基于云边协同计算的主动配电网调度研究评述

李知艺，宋克轩

（浙江大学 NGICS 大平台/电气工程学院，杭州 310027）

摘 要：随着增量配电改革推进，多元利益主体涌现，主动配电网呈现供需多方互动、信息物理融合等显著特点，而传统的集中调度决策方式难以继续适用。立足于云计算、边缘计算等前沿信息技术在主动配电网中应用的适用性和安全性，依次评述了电力系统联合调度、云计算与边缘计算、电力信息安全防御等研究热点的现有进展与发展动态，旨在为解决调控资源分散、计算资源异构、安全防御薄弱等关键问题厘清思路。最后，强调了能源革命和数字革命协同发展趋势下开展主动配电网调度决策与安全防护的重要性。

关键词：主动配电网；电力系统调度；云计算；边缘计算；电力信息安全

文章编号：1007-1881(2021)06-0015-07 **DOI:** 10.19585/j.zjdl.202106003

中图分类号：TM734 **文献标志码：**A **开放科学(资源服务)标识码(OSID)：**

An Overview of ADNs Dispatching Based on Coordinated Cloud-Edge omputing

LI Zhiyi, *SONG Kexuan*

(NGICS Platform/College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China)

Abstract: With the advancement of expanded electricity distribution reform and the emergence of multiple stakeholders, active distribution networks are characterized by interactions between supply party and demand party, and tend to be cyber-physical systems (CPS). Therefore, the traditional centralized dispatching decision can no longer be applied. Based on the applicability and security of cloud computing, edge computing and other frontier information technologies applied in active distribution networks, the paper gives a commentary about the progress and development of joint dispatch of power system, cloud computing and edge computing, safeguard of power information security to clarify ideas for solving the decentralization of dispatching and control sources, heterogeneous computing resources as well as vulnerable cybersecurity safeguard. Finally, this paper stresses the significance of dispatch decision-making and security safeguard of active distribution networks with the coordinated development of the energy revolution and the digital revolution.

keywords: active distribution network; power system dispatch; cloud computing; edge computing; power information security

0 引言

我国配电网的运行形态和技术特征正在经历重大变革。一方面，随着配电业务日渐开放，新涌现的利益主体成为投资、建设和运营增量配电项目的主要力量。2015 年 3 月，国务院印发了《关于进一步深化电力体制改革的若干意见》，正式开启新一轮电力改革的序幕，允许社会资本投资增量配电项目则成为配电业务发展的标志性特征[1]。2018 年 7 月，国家能源局印发的《关于简化优化许可条件、加快推进增量配电项目电力业务许可工作的通知》[2]进一步简化了增量配电项目参与配电业务的许可条件。因此，日渐增多的利益主体将独立于配电网调控中心之外，具备电能生产者和消费者的双重身份，并通过自主运营和管理增量配电部分参与各项配电业务[3]。另一方面，随着物联网和人工智能等技术的蓬勃发展和渗透接入，配电网的运营将融合能源革命和数字革命的最新成果，迅速向主动配电网跃迁[4]。在此趋势下，主动配电网将成为承载多元利益主体供需

基金项目：中央高校基本科研业务费专项资金(浙江大学 NGICS 大平台)(K20210001)；国家自然科学基金项目(52007164)

互动的主要平台(如图 1 所示)，通过促成能源和信息在利益主体间的按需双向流动，提升可再生能源的消纳水平和整体的配电效率。

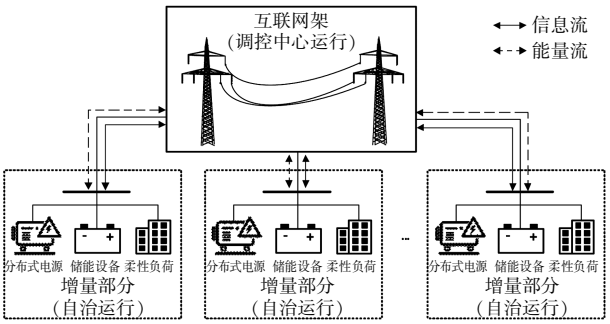

图 1　主动配电网形态特征

为顺应利益主体多元化的趋势，主动配电网的调度方式将发生显著改变。不同主体间差异化的利益诉求将直接增加配电网运营复杂度，传统的单主体(调控中心)集中调度方式将难以继续适用[5]。增量配电部分(如微电网、智慧园区等)集成了分布式电源、储能设备、柔性负荷等灵活性资源，通常具备主动孤岛能力，且在满足本地用电需求的基础上能对外进行电能返送。然而，利益主体在调度本地灵活性资源时往往只考虑自身效用，而忽略了对配电网整体运行的影响。潮流过路[6]等问题的出现，更将迫使相关利益主体的调度决策无法完全独立，转而需要在分布自治运行的基础上实现合作和协同[7]。同时，随着统一潮流控制器等软开关技术[8]的应用，配电网调控中心能灵活调整电力互联网架的拓扑结构，从而具备管理和协调利益主体多方互动的天然优势。因此，有必要融合分布自治和集中协调的能量管理理念，建立面向多元利益主体的联合调度范式，进而优化整合分散的灵活性资源达成供需实时平衡。

高效、可信的调度决策过程，是主动配电网快速、前瞻地应对可再生能源发电等不确定性的重要支撑。由于主动配电网将接入数量庞大、分布广泛的量测终端，急剧增加的量测信息不可避免地加重了数据储存和分析负担。此外，利益主体为防范隐私泄漏不会轻易分享增量配电部分的真实物理细节，使得调度决策过程面临模型完备性的挑战。为突破以上困境，主动配电网的调度决策过程将由调控中心统一实现向利益主体协同实现变革。新兴的云边协同计算模式契合主动配电网计算资源的分布特征，是促成多主体分层分布式协同决策的合适选择。事实上，配电网调控中心通常配备有高性能的计算和存储资源，能快速处理复杂计算问题，符合云计算中心的功能特征；而其他利益主体自有的计算资源则能构成边缘计算节点，为自治运行的增量配电部分就近提供计算和存储服务，以减少通信时延、提高响应速度。因此，构建云边协同、层级化的计算体系能有效整合分散、异构的计算资源，提升利益主体决策互动的整体效率(如图 2 所示)。在此基础上，有必要结合主动配电网运行特性，挖掘云边协同计算优势，提升多主体参与调度决策的协同性和灵活性。

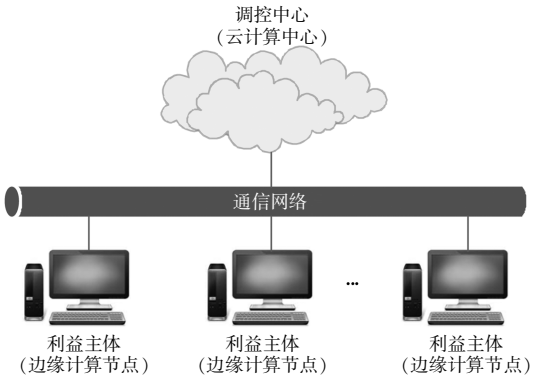

图 2　主动配电网云边协同计算体系

与此同时，随着电力物联网技术的发展，主动配电网的信息系统将由封闭、孤立转向包容、开放，并进一步聚合具备传感、通信、计算功能的海量终端设备，安全边界模糊化和复杂化的趋势明显。黑客极有可能通过挖掘和利用终端设备的安全漏洞，实现对边缘计算节点的远程操纵，影响云边协同计算流程，进而破坏调度决策的时效性和最优性。因此，多主体协同决策面临比传统集中式决策更为严重的信息安全风险。然而，目前电力信息安全措施(如防火墙、单向隔离装置等)以被动的基础防御为主，面对专业性强、渗透点多的网络攻击缺乏足够的应对能力。目前，网络空间已经成为继陆、海、空、天之后各国争夺的第五大战略空间，针对电力系统的网络攻击事件层出不穷。乌克兰电网在 2015 年和 2016 年先

后 2 次遭到网络攻击而引发大面积停电，引起国内外舆论的高度关注[9]。2019 年起，委内瑞拉多次发生全国性大规模停电，事故起因也被多数专家归为网络攻击[10]。我国各级电网也面临日趋严重的网络攻击威胁。比如，2019 年我国东北电网的发电生产实时数据平台被黑客利用漏洞成功渗透，虽未直接造成停电事故但造成了恶劣的社会影响[11]。因此，针对主动配电网云边协同计算体系的信息安全防御研究刻不容缓。2019 年 12 月，我国正式开始实施网络安全等级保护 2.0 标准体系[12]，把云计算、物联网等新兴应用场景纳入标准范围，为管理主动配电网信息安全风险指明了方向。为顺应国家网络安全 2.0 的发展要求，有必要融合云边协同计算的方法特征和配电网调度的决策机理制定信息安全防御策略，以保障多主体协同决策过程的可信程度。

综上所述，构建满足多元利益主体联合调度需求的主动配电网调度方法，并提升云边协同计算过程中数据流的信息安全性(即机密性、完整性和可用性)，是实现主动配电网安全经济运行的重要保障，也是促成前沿 IT(信息技术)与 OT(电网运营技术)安全融合的重要探索，对推动能源革命和数字革命协同发展具有重要意义。

1　电力系统联合调度

电力调度是保障电力系统安全经济运行的重要理念，也是应对复杂条件下供需不平衡挑战的核心方法。因此，电力调度一直受学术界和工业界关注。尤其在面向电网调控中心的集中调度领域，已取得丰富的理论成果和成功的工程经验。随着能源革命的发展，电力系统的形态特征和业务模式面临重大变革，参与调度的利益主体呈现多元化趋势。在此背景下，考虑多个利益主体的联合调度方式成为研究热点。然而，不同利益主体在多个时空尺度下的博弈互动将导致电力供需关系复杂化，调度建模和求解机制成为理论难题。针对这个难题，分层分区协同调度是主流的解决思路，其通过按逻辑分层使复杂调度问题可以被迭代求解，同时通过按地理位置分区实现求解效率的进一步提升。目前，这方面的研究以协同输、配电网的调度为主，比如：文献[13]针对输、配电网协同调度问题，设计了满足迭代过程有限步收敛性的异构分解算法；文献[14]基于多参数规划理论，提出了适合输、配电网协同调度的分布式求解策略并验证了最优解的可达性；文献[15]建立了考虑高比例风电接入的输、配电网层次化调度模型，并提出了分层优化和层间协调相结合的求解方式。

另外，部分学者将输、配电网协同调度的理念下沉，用于指导配电网中多个利益主体的联合调度，比如：文献[16]搭建了基于分布式集群控制的配电网能量管理与运行调控体系结构，并分析了实现集群自律、群间协调等功能的关键技术；文献[17]和[18]分别采用 Benders 分解法和目标级联分析法，实现了微电网群和配电网的分散自治运行和迭代调度决策；文献[19]从弱中心化配电网电力市场的角度，进一步研究了分布式的双边市场出清方法。然而，由于配电网运行特性更为复杂(如三相不平衡、电压安全)以及灵活性资源更为丰富(如分布式电源、储能设备)，多主体联合调度模型在理论上更为复杂。具体来说，由于连续变量(如储能设备输出功率)和整数变量(如储能设备充/放电状态)大概率并存，每个利益主体的调度模型都可能符合混合整数规划的特征，照搬输、配电网协同调度的求解方式将面临收敛困难、陷入局部最优等痛点。文献[20]提出了增广 Benders 分解法，并证明存在整数变量时分布式迭代求解过程的有限步收敛性和最优解可达性，为求解此类联合调度问题提供了一种可行思路。

然而，以上文献都是基于整体理性的假设，即所有利益主体遵从同一个调度目标开展合作以保障整体利益(如总运行成本最小化、社会效益最大化)。事实上，利益主体在博弈互动时往往呈现个体理性的特征，即追求自身利益的最大化而忽略整体利益。理论上，满足整体理性假设的联合调度模型都可以等价转化为单层优化问题，而在个体理性假设下联合调度模型则为更难求解的多层优化问题，其中每一层分别对应目标需求相似的利益主体。目前只有少数学者对个体理性下的联合调度方式进行了探索，主要是把配电网调控中心和其他利益主体分别作为主从博弈的上层和下层决策者，比如：文献[21]和[22]基于双层优化思想构建了协同配电网和微电网群的调度模型，并分别根据 KKT(库恩–塔克)条件和强对偶理论

将下层(微电网)线性规划问题等价转换成上层(配电网)问题的约束，进而以一体化求解的方式兼顾配电网和微电网多方的目标需求；文献[23]和[24]分别将负荷调用状态和备用选择方案等整数变量考虑进代表工业园区和微电网的下层问题，并应用遗传算法使其与代表配电网的上层问题决策互动，进而保障联合调度决策结果能有效权衡差异化的目标需求。值得指出，当下层问题是混合整数规划问题时，双层优化问题的精确求解面临严峻挑战。文献[25]构建了基于 C&CG(列–约束生成法)的双层优化模型转换和分解框架，通过隐性枚举下层问题整数变量的极值保证了上下层交替迭代过程能在有限步到达最优解，为个体理性假设下的优化调度提供了基础性的理论指导。然而，此求解框架需要多次复制下层信息到上层问题，数据传输和存储量大，且尚未考虑利益主体的隐私防护需求，有待结合配电网运行特性和多主体互动需求加以改进。

综上所述，现有研究大多局限于集体理性假设，且没有充分考虑不确定性因素对联合调度的影响，亟待开展个体理性假设下的多元利益主体联合调度研究，并在不确定性表征、模型精确求解、个体隐私防护等方面取得突破性进展。

2 电力系统云、边计算

云计算和边缘计算是信息技术的发展前沿，也是学术界和工业界关注的热点领域。云计算主要依托虚拟化服务技术，将各类计算、存储和网络资源虚拟化后集中管理，从而给用户提供高性能的数据存储和计算服务。关于云计算在电力系统中的应用，目前主要基于以下 2 个思路开展理论研究和工程实践。其一，业务外包，即租赁第三方公司已经开发成熟的云平台，将本地计算任务迁移到云平台上执行。这方面的代表性成果有：文献[26]探讨了电网独立运营商在亚马逊网页服务平台构建虚拟私有云的可行性，并验证了大规模电网规划仿真以云计算方式实现的有效性；文献[27]设计了求解经济调度等线性规划问题的外包机制，并指出基于云平台的应用开发具有计算性能强、可扩展性好、性价比高等优势；文献[28]提出了能实现外包计算任务脱敏的信息掩码理论，并在终端用户能量管理、区域负荷聚合管理和多区电网经济调度等线性规划典型场景下进行了实用性验证。其二，自主建设，即在本地硬件资源虚拟化的基础上实现数据标准化和应用服务化等私有云功能。这方面的代表性成果有：文献[29]系统地阐述了国家电网公司构建企业管理云、公共服务云和生产控制云的必要性和实用性，并指出云计算能显著提升信息感知同步、在线电网分析、精益调度管理和数据深度应用等层面的支撑能力；文献[30]进一步提出了基于云平台的计算、存储资源自动搜索与定位机制，旨在支撑状态估计等调控应用的在线计算。

当数据源离云平台距离较远时，通信延迟概率往往较高，影响云计算的实时响应能力。为解决以上痛点，云计算的模式应下移到通信网络边缘，使计算、存储等资源更靠近数据源，从而降低通信延迟、隐私泄漏等风险。文献[31]把此类在通信网络边缘执行的计算模式正式定义为边缘计算，并指出边缘计算可以由从数据源到云平台通信路径上的任意计算资源执行(如本地服务器、边缘网关和智能终端)。思科公司基于边缘计算的理念开发了名为雾计算的虚拟化计算平台，为云计算的本地化执行提供了技术解决方案[32]。由于边缘计算具有数据本地存储、计算本地执行的优势，部分学者就边缘计算在电力系统中的应用开展了理论探索，比如：文献[33]探讨了在广域发电控制、站域保护控制与负荷建模评估等场景下边缘计算的部署方式和应用前景；文献[34]提出了借助边缘计算实现自动需求响应的设想，并针对接口服务等问题给出了相应的解决思路。

边缘计算节点本质上是对云计算中心的主动延伸和有效补充。然而受资源部署的限制，边缘计算节点的存储、计算性能和云计算中心存在较大差距。为结合边缘计算和云计算的优势，云边协同计算成为了理想选择，相关研究方兴未艾。其中，代表性的成果有：文献[35]面向实时视频分析、智慧城市管理等应用场景，构建了云与边缘节点间计算任务流的优化管理框架，为解决应用分解、任务分配、资源管理和分布执行等问题奠定了基础；文献[36]为缩减数据传输的整体延时，应用遗传–粒子群融合算法实现了云和边缘节点数据存储的优化分配；文献[37]提出了以用户体验质量为核心理念的云计算与边缘计算集成

方案，并建立了基于综合信任度的边缘计算资源协同优化模型。值得指出，云边协同的计算模式与电力系统的层级化管理方式天然契合。目前，只有少数学者对云边协同计算在电力系统调控环节的应用开展了探索性研究，比如：文献[38]针对电动汽车有序充电场景，探讨了如何应用云边协同计算模式实现配电台区的自治管理以及物联网云平台的监督控制。然而，大多数研究都假定云计算中心和边缘计算节点归属于同一个利益主体，通过统一调度计算资源权衡各节点的计算量和通信量。此外，为实现节点计算负载的均衡分布，调度计算资源时往往只考虑了计算任务的数学特征，使得计算任务迁移时用户隐私难以保障。

综上所述，云计算和边缘计算在电力系统领域的应用研究刚刚起步，且缺乏灵活可靠的协同机制，亟待开展考虑计算资源归属方多元化的云边协同计算研究，并在计算资源共用、计算过程容错、计算任务脱敏等方面取得突破性进展。

3　电力信息安全防御

现代电力系统中信息流与能量流紧密耦合、相互依存，因此电力信息安全防御比传统的互联网安全防御在机理上更为复杂。总体而言，电力信息安全防御既要满足信息安全的通用要求，又要结合电力系统运营特征定向扩展。目前，相关研究领域在机理性、系统性和普适性等方面存在广阔的发展空间。部分学者针对如何构建电力信息安全防御体系提出了指导性建议，比如：文献[39]强调数据流的机密性、完整性和可用性是实现电力等工控系统信息安全的三大要素，即要保障数据不能因泄露而被非法利用、不能被随意篡改或伪造以及能随时按需使用；文献[40]基于对乌克兰电网遭受网络攻击的思考，指出电力信息基础设施的脆弱性客观存在，因而必须变被动防御为主动防御；文献[41]具体分析了电力信息安全防御面临的挑战，并强调必须要以立体化、全局式的视角设计安全防御架构。

与互联网相比，电力系统面临的网络攻击专业性和目标性更强。为实现电力信息安全防御时知己知彼，部分学者探究了潜在的网络攻击，比如：文献[42]基于实际量测系统特征研究了针对配电网调控运行的虚假数据注入攻击，指出黑客可能只需依靠少量历史数据就可以更改状态估计结果；文献[43]分析了拒绝服务攻击对负荷频率控制的影响，并揭示了通信参数与系统可耐受攻击时间的相关性；文献[44]分析了物联网攻击对配电网安全运行的破坏性，指出黑客可能通过规模化操纵家用电器引发严重停电事故。面向如何最优化部署安全防御资源的难题，部分学者对网络攻防博弈进行了数学建模，比如：文献[45]通过构建表征攻防双方交互影响的数学模型，提出了防御虚假数据注入攻击的有效方法；文献[46]通过研究电力系统的信息物理耦合特性，设计了系统结构冗余度强化策略以降低网络攻击对安全运行的影响；文献[47]综合考虑网络攻击的破坏程度与成功概率，从攻防博弈角度进一步提出了优化分配防御资源的数学方法。

以上文献从宏观角度分析了电力信息安全防御的迫切性和重要性，但未涉及实现防御的具体措施。传统的电力信息安全防御体系集成了防火墙、单向隔离装置、入侵检测系统和密钥系统等被动防御措施，比如：文献[48]根据事前预防和事后应对的不同要求，梳理了以被动防御为主的传统防御措施。为提升对网络攻击威胁的应对能力，少数学者对电力信息安全主动防御措施开展了理论探索，比如：笔者在文献[49]中提出了针对微电网状态估计的移动目标防御思路，通过随机筛选冗余的量测数据有效降低了网络攻击的成功率；文献[50]提出了基于虚构线路的主动诱骗思路，有效提升了电力调度系统的容侵性。

综上所述，考虑信息–物理耦合特性的电力信息安全防御理论研究尚处于起步阶段，且缺少支撑性的技术实现方法，亟待开展切合主动配电网发展需求的主动防御研究，并在防御资源分配、移动目标防御、网络攻击诱捕等方面取得突破性进展。

4　结语

本文面向能源革命和数字革命协同发展的实际需求，评述了主动配电网背景下电力系统联合调度、云计算与边缘计算、电力信息安全防御等方面的研究现状与发展动态。特别指出，为顺应国家网络安全 2.0 的发展要求，有必要融合云边协同计算技术和配电网运行机理构建多元融合、

多方互动的主动配电网调度决策体系，并制定相应的信息安全防御策略变传统的被动防御为精准的主动防御，保障多主体协同决策过程的灵活性和可信度。希望本文能在主动配电网主从博弈模型、分解协调机制、主动防御策略等方面，启迪科研工作者突破理论难题与瓶颈，为能源革命和数字革命协同发展做出贡献。

参考文献：

[1] 中共中央国务院. 关于进一步深化电力体制改革的若干意见[R/OL].(2015-03-09)[2021-01-04].http://www.gov.cn/xinwen/2015-03/09/content_2831228.htm.

[2] 国家能源局综合司.关于简化优化许可条件、加快的推进增量配电项目电力业务许可工作的通知[R/OL].(2018-07-11)[2021-01-04].http://zfxxgk.nea.gov.cn/auto79/201807/20180730-3218.htm.

[3] PARAG Y,SOVACOOL K.Electricity market design for the prosumer era[J].Nature Energy,2016,1:16032.

[4] 王成山,李鹏,于浩.主动配电网的新形态及其灵活性特征分析与应用[J].电力系统自动化,2018,42(10):13-21.

[5] PEREIRA I,SPECHT M,SILVA P,et al.Technology,business model,and market design adaptation toward smart electricity distribution: insights for policy making[J].Energy Policy,2018,121:426-440.

[6] 吴春潮,薛飞,徐晓彤,等.基于电气关联强度的虚拟微电网划分方法[J].电力系统自动化,2019,43(13):54-62.

[7] 孙宏斌,张伯明,吴文传,等.自律协同的智能电网能量管理系统家族：概念、体系架构和示例[J].电力系统自动化,2014,38(9):1-5.

[8] 马望,高红均,李海波,等.考虑智能软开关的配电网灵活性评估及优化调度模型[J].电网技术,2019,43(11):3935-3943.

[9] LIANG G,WELLER S R,ZHAO J,et al.The 2015 ukraine blackout: implications for false data injection attacks[J].IEEE Transactions on Power Systems,2017,32(4):3317-3318.

[10] LI E,KANG C,HUANG D,et al.Quantitative model of attacks on distribution automation systems based on CVSS and attack trees[J].Information,2019,10(8):251.

[11] 卢英佳.我国电力信息系统面临的网络安全风险及处置建议[J].中国信息安全,2019,11:97-99.

[12] 国家市场监督管理总局,国家标准化管理委员会.信息安全技术网络安全等级保护基本要求：GB/T 22239—2019[S].北京：中国标准出版社,2019.

[13] LI Z,GUO Q,SUN H,et al.Coordinated economic dispatch of coupled transmission and distribution systems using heterogeneous decomposition[J].IEEE Transactions on Power Systems,2016,31(6):4817-4830.

[14] LIN C,WU W,CHEN X,et al.Decentralized dynamic economic dispatch for integrated transmission and active distribution networks using multi-parametric programming[J].IEEE Transactions on Smart Grid,2018,9(5):4983-4993.

[15] 张旭,王洪涛.高比例可再生能源电力系统的输配协同优化调度方法[J].电力系统自动化,2019,43(3):67-83.

[16] 吴文传,张伯明,孙宏斌,等.主动配电网能量管理与分布式资源集群控制[J].电力系统自动化,2020:1-10.

[17] ZHAO Y,YU J,BAN M,et al.Privacy-preserving economic dispatch for an active distribution network with multiple networked microgrids[J].IEEE Access,2018,6:38802-38819.

[18] 谢敏,吉祥,柯少佳,等.基于目标级联分析法的多微网主动配电系统自治优化经济调度[J].中国电机工程学报,2017,37(17):4911-4921.

[19] 窦晓波,曹水晶,刘之涵,等.弱中心化的配电网市场交易机制、模型与技术实现[J].电力系统自动化,2019,43(12):104-120.

[20] LI Z,SHAHIDEHPOUR M.Privacy-preserving collaborative operation of networked microgrids with the local utility grid based on enhanced benders decomposition[J].IEEE Transactions on Smart Grid,early access at 10.1109/TSG.2019.2959242.

[21] JALALI M,ZARE K,SEYEDI H.Strategic decision-making of distribution network operator with multi-microgrids considering demand response program[J].Energy,2017,141:1059-1071.

[22] BAHRAMARA S,PARSA MOGHADDAM M,HAGHIFAM M R.A bi-level optimization model for operation of distribution networks with micro-grids[J].International Journal of Electrical Power & Energy Systems,2016,82:169-178.

[23] 智勇,郭帅,何欣,等.面向智慧工业园区的双层优化调度模型[J].电力系统自动化,2017,41(1):31-38.

[24] 吕天光,艾芊,孙树敏,等.含多微网的主动配电系统综合优化运行行为分析与建模[J].中国电机工程学报,2016,36(1):122-132.

[25] ZENG B,AN Y.Solving bilevel mixed integer program by reformulations and decomposition[J].Optimization online,2014:1-34.

[26] MA F,LUO X,LITVINOV E.Cloud computing for power system simulations at ISO new england: experiences and challenges[J].IEEE Transactions on Smart Grid,2016,7(6):2596-2603.

[27] SARKER M R,WANG J,LI Z,et al.Security and cloud out

sourcing framework for economic dispatch[J].IEEE Transactions on Smart Grid,2018,9(6):5810-5819.
[28] XIN S,GUO Q,WANG J,et al.Information masking theory for data protection in future cloud-based energy management[J].IEEE Transactions on Smart Grid,2018,9(6):5664-5676.
[29] 许洪强.调控云架构及应用展望[J].电网技术,2017,41(10):3104-3111.
[30] 郭健,周京阳,李强,等.高性能在线分析计算现状与协同计算关键技术[J].电力系统自动化,2018,42(3):149-159.
[31] SATYANARAYANAN M,BAHL P,CACERES R,et al.The Case for VM-based cloudlets in mobile computing[J].IEEE Pervasive Computing,4(8):14-23.
[32] BONOMI F,MILITO R,ZHU J,et al.Fog computing and its role in the internet of things[C].First Edition of the MCC Workshop on Mobile Cloud Computing,2012:13-16.
[33] 白昱阳,黄彦浩,陈思远,等.云边智能:电力系统运行控制的边缘计算方法及其应用现状与展望[J].自动化学报,2020,46(3):397-409.
[34] 李彬,贾滨诚,曹望璋,等.边缘计算在电力需求响应业务中的应用展望[J].电网技术,2018,42(1):79-87.
[35] LIN L,LIAO X,JIN H,et al.Computation offloading toward edge computing[J].Proceedings of the IEEE,2019,107(8):1584-1607.
[36] LIN B,ZHU F,ZHANG J,et al.A time-driven data placement strategy for a scientific workflow combining edge computing and cloud computing[EB/OL].2019:arxiv:1901.07216[cs.DC].http://arxiv.org/abs/1901.07216.,2019,15(7):4254-4265.
[37] 邓晓衡,关培源,万志文,等.基于综合信任的边缘计算资源协同研究[J].计算机研究与发展,2018,55(3):449-477.
[38] 孙浩洋,张冀川,王鹏,等.面向配电物联网的边缘计算技术[J].电网技术,2019,43(12):4314-4321.
[39] SATDHARI O S.Engineering Trustworthy Systems[J].Communications of the ACM,2019,62(6):63-69.
[40] 李中伟,佟为明,金显吉.智能电网信息安全防御体系与信息安全测试系统构建：乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J].电力系统自动化,2016,40(8):147-151.
[41] 王栋,陈传鹏,颜佳,等.新一代电力信息网络安全架构的思考[J].电力系统自动化,2016,40(2):6-11.
[42] DENG R,ZHUANG P,LIANG H.False data injection attacks against state estimation in power distribution systems [J].IEEE Transactions on Smart Grid,2019,10(3):2871-2881.
[43] PENG C,LI J,FEI M.Resilient event-triggering load frequency control for multi-area power systems with energy-limited DoS attacks[J].IEEE Transactions on Power Systems,2017,32(5):4110-4118.
[44] SOLTAN S,MITTAL P,POOR H V.BlackIoT: IoT botnet of high wattage devices can disrupt the power grid[C]// 27th USENIX Security Symposium,2018:15-32.
[45] WANG Q,TAI W,TANG Y,et al.A two-layer game theoretical attack-defense model for a false data injection attack against power systems[J].International Journal of Electrical Power & Energy Systems,2019,104:169-177.
[46] CHEN L,YUE D,DOU C.Optimization on vulnerability analysis and redundancy protection in interdependent networks[J].Physica A: Statistical Mechanics and its Applications,2019,523:1216-1226.
[47] 陈武晖,陈文淦,薛安成.面向协同信息攻击的物理电力系统安全风险评估与防御资源分配 [J]. 电网技术,2019,43(7):2353-2360.
[48] 汤奕,李梦雅,王琦,等.电力信息物理系统网络攻击与防御研究综述(二):检测与保护[J].电力系统自动化,2019,43(10):1-9.
[49] LI Z,SHAHIDEHPOUR M,AMINIFAR F.Cybersecurity in distributed power systems[J].Proceedings of the IEEE,2017,105(7):1367-1388.
[50] 李志强,苏盛,曾祥君,等.基于虚构诱骗陷阱的电力调度系统针对性攻击主动安全防护[J].电力系统自动化,2016,40(17):106-112.
[51] 邓科,张丽红,蔡昂,等.基于分级调度算法的交换机路由信息处理技术[J].电网与清洁能源,2020,36(1):8-13.
[52] 赵彦博,王云龙,王烁罡,等.电力调度数据网地址分析系统设计与开发[J].内蒙古电力技术,2018,36(1):45-48.
[53] 邓佃毅,张旭.新能源场站调度管理优化分析[J].内蒙古电力技术,2019,37(1):85-89.

收稿日期：2021-02-08

作者简介：李知艺(1989)，男，博士，研究员(正高级)，研究方向为智慧能源系统。

(本文编辑：徐玮韡)