知识和建立规则数据库，在资源占用方面相较于误用检测和规程检测更少，对从 CPPS 末端发起的入侵具有更好的检测效果。从检测能力看，异常检测通过特征学习捕获攻击模式，可以检测未知攻击。

2.3 数据驱动下的入侵检测系统发展

信息技术的变革与进步，推动了现代电力系统的数字化发展。随着电力系统末端数据下沉、计算机硬件资源不断丰富以及 AI 技术的快速发展，基于机器学习的入侵检测系统将成为 CPPS 安全防护的重要支撑。据统计，仅国家电网所辖电网中的各类智能终端数量已突破 5 亿套，数据日增量达 60 TB 级，可整理形成大量适用于机器学习的应用数据集。此外，高性能 CPU 与通用 GPU 的出现提高了硬件计算能力，5G 通信技术和分布式计算软件基础设施的完善，促使人工神经网络规模迅速扩大。机器学习可使用的基准数据规模、模型规模与入侵检测系统的自动化程度的变化如图 4 所示。

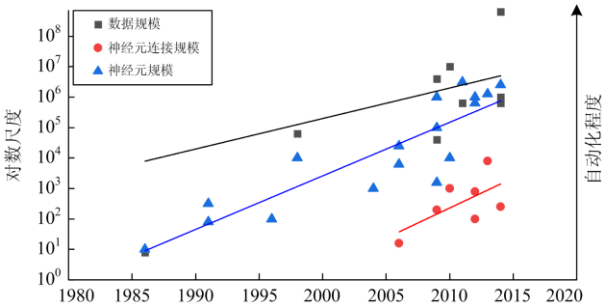

图 4 数据驱动下的入侵检测系统发展趋势

Fig. 4 Development of intrusion detection system under data-driven

更庞大的数据和更强劲的计算资源促使机器学习模型在深度和广度上同时进步，基于机器学习的动态入侵检测方法灵活而鲁棒，应该作为数据驱动背景下入侵检测的主要方法。但是，考虑到电力信息物理系统本体特征，仍有重要问题有待进一步研究，具体包括：1) 数据不均衡，安防事件数据非常稀缺，而系统运行数据却极为丰富，且大部分数据为未标注样本，通过无监督学习充分利用未标注样本在小数据集上获得强泛化能力是一个重要研究方向；2) 系统异构，电力信息物理系统宏观上信息、物理异构集成，微观上结构化数据与非结构化数据、离散数据与连续数据并存，如何高效管理数据是系统安防技术发展的重要基础。

3 信息物理穿透式风险评估

智能电网风险评估的目的是对系统安全态势做分级或量化，一般采用事件驱动型指标[42]，其整体

评估框架如图 5 所示。

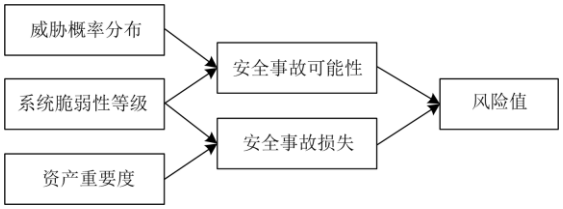

图 5 风险评估框架

Fig. 5 Framework of risk assessment

由图 5 可知，智能电网风险评估涵盖两个核心环节：1) 系统脆弱性评估；2) 系统安全风险评估。前者指系统中薄弱节点或二次侧漏洞被利用的概率，后者指系统遭受攻击的后果期望值[43]。一般程度的网络攻击仅对电力监控系统若干子功能造成降级，但当攻击穿透信息系统与物理系统边界时，则有可能造成失负荷甚至连锁故障[44]。因此信息物理穿透式风险评估对现代智能电网更具现实意义。

3.1 智能电网系统结构脆弱性评估

智能电网是信息系统与物理系统深度交互而形成的耦合系统，节点规模庞大、拓扑结构灵活、故障传播机制复杂，是典型的复杂网络。数字化发展趋势使得智能电网正从传统的模型驱动转变为数据驱动，同时也发生了从设备导向建模到功能导向建模的深刻改变。关键节点的失效将导致系统可观性、可控性的降级，引发严重后果。因此，需要从复杂网络角度出发，分析智能电网连锁故障问题和耦合网络脆弱性问题。

3.1.1 信息物理系统一体化建模

自从 2006 年欧美兴起信息物理系统的研究以来，融合建模一直是研究焦点之一，在信息物理异构性[45]、信息系统时序性[46]等方面都取得了一定进展，但现阶段的建模对象大多以设备、元件为主。设备导向型的信息物理系统融合建模通常借助有穷自动机、随机过程等数据工具，采用设备状态分析、概率统计、故障率函数生成等方法，联立信息系统与物理系统的微分代数方程组，形成统一模型。文献[47]利用上述理论方法，对传感单元、传输单元及计算单元分别建立稳态与动态模型，并对电力信息物理系统进行可靠性和安全性分析。文献[48]提出基于有限状态机(Finite State Machine, FSM)及混合逻辑动态(Mixed Logical Dynamical, MLD)的信息物理系统融合模型，并建立相应的源荷储协调控制模型。文献[49]采用混合系统建模方法研究了潮流越限及系统失稳问题。文献[50]在信息模型属性和物理模型参数之间建立完整的对应关系，并集成光储微网协调控制模型。

上述建模方法以解决系统实际需求为目的，并不涉及信息物理的实质融合。此外，智能电网运行场景丰富、设备数量庞大，传统的设备导向型建模在完备性、通用性、灵活性、协同性等方面均有重大欠缺。具体来说：1) 随着智能电网信息化程度的提高，电网设备集合中包含了硬件实体设备和软件虚拟设备，其数量近乎无限，因此无法建立完备的模型库；2) 面向某一设备建立的模型通常包含了该设备的若干特点，即使是功能类似的设备也无法直接移植模型，通用性欠佳；3) 设备导向型建模各子模块之间耦合程度相对较高，极难对其解耦实现模块间自由组合，因此建模效率极低；4) 设备导向型建模难以消除信息系统和物理系统的天然壁垒、建立有效的协同互动机制，无法实现信息物理一体化。同时，智能电网的发展必然引来社会系统广泛参与电网的运行控制与风险调度，如何分析、挖掘、量化人为因素的逻辑价值，如何建立考虑信息-物理-社会协同的一体化模型作为未来智能电网信息安全风险评估中的基础性核心问题，亟待研究。

3.1.2 考虑动力学和统计学特征的系统结构脆弱性分析

20 世纪末，随着小世界网络和无标度网络概念的提出[51-52]，大量关于复杂网络的理论研究逐步展开，复杂网络理论体系初步成型。大量基于网络结构的节点重要性评估经典方法被提出，包括：度中心性方法[53]、介数中心性方法[54]、K-壳分解法[55]、PageRank 方法[56]等。但上述方法都基于统计学拓扑特征，并未计及节点行为及自身特性，在分析连锁故障问题以及网络脆弱性时有一定局限。

复杂网络动力学模型在考虑网络拓扑特性的同时也包括了对节点行为特性的思考，对研究网络连锁故障、脆弱性具有重要的理论价值。文献[57]构建了无向加权网络的动力学模型，以偏离均值和方差作为节点重要性评估指标，根据节点偏离平衡态对全网的影响程度确定节点重要性。文献[58]利用镜像拉普拉斯矩阵最小特征值判断节点重要度，研究表明该方法可广泛应用于复杂网络和多层网络的可控性分析及牵引控制中。文献[59]利用特征向量中心性实现了在拓扑约束下的最小全局资源使用和最高信息传输效率，配电网连锁故障与信息传输方式的内在联系需要进一步研究。文献[60-61]研究表明复杂网络可控性与网络结构和网络耦合强度直接相关，以增强拉普拉斯矩阵特征值比灵敏度作为度量节点影响力的指标，选择出网络中的最佳控制节点集。

模型与数据双重驱动背景下，智能电网可观性

与可控性深度耦合，关键节点识别和价值量化将为耦合系统连锁故障和网络脆弱性分析提供坚强的理论支撑。

3.2 智能电网的信息物理穿透式风险评估

一二次融合配电开关、分布式自愈终端、能量路由器、用户智慧网关等设备的投入，加强了信息系统、物理系统之间的耦合强度和动态交互，周期性信息安全风险评估难以满足实际需求。未来智能电网强调可观性与可控性并重，多元系统拓扑结构动态扩展，灵活组合，以达到源网荷储全局互动、高效稳定运行和能源高效利用的目的。单纯的二次系统信息安全评估无法展示电网安全细节，网络攻击带来的安全风险贯穿信息层和物理层，具体来讲，从耦合系统角度看，随着电网数字化发展，物理设备将被若干信息设备包围，同时又存在大量人机接口，社会因素对信息自身属性和信息物理耦合方式都产生影响；从单一系统角度看，智能电网的高效运行和源网荷储的灵活互动很大程度上依赖于系统的动态扩展，针对不同需求，调整设备组合，改变观测和控制目标，这就要求智能电网风险评估具有预测和实时评估能力。

关于电力信息安全风险评估的研究大多围绕评估模型展开，包括层次分析模型[62]、模糊神经网络[63]等。文献[64-65]针对基于 IEC61850 的电力控制系统信息安全风险评估问题，定义了信息交互价值、信息资产功能价值及信息资产系统价值等三个层级的价值量化方法，并应用于变电站自动化系统的风险评估中。文献[66]提出了基于功能分解的变电站自动化系统安全风险评估方法，建立功能风险等级评定方法和基于层次分析法的系统风险量化方法。文献[67]提出了一种调度自动化主站局域网冗余可靠性风险分析方法，经过机制分析和研究给出了相关推荐方案。文献[68]构建了基于关联规则挖掘算法的二次侧设备态势风险评估体系，主客观权重经合作博弈模型组合。文献[69]在智能变电站的安全风险计算中考虑了设备应用软件和电网管理服务系统软件失效带来的影响。但上述评估计算方法中的权重判定过度依赖人的主观判断，评估结果的客观性有待验证。

此外，从攻击后果展开的 CPPS 风险评估也是目前重要的研究方向，例如实时电价[70]、拓扑损失[71]、供需匹配[72-74]等指标。文献[75]提出了基于 CPPS 建模和信息物理交互机理的安全评估框架并从信息网络结构优化、路由优化和网络安防等三个方面总结了 CPPS 安全防御方法。但上述指标的相关性导致综合量化评估的结果存在一定失真。

当前针对模型与数据双重驱动背景下的智能电网信息物理穿透式风险评估及可靠性分析研究相当有限，未来的研究主要集中在以下几点。

1) 智能电网必然要实现多源异构数据的规范统一，信息深加工的可靠性分析是实现智能电网全景可观、全局可控的关键。因此需要深入研究泛在数据的规范建模问题。

2) 大量智能终端的接入赋予电网极强的主动响应能力，在智能电网风险评估中如何量化终端资源的响应能力对评估结果的准确性具有重大影响。

3) CPPS 拓扑结构复杂多变，在风险的量化计算中不仅要考虑信息资产价值，更需要综合网络拓扑价值，同时建立具有数学理论支撑的量化方法。

4 协同安全决策

CPPS 不同于传统信息系统或一般工业信息物理系统，电力信息系统的运行目标是保证电力物理系统正常运行，因此安全决策必须保障物理系统的可用性。

安全决策需要综合考虑网络攻击特征、系统风险态势、系统运行状况及系统安全知识，选取最优安全防御措施。从数学上看，这是一个多目标协同优化问题。安全决策方法总体可以分为两类：1) 静态决策；2) 动态决策。前者制定于系统设计阶段，策略相对固定，鲁棒性好但自适应能力差；后者属于主动防御，实时性高，自适应能力强但对系统可用性的影响相对较高。

4.1 智能电网静态安全决策

智能电网静态安全防御策略在离线阶段制定，在生产、运行、安全等多约束条件下实现对系统脆弱点的加固和攻防映射。文献[76]针对身份验证和授权服务设计了一种鲁棒且弹性的架构，并在 DoS 攻击、资源耗尽攻击、数据包损坏等网络攻击下进行测试，系统仍然可以正常运行。文献[77]建立了 PMU 网络的攻击优化响应模型，以保证网络可观性、最大程度降低安全威胁级别为约束，将最佳响应问题转化为混合整数线性规划问题。但高维线性规划问题求解耗时较多，难以在大规模电力系统中应用。文献[78]提出了一种基于软件定义网络(SDN)的通信网络架构，用于提高微电网在应对网络攻击时的弹性和安全性。

除了上述传统静态防护策略外，区块链作为一种革命性的去中心化技术也越来越多地被应用到能源领域，基于区块链技术的电力信息安全防护正成为一个重要的新研究方向[79]。文献[80]基于多层级可信思想构建了地市级能源互联网安全可信防护方

案。文献[81]针对电力市场多级交易链中的安全风险，设计了基于区块链框架的信息传递安全机制。文献[82]充分考虑 CPPS 数据私有化特征，提出了一种安全可行的数据区块链生成算法。但区块链作为新兴技术在 CPPS 安全防护领域实践案例较少，技术层面也暴露出诸多问题，具体包括：1) 数据处理效率及响应速度与网络规模成反比，在处理 CPPS 实时防护问题时可能无法满足需求；2) 分布式节点算力有限，难以实现本体安全；3) 与 IEC61850 等现有电力通信协议的兼容性问题。

静态安全决策对已知攻击具有较高防御成功率，而且易于实现，但其策略相对固化，难以应对智能电网拓扑灵活拓展和网络攻击未知变化。随着网络攻击智能化程度提升、未知攻击方法增多，单纯的静态安全策略极易被攻击者破解利用，成为优化攻击策略的重要资源，需要和动态安全决策相互配合。

4.2 智能电网动态安全决策

动态安全决策是根据入侵检测和风险评估结果，实时制定适用于当前攻击的防御策略，实现快速准确的入侵反应。基于 CPPS 对实时性的要求，应当尽量避免对人工操作的依赖，自动安全决策必然成为科学研究和工程实践的主流。

基于博弈论的资源配置策略是动态安全决策的重要研究方向，国内外专家学者建立了两阶段最大最小博弈[74]、多阶段随机博弈[83]等多种攻防博弈模型描述网络攻击的随机性。文献[84]针对 DoS 攻击提出了基于博弈论的弹性控制方法，对多任务结构和中心任务结构分别开发最优防御策略和最优攻击策略。文献[85]采用自适应马尔可夫策略(Adaptive Markov Strategy, AMS)保护智能电网抵御未知攻击，理论上可以保证收敛于最佳响应策略，即便攻击具有高级智能，可以利用 AMS，结果依然可以收敛至纳什均衡。该策略在变电站错误数据注入攻击中进行测试评估，结果表明可有效减少系统切负荷量。

此外，基于物理系统运行状态校正的安全决策方法也是目前的研究焦点之一。文献[86]针对数据注入攻击采用电力系统动态模型和分布式贝叶斯近似滤波器进行攻击检测和攻击向量估计，修正 PMU 量测数据误差。文献[87]设计了具有在线参数估计功能的自适应滑动观测器检测注入攻击。文献[88]针对数据完整性和可用性攻击提出了自适应网络使能参数反馈线性化控制策略，提高智能电网暂态稳定性。

上述动态安防策略虽然在自适应性和自动化程度上有所提高，但是决策的智能性和准确性高度依赖于学习模型和决策模型的粒度，同时必须充分考虑电网运行的多约束条件，因此在面对大规模智能电网系统或者多攻击者协同进攻的场景中，高昂的计算代价使动态决策方法难以实施。目前针对 CPPS 动态安全决策的研究还较少，需要解决的问题较为集中，具体包括：1) 构建跨层的精准统一决策模型；2) 复杂问题约束空间的降维和参数自学习方法；3) 安防域和工控域的有效隔离，在确保智能电网信息物理协同安全的同时保证电网正常运行。

5 结论

本文总结回顾了现阶段国内外专家学者在智能电网信息物理协同安全入侵检测、风险评估、安全决策等方面的研究成果，重点分析探讨了模型与数据双重驱动背景下智能电网信息物理协同安全防护的理论方法及其缺陷，提出智能电网安全防护亟待解决的关键科学问题和未来研究方向，为高度智能化、自动化的智能电网安全防护奠定理论基础。

模型与数据双重驱动下的智能电网信息物理协同安全问题可以分解为未知攻击快速入侵检测、信息物理穿透式风险评估及协同安全决策等 3 个科学问题，从智能电网运行特点和安全需求出发，分析了上述科学问题的主要研究方向和发展趋势，提出充分利用大数据、功能导向型建模等技术，实现智能电网信息物理协同安全防护的闭环控制的构想。随着智能电网数字化的相关科学研究和工程实践的深入展开，信息系统、物理系统及社会系统的交互方式不断变化，耦合程度不断提高，信息物理协同安全成为智能电网安全稳定运行的根本保障，安防域和工控域协同防护的理论意义和实践价值将不断提高。

参考文献

[1] RIFKIN J. The third industrial revolution: how lateral power is transforming energy, the economy, and the world[M]. New York: Palgrave Mac Millan, 2011.

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

[3] 邓杰, 姜飞, 涂春鸣. 美国 NIST 互操作性智能电网框架分析与启示[J]. 电力系统保护与控制, 2020, 48(3): 9-21.
DENG Jie, JIANG Fei, TU Chunming. Study of NIST's iteroperable smart grid technology architecture[J]. Power System Protection and Control, 2020, 48(3): 9-21.

[4] BEDI G, VENAYAGAMOORTHY G K, SINGH R, et al. Review of internet of things (IoT) in electric power and energy systems[J]. IEEE Internet of Things Journal, 2018, 5(2): 847-870.

[5] MCLAUGHLIN S, KONSTANTINOU C, WANG X, et al. The cybersecurity landscape in industrial control systems[J]. Proceedings of the IEEE, 2016, 104(5): 1039-1057.

[6] LANGNER R. Stuxnet: dissecting a cyberwarfare weapon[J]. IEEE Security & Privacy, 2011, 9(3): 49-51.

[7] 赵俊华, 梁高琪, 文福拴, 等. 乌克兰事件的启示: 防范针对电网的虚假数据注入攻击[J]. 电力系统自动化, 2016, 40(7): 149-151.
ZHAO Junhua, LIANG Gaoqi, WEN Fushuan, et al. Lessons learnt from Ukrainian blackout: protecting power grid against false data injection attacks[J]. Automation of Electric Power Systems, 2016, 40(7): 149-151.

[8] National Institute for Standards and Technology (NIST). Guide to industrial control systems (ICS) security-supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC): NIST.SP.800-82[S]. 2011.

[9] 程群, 何奇松. 德国网络空间透明与信任建设简析[J]. 德国研究, 2017, 32(2): 25-41, 124-125.
CHENG Qun, HE Qisong. A brief analysis of transparency and trust building in German cyberspace[J]. Deutschland-Studien, 2017, 32(2): 25-41, 124-125.

[10] 国家发展与改革委员会. 电力监控系统安全防护规定[EB/OL]. [2014-08-01]. https://www.ndrc.gov.cn/xxgk/zcfb/fzggwl/201408/t20140814_960784.html?code=&state=123.
Safety protection regulations for power monitoring system[EB/OL]. [2014-08-01]. https://www.ndrc.gov.cn/xxgk/zcfb/fzggwl/201408/t20140814_960784.html?code=&state=123.

[11] National Institute for Standards and Technology (NIST). Guidelines for smart grid cyber security: vol. 3, supportive analyses and references: NISTIR 7628[S]. 2010.

[12] BROOKS R R. Disruptive security technologies with mobile code and peer-to-peer networks[M]. USA: CRC Press, 2005.

[13] SRIKANTHA P, KUNDUR D. Denial of service attacks and mitigation for stability in cyber-enabled power grid[C] // IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), February 18-20, 2015, Washington, DC, USA: 1-5.

[14] MOLDE B E, ANIS Y, HERRERA V E, et al. DoS and DDoS mitigation using variational autoencoders[J]. Computer Networks, 2021, 199.

[15] BEASLEY C, ZHONG X, DENG J, et al. A survey of electric power synchrophasor network cyber security[C] // IEEE PES Innovative Smart Grid Technologies, Europe, October 12-15, 2014, Istanbul, Turkey: 1-5.

[16] DAS D, MAITY S, NASIR S B, et al. ASNI: attenuated signature noise injection for low-overhead power side-channel attack immunity[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2018, 65(10): 3300-3311.

[17] CONTI M, DRAGONI N, LESYK V. A survey of man in the middle attacks[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2027-2051.

[18] YANG Y, MCLAUGHLIN K, LITTLER T, et al. Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems[C] // International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012), September 8-9, 2012, Hangzhou, China: 1-8.

[19] GU H, ZHANG J, LIU T, et al. DIAVA: a traffic-based framework for detection of SQL injection attacks and vulnerability analysis of leaked data[J]. IEEE Transactions on Reliability, 2020, 69(1): 188-202.

[20] MEDEIROS I, BEATRIZ M, NEVES N, et al. SEPTIC: detecting injection attacks and vulnerabilities inside the DBMS[J]. IEEE Transactions on Reliability, 2019, 68(3): 1168-1188.

[21] LI Q, LI W, WANG J, et al. A SQL Injection detection method based on adaptive deep forest[J]. IEEE Access, 2019, 7: 145385-145394.

[22] SRIDHAR S, HAHN A, GOVINDARASU M. Cyber-physical system security for the electric power grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.

[23] PRADHAN P, NAGANANDA K, VENKITASUBRAMANIAM P, et al. GPS spoofing attack characterization and detection in smart grids[C] // IEEE Conference on Communications and Network Security (CNS), October 17-19, 2016, Philadelphia, USA: 391-395.

[24] 赵丽莉, 刘忠喜, 孙国强, 等. 基于非线性状态估计的虚假数据注入攻击代价分析[J]. 电力系统保护与控制, 2019, 47(19): 38-45.
ZHAO Lili, LIU Zhongxi, SUN Guoqiang, et al. Cost analysis of the false data injection attack based on nonlinear state estimation[J]. Power System Protection and Control, 2019, 47(19): 38-45.

[25] 王电钢, 黄林, 刘捷, 等. 考虑负荷虚假数据注入攻击的电力信息物理系统防御策略[J]. 电力系统保护与控制, 2019, 47(1): 28-34.
WANG Diangang, HUANG Lin, LIU Jie, et al. Cyber-physical system defense strategy considering loaded false data injection attacks[J]. Power System Protection and Control, 2019, 47(1): 28-34.

[26] MITCHELL R, CHEN I R. A Survey of intrusion detection techniques for cyber-physical systems[J]. ACM Computing Surveys, 2014, 46(4): 55-65.

[27] PREMARATNE U K, SAMARABANDU J, SIDHU T S, et al. An intrusion detection system for IEC61850 automated substations[J]. IEEE Transactions on Power Delivery, 2010, 25(4): 2376-2383.

[28] PAPAMARTZIVANOS D, MÁRMOL F G, KAMBOURAKIS G. Introducing deep learning self-adaptive misuse network intrusion detection systems[J]. IEEE Access, 2019, 7: 13546-13560.

[29] RADIVILOVA T, KIRICHENKO L, ALGHAWLI A S, et al. The complex method of intrusion detection based on anomaly detection and misuse detection[C] // Proceedings of the IEEE 11th International Conf. Dependable System, Services and Technology, May 14-18, 2020, Kyiv, Ukraine: 133-137.

[30] VARAL A S, WAGH S K. Misuse and anomaly intrusion detection system using ensemble learning model[C] // Proceedings of the International Conference Recent Innovations in Electrical, Electronics & Communication Engineering, July 27-28, 2018, Bhubaneswar, India: 1722-1727.

[31] ZHOU C, HUANG S, XIONG N, et al. Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2015, 45(10): 1345-1360.

[32] FOVINO I N, COLETTA A, CARCAN A, et al. Critical state-based filtering system for securing SCADA network protocols[J]. IEEE Transactions on Industrial Electronics, 2012, 59(10): 3943-3950.

[33] HUANG K, ZHANG Q, ZHOU C, et al. An efficient intrusion detection approach for visual sensor networks based on traffic pattern learning[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017, 47(10): 2704-2713.

[34] VALENZUELA J, WANG J, BISSINGER N. Real-time intrusion detection in power system operations[J]. IEEE Transactions on Power Systems, 2013, 28(2): 1052-1062.

[35] AHMAD I, BASHERI M, IQBAL M J, et al. Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection[J]. IEEE Access, 2018, 6: 33789-33795.

[36] HU W, GAO J, WANG Y, et al. Online Adaboost-based parameterized methods for dynamic distributed network intrusion detection[J]. IEEE Transactions on Cybernetics, 2014, 44(1): 66-82.

[37] YIN C, ZHU Y, FEI J, et al. A deep learning approach for intrusion detection using recurrent neural networks[J]. IEEE Access, 2017, 5: 21954-21961.

[38] AL-QATF M, LASHENG Y, AL-HABIB M, et al. Deep learning approach combining sparse autoencoder with SVM for network intrusion detection[J]. IEEE Access, 2018, 6: 52843-52856.

[39] ALMALAWI A, YU X, TARIA Z, et al. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems[J]. Computers & Security, 2014, 46: 94-110.

[40] NTALAMPIRAS S. Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling[J]. IEEE Transactions on Industrial Informatics, 2015, 11(1): 104-111.

[41] HE Y, MENDIS G J, WEI J. Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2505-2516.

[42] 崔建磊, 文云峰, 郭创新, 等. 面向调度运行的电网安全风险管理控制系统: (二)风险指标体系、评估方法与应用策略[J]. 电力系统自动化, 2013, 37(10): 92-97.
CUI Jianlei, WEN Yunfeng, GUO Chuangxin, et al. Design of a security risk management system for power system dispatching and operation part two: risk index, assessment methodologies and application strategies[J]. Automation of Electric Power Systems, 2013, 37(10): 92-97.

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

[44] 刘念, 余星火, 张建华. 网络协同攻击: 乌克兰停电事件的推演与启示[J]. 电力系统自动化, 2016, 40(6): 144-147.
LIU Nian, YU Xinghuo, ZHANG Jianhua. Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid[J]. Automation of Electric Power Systems, 2016, 40(6): 144-147.

[45] HU L, XIE N, KUANG Z, et al. Review of cyber-physical system architecture[C] // Proceedings of the 15th IEEE International Symposium on Object/ Component/ Service-Oriented Real-Time Distributed Computing Workshops, April 11, 2012, Shenzhen, China: 25-30.

[46] WOLF W. The goodnews and the bad news[J]. Journal Computer, 2007, 40(11): 104-105.

[47] 赵俊华, 文福拴, 薛禹胜, 等. 电力信息物理融合系统的建模分析与控制研究框架[J]. 电力系统自动化, 2011, 35(16): 1-8.
ZHAO Junhua, WEN Fushuan, XUE Yusheng, et al. Modeling analysis and control research framework of cyber physical power systems[J]. Automation of Electric Power Systems, 2011, 35(16): 1-8.

[48] 王云, 刘东, 陆一鸣. 电网信息物理系统的混合系统建模方法研究[J]. 中国电机工程学报, 2016, 36(6): 1464-1470.
WANG Yun, LIU Dong, LU Yiming. Research on hybrid system modeling method of cyber physical system for

power grid[J]. Proceedings of the CSEE, 2016, 36(6): 1464-1470.

[49] SUSUKI Y, KOO T, EBINA H, et al. A hybrid system approach to the analysis and design of power grid dynamic performance[J]. Proceedings of the IEEE, 2012, 100(1): 225-239.

[50] 曾倬颖, 刘东. 光伏储能协调控制的信息物理融合建模研究[J]. 电网技术, 2013, 37(6): 1506-1513.
ZENG Zhuoying, LIU Dong. Study on cyber-physical system modeling on coordinated control of photovoltaic generation and battery energy storage system[J]. Power System Technology, 2013, 37(6): 1506-1513.

[51] JIANG Y, GE X, ZHONG Y, et al. A new small-world IoT routing mechanism based on cayley graphs[J]. IEEE Internet of Things Journal, 2019, 6(6): 10384-10395.

[52] PARK J. Distributed algorithm for making scale-free network by preferential rewiring without growth[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3125-3132.

[53] MENDONÇA M R F, BARRETO A M S, ZIVIANI A. Approximating network centrality measures using node embedding and machine learning[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(1): 220-230.

[54] MILANOVIĆ J V, ZHU W. Modeling of interconnected critical infrastructure systems using complex network theory[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4637-4648.

[55] JEYARAJAH R, KEILAR M, FRANTZ N, et al. Identification of Influential spreaders in complex networks[J]. Nature Physics, 2010, 6(11): 888-893.

[56] AVELLA-MEDINA M, PARISE F, SCHAUB M T, et al. Centrality measures for graphons: accounting for uncertainty in networks[J]. IEEE Transactions on Network Science and Engineering, 2020, 7(1): 520-537.

[57] 孔江涛, 黄健, 龚建兴, 等. 基于复杂网络动力学模型的无向加权网络节点重要性评估[J]. 物理学报, 2018, 67(9): 255-271.
KONG Jiangtao, HUANG Jian, GONG Jianxing, et al. Evaluation methods of node importance in undirected weighted networks based on complex network dynamics models[J]. Acta Physica Sinica, 2018, 67(9): 255-271.

[58] ZHOU J, YU X, LU A. Node importance in controlled complex network[J]. IEEE Transactions on Circuits and Systems, 2019, 66(3): 437-441.

[59] BALDESI L, MACCARI L, CIGNO R L. On the use of eigenvector centrality for cooperative streaming[J]. IEEE Communications Letters, 2017, 21(9): 1953-1956.

[60] AMANI A M, M JALILI, YU X, et al. Finding the most influential nodes in pinning controllability of complex networks[J]. IEEE Transactions on Circuits and Systems, 2017, 64(6): 685-689.

[61] ZHOU J, LU J, LÜ J. Pinning adaptive synchronization of a general complex dynamical network[J]. Automatica, 2008, 44(4): 996-1003.

[62] 韩霞, 郭易鑫, 王晖南, 等. 基于 AHP 的电力运行信息安全管理风险评估的研究[J]. 国外电子测量技术, 2018, 37(5): 32-37.
HAN Xia, GUO Yixin, WANG Huinan, et al. Study on the risk assessment of power operation information security management based on AHP[J]. Foreign Electronic Measurement Technology, 2018, 37(5): 32-37.

[63] 马虹哲. 电力企业信息安全风险动态评估模型的构建与应用[J]. 电力信息与通信技术, 2017, 15(11): 22-25.
MA Hongzhe. Construction and application of the dynamic assessment model of information security risk in the power grid enterprise[J]. Electric Power Information and Communication Technology, 2017, 15(11): 22-25.

[64] LIU Nian, ZHANG Jianhua, WU Xu. Asset analysis of risk assessment for IEC 61850-based power control systems—part I: methodology[J]. IEEE Transactions on Power Delivery, 2011, 26(2): 869-875.

[65] LIU Nian, ZHANG Jianhua, WU Xu. Asset analysis of risk assessment for IEC 61850-based power control systems—part II: application in substation[J]. IEEE Transactions on Power Delivery, 2011, 26(2): 876-881.

[66] 郭创新, 俞斌, 郭嘉, 等. 基于 IEC61850 的变电站自动化系统安全风险评估[J]. 中国电机工程学报, 2014, 34(4): 685-694.
GUO Chuangxin, YU Bin, GUO Jia, et al. Security risk assessment of the IEC61850-based substation automation system[J]. Proceedings of the CSEE, 2014, 34(4): 685-694.

[67] 吴坡, 张江南, 王丹, 等. 调度自动化主站局域网冗余可靠性风险分析[J]. 电力系统保护与控制, 2021, 49(11): 172-180.
WU Po, ZHANG Jiangnan, WANG Dan, et al. Risk analysis on redundancy reliability of a local area network in the master station of a dispatching automation system[J]. Power System Protection and Control, 2021, 49(11): 172-180.

[68] 南东亮, 王维庆, 张陵, 等. 基于关联规则挖掘与组合赋权-云模型的电网二次设备运行状态风险评估[J]. 电力系统保护与控制, 2021, 49(10): 67-76.
NAN Dongliang, WANG Weiqing, ZHANG Ling, et al. Risk assessment of the operation state of power grid secondary equipment based on association rule mining and combination weighting-cloud model[J]. Power System Protection and Control, 2021, 49(10): 67-76.

[69] 韩宇奇, 郭嘉, 郭创新, 等. 考虑软件失效的信息物理融合电力系统智能变电站安全风险评估[J]. 中国电机工程学报, 2016, 36(6): 1500-1508.
HAN Yuqi, GUO Jia, GUO Chuangxin, et al. Intelligent substation security risk assessment of cyber physical power systems incorporating software failures[J]. Proceedings of the CSEE, 2016, 36(6): 1500-1508.

[70] TAN S, SONG W, STEWART M, et al. Online data integrity attacks against real-time electrical market in smart grid[J]. IEEE Transactions on Smart Grid, 2018, 9(1): 313-322.

[71] VELLAITHURAI C, SRIVASTAVA A, ZONOUZ S, et al. CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures[J]. IEEE Transactions on Smart Grid, 2015, 6(2): 566-575.

[72] GIRALDO J, CÁRDENAS A, QUIJANO N. Integrity attacks on real-time pricing in smart grids: impact and countermeasures[J] IEEE Transactions on Smart Grid, 2017, 8(5): 2249-2257.

[73] 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, 2013, 28(2): 1676-1686.

[74] MO H, SANSAVINI G. Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks[J]. IEEE Transactions on Reliability, 2017, 66(4): 1253-1265.

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

[76] KREUTZ D, MALICHEVSKYY O, FEITOSA E, et al. A cyber-resilient architecture for critical security services[J]. Journal of Network and Computer Applications, 2016, 63: 173-189.

[77] MOUSAVIAN S, VALENZUELA J, WANG J. A probabilistic risk mitigation model for cyber-attacks to PMU networks[J]. IEEE Transactions on Power Systems, 2015, 30(1): 156-165.

[78] JIN D, LI Z, HANNON C, et al. Toward a cyber resilient and secure microgrid using software-defined networking[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2494-2504.

[79] 赵曰浩, 彭克, 徐丙垠, 等. 能源区块链应用工程现状与展望[J]. 电力系统自动化, 2019, 43(7): 14-22, 58.
ZHAO Yuehao, PENG Ke, XU Bingyin, et al. Status and prospect of pilot project of energy blockchain[J]. Automation of Electric Power Systems, 2019, 43(7): 14-22, 58.

[80] 龚钢军, 高爽, 陆俊, 等. 地市级区域能源互联网安全可信防护体系研究[J]. 中国电机工程学报, 2018, 38(10): 2861-2873.
GONG Gangjun, GAO Shuang, LU Jun, et al. Study on secure trusted protection architecture for prefecture-level regional energy internet[J]. Proceedings of the CSEE, 2018, 38(10): 2861-2873.

[81] 李彬, 曹望璋, 卢超, 等. 非可信环境下基于区块链的多级 DR 投标安全管理及技术支撑[J]. 中国电机工程学报, 2018, 38(8): 2272-2283.
LI Bin, CAO Wangzhang, LU Chao, et al. Security management and technique support for multi-level DR bidding under untrusted environment based on blockchain[J]. Proceedings of the CSEE, 2018, 38(8): 2272-2283.

[82] 杨挺, 赵俊杰, 张卫欣, 等. 电力信息物理融合系统数据区块链生成算法[J]. 电力自动化设备, 2018, 38(10): 74-80.
YANG Ting, ZHAO Junjie, ZHANG Weixin, et al. Data blockchain generation algorithm of cyber physical power system[J]. Electric Power Automation Equipment, 2018, 38(10): 74-80.

[83] WEI L, 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.

[84] YUAN Y, YUAN H, GUO L, et al. Resilient control of networked control system under DoS attacks: a unified game approach[J]. IEEE Transactions on Industrial Information, 2016, 12(5): 1786-1794.

[85] HAO J, KANG E, SUN J, et al. An adaptive markov strategy for defending smart grid false data injection from malicious attackers[J]. IEEE Transactions on Smart Grid, 2018, 9(4): 2398-2408.

[86] KHALID H M, PENG J C. A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks[J]. IEEE Transactions on Smart Grid, 2016, 7(4): 2026-2037.

[87] AO W, SONG Y, WEN C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems[J]. IET Control Theory & Applications, 2016, 10(12): 1458-1468.

[88] FARRAJ A, HAMMAD E, KUNDUR D. A distributed control paradigm for smart grid to address attacks on data integrity and availability[J]. IEEE Transactions on Signal and Information Processing over Networks, 2018, 4(1): 70-81.

收稿日期：2021-07-13；　修回日期：2021-10-31

作者简介：

杨　杰(1992—)，男，博士研究生，研究方向为电力信息物理融合系统；E-mail: yangjie_1113@zju.edu.cn

郭逸豪(1995—)，男，博士研究生，研究方向为电力信息物理融合系统；E-mail: guoyihao@zju.edu.cn

郭创新(1969—)，男，通信作者，博士，教授，博士生导师，研究方向为电力信息物理融合系统、智能电网风险评估。E-mail: guochuangxin@zju.edu.cn

（编辑　魏小丽）