•新型电力系统•

DOI:10.12454/j.jsuese.202400920

本刊网刊

应对虚假数据注入攻击的新型电力系统移动目标防御研究现状与展望

臧天磊[1,2],龚亚辉[1,2],李创芝[1,2],王世俊[1,2],刘云飞[1,2],周步祥[1,2]

(1.四川大学 电气工程学院,四川 成都 610065;2.智能电网四川省重点实验室(四川大学),四川 成都 610065)

摘　要:随着能源网络与信息网络的深度耦合,能源系统对自身的感知和控制能力显著提升。然而,这一耦合也使信息层面的攻击能够蔓延至物理层,增加了电力系统面临的安全威胁。虚假数据注入攻击(FDIA)是其中常见且具有破坏性的攻击形式,针对FDIA的防御策略已成为研究的焦点。面向电力系统的安全防护,移动目标防御(MTD)通过主动动态改变电力系统状态,使攻击者掌握的系统信息部分或完全失效,进而增强FDIA的检测能力。因此,本文探讨MTD作为主动防御策略在新型电力系统中的应用。首先,介绍电力信息物理系统主动防御技术的发展趋势、MTD的概念及起源、电力系统MTD的基本原理。随后,系统梳理现有电力系统领域的MTD研究,总结MTD实施的完备性分析、一般策略和特殊策略;分析其具体实施策略,包括线路电抗扰动、传感器增益扰动等。现有研究集中于传统输电网络,难以适应新型电力系统发展。针对这一现状,本文重点分析MTD在新型电力系统中的应用潜力;进而,基于新型电力系统发、输、配、用各环节的特点,详细探讨MTD的具体实施策略。最后,结合新型电力系统的复杂性及现有技术的局限性,总结新型电力系统MTD技术所面临的挑战。本研究强调MTD在提升电力系统安全性方面的重要作用及其在新型电力系统中的广阔应用前景,为未来智能电网和多能互联场景下的MTD技术发展提供了参考框架。

关键词:新型电力系统;虚假数据注入攻击;移动目标防御;信息物理系统;多能互联

中图分类号:TM73　　**文献标志码:**A　　**文章编号:**2096-3246(2025)05-0114-20

建设新型电力系统,发展“新质生产力”,是推动电力系统升级与能源转型的核心动力。新型电力系统融合通信、信息处理、人工智能等多学科,为新质生产力提供基础与应用场景。然而,供能与信息网络的深度耦合也使系统更易受攻击,威胁网络安全与稳定。为应对开放性带来的防御挑战,需发展新型主动防御技术,确保能源网络安全。

随着通信与信息处理技术广泛应用,传统电力系统逐渐转型为新型电力信息物理系统(CPS)[1]。这一变革与智能电网、综合能源系统(IES)、能源互联网等概念的提出相互促进,多能互联展现出广阔潜力。然而,在含多能耦合的系统中,能源间的相互依赖使得攻击对系统安全和稳定的影响更加严重,亟需更行之有效的防御技术[2]。

在信息技术不断发展和电力系统智能化程度不断提升的同时,电力系统的安全性也面临着新的挑战。2010年,伊朗核设施受到攻击[3];2015年,乌克兰电网遭受BlackEnergy攻击导致大范围事故;2016年,以色列电网遭受网络攻击[4];2018年,美国发布报告称攻击者通过多种攻击获取数据采集与监控系统的机密文档[5]。新技术与新设备的引入增强了电力系统运行的经济性和稳定性,但同时也为潜在的攻击者提供了更多的攻击入口。新型电力系统比传统电力系统更容易受到攻击,并且不同供能系统间的风险有可能跨系统传播,导致更为严重的后果。

在网络安全领域,传统网络防御技术主要包括入侵检测、防火墙等静态化手段[6],但这些技术面临高级持续性威胁(APT)等挑战。面对电力系统可能遭受的攻击,学者们提出电力CPS可靠性评估[7]、防御方法和恢复策略[8]。然而,这些被动防御难以应对所

收稿日期:2024 – 11 – 07　　**修回日期:**2025 – 03 – 10　　**网络出版日期:**2025 – 06 – 10

基金项目:国家自然科学基金项目(52377115)

作者简介:臧天磊(1986—),男,副教授,博士.研究方向:综合能源系统运行优化与控制;能源信息物理系统安全分析与主动防护.E-mail:zangtianlei@126.com

有可能的攻击行为，且新型攻击不断出现，故研究开始转向主动防御策略以应对日益复杂的网络安全形势。鉴于传统被动防御的劣势，研究逐渐聚焦于网络欺骗、移动目标防御（MTD）等主动防御技术。

MTD作为一种主动防御方法最初在网络安全领域中被提出，之后被应用到电力系统以应对虚假数据注入攻击（FDIA）。FDIA能够利用收集到的目标系统信息构建攻击向量，绕过不良数据检测（BDD），成功实施攻击[9]。而MTD通过控制输电线路上部署的分布式柔性交流输电系统（D–FACTS）设备来主动改变输电线路参数，使得攻击者先前获取的关于目标系统的信息失效。当MTD动作后，攻击者试图利用先前获取的目标系统信息来发动FDIA时，其攻击行为更容易暴露，从而保障目标系统的安全。作为一种纵深防御技术，MTD能够增加攻击者的攻击成本，且已被证明是阻止FDIA去攻击交流电力系统状态估计（SE）过程的一种潜在有效方法[10]。

鉴于此，本文介绍MTD在电力系统领域的引入和发展历程，梳理相关研究发展脉络，分析学术界如何逐步丰富和发展MTD策略。在新的发展理念下，新型电力系统、IES成为供能系统的发展趋势，本文借助传统电力系统的MTD研究，分析新型电力系统的MTD策略构建思路，为相关研究提供可行的框架。总结新型电力系统MTD研究面临的挑战。

1　电力CPS主动防御

MTD属于主动防御策略，了解电力系统主动防御思想有利于分析电力系统MTD的构建思路。根据现有文献，从时间尺度上来看，按不同的分类方式，电力系统防御方法可以分为：攻击前安全防御、攻击中安全防御、攻击后校正恢复[8]；攻击前防御、攻击中检测、攻击时抑制[11]；事前防御、事后校正[12]。上述不同的分类存在表述重复之处，本文不区分攻击中与攻击后的防御，将电力系统防御方法分为：攻击前防御和攻击中防御[13]。

1.1　攻击前主动防御

攻击前主动防御通过预先部署多层次、多维度的安全策略，构建全面的纵深防御体系，实现防御手段的协同联动。多种策略的结合，不仅保障数据传输的保密性和完整性，还能够提升系统的入侵检测能力和容错性。多策略协同使系统具备更强的适应性，可有效应对已知和未知威胁，在攻击发生前建立稳健、高效的防御屏障，为中后期防御奠定基础。现有研究中有关攻击前的主动防御策略如表1所示，涵盖多种提升电力系统安全性的技术手段。表1中，新型电力系统第1道防线旨在建立基础性的安全屏障，以防范潜在攻击的侵入。加密通信通过加密技术保障信息的机密性和完整性，防止数据篡改与窃听。此外，欺骗防御利用伪装、误导或诱导攻击者的手段，使其难以获取真实系统信息，进而提升防御效果。基于韧性提升的主动防御策略则依托物理层面的强化措施，提高系统的抗攻击能力；针对连锁故障的攻击前防御方案主要关注连锁故障的传播机制，设计有效的防御策略以降低系统级联故障发生的可能性。这些防御策略为研究人员提供了不同层面的安全措施参考，以优化电力系统的主动防御能力。

表1　攻击前主动防御策略分类

Tab. 1　Classification of proactive defense strategies before attack

攻击前防御策略	文献
新型电力系统第1道防线	[14–20]
加密通信	[21–24]
欺骗防御	[3,13,25–27]
基于韧性提升的主动防御策略	[28]
针对连锁故障的攻击前防御	[29]

欺骗防御具有较好的发展前景，常用的欺骗防御技术有4种：蜜罐、蜜网、蜜饵和MTD，而蜜罐是欺骗防御中最基本的工具[27]。主动诱骗防御策略是对欺骗防御更深入的研究，旨在设计一个严格控制的欺骗环境，在系统遭受攻击时，诱导攻击者将其攻击行为引向该环境[25]；该策略在攻击发生时提供预警功能，并监视和记录攻击者的行为。通过收集和分析入侵信息，可以更深入地了解攻击者的技术手段，进而改进系统的防御措施。

MTD与欺骗防御间的关系存在争议，二者之间的界限并不清晰[27]。欺骗防御主要通过部署虚假资源来误导攻击者，而MTD则侧重于通过动态变化来干扰攻击者的行为。尽管MTD最初的设计理念并未明确包含欺骗元素，但有效的欺骗防御通常依赖于动态调整诱饵资源的位置和数量，两者之间存在潜在的互补性。理解欺骗防御相关研究有利于促进电力系统MTD的应用。

1.2　攻击中主动防御

有别于攻击前主动防御有足够的时间实施防御策略，攻击中主动防御强调一定的实时性。在攻击中的主动防御阶段，主动防御策略通过主动动作辨识出攻击行为，并对其定位。通过对电力系统的主动控制和防御资源的紧急调配，实现对攻击的阻断或削减攻击造成的影响。

与第 1.1 节介绍的攻击前防御策略不同，攻击中防御涉及攻击中检测，进而实现基于攻击向量移除和设计补偿器的攻击时抑制[11]。根据具体的防御实施方法，攻击中的主动防御策略分类如表 2 所示。电力系统第 2 道防线，通过对系统进行自主控制以及应急切除故障并恢复，消除短时故障。若故障无法在短时间内消除，则实施基于灾备切换、紧急干预的电力系统第 3 道防线。攻击辨识与定位技术通过实时监测和数据分析，快速识别攻击来源和影响范围。加密通信在攻击期间仍然是保障数据完整性和安全性的关键手段；而欺骗防御则利用伪装和诱导机制，使攻击者难以实施精准攻击。基于韧性提升的攻击中防御策略通过强化物理层安全性，提高系统对攻击的抵御能力；针对连锁故障的攻击中防御则关注故障传播机制，采取措施防止级联效应的发展和演化。此外，基于主动割集的方法利用关键节点的动态调整来优化防御效果。这些防御策略共同构成了攻击发生期间的主动安全体系。

表 2 攻击中主动防御策略分类

Tab. 2 Classification of proactive defense strategies during attack

攻击中防御策略	文献
基于自主控制，应急切除故障并恢复的电力系统第 2 道防线	[20,30–31]
基于灾备切换、紧急干预的电力系统第 3 道防线	[20,32–33]
攻击辨识与定位	[34]
加密通信	[21–24]
欺骗防御	[3,13,25–27,35]
基于韧性提升的攻击中防御	[36]
针对连锁故障的攻击中防御	[29]
基于主动割集	[37]

欺骗防御与 MTD 都是通过增加攻击者决策过程中的不确定性来迷惑攻击者。欺骗防御比 MTD 更加积极主动，其故意向攻击者提供错误的信息[38]。相比之下，MTD 则通过变换系统的参数来提升系统的防御能力，但在此过程中并不向攻击者提供虚假信息。

为对抗 FDIA，一些学者研究了保护关键量测值的策略[39]，以确保控制指令和传感器量测的完整性。然而，在关键仪表上部署保护措施会带来额外的成本；此外，一些设备受限于自身的使用条件，无法采用此类措施[40]。Liu 等[41]指出，并非所有数据包在通信过程中都经过加密。此外，基于加密的关键量测值保护会降低监控系统的冗余，导致一些未受保护的量测可信度降低[42]。

2 电力系统 MTD 的概念、原理与策略

2.1 MTD 的概念及其发展

传统的网络防御手段，如入侵检测和防火墙，主要依赖静态配置，难以应对 APT 等复杂攻击。攻击者能够通过长期分析系统的固有脆弱性，利用网络系统的确定性和静态性进行持续渗透，逐渐掌握攻击的主动性。鉴于攻击者在时间、信息和成本上的优势，单纯依赖静态防御手段已不足以保障网络安全，动态防御策略（如 MTD）应运而生，通过持续改变系统状态，打破攻击者的预测和优势。

MTD 于 2011 年被美国国土安全部赛博安全研发中心提出，旨在限制网络空间中的攻防不对称性，使防御者摆脱易攻难守的困境。MTD 策略的思想是增加系统不确定性，增加攻击难度和攻击成本，提高系统安全性。Cho 等[38]对 2020 年及以前网络安全领域的 MTD 技术进行综合总结，展示了相关技术研究的总体趋势，为主动防御、自适应 MTD 研究方向的学者提供研究思路。根据 MTD 的操作类型，可将其分为混洗、多样性和备份冗余 3 类；按照时间性，MTD 可分为基于时间的 MTD、基于事件触发的 MTD、混合 MTD。

另外，姚倩等[43]也对现有的 MTD 技术进行了更为细致的归纳总结，将其主要分为跳变、变换、冗余 3 大类。跳变技术包括地址空间布局随机化、指令集随机化、数据随机化、IP 地址跳变、端口跳变、虚拟机热迁移、动态网络、HTML 元素随机化等；变换技术则包括编程语言转换、动态平台、动态软件；冗余技术主要指服务器副本。综合来看，跳变技术能够使攻击者收集到的信息失效，同时减少防御方的资源消耗，但其稳定性较差，防御效果不稳定；变换技术能够使某一版本的攻击失效，但消耗的防御资源较大，可变换的目标数量也受到限制；而冗余技术具有高可靠性和服务可用性，但建设成本与维护成本较高。在实际应用中，可以根据具体情况综合运用不同的 MTD 技术，以达到防御效果与防御成本之间的平衡。

2.2 电力系统 MTD 原理

在 MTD 相关研究中，研究人员经常使用非线性交流潮流模型和线性直流潮流模型。直流潮流模型相较于交流非线性模型计算量更小，因此在对实时性有一定要求的 MTD 研究中得到广泛应用。除了 MTD 策略研究以外，直流潮流模型还被广泛应用于故障分析、安全潮流计算、经济调度等领域，这些领域同样对实时性有一定要求[44]。何宗伦等[45]提出一种快速转换算法，将直流攻击向量转化为交流攻击向量，从而有效解决了交流模型非线性所导致的求解困难及直流

状态估计精度较低的问题。

电力系统MTD原理相关公式见附录A。由附录A的式(A7)～(A9)可知，若攻击者能够获取目标系统的量测矩阵，那么便有可能成功实施FDIA而不被BDD所察觉。电力系统作为重要的基础设施，其参数和拓扑结构对攻击者而言不易直接获取。同时，系统运行状态在不断变化，即使攻击者获取某时刻的参数和拓扑，也难以直接应用于其他时刻的FDIA。然而，攻击者可能通过对目标系统进行长期监测收集历史数据，并结合实时获取的数据来推断系统参数和拓扑结构[46]。文献[47]的攻击模型中，假设攻击者可以根据输电线路上的功率流和节点注入功率来推测系统状态向量，从而可以构建符合量测矩阵列向量线性组合的攻击向量。若攻击者掌握了足够多的历史数据，便能够发动绕过BDD的FDIA。

D–FACTS设备最初作为潮流的调控设备被应用到电力系统[48]，MTD的具体实施在很大程度上依赖于D–FACTS设备，MTD的概念因此被引入到电力系统的物理层[41]。D–FACTS设备能够主动改变输电线路参数，使攻击者对目标系统的历史知识失效。由附录A的式(A2)、(A9)、(A10)可知，若构建的攻击向量处于量测矩阵的列向量空间内，即攻击向量是量测矩阵列向量的线性组合，那么所构建的攻击向量在BDD看来与正常量测值无异，不会触发警报。而经MTD动作之后，D–FACTS设备的运行参数发生改变，量测矩阵由$\boldsymbol{H}$变为$\boldsymbol{H}'$。攻击者根据$\boldsymbol{H}$设置的攻击向量很难落在$\boldsymbol{H}'$的列向量空间中，进而更容易触发报警。

2.3　电力CPS的MTD策略

现有电力系统的MTD研究的防御对象主要是FDIA[10,41,48–50]。Liu等[9]指出BDD算法存在漏洞，表明攻击者能够绕过BDD而成功发动攻击。了解系统拓扑、运行机制且能够篡改系统量测数据的攻击者所设计的FDIA可能会使调度中心完全失去对系统状态的感知[47,50]，因此Tian等[50]建议应用MTD来检测隐蔽性Stuxnet–Like(SL)攻击。Liu等[51]则进一步指出隐蔽FDIA可通过量测矩阵来绕过基于量测残差的BDD。

根据保护关键量测值及引入数据完整性机制的不足[39–41]，主动防御方法逐渐进入更多学者的研究视野，将网络信息安全的主动防御方法MTD引入到电力系统领域。2012年，Morrow等[52]将MTD应用于电力系统的主动防御研究，尽管在该文献中未使用MTD这一术语，而是以线路电抗扰动作为研究方法的名称，但其提出的一些概念成为了日后其他学者的研究方向，相关思想推动了后续MTD的进一步发展，并将可行的一组D–FACTS设备的设定值向量称为密钥，所有的密钥构成密钥空间。类似地，张镇勇[44]将MTD作用前后的量测矩阵中未被扰动的列向量构成的空间称为隐蔽攻击空间。现有MTD策略研究的时间维度分类如表3所示。

表3　MTD策略研究时间维度分类

Tab.3　Classification of MTD strategy research by temporal stages

MTD策略分类	文献
MTD的规划	[42,53–54]
MTD的运行	[10,47,49–50,55–59]
MTD的规划和运行	[41,46,48,60–66]

然而，MTD策略的研究内容远不止时间维度的划分，还涉及技术特性和应用场景的多样性。为进一步揭示MTD研究的技术内涵，将表3中具有共性研究内容的文献按具体研究内容进行划分。根据已有文献，从完备性、隐蔽性、微电网、特殊攻击、电压稳定、保护特定线路、配电系统、交流模型，以及拓扑变换等多个技术维度，对文献的MTD研究进行细化总结，如表4所示。表4的这种多维度的划分也为后续从完备性分析、一般策略和特殊策略等研究维度的深入综述提供了基础。

表4　MTD策略研究的技术内容分类

Tab.4　Classification of MTD strategy research by technical themes

MTD研究内容分类	文献
涉及完备性	[41–42,48,53–54,60,63]
涉及隐蔽性	[41,47–48,58–59,62]
涉及微电网	[10,56]
涉及特殊攻击	[50,53,57,61]
涉及电压稳定	[61–62]
涉及保护特定线路	[64–65]
涉及配电系统	[47,62]
涉及交流模型	[46–47,49,66]
涉及拓扑变换	[55,58]

为进一步提炼MTD研究的核心逻辑，本文从实施视角出发，将表4中的研究内容归纳为MTD实施的完备性分析、一般策略和特殊策略3个研究维度，对现有电力系统MTD的研究进行具体综述。需要说明的是，这3个研究维度并非完全独立，而是交叉和互补的。同一文献可能涉及其中一个或多个维度，具体分类依据其研究侧重点而定。

2.3.1　MTD实施的完备性分析

研究表明，MTD的完备性对其性能至关重要，MTD的性能受到实际电网拓扑结构的影响，相关的理论研究集中在MTD的完备性分析。

Liu 等[40]首先推导在无噪声假设下 FDIA 的检测条件，并将 FDIA 的检测概率与复合矩阵的秩相关联，相较于其他研究，该研究进一步放宽检测 FDIA 的条件，并证明量测噪声对 FDIA 的检出概率无显著影响；并且指出，要实现 MTD 的完备性，输电线路的数量必须不少于状态数量的两倍，量测仪表对应的量测矩阵的秩必须不少于状态数量的两倍；FDIA 的检出概率随着复合矩阵秩的增加而显著增加，当复合矩阵满秩的时候，几乎可以检测出所有的 FDIA。Zhang 等[60]对 MTD 的完备性进行证明，同时指出要实现完备的 MTD，需要保证输电线路的数量不少于系统状态变量的两倍，并且被扰动的输电线路要覆盖所有的节点。

若系统中存在仅由一条输电线路连接的节点，其状态变量易被攻击者篡改且无法检测，从而导致 MTD 无法实现完备性。Zhang 等[53]对此情况进行深入研究，提出两种解决方案：一是，完全保护此类节点；二是，增加输电线路以消除度为 1 的节点。然而，实际系统中常存在 MTD 无法保护的节点。在 MTD 完备性受限时，应尽量减小 MTD 动作后的隐蔽攻击空间，以最大化其保护范围。

2.3.2 MTD 实施的一般策略

MTD 实施的一般策略是指通过输电线路上的 D–FACTS 设备实现的 MTD。根据文献[41,61]可知，MTD 需要解决的问题主要集中在规划阶段与运行阶段。MTD 的规划问题涉及如何在电力系统中合理部署相关设备以达到最佳防御效果；MTD 的运行问题则是考虑如何设定相关设备的运行参数以最大程度地优化 MTD 效果，其核心思想是要实现低成本和高效的检测效果。为了更好地梳理这两部分的研究内容，分别对规划阶段和运行阶段电力系统 MTD 实施的一般策略分类分析。

1）MTD 规划的策略研究

受限于设备成本和实际应用条件，需要在规划阶段对 D–FACTS 设备的部署进行优化，在保护性能和防御成本之间进行平衡进而确定 D–FACTS 设备的安装数量和位置。综合现有的文献，MTD 规划策略方面主要关注设备配置的条件和要求。

Morrow 等[52]通过灵敏性分析探讨 D–FACTS 设备的设置和配置位置，要求 D–FACTS 设备的设定值对整个系统的潮流和稳定性的影响最小化。Rahman 等[67]提出一种随机 MTD 操作方法，该方法在不考虑检测效果的情况下，随机改变配备 D–FACTS 的输电线路的电抗；然而，随机的 MTD 操作无法稳定地实现预期防御效果。后续研究中，更多以 MTD 动作前后复合矩阵的秩最大为优化目标[40]。进一步地，Liu 等[54]基于图论的拓扑分析，提出完备 MTD 的设备配置条件，确保 MTD 能使复合矩阵具有最大秩；Liu 等[41]基于图论拓扑分析，推导出一个充分条件以确保隐蔽 MTD（HMTD）的存在及复合矩阵的最大秩。Lakshminarayana 等[63]则更进一步指出，通过求解与电网相关的图形上的反馈边缘集问题，可以找到 D–FACTS 部署的最佳链路子集，从而实现设备的优化部署。Zhang 等[42]提出的算法并未遍历 D–FACTS 设备的所有可能部署情况，而是为给定数量的 D–FACTS 设备随机生成给定数量的部署案例。Tian 等[48]分析当线路子集配备 DFACTS 时隐藏 MTD 的基本可行性条件。Zhang 等[64]研究了保护特定节点所需要的最小 D–FACTS 设备数量。Xu 等[46]结合无噪声假设进行研究，并探讨噪声环境下的 MTD 设计问题。

2）MTD 运行的策略研究

电力系统 MTD 的运行实现策略分为扰动系统拓扑结构和扰动系统参数。Liu 等[68]首次将配电网网络重构与 MTD 联系起来，构建隐蔽 MTD，并使用改进遗传算法进行求解。基于拓扑变换的 MTD 方法通过断开预选传输线来切换电网拓扑，其有效性已经通过理论推导和仿真得到验证[69]。然而，传统的拓扑变换方法仅切换少数预定传输线，限制了其检测效果。为克服这一局限，He 等[70]提出一种基于备用线路灵活切换拓扑的 MTD 方法，该方法在一定程度上提升了系统的灵活性。然而，基于模型驱动的方法在面对时变或大规模系统时，其应用时效性会受到限制，影响了 MTD 方法的广泛适用性。Higgins 等[58]基于无监督学习的 MTD，与物理水印结合，实现隐蔽 MTD，并考虑通过操作断路器来改变系统拓扑，从而实现 MTD。为实现适用对象更广的 MTD，Wang 等[55]基于强化学习，提出通过备用母线开关进行拓扑扰动，进而实现鲁棒性更优的 MTD。

MTD 的运行阶段需要确定 D–FACTS 设备的运行参数，提升检测效果，并最小化对原有系统潮流的影响，甚至实现隐蔽防御。

MTD 的检测能力和相关成本取决于扰动前后量测矩阵的列向量空间的差别[66]。Xu 等[46]首次提出鲁棒 MTD 的概念，将 MTD 作用前后的雅可比子空间最小主角作为最坏攻击情况。并以最小主角下的防御性能为优化目标，保证对所有未知攻击的最坏情况下的检测率。

Lakshminarayana 等[66]提出一种基于直流最优潮流（OPF）的 MTD 运行策略，该策略阐释了 D–FACTS 设备的配置策略如何影响防御效果和运行成本。此外，Liu 等[41]提出一种基于优化的直流 HMTD 运行模

型，以最大化电抗变化，从而能够更高效地获取 D–FACTS 设定值，并在发电成本和 MTD 隐蔽性之间进行权衡。

MTD 策略的性能评估除了要尽可能提高对攻击的检出率，还需综合考虑其对系统运行的影响。在评估对系统运行的影响时，一方面是尽可能不增加系统运行损耗；另一方面是防御激活前后，系统潮流变化尽可能小，以防止攻击者察觉到系统激活 MTD。攻击者有可能根据 MTD 激活前后造成的电力系统潮流变化获知目标电力系统已经激活了 MTD，进而据此发动性能更优的 FDIA 来对抗 MTD。在这种情况下，MTD 对 FDIA 的检测性能将会显著降低，FDIA 对目标系统的不良影响将会加剧。相关研究者提出多种策略和方法来解决上述问题。Liu 等[40]提出的 MTD 策略可以在不显著影响系统正常运行的情况下，最大限度地提高对 FDIA 的检测性能。Zhang 等[49]在交流潮流模型下，考虑 D–FACTS 设备成本，并对 MTD 的防御时间间隔进行优化。Lakshminarayana 等[63]研究了防御者和攻击者之间通过零和非合作博弈之间的相互作用，用强化学习算法降低 MTD 的运行成本。Zhang 等[64]量化 MTD 保护级别的指标，实现隐蔽性 MTD 和降低防御成本。

为应对攻击者可能意识到防御存在的情况，Tian 等[48]提出一种隐蔽 MTD 策略，将在攻击之前检测 MTD 是否激活的 FDIA 称为参数确认 FDIA；在分析 MTD 的完备性后发现，任何隐蔽 MTD 都是不完备的，隐蔽性与完备性在 MTD 构建过程中相互冲突；并且，证明构建隐蔽 MTD 的充要条件是其激活前后系统的潮流保持不变；这一研究结果为设计隐蔽 MTD 提供了理论基础。Liu 等[41]提出一种基于深度优先搜索的 D–FACTS 的配置算法，旨在保证 MTD 的隐蔽性的同时最大化其检测有效性。Zhang 等[64]提出两种运行策略：MTD 激活前后线路潮流不变和节点注入功率不变，这两种策略使得激活 MTD 时增加的运行成本为零。Liu 等[47]构建两个明确的指标来量化交流潮流模型下的 MTD 有效性和隐蔽性，算例表明，基于显式残差的 MTD（EXR–MTD）相较于现有 MTD 策略具有更强的隐蔽性，同时有效性强于现有 MTD 策略。

2.3.3　MTD 实施的特殊策略

第 2.3.1、2.3.2 节主要是基于 D–FACTS 设备实现的 MTD，有学者针对特殊攻击和特殊保护对象及更为细致的建模进一步丰富了 MTD 研究。特殊 MTD 策略分为借助非 D–FACTS 设备实现动态防御、针对特定攻击制定精准策略、面向关键节点强化安全保护、依托复杂建模支持深度分析等 4 个部分。

1）借助非 D–FACTS 设备实现动态防御

Liu[10]和 Giraldo[56]等并没有直接改变线路的物理状态，而通过如图 1 所示的方式修改传感器量测和控制命令增益，使传感器的可用性随时间改变。这些措施增加攻击者对系统感知的不确定性，同时不会影响系统正常运行，且易于在现有的物理量测单元上实现。类似地，Liu 等[57]将联合仪表编码和 MTD 相结合，利用编码矩阵来检测隐蔽的 FDIA；另外，还可以利用物理水印[58]及最新的信息处理和通信技术，如 D–FACTS 和多传感器信息融合[50]来实施 MTD。

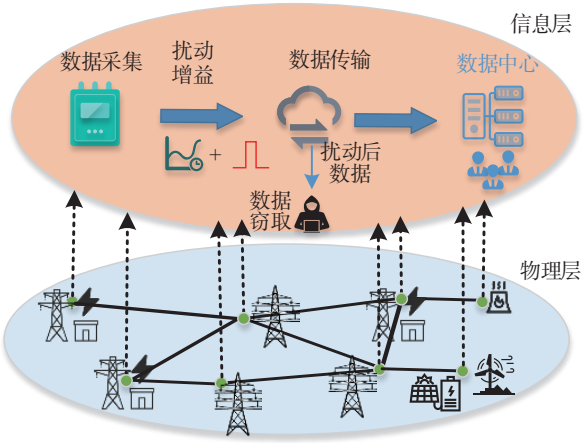

图 1　扰动传感增益实现 MTD

Fig. 1　Changing the sensor gain to achieve MTD

在对 MTD 运行阶段的研究中，Higgins 等[58]将 MTD 与物理水印相结合，水印模仿了系统潜在的高斯噪声，这种设计能够在 MTD 运行时保持隐蔽状态，同时能够发现系统中微小但持续变化的攻击。Xu 等[59]将数据驱动的攻击检测器与基于物理的 MTD 相结合，有效降低了数据驱动检测器的误报率，同时降低了 MTD 的运行成本。Zhang 等[65]发现适当的策略不仅不会增加系统的运行成本，还能够在实现 MTD 的同时降低系统的运行成本，实现双效益的 MTD。因此，将 MTD 与其他检测方法相结合，能够在有效降低防御成本的同时，显著提升检测效果。

2）针对特定攻击制定精准策略

针对特定攻击，需要特别设计的 MTD 以实现更优的检测效果，例如，Liu 等[10]将 MTD 防御对象从 FDIA 扩展欺骗攻击（包括 FDIA 和重放攻击），以及应对隐蔽 FDIA[57]和负荷重分配攻击[61]。Stuxnet 攻击作为一种特殊的攻击策略，通过将恶意控制命令注入执行设备的同时攻击量测仪器，这类对控制器与传感器的数据完整性进行协调攻击的方法被称为 SL 攻击。Tian 等[50]研究了 SL 攻击的检测方法，并发现 SL 攻击与针对 SE 的基于量测残差 BDD 的 FDIA 具有本质区别：SL 攻击绕过对控制/传感器数据时间序列的基于

时间相关性的检查，而不像FDIA那样绕过基于空间相关性的检查。因此，现有的FDIA检测方法不适用于SL攻击检测。SL可分为测量无关隐身攻击（MISA）、测量依赖隐身攻击（MDSA）。对于MISA，攻击者利用对目标系统的全部了解来构建对异常检测器完全隐蔽的SL攻击；MDSA则利用窃听量测来减少攻击对目标系统知识的依赖，但这也降低了攻击的隐蔽性。针对这种特殊的攻击，Tian等[50]还提出特殊的MTD构造策略，通过扰动控制单元，MTD可以处理MISA，而仅扰动传感单元的MTD可排除本文考虑的任何隐蔽MISA和MDSA。Zhang等[53]进一步指出MTD无法防御可被零参数信息FDIA入侵的节点，这类节点需要进行关键节点强化安全保护。

3）面向关键节点强化安全保护

多数研究往往假设攻击者了解目标系统的全部信息，进而能够利用这些信息发动全信息FDIA。尽管这种假设对防御策略提出更高的要求，但在构建MTD策略时，这种假设通常是可接受的。然而，在实际情况中，特别是对于大规模的电力系统而言，要想获取系统的拓扑结构和参数信息不太现实[44]。当攻击者仅获知部分目标系统的拓扑结构和参数信息时，也有可能发动隐蔽FDIA。甚至在更极端的情况下，攻击者可以无需获取目标系统的拓扑结构和参数信息，即可发动零参数信息FDIA，也就是基于“割”的FDIA[53]。

Zhang等[53]针对图2所示的度为1的节点（仅与割线相连的节点）、度为1的超级节点（仅与割线相连的节点群），以及仅与割线相连接的节点和超级节点的3种场景构建基于割线的零参数信息数据完整性攻击（ZDIA）。然而，MTD对于此种ZDIA并不能形成有效的防御。针对这种情况，可以利用加密和编码策略对相关节点的量测进行保护，此外，还可以增加输电线路以消除割线，从而提高系统的安全性。

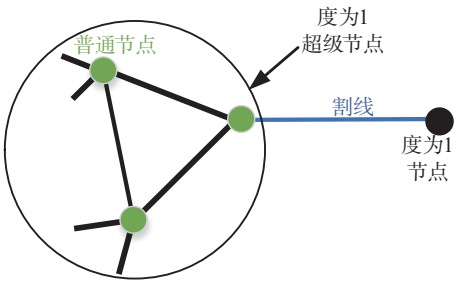

图2 度为1节点、度为1超级节点的等效模型

Fig. 2 Equivalent model of degree 1 node, degree 1 super node

4）依托复杂建模支持深度分析

传统的MTD策略将线路参数简化为单相等效值的假设对于三相不平衡配电系统并不适用，因为攻击者同时攻击三相线路的情况并不现实。为了建立更加贴近实际的数学模型，Cui等[62]将平衡的直流传输系统扩展到三相不平衡的交流配电系统，考虑输电线路的自抗和互抗，提出三相不平衡配电场景下的MTD策略。

Zhang等[61]关注MTD运行后所引起的电压不稳定问题，并提出一种防御策略，该策略在考虑对电压稳定性的影响时，平衡MTD的运行成本与检测性能。随着分布式电源的普及与发展，直流微电网的应用也将日益广泛。然而，分布式能源系统需要通信进行统筹协调，这为潜在的攻击提供了条件。在这一背景下，Liu等[10]研究了基于转换器的MTD策略对FDIA和重放攻击的增强可检测性，将研究对象转移到微电网。Giraldo等[56]进一步提出分布式MTD来保护微电网。

3 新型电力系统MTD的关键技术与实施展望

随着电力系统的不断发展，智能化程度的提升及能源互联网概念的兴起，未来供能网络的发展趋势将朝向更加用户友好的方向。用户不仅是能源的消耗者，还将成为能源的供应者，使得系统运行状态变得更加复杂，系统面临的被攻击风险也将随之增加。然而，现阶段的MTD技术主要应用在输电网络，难以满足新型电力系统防御攻击的需要。

根据第2.3节总结的电力系统MTD策略可知，多数文献通过D–FACTS设备改变输电线路电抗来实现MTD。新型电力系统MTD在继承传统方法核心思想的基础上，通过引入智能信息处理[58]、微电网[10,56]、新能源，以及多能耦合等前沿技术，构建了更为广泛和动态的防御体系，为提高电力系统的安全性和韧性提供了新的理论与实践支撑。在发电侧，动态控制新能源接入与断开，实现电力系统拓扑结构的实时调节；在输能网络中，引入多能耦合系统，提升系统灵活性并拓展MTD动作空间；在配电网方面，利用电动汽车和分布式电源，通过能源微网运行、动态重构技术实现移动目标防御；在用能阶段，基于数据预测与用能行为引导，优化系统灵活性和经济性；借助通信与信息处理技术，实现多能系统子系统的信息共享与协同防御，增强整体抗攻击能力。这些技术有效提高了电力系统的安全性与韧性。

推动新型电力系统建设的过程，即是促进电网向能源互联网升级的过程[71]。在新型电力系统中实现MTD，一方面，要借助新型电力系统中的先进传感、通信和信息处理技术；另一方面，要借助系统中的多能互补优势。其中的关键技术是实现新型电力系统MTD

的重要保证。

3.1　新型电力系统MTD关键技术

实现MTD的关键在于多层面的协同推进：设备层聚焦于复杂建模技术，以提供基础数据；系统层依靠多能协同感知技术，以提升态势掌控力；通信层利用动态路径控制技术阻断攻击路径；优化层以智能协同控制技术，实现系统高效运行；安全层通过智能防护技术，增强应变能力。这些关键技术共同构建了新型电力系统MTD动态、防御纵深的体系，确保新型电力系统的稳定运行与安全防护。

3.1.1　设备层精细建模技术

新型电力系统集成了大量先进的通信、信息处理和控制技术，这些技术依赖于不同类型的电子设备。电力电子装备单体建模、新能源聚合建模、分布式负荷建模是电力系统仿真中的难题[72]，对其准确建模是实现新型电力系统感知和控制的基础。针对现有电力系统MTD模型过于简化问题，需要研究设备层的精细建模技术。

设备精细建模通过精确地模拟系统在多种操作模式下的响应行为，为MTD策略提供支持，帮助系统识别和定位潜在的攻击路径及薄弱环节。同时，精细建模技术需要在建模精度与计算速度之间取得平衡，使系统能够快速响应和调整，从而提高防御效果。随着分布式能源、微电网的广泛应用，电力系统架构日益复杂，精细化建模有助于增强MTD的灵活性和适应性，从而确保在多样化的设备环境中系统防御策略能有效实施。

3.1.2　通信层动态路径控制技术

设备采集到的系统数据需传输到信息处理中心进行分析和决策。针对信息在传输过程中容易受到攻击的问题，需要研究考虑能源网络的通信层动态路径控制技术。

通信层具备灵活的架构和可动态调整的特性，为部署MTD策略提供了有利条件。网络与通信层的关键技术包括软件定义网络[27,35]、虚拟网络，以及CPS的耦合分析；其通过动态化的通信路径与网络资源管理为新型电力系统MTD提供支撑。在新型电力系统中，通信网络的动态调整能够有效阻碍攻击者对系统通信链路的掌握。软件定义网络技术的可编程性使系统能够实时调整通信路径[35]，确保攻击者无法预测或控制关键数据流。此外，CPS的耦合分析技术能够揭示网络攻击对电力系统运行的潜在影响，为MTD策略的优化提供了理论支持。

3.1.3　系统层多能协同感知技术

量测得到的“生数据”需经进一步处理得到“熟数据”，以获得更加真实的系统运行状态[73]。随着新型电力系统向IES的发展，电力系统不再局限于电能，而是包含电、热（冷）、气等多种能源形式。电网态势感知通常分为觉察层、理解层和预测层[74]，但单一能源系统的传统感知手段已无法全面捕捉系统的动态变化。针对上述问题，需要研究多能协同感知技术。

多能协同感知技术实现对多能系统运行状态精准的监控、分析与预测。新型电力系统MTD中，SE为态势感知提供基础数据支持；态势感知通过高层次的分析与预测，帮助系统做出动态调整和策略决策，干扰攻击者的判断，确保系统防御的灵活性和有效性。FDIA通过注入虚假数据干扰状态估计，可能导致错误的调度决策，威胁电网安全。状态估计通过实时处理量测数据，支持电网可观测性，并识别异常数据，进而发现潜在的FDIA。MTD的原理是比较MTD动作前后状态估计的偏差，一旦偏差超过阈值，则判定存在FDIA。新型电力系统中的MTD涉及多能耦合系统，因此，综合能源系统状态估计技术对于理解和实施新型电力系统MTD至关重要。在IES的SE研究中，学者们进行了电-气IES[75-79]、电-热IES[80-81]、电-气-热IES[82-83]的SE研究。多能协同感知技术是在多能SE的基础上，进一步处理这些数据，提供系统整体的运行动态，预测潜在的安全威胁和隐患，为MTD策略生成提供实时支持。

3.1.4　优化层智能协同控制技术

仅获取系统信息不足以确保系统的安全与稳定，还需对系统进行控制。针对单一的控制策略难以应对多类型设备的动态变化和相互影响等问题，需要研究智能协同控制技术。

随着分布式光伏、风电、储能系统的大量接入及多能流系统的发展，需要依托多能流分布自治控制、IES集群协同优化技术[71]。在智能协同控制下，大规模的动态参数调控、分布式能源协调控制，以及柔性输电系统的实时调度得以实现。上述技术能够确保设备状态的动态性与不可预测性，构成了实现新型电力系统MTD的基础。人工智能的感知与智能决策，为能源领域新型电力系统的数字化转型提供了解决方案[84]。随着强化学习等人工智能技术的进步，该技术在新型电力系统的攻击检测和安全防御方面已经展现出显著的应用效果[8]。这些技术应用到MTD中，能够将系统的防御策略从静态转向动态，使系统具备更高的自适应性和恢复能力，未来应着重于提升动态控制算法的自适应性，寻求MTD性能与控制实时性的平衡。

3.1.5 安全层智能主动防护技术

精心设计的攻击行为可能对系统稳定性构成严重威胁；针对依赖协同控制不能完全保证系统安全性的问题，需要发展智能主动防护技术。

安全防护的核心技术包括动态信任管理[85–86]、博弈论分析，以及基于人工智能的异常检测[87]，确保了MTD在复杂攻击环境中的有效性与适应性。动态信任管理通过对设备和通信节点的信任等级进行主动动态调整，能够及时识别和隔离潜在威胁，提升系统的内部主动防护能力。博弈论分析为防御策略的制定与优化提供数学模型，使系统能够在动态攻防环境中不断调整策略，实现防御资源的最优配置。基于人工智能的异常检测技术则通过深度学习算法实现对异常行为的实时识别和早期预警，为MTD策略的高效实施提供支撑。未来应专注于信任管理系统的智能化升级，以及防御策略的多层次优化，以确保系统在面对多重威胁时保持高效稳定。

3.2 新型电力系统MTD实施策略

基于电力系统MTD研究、新型电力系统MTD关键技术及新型电力系统特点，对新型电力系统MTD策略进行分析。新型电力系统MTD的基础框架如图3所示。

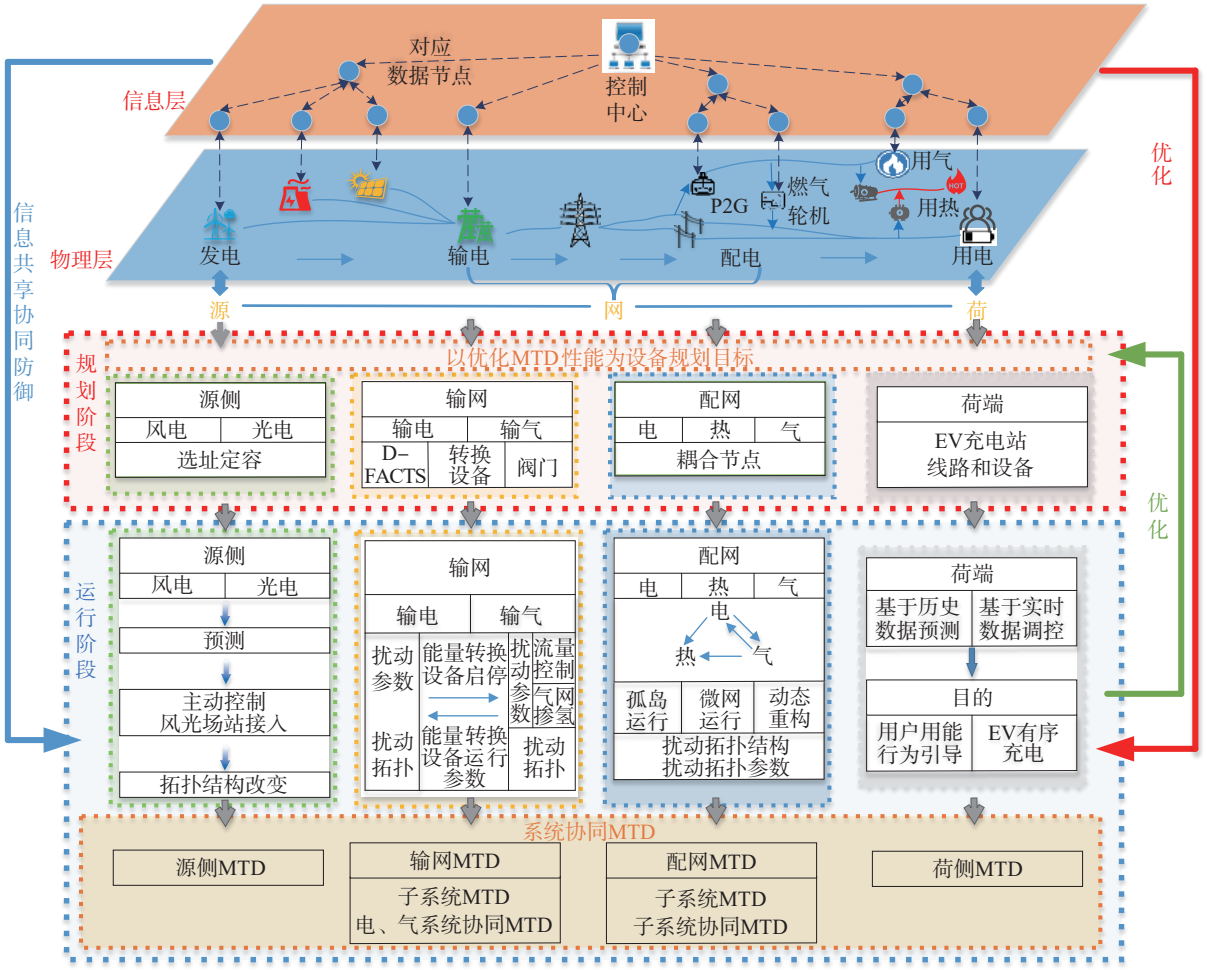

图3 新型电力系统MTD框架

Fig. 3 MTD framework of the new power system

依托信息层，物理层在运行阶段实现运行状态优化和协同防御；运行数据用于优化现有规划。研究对象分为发、输、配、用，以及信息共享协同防御5个部分，并将MTD策略分为规划、运行两个阶段。

3.2.1 基于新能源接入规划与运行状态的MTD

风电和光伏等新能源出力的不确定性使得攻击者难以准确预测系统状态，为MTD提供了可行条件。图4展示了发电侧MTD策略。

由图4可知，该策略分为规划阶段和运行阶段。在规划阶段，考虑风光资源分布、负荷需求及最大化MTD在运行阶段效用，优化基础设施配置，并给出定容方案，为运行阶段奠定基础。在运行阶段，基于规划方案，精确控制风电场和光伏电站的接入；通过负荷预测调整能源接入，并根据需要调整系统拓扑以实现源侧MTD。同时，根据运行阶段的表现，持续优化规划阶段的部署，制定滚动规划方案。

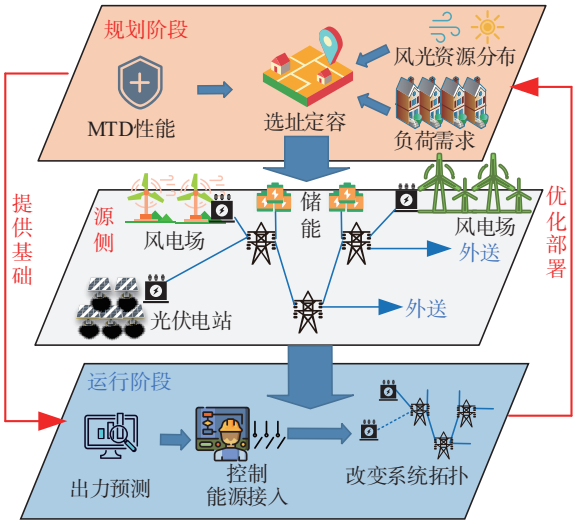

图4　发电侧MTD策略

Fig. 4　MTD strategy on the power generation side

1）规划阶段

在新能源场站规划阶段，基于新能源分布和供电能力的随机性，优化系统结构，增加系统的不确定性，为后续的运行防御奠定基础。考虑如图4所示的风能、太阳能等新能源接入的多样性。多样化的能源接入将提升系统的复杂性和不确定性，为MTD实施提供可行条件。同时，还需考虑负荷分布及最大化MTD在运行阶段的性能，以应对系统可能出现的故障，提升MTD抵御攻击的鲁棒性。借助新能源聚合建模、分布式负荷建模[72]，进一步优化新能源场站的规划。

2）运行阶段

在运行阶段，利用新能源出力的间歇性和不确定性，增加系统运行状态的不可预测性。借助对设备的协同动态控制技术，主动控制新能源的接入状态，主动管理系统的能源供应。通过控制新能源的接入与断开，动态地调整电力系统的拓扑结构，提升攻击者对系统进行有效攻击的难度，实现新型电力系统的源侧MTD。

3.2.2　基于输能通道规划与优化配置的MTD

基于输能通道规划与优化配置的MTD策略，利用输电和输气系统的不确定性，通过动态调整系统参数和拓扑结构来提升电力系统的抗攻击能力。图5展示了能源输送环节的MTD策略。

由图5可知：在规划阶段，主要考虑输电、输气通道的布局与D–FACTS设备、阀门、掺氢节点配置。通过选择合理的扰动参数和设置冗余拓扑，增强系统结构的灵活性和不确定性，为后续运行防御奠定基础。在运行阶段，着重于实时调节输电、输气通道的扰动参数和拓扑结构，使系统状态持续变化。

1）系统参数扰动

在电力系统中，通过调节图5所示的D–FACTS设备的参数来主动改变线路阻抗。在多能系统中，存在更多的可控设备和可调系统参数，这使得扰动输电线路参数的方法得以推广应用于新型电力系统的多能输能网络。下面以含气新型电力系统为例进行分析。

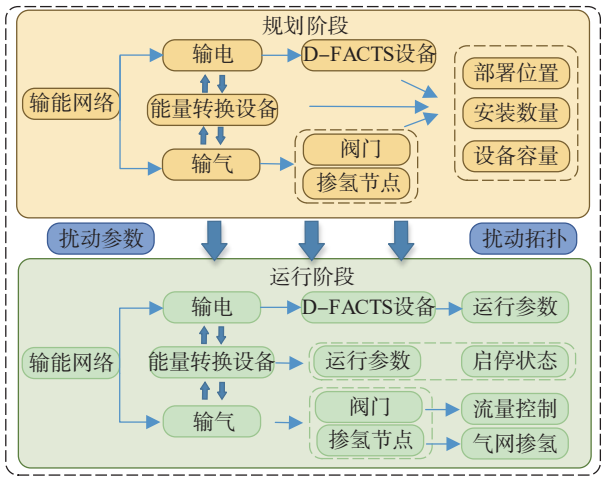

图5　能源输送环节MTD策略

Fig. 5　MTD strategy for energy transmission

a. 气网

根据气网量测方程、约束方程，参照电网，MTD改变输电线路阻抗可以考虑主动改变输气管道阻力系数。改变管道阻力系数能够改变气网的量测方程，增加系统信息的不确定性，进而增加攻击难度。

天然气相关量测方程中天然气管道的暂态常数[73]、特征阻抗[88]，取决于管道的物理特性和气体的性质，表征天然气管道的传输能力。考虑以下形式来改变暂态常数：一是，在输气管道上增加阀门，通过改变阀门的开闭程度，等效改变该输气管道的直径，达到改变暂态常数的目的；二是，在天然气中掺氢，通过向输气管道的天然气中掺入氢气改变管道中气体的性质。目前，已有天然气掺氢的相关研究，例如：魏震波等[89]将掺氢比例上限设置为1%～24%；在宁夏银川的宁东天然气管道掺氢实验中，最高掺氢比已达24%[90]。

b. 能量转换设备

能量转换设备的运行状态和控制策略与气网的动态调整密切相关。在气网动态调整的过程中，能量转换设备需同步调整其运行模式。气网中，天然气流量的变化促使燃气轮机根据新的气体供应条件，调整其发电能力和运行效率。

能量转换设备运行参数（转换效率、输入输出功率等）及启停状态的调整能够影响整个IES的系统参数和系统拓扑。借助能量转换设备的动态控制技术改变能源在系统中的流动路径和分配比例，增加系统的不确定性进而实现MTD。

2）系统拓扑变化

a. 能量转换设备部署策略

在IES中，能量转换设备是将不同供能子系统进行耦合的关键设备，改变能量转换设备的启停状态可以改变系统的拓扑结构，进而扰动系统拓扑，为实现MTD创造条件。同时，能量转换设备是IES的重要组成部分，不需要单独安装MTD设备，节省成本。在IES的规划建设阶段，可以研究能量转换设备的位置部署，使得MTD动作时达到最大的拓扑结构扰动效果，提高MTD性能。

b. 储能设备部署策略

将储能设备与D–FACTS设备的部署策略相配合，能增加MTD的运行灵活性，降低MTD动作对系统潮流影响。改变储能设备和电动汽车的充放能规律，增加该节点对于攻击者的不确定性。储能设备部署策略是通过部署较少的储能设备或是尽可能利用现有的充电站和保护范围覆盖较多的节点，提升系统整体MTD的性能。

3.2.3 基于配网灵活运行与动态防御的MTD

配电网中大量的量测设备和智能电表增加了系统潜在攻击目标。随着电动汽车保有量与分布式能源装机量的持续增加，用户与系统的交互功率越来越大，其受到攻击后的损失也更大。因此，在配电网中实施MTD来提高系统的安全性变得十分必要。在配电网实施MTD面临的挑战是高密度量测设备带来的经济成本和管理复杂性，这在初期阶段会限制其可行性。然而，电动汽车不仅能够充当电力负荷，还可以作为动态量测设备，提供充电状态、充电功率等实时数据，从而弥补传统量测设备的不足。电动汽车与负荷调度系统结合，增强系统运行灵活性，有助于实现更广泛的MTD应用。分布式能源（如光伏、风力发电）的广泛接入为配电网运行带来了更大的灵活性，通过控制这些能源的接入与退运，能够优化配电网的拓扑结构，从而实现配电网MTD。现有研究也已将电力系统MTD扩展到配电网[62,68]；Liu等[47]提出的MTD策略中未对电力系统做出任何假设，因此该策略既适用于输电也适用于配电系统，并给出输配电系统MTD的统一设计方法。

基于配电网灵活运行与动态防御的MTD策略中，利用配电网灵活的运行与控制来提升系统检测和抵抗攻击的能力，能源分配环节MTD策略的总体思路如图6所示。配电网的分布式电源出力和负荷需求等因素具有随机性和波动性，这种不确定性使得攻击者难以准确预测系统状态。通过借助多能协同感知和控制优化技术，MTD策略与配电网灵活运行相结合，动态调整系统运行方式，使得攻击者难以构建有针对性的攻击。如图6所示，在规划阶段，结合多种能源的耦合关系，通过优化资源配置和控制策略设计，提高系统的灵活性和不确定性，为运行阶段动态防御奠定基础。在运行阶段，依托多能协同感知技术和协同控制优化技术，实时调整系统状态，使得配电网在不同条件下保持动态化。

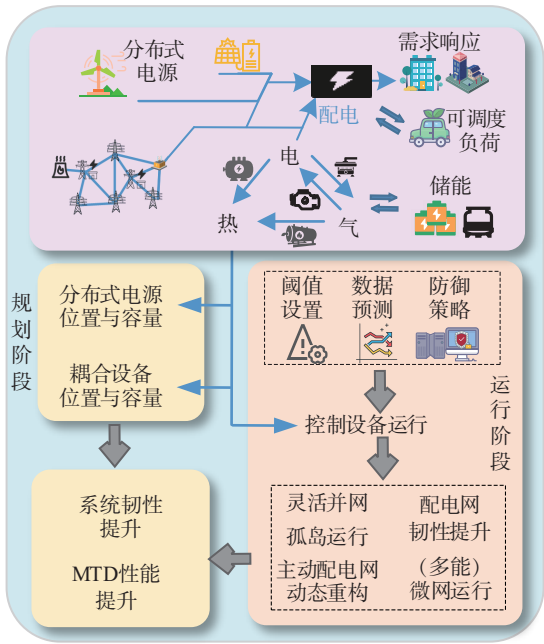

图6 能源分配环节MTD策略

Fig. 6 MTD strategy for energy distribution

1）考虑灵活并网与孤岛运行

图6中的分布式电源在电网中的接入与断开操作，直接对应着相关线路的接入与断开。随着线路的通断状态变化，电力系统的拓扑结构也会相应调整。在分布式电源与系统的交互过程中，其接入与退出的灵活性成为了一种重要的防御资源。在MTD的框架下，分布式电源的接入与断开，一方面，能满足变化的负荷需求；另一方面，主动制造系统的不确定性，使得潜在的攻击者难以掌握系统的实时状态和运行规律。通过动态调整分布式电源的接入状态，可以改变系统的拓扑结构，从而实施一种有效的MTD策略。

分布式电源的灵活并网或孤岛运行模式为MTD的实施提供了有力支撑。在并网模式下，分布式电源与主电网相连，共同为负荷供电；在孤岛模式下，分布式电源可以独立运行，为本地负荷提供电力。在遭受攻击时，迅速切换运行模式，以降低攻击的影响。通过合理划分孤岛区域、设置并网/孤岛切换的阈值等拓扑参数，可以进一步优化系统的运行效率和安全性。这些参数的动态调整增加了系统的不确定性，使得攻击者难以准确预测和攻击系统的脆弱点。

2）考虑能源微网运行

按照新能源出力与负荷情况调整新能源的并网模式，系统有可能处于孤岛运行模式。孤岛运行模式下，仍然涉及较大规模的电网系统，虽然相较于解列前的系统改变了拓扑结构，但是拓扑变化有限。在单一供电系统下，为保证重要负荷的供电可靠性，系统的运行方式受到限制，不利于MTD动作。

因此，在IES的框架下，考虑将电力系统的孤岛运行模式进一步转变为微电网运行。通过定期或不定期地更换网络设备的位置、调整数据传输和通信的路径，或者改变系统的控制逻辑和策略，微电网可以呈现出动态和不确定性。该动态和不确定性正是MTD策略的核心思想。在微电网中，利用上述特性，可以提升MTD的性能，更有效地保护系统免受潜在的网络攻击。

3）考虑主动配电网动态重构

配电网通常采用环网规划，以开环形式运行，该策略导致部分线路在特定时段内处于闲置状态。一方面，闲置线路的有效投切可优化系统潮流；另一方面，通过闲置线路的优化连接，可以灵活地改变系统的拓扑结构。这一特性使配电网在MTD策略中具有一定的应用潜力。

主动配电网通过调节分段开关和联络开关的状态，实现对系统拓扑结构的动态调整。基于多能协同感知技术的实时数据和预测数据，配电网可以进行如开关操作、变压器投切等动态调整，以达到能源分配的最优化，并降低损耗及提高电压稳定性。上述动态调整提升了电网的可靠性、效率和安全性，为MTD策略的实施提供支持。将主动配电网的这一特性应用到供能系统的MTD之中，可以采取以下策略：

a. 动态调整网络拓扑

利用主动配电网中的可调节开关，系统定期或根据安全需求不定期地改变电网的拓扑结构。攻击策略通常需要针对特定的、静态的网络拓扑来设计和实施，持续的变化增加了攻击者的攻击难度。网络拓扑的动态变化使得攻击者的预先攻击策略可能失效，从而提高系统的安全性。除了定期的网络拓扑调整，还可以通过随机化开关的操作时间和状态，在电网运行中引入更多的不确定性和随机性。这种随机性使得攻击者难以准确预测和把握电网的实际运行状态。

b. 结合多样化的能源供应

主动配电网支持包括可再生能源和传统能源在内的多样化能源输入和输出。通过动态调整不同能源之间的供应比例和方式，系统可以进一步增加电网的复杂性和多样性。这种复杂性和多样性的提升提高了攻击者探测和利用系统漏洞的成本，从而增强了MTD策略的有效性。

4）考虑配电网韧性提升

系统在线状态感知有利于配电网抵抗外部干扰，灾后状态感知有利于恢复[91]。IES多能互补特性提升了配网韧性，使其在部分线路断开时仍能维持一定的供电能力，减轻对系统稳定性的影响。面对极端自然灾害或人为故障时，多能互补确保供电可靠性，主动断开线路为拓扑结构调整提供条件。IES多能互补特性与MTD策略相结合，实现灵活防御，并提升安全性和韧性。

3.2.4　基于用户用能数据与需求侧管理的MTD

基于用户用能数据与需求侧管理的MTD策略，利用用户侧用能行为的多样性和不确定性，通过感知和引导用户需求变化来提升系统的防御效果。为进一步提升系统防御性能，本文构建了面向用户侧的MTD策略，其运行机制见图7。通过对用户用能行为的感知和适度引导，MTD策略能够不断调整需求侧的负荷状态，增加系统的动态性，从而提升抗攻击能力。如图7所示，用户侧MTD依托协同感知技术和协同控制优化技术，实时监测用户的用能行为，并在必要时加以引导，以动态优化系统的防御能力。通过这种方式，系统基于用户用能的不确定性和对用能行为的主动控制，扰乱攻击者的预测，使得攻击者难以准确掌握系统状态。

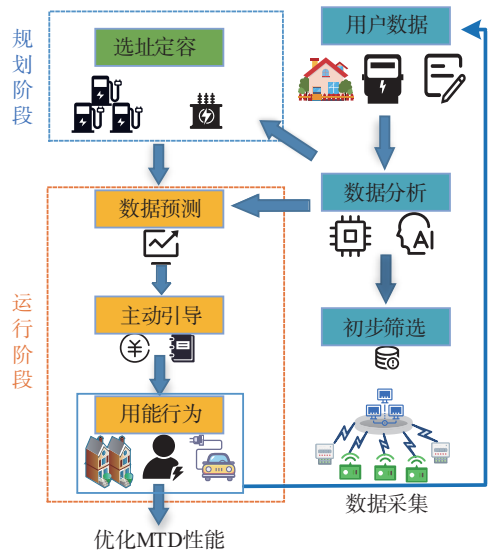

图7　用户侧MTD策略

Fig. 7　MTD strategy on the energy consumption side

1）基于用户用能信息的MTD策略优化

在MTD策略中，用户行为数据可以作为可调度资源来优化和调整防御机制。利用智能电表、传感器等设备收集用户的实时用能数据，包括用电量、用电时间、用电设备类型等信息。通过多能协同感知技术

收集和分析用户的用能行为数据，预测未来的负荷变化。基于预测数据更合理地调整能源分配、系统拓扑，以及提前进行MTD部署和MTD运行参数设定，提升MTD效果。为保护用户隐私，对负荷可进行分布式协同优化调度[92]。

2）基于用户行为引导的MTD策略优化

根据多能协同感知技术获取的数据，利用智能协同控制技术，控制可调度负荷。在用户与供能网络交互更频繁、更方便的背景下，通过激励机制，可以对用户的用能、售电行为进行调控。系统层面的主动调控增加了系统对攻击者的不确定性。需求侧管理通过引导用户行为，主动调整系统的运行状态，使得系统的拓扑参数和拓扑结构不断发生变化。因此，攻击者难以准确掌握系统的实时状态，其针对特定状态所设计的攻击策略失效，从而实现MTD。电动汽车的智能化有望实现对激励机制更为及时的响应，以满足MTD的实时性需求。

3.2.5 基于信息共享机制与协同防御的MTD

在多能系统中，各子系统通过信息共享和协同防御可以增强整体的抗攻击能力。基于信息共享的MTD策略利用各子系统间的动态数据传递，使系统能够快速识别并响应潜在的攻击威胁。同时，能源子系统之间的物理耦合效应允许一个子系统的防御动作传导至其他子系统，从而形成跨子系统的动态防御体系。

1）考虑子系统信息共享的MTD

通过动态、实时地在不同子系统间共享关键运行状态和安全信息，提升各子系统的状态感知，增强整个IES系统的协同防御能力。因此，本文进一步提出了面向多能系统的跨子系统信息共享型MTD策略，其工作原理如图8所示。动态路径控制技术和智能防护管理技术在信息层为能源子系统内部及系统间的信息传输提供安全保障。

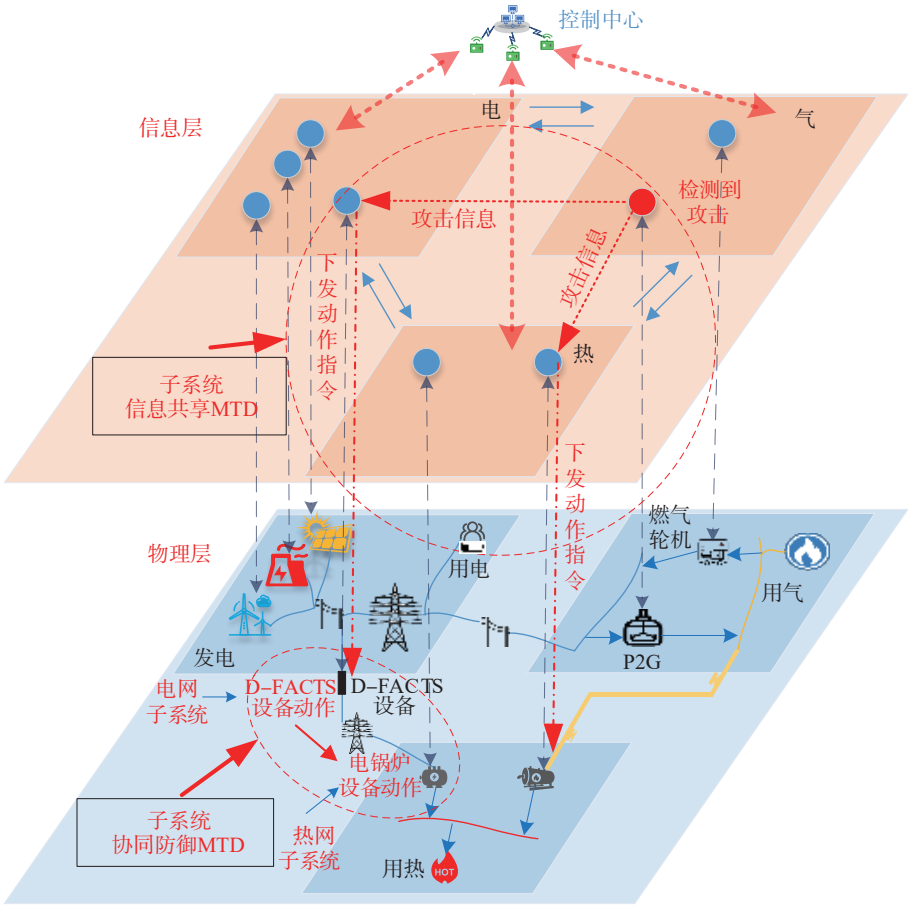

图8 基于信息共享与协同防御的MTD

Fig. 8 MTD based on information sharing and collaborative defense

当某个子系统检测到潜在的攻击行为或异常状态时，该子系统迅速将此信息传递给其他子系统。如图8所示，当天然气子系统信息节点的数据发生异常时，系统将异常情况传递给供电子系统和供热子系统，对相应设备下发动作指令，做好防御准备。该信息共享机制使得MTD能依托于其他能源子系统的数据进行有针对性的防御动作，基于这些信息，其他子系统可以迅速调整自身的防御策略，而无需进行全面的、可能干扰正常运行的MTD动作。基于信息共享的MTD策略提高了单个子系统的安全性，从整体上强化

IES的鲁棒性和抗攻击能力。

2）考虑子系统协同防御的MTD

不同能源子系统通过信息共享实现MTD协同运行。如图8所示，当供热子系统的设备运行状态发生改变时，造成的影响会传递至供气子系统。若图8供电子系统中D–FACTS相连节点的量测数据发生变化，而电锅炉的运行状态没有发生变化，则可以判定系统中存在攻击行为。在物理层面上，电、热、气系统之间的耦合关系构成了协同防御的基础。攻击者在尝试篡改数据时需要同时考虑多个系统之间的交互关系，使得攻击者更难推测系统的信息，从而为系统提供保护屏障。

当供热系统因MTD动作而运行参数发生改变时，这种扰动会通过物理层的耦合传播到供电系统和供气系统的相关节点，并在量测数据上体现出来。该特性使得系统可以在不同的子系统中进行扰动参数和量测数据的校验，跨子系统实施MTD策略。通过这种跨子系统的MTD实施策略，能更灵活地应对潜在的网络攻击，以提升整体防御能力。

4　新型电力系统MTD面临的应用挑战

MTD通过动态调整系统参数，增强新型电力系统对网络攻击的防御能力。这种灵活的主动防御策略能够有效迷惑攻击者，降低其成功篡改系统信息的可能性。然而，MTD在实际应用中仍面临建模复杂、预警困难、性能受限等问题。这些挑战亟需进一步研究与解决，以充分发挥MTD在新型电力系统中的优势。

4.1　建模复杂

现有电力系统MTD研究涉及的攻击与主动防御模型做了简化和一定的假设。为简化计算和分析，目前所使用的MTD模型多基于直流潮流模型。随着电力系统的发展和电力电子设备的大量使用，系统呈现出明显的非线性特征，直流潮流模型已不再适用，需要更加复杂的设备建模及设备间复杂的耦合模型。

随着新能源的出力占比的逐渐增加，以及新型电力系统、智能电网、能源互联网等概念的提出，未来电力系统将迈向更加智能、更加灵活的方向。在多能耦合系统中，不同能源的物理动态特性不同，其所对应的调度时间尺度不同步，进一步加大了系统的建模难度。用户侧的灵活性与可调度特性，使得用户侧具有较大的发展潜力。同时，也需要用更复杂的模型刻画用户与供能系统之间更加频繁与深入的交互。

4.2　预警困难

随着分布式能源的发展，用户不再仅仅是单一消费者，还将成为能源的生产者，实现产消合一，并积极参与到能源系统的交互中。分布式能源受外界环境影响较大，可能在短时间内形成巨大的出力波动，并与FDIA引发的量测功率波动有极大的相似性。分布式电源的功率波动将与FDIA的虚假功率注入混合在一起，淹没攻击特征，造成MTD的漏检和误检。区分正常运行时的短时大幅度功率波动与FDIA造成的虚假功率波动变得困难，而现有文献很少考虑到该问题。

同时，攻击者可能会利用新能源出力的波动性来优化攻击参数，从而使攻击行为更加隐蔽。特别是将MTD应用于配电网时，问题可能变得更加复杂。在负荷侧，电动汽车的充电行为可能导致负荷的短时大幅波动，这与分布式能源出力的波动性相似。从MTD的角度来看，难以将这种负载波动与FDIA造成的虚假功率波动区分开来。

4.3　性能受限

在网络安全领域，随机MTD策略的防御成本较高，针对性不强，且不适用于隐蔽性MTD场景；基于博弈论的MTD策略复杂度较高，现有方法往往基于先验知识，难以满足实时性防御要求；而基于机器学习的MTD可能受到动态目标攻击（MTA）的影响[43]。这提示在设计和应用新型电力系统MTD策略时，必须更谨慎地评估其实际可行性和适用性。

由于拓扑结构是电力系统固有的特征，在不集成其他防御策略的情况下，单一MTD的检测效果很难再有显著提高，如文献[40]中的算例结果表明，受电力系统拓扑限制，在57节点系统中MTD对FDIA的检测概率不超过40%。需要将MTD与其他防御方法相结合，从而进一步提高FDIA的检测率。针对MTD并未根本解决系统薄弱节点的问题，需要将MTD与其他主动防御手段相结合（如主动诱捕、脆弱节点加固等），避免因使用单一防御手段带来高昂的防御成本。

5　结　语

作为一种主动防御策略，MTD已在电力系统防御中逐渐展现出显著优势。在新型电力系统信息层与物理层之间的紧密耦合中，信息侧的攻击可能直接影响物理层的运行；在含多能耦合的系统中，供能子系统间存在攻击扩散的风险。然而，CPS和多能系统的建设也引入了丰富的可调度资源和主动智能控制手段，为MTD的实施创造了良好的条件。

CPS及信息处理和通信技术为新型电力系统MTD提供了高效的数据管理和风险控制支持；多能系统为MTD提供了更灵活的运行方式和更大的运行空间。这些新特性、新技术使得新型电力系统MTD能够有效预警并迅速响应变化的攻击态势，进而在更大的

MTD运行空间内最大限度地降低攻击对系统的影响。通过动态调整系统运行参数，MTD不仅能有效迷惑潜在攻击者，还能实时监测和评估系统状态，以快速适应下一阶段的FDIA。尽管当前的MTD模型仍存在建模不够精细等问题，但其防御理念、方法和技术在电力系统中的应用优势依然显著、前景广阔。

新型电力系统的持续演进，包括新能源接入、配电网的智能化、IES的发展及用户侧的动态管理，为MTD的进一步应用提供了更广阔的发展空间。在这些复杂环境中，MTD可以与其他防御措施相结合，形成多层次的防御体系，从而更有效地应对不断演变的安全威胁。

附录见本刊网络版，扫描标题旁的二维码可阅读网络全文。

参考文献：

[1] Zang Tianlei, Gao Shibin, Liu Baoxu, et al. Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks[J]. Reliability Engineering & System Safety, 2019, 189: 232–241.

[2] Zhou Buxiang, Min Xinwei, Zang Tianlei, et al. Loss assessment and vulnerability analysis of an integrated electricity natural gas system under load redistribution attack[J]. Advanced Engineering Sciences, 2023, 55(1): 3–13. [周步祥, 闵昕玮, 臧天磊, 等. 负荷重分配攻击下电–气系统损失评估与脆弱性分析[J]. 工程科学与技术, 2023, 55(1): 3–13.]

[3] Li Zhiqiang, Su Sheng, Zeng Xiangjun, et al. Fabricated traps based active cyber security defense against targeted cyber-attack in electric power dispatching systems[J]. Automation of Electric Power Systems, 2016, 40(17): 106–112. [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.]

[4] 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. [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.]

[5] Wang Qi, Li Mengya, Tang Yi, et al. A review on research of cyber-attacks and defense in cyber physical power systems part one modelling and evaluation[J]. Automation of Electric Power Systems, 2019, 43(9): 9–21. [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.]

[6] Gao Chungang, Wang Yongjie, Xiong Xinli. MTD enhanced cyber deception defense system[J]. Computer Engineering and Applications, 2022, 58(15): 124–132. [高春刚, 王永杰, 熊鑫立. MTD增强的网络欺骗防御系统[J]. 计算机工程与应用, 2022, 58(15): 124–132.]

[7] Zhou Buxiang, Cai Yating, Zang Tianlei, et al. Reliability assessment of cyber-physical distribution systems considering cyber disturbances[J]. Applied Sciences, 2023, 13(6): 3452.

[8] Yang Ting, Xu Zheming, Zhao Yingjie, et al. Review on research of attack and defense methods for digitalized new power system[J]. Automation of Electric Power Systems, 2024, 48(6): 112–126. [杨挺, 许哲铭, 赵英杰, 等. 数字化新型电力系统攻击与防御方法研究综述[J]. 电力系统自动化, 2024, 48(6): 112–126.]

[9] Liu Yao, Ning Peng, Reiter M K. False data injection attacks against state estimation in electric power grids[C]// Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009: 21–32.

[10] Liu Mengxiang, Zhao Chengcheng, Zhang Zhenyong, et al. Converter-based moving target defense against deception attacks in DC microgrids[J]. IEEE Transactions on Smart Grid, 2022, 13(5): 3984–3996.

[11] Le Jian, Lang Hongke, Tan Tianyuan, 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. [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.]

[12] 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. [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.]

[13] Tang Yi, Li Mengya, Wang Qi, et al. A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection[J]. Automation of Electric Power Systems, 2019, 43(10): 1–9. [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.]

[14] Nejabatkhah F, Li Yun wei, Liang Hao, et al. Cyber-security of smart microgrids: A survey[J]. Energies, 2021, 14(1): 27.

[15] Ashok A, Govindarasu M, Wang Jianhui. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid[J]. Proceedings of the IEEE, 2017, 105(7): 1389–1407.

[16] Gao Weiyu, Li Hong, Zhong Minghan, et al. An underestimated cybersecurity problem: Quick-impact time synchronization attacks and a fast-triggered detection method[J]. IEEE Transactions on Smart Grid, 2023, 14(6): 4784–4798.

[17] Liu Dongchao, Chen Zhigang, Cui Longfei. Online monitoring technology of a ring network cabinet based on the Internet of Things[J]. Power System Protection and Control, 2022, 50(20): 60–67. [刘东超, 陈志刚, 崔龙飞. 基于物联网

的环网柜在线监测技术研究[J].电力系统保护与控制，2022,50(20):60–67.]

[18] Ma Jiaqi,Wang Fenghua,Sheng Gehao,et al.Fault diagnosis of GIS disconnector based on synchrosqueezing transform and deep transfer learning[J].Electric Power Automation Equipment,2024,44(2):218–224.[马佳琪,王丰华,盛戈皞,等.基于同步挤压变换和深度迁移学习的GIS隔离开关故障诊断[J].电力自动化设备,2024,44(2):218–224.]

[19] Zhang Taimin,Ji Xiaoyu,Xu Wenyuan.Jamming-resilient backup nodes selection for RPL-based routing in smart grid AMI networks[J].Mobile Networks and Applications,2022,27(1):329–342.

[20] Xue Yusheng,Ni Ming,Yu Wenjie,et al.Power grid blackout defense system including communication/information security early warning and decision support[J].Automation of Electric Power Systems,2016,40(17):3–12.[薛禹胜,倪明,余文杰,等.计及通信信息安全预警与决策支持的停电防御系统[J].电力系统自动化,2016,40(17):3–12.]

[21] Yan Longchuan,Chen Zhiyu,Yu Xuehao,et al.Security interaction framework for electricity service in new-type town based on quantum key distribution[J].Automation of Electric Power Systems,2020,44(8):28–35.[闫龙川,陈智雨,俞学豪,等.基于量子密钥分发的新型城镇电力业务安全交互架构[J].电力系统自动化,2020,44(8):28–35.]

[22] Yang Ting,Zhai Feng,Zhao Yingjie,et al.Explanation and prospect of ubiquitous electric power Internet of Things[J].Automation of Electric Power Systems,2019,43(13):9–20.[杨挺,翟峰,赵英杰,等.泛在电力物联网释义与研究展望[J].电力系统自动化,2019,43(13):9–20.]

[23] Chen Biwen,Wu Libing,Wang Huaqun,et al.A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks[J].IEEE Transactions on Vehicular Technology,2020,69(6):5813–5825.

[24] Tur M R,Ogras H.Transmission of frequency balance instructions and secure data sharing based on chaos encryption in smart grid-based energy systems applications[J].IEEE Access,2021,9:27323–27332.

[25] Cheng Bo,Zhang Xinyou,Fu Hualing,et al.Design and implementation of a security increasing strategy based on proactive deceiving strategy for the power network[J].Automation of Electric Power Systems,2004,28(21):73–76.[程渤,张新有,浮花玲,等.基于主动诱骗的电力网络安全提升策略设计与实现[J].电力系统自动化,2004,28(21):73–76.]

[26] Li Zhiyi,Yuan Cen,Yang Fu,et al.Deception-based privacy preservation method of dispatch decision-making model for distribution network in cloud computing environment[J].Automation of Electric Power Systems,2023,47(8):80–88.[李知艺,袁涔,杨福,等.云计算环境下配电网调度决策模型诱骗式隐私保护方法[J].电力系统自动化,2023,47(8):80–88.]

[27] Wang Rui,Yang Changjiang,Deng Xiangdong,et al.Development of deception defense technology and exploration of its large language model applications[J].Journal of Computer Research and Development,2024,61(5):1230–1249.[王瑞,阳长江,邓向东,等.欺骗防御技术发展及其大语言模型应用探索[J].计算机研究与发展,2024,61(5):1230–1249.]

[28] Zhang Huanqing,Liu Chunming,Zhao Yulong,et al.A novel proactive operation strategy to enhance power system resilience[J].Power System Technology,2024,48(5):2012–2021.[张焕青,刘春明,赵宇龙,等.一种提升电力系统韧性的新型主动防御策略[J].电网技术,2024,48(5):2012–2021.]

[29] Liu Yihan,Wang Yufei.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.[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.]

[30] Liu Shuo,Liu Hao,Bi Tianshu,et al.Fault detection of distribution network considering high impedance faults[J].Power System Technology,2023,47(8):3438–3447.[刘硕,刘灏,毕天姝,等.考虑高阻接地的配电网故障检测方法[J].电网技术,2023,47(8):3438–3447.]

[31] Lin Hui,Chen Chen,Wang Jianhui,et al.Self-healing attack-resilient PMU network for power system operation[J].IEEE Transactions on Smart Grid,2018,9(3):1551–1565.

[32] Han Ouzhu,Chen Zhiming,Ding Tao,et al.Power system black-start restoration model considering wind power uncertainties[J].Power System Technology,2023,47(8):3289–3304.[韩讴竹,陈志铭,丁涛,等.计及风电不确定性的电力系统黑启动恢复模型[J].电网技术,2023,47(8):3289–3304.]

[33] Ghasemi S,Moshtagh J.Distribution system restoration after extreme events considering distributed generators and static energy storage systems with mobile energy storage systems dispatch in transportation systems[J].Applied Energy,2022,310:118507.

[34] Wang Xiao.Research on malicious data attack and identification of energy Internet[D].Beijing:North China Electric Power University,2022.[王潇.能源互联网恶意数据攻击及辨识研究[D].北京:华北电力大学,2022.]

[35] Shi Leyi,Li Yang,Ma Mengfei.Latest research progress of honeypot technology[J].Journal of Electronics & Information Technology,2019,41(2):498–508.[石乐义,李阳,马猛飞.蜜罐技术研究新进展[J].电子与信息学报,2019,41(2):498–508.]

[36] Zhang Yachao,Ding Zhilong,Xie Shiwei,et al.Review and prospect of power distribution network resilience enhancement for energy Internet[J].Power System Technology,2023,47(5):2054–2069.[张亚超,丁志龙,谢仕炜,等.面向

能源互联网的配电网韧性提升研究综述及展望[J]. 电网技术,2023,47(5):2054–2069.]

[37] Yang Ting,Yan Peng,Cai Shaotang,et al.Research on saturation defense method of power cyber-physical system based on active cut set[J].Proceedings of the CSEE,2022,42(2):475–487.[杨挺,闫鹏,蔡绍堂,等 . 基于主动割集的电力信息物理系统饱和防御方法[J]. 中国电机工程学报,2022,42(2):475–487.]

[38] Cho J H,Sharma D P,Alavizadeh H,et al.Toward proactive, adaptive defense:A survey on moving target defense[J]. IEEE Communications Surveys & Tutorials,2020,22(1):709–745.

[39] Kosut O, Jia Liyan, Thomas R J, et al. Malicious data attacks on the smart grid[J]. IEEE Transactions on Smart Grid,2011,2(4):645–658.

[40] Liu Chensheng, Wu Jing, Long Chengnian, et al. Reactance perturbation for detecting and identifying FDI attacks in power system state estimation[J].IEEE Journal of Selected Topics in Signal Processing,2018,12(4):763–776.

[41] Liu Bo,Wu Hongyu. Optimal planning and operation of hidden moving target defense for maximal detection effectiveness[J].IEEE Transactions on Smart Grid,2021,12(5):4447–4459.

[42] Zhang Zhenyong, Deng Ruilong, Cheng Peng, et al.Strategic protection against FDI attacks with moving target defense in power grids[J]. IEEE Transactions on Control of Network Systems,2022,9(1):245–256.

[43] Yao Qian,Xiong Xinli,Wang Yongjie,et al.Review of moving target defense: An analysis of vulnerability and applications in new scenarios[J].Control and Decision,2023,38(11):3025–3038.[姚倩,熊鑫立,王永杰,等 . 移动目标防御综述:脆弱性分析及新场景应用[J]. 控制与决策,2023,38(11):3025–3038.]

[44] Zhang Zhenyong.Moving target defense against false data injection attack in smart grid[D].Hangzhou:Zhejiang University,2020.[张镇勇 . 智能电网中面向错误数据注入攻击的移动目标防御研究[D]. 杭州:浙江大学,2020.]

[45] He Zonglun,Gao Shibin,Wei Xiaoguang,et al.Research on offensive and defensive game model of false topology attack based on collaborative tampering with branch and protection[J].Power System Technology,2022,46(11):4346–4355.[何宗伦,高仕斌,韦晓广,等 . 支路与保护协同篡改的虚假拓扑攻击攻防博弈模型研究[J]. 电网技术,2022,46(11):4346–4355.]

[46] Xu Wangkun,Jaimoukha I M,Teng Fei.Robust moving target defence against false data injection attacks in power grids[J]. IEEE Transactions on Information Forensics and Security,2022,18:29–40.

[47] Liu Mengxiang,Zhao Chengcheng,Zhang Zhenyong,et al. Explicit analysis on effectiveness and hiddenness of moving target defense in AC power systems[J].IEEE Transactions on Power Systems,2022,37(6):4732–4746.

[48] Tian Jue,Tan Rui,Guan Xiaohong,et al. Enhanced hidden moving target defense in smart grids[J].IEEE Transactions on Smart Grid,2019,10(2):2208–2223.

[49] Zhang Meng, Fan Xuzhen, Lu Rongxing,et al.Extended moving target defense for AC state estimation in smart grids [J].IEEE Transactions on Smart Grid,2023,14(3):2313–2325.

[50] Tian Jue,Tan Rui,Guan Xiaohong,et al.Moving target defense approach to detecting stuxnet-like attacks[J].IEEE Transactions on Smart Grid,2020,11(1):291–300.

[51] Liu Chensheng,Zhou Min,Wu Jing,et al.Reactance perturbation for enhancing detection of FDI attacks in power system state estimation[C]//Proceedings of the 2017 IEEE Global Conference on Signal and Information Processing. Montreal:IEEE,2017:523–527.

[52] Morrow K L,Heine E,Rogers K M,et al.Topology perturbation for detecting malicious data injection[C]//Proceedings of the 2012 45th Hawaii International Conference on System Sciences.Maui:IEEE,2012:2104–2113.

[53] Zhang Zhenyong, Deng Ruilong, Yau D K Y, et al. Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid[J].IEEE Internet of Things Journal,2021,8(8):6608–6623.

[54] Liu Bo,Wu Hongyu.Optimal D–FACTS placement in moving target defense against false data injection attacks[J]. IEEE Transactions on Smart Grid,2020,11(5):4345–4357.

[55] Wang Qi,Wu Shutan,Wu Zhong,et al.Topology switching-based moving target defense against false data injection attacks on a power system[J].International Journal of Electrical Power & Energy Systems,2024,163:110350.

[56] Giraldo J,El Hariri M,Parvania M.Decentralized moving target defense for microgrid protection against false-data injection attacks[J].IEEE Transactions on Smart Grid,2022,13(5):3700–3710.

[57] Liu Chensheng,Tang Yang,Deng Ruilong,et al.Joint meter coding and moving target defense for detecting stealthy false data injection attacks in power system state estimation[J].IEEE Transactions on Industrial Informatics,2024,20(3):3371–3381.

[58] Higgins M,Teng Fei,Parisini T.Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems[J]. IEEE Transactions on Information Forensics and Security,2020,16:1275–1287.

[59] Xu Wangkun,Higgins M,Wang Jianhong,et al.Blending data and physics against false data injection attack:An event-triggered moving target defence approach[J]. IEEE Transactions on Smart Grid,2023,14(4):3176–3188.

[60] Zhang Zhenyong,Deng Ruilong,Yau D K Y,et al.Analysis of moving target defense against false data injection attacks on power grid[J].IEEE Transactions on Information

Forensics and Security,2019,15:2320–2335.

[61] Zhang Hang,Liu Bo,Liu Xuebo,et al.Voltage stability constrained moving target defense against net load redistribution attacks[J].IEEE Transactions on Smart Grid,2022,13(5):3748–3759.

[62] Cui Mingjian,Wang Jianhui.Deeply hidden moving-target-defense for cybersecure unbalanced distribution systems considering voltage stability[J].IEEE Transactions on Power Systems,2021,36(3):1961–1972.

[63] Lakshminarayana S,Belmega E V,Poor H V.Moving-target defense against cyber-physical attacks in power grids via game theory[J].IEEE Transactions on Smart Grid,2021,12(6):5244–5257.

[64] Zhang Zhenyong,Deng Ruilong,Yau D K Y,et al.Security enhancement of power system state estimation with an effective and low-cost moving target defense[J].IEEE Transactions on Systems,Man,and Cybernetics:Systems,2023,53(5):3066–3081.

[65] Zhang Zhenyong,Tian Youliang,Deng Ruilong,et al.A double-benefit moving target defense against cyber-physical attacks in smart grid[J].IEEE Internet of Things Journal,2022,9(18):17912–17925.

[66] Lakshminarayana S,Yau D K Y.Cost-benefit analysis of moving-target defense in power grids[J].IEEE Transactions on Power Systems,2021,36(2):1152–1163.

[67] Rahman M A,Al–Shaer E,Bobba R B.Moving target defense for hardening the security of the power system state estimation[C]//Proceedings of the First ACM Workshop on Moving Target Defense.New York:ACM,2014:59–68..

[68] Liu Bo,Wu Hongyu,Pahwa A,et al.Hidden moving target defense against false data injection in distribution network reconfiguration[C]//Proceedings of the 2018 IEEE Power & Energy Society General Meeting.Portland:IEEE,2018:1–5.

[69] Wang Shaocheng,Ren Wei,Al–Saggaf U M.Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks[J].IEEE Systems Journal,2017,11(4):2640–2651.

[70] He Quanpeng,Wang Qi,Wu Zhong.A moving target defense strategy against FDIA based on flexible switching of spare lines[C]//Proceedings of the 2022 IEEE/IAS Industrial and Commercial Power System Asia.Shanghai:IEEE,2022:1082–1087.

[71] Zhao Peng,Pu Tianjiao,Wang Xinying,et al.Key technologies and perspectives of power Internet of Things facing with digital twins of the energy Internet[J].Proceedings of the CSEE,2022,42(2):447–458.[赵鹏,蒲天骄,王新迎,等.面向能源互联网数字孪生的电力物联网关键技术及展望[J].中国电机工程学报,2022,42(2):447–458.]

[72] Li Yalou,Zhang Xing,Hu Shanhua,et al.Modeling and simulation technology for stability analysis of power system with high proportion of power electronics[J].Automation of Electric Power Systems,2022,46(10):33–42.[李亚楼,张星,胡善华,等.含高比例电力电子装备电力系统安全稳定分析建模仿真技术[J].电力系统自动化,2022,46(10):33–42.]

[73] Zang Haixiang,Geng Minghao,Huang Manyun,et al.Review and prospect of state estimation for electricity–heat–gas integrated energy system[J].Automation of Electric Power Systems,2022,46(7):187–199.[臧海祥,耿明昊,黄蔓云,等.电–热–气混联综合能源系统状态估计研究综述与展望[J].电力系统自动化,2022,46(7):187–199.]

[74] Liu Quanying,Li June,Ni Ming,et al.Situation awareness of grid cyber-physical system:Current status and research ideas[J].Automation of Electric Power Systems,2019,43(19):9–21.[刘权莹,李俊娥,倪明,等.电网信息物理系统态势感知:现状与研究构想[J].电力系统自动化,2019,43(19):9–21.]

[75] Pan Hao,Wei Zhinong,Huang Manyun,et al.Distributed robust state estimation of integrated electricity–gas system based on time-domain model[J].Automation of Electric Power Systems,2023,47(17):89–98.[潘浩,卫志农,黄蔓云,等.基于时域模型的电–气综合能源系统分布式鲁棒状态估计[J].电力系统自动化,2023,47(17):89–98.]

[76] Xu Junjun,Hu Qinran,Zhang Tengfei,et al.Coordinated state estimation for electricity and gas integrated system considering timing sequence of multi-energy flow operation[J].Electric Power Automation Equipment,2023,43(11):34–42.[徐俊俊,胡秦然,张腾飞,等.计及多能流运行时序性的电–气互联系统协同状态估计[J].电力自动化设备,2023,43(11):34–42.]

[77] Lin Zhengyang,Jiang Fei,He Guixiong,et al.Interval state estimation of electricity–gas integrated energy system based on model–data joint driven[J].Power System Technology,2023,47(7):2613–2624.[林政阳,姜飞,何桂雄,等.基于模型–数据联合驱动的电–气综合能源系统区间状态估计[J].电网技术,2023,47(7):2613–2624.]

[78] Lin Zhengyang,Jiang Fei,Tu Chunming,et al.Data-driven electricity–gas integrated energy system situation awareness considering time series correlation[J].Power System Technology,2022,46(9):3385–3394.[林政阳,姜飞,涂春鸣,等.考虑时序相关性的数据驱动电–气综合能源系统态势感知[J].电网技术,2022,46(9):3385–3394.]

[79] Lan Puzhe,Han Dong,Xu Xiaoyuan,et al.Bayesian state estimation for electricity–gas coupled integrated energy system based on long short-term memory[J].Automation of Electric Power Systems,2021,45(20):18–28.[兰浦哲,韩冬,徐潇源,等.基于长短期记忆的电–气耦合综合能源系统贝叶斯状态估计[J].电力系统自动化,2021,45(20):18–28.]

[80] Liu Junwei,Liu Chunyang,Zhao Haoran,et al.State estimation of integrated electric–heat system based on knowledge-guided deep neural network[J].Power System Technology,2022,46(11):4288–4300.[刘俊伟,刘春阳,赵浩然,等.基于

知识引导深度神经网络的电–热综合能源系统状态估计[J]. 电网技术,2022,46(11):4288–4300.]

[81] Chen Yanbo, Yao Yuan, Gao Yulong, et al. Two-level robust state estimation method for the integrated electricity–heat system[J]. High Voltage Engineering, 2022, 48(4): 1226–1236.[陈艳波,姚远,高瑜珑,等. 面向电–热综合能源系统的双层抗差状态估计方法[J]. 高电压技术,2022,48(4):1226–1236.]

[82] Liu Xinrui, Li Yao, Sun Qiuye, et al. Interaction and joint state estimation of electric–gas–thermal coupling network [J]. Power System Technology, 2021, 45(2): 479–490.[刘鑫蕊,李垚,孙秋野,等. 基于多时间尺度的电–气–热耦合网络动态状态估计[J]. 电网技术,2021,45(2):479–490.]

[83] Chen Yanbo, Gao Yulong, Zhao Junbo, et al. Review on integrated energy system state estimation[J]. High Voltage Engineering, 2021, 47(7): 2281–2292.[陈艳波,高瑜珑,赵俊博,等. 综合能源系统状态估计研究综述[J]. 高电压技术,2021,47(7):2281–2292.]

[84] Guo Jianbo, Fan Shixiong, Cai Zhongmin, et al. Human-machine hybrid-augmented intelligence for power system dispatching: Concept connotation, application framework, key technologies and system verification[J]. Proceedings of the CSEE, 2024, 44(17): 6787–6811.[郭剑波,范士雄,蔡忠闽,等. 大电网调控人机混合增强智能:概念内涵、应用框架、关键技术以及系统验证[J]. 中国电机工程学报,2024,44(17):6787–6811.]

[85] You Jing, Shangguan Jinglun, Xu Shoukun, et al. Distributed dynamic trust management model based on trust reliability [J]. Journal of Software, 2017, 28(9): 2354–2369.[游静,上官经伦,徐守坤,等. 考虑信任可靠度的分布式动态信任管理模型[J]. 软件学报,2017,28(9):2354–2369.]

[86] Liu Wenfen, Dai Zhiyong, Gao Yan. Distributed dynamic trust management model based on trusted domains[J]. Journal of Sichuan University(Engineering Science Edition), 2014, 46(4): 61–66.[刘文芬,代致永,郜燕. 基于信任域的分布式动态信任管理模型[J]. 四川大学学报(工程科学版),2014,46(4):61–66.]

[87] Zhang Bo, Liu Xuan, Yu Zongchao, et al. Review on artificial intelligence-based network attack detection in power systems[J]. High Voltage Engineering, 2022, 48(11): 4413–4426. [张博,刘绚,于宗超,等. 基于人工智能的电力系统网络攻击检测研究综述[J]. 高电压技术,2022,48(11):4413–4426.]

[88] Chen Binbin, Sun Hongbin, Chen Yuwei, et al. Energy circuit theory of integrated energy system analysis (I): Gaseous circuit[J]. Proceedings of the CSEE, 2020, 40(2): 436–444.[陈彬彬,孙宏斌,陈瑜玮,等. 综合能源系统分析的统一能路理论(一):气路[J]. 中国电机工程学报,2020,40(2):436–444.]

[89] Wei Zhenbo, Li Jie, Yang Chao, et al. Low-carbon economic scheduling for integrated energy system based on dynamic hydrogen doping strategy[J]. Power System Technology, 2024, 48(8): 3155–3164.[魏震波,李杰,杨超,等. 基于动态掺氢策略的综合能源系统低碳经济调度[J]. 电网技术,2024,48(8):3155–3164.]

[90] Chen Sheng, Zhang Jingchun, Wei Zhinong, et al. Energy transition oriented planning and operation of electricity–gas–hydrogen integrated energy system[J]. Automation of Electric Power Systems, 2023, 47(19): 16–30.[陈胜,张景淳,卫志农,等. 面向能源转型的电–气–氢综合能源系统规划与运行[J]. 电力系统自动化,2023,47(19):16–30.]

[91] Song Meng, Zhou Jiani, Gao Ciwei, et al. High-resilience coordinated operation of urban buildings and distribution networks from cyber-physical-social system perspective: Research review and prospect[J]. Automation of Electric Power Systems, 2023, 47(23): 105–121.[宋梦,周佳妮,高赐威,等. CPSS 视角下城市建筑与配电网高韧性协调运行:研究述评与展望[J]. 电力系统自动化,2023,47(23):105–121.]

[92] Chen Chunyu, Tu Ge, Zang Tianlei, et al. Privacy-preserving multi-agent coordinated economic dispatch with generation-grid-load-storage interaction[J]. Advanced Engineering Sciences, 2024, 56(2): 45–54.[陈春宇,涂歌,臧天磊,等. 面向多主体隐私保护的源网荷储分布式协同优化调度[J]. 工程科学与技术,2024,56(2):45–54.]

Research Status and Prospects of New Power Systems Moving Target Defense Against False Data Injection Attacks

ZANG Tianlei[1,2], *GONG Yahui*[1,2], *LI Chuangzhi*[1,2], *WANG Shijun*[1,2], *LIU Yunfei*[1,2], *ZHOU Buxiang*[1,2]

(1.College of Electrical Engineering, Sichuan University, Chengdu 610065, China;
2.Key Laboratory of Intelligent Electric Power Grid in Sichuan Province (Sichuan University), Chengdu 610065, China)

Abstract:

Significance With the integration of energy systems and information networks, power systems now rely on large-scale data acquisition, state monitoring, and dynamic scheduling. Although these advancements improve real-time sensing and control, they also introduce new security risks. The impact of information-level attacks gradually extends to the physical system, posing a significant threat to the security of the power system. The false data injection attack (FDIA) is a common and destructive network attack. FDIA interferes with state estimation, causing system operation to deviate from the normal operational range by tampering with or injecting forged data. Therefore, serious power supply failures can occur. At present, defending against FDIA has become a key area of power system security research. Moving target defense (MTD) is an emerging ac-

tive defense method that provides significant advantages in countering FDIA. MTD dynamically changes the state of the system, disrupting the attacker's control over system information. This approach makes it difficult for attackers to obtain the real state information of the system. MTD effectively increases the difficulty and cost of attacks by continuously perturbing key parameters of the power system. With the continuous evolution of network threats, the importance of MTD strategies in new power systems is steadily increasing. Their application not only enhances the overall security of the system but also provides an active defense against complex and dynamic cyber threats.

Progress MTD technology originated in the field of network security defense, and its concepts were later introduced into power systems by scholars. The initial MTD strategy for power systems adopted a random perturbation approach, which was insufficient for stable and effective defense. As research advanced, scholars successively optimized the performance of MTD with the primary objective of maximizing the rank of the measurement matrix. This optimization aimed to reduce defense blind spots and improve overall system security. One approach, known as hidden MTD, minimized the impact of MTD on power flow while ensuring the normal operation of the system to maintain stability. The hidden MTD strategy emphasized the stealth of defense actions, making it more difficult for attackers to detect defensive behaviors. In addition, the AC current model-based MTD adapted defenses to the actual characteristics of the power system through a more realistic modeling approach. Perturbation sensor gain-based MTD further reduced the impact on the power system by adjusting sensor gains to induce state perturbations.

Conclusions and Prospects MTD, as an active defense method, demonstrates significant potential for application in new power systems. With the growing complexity and intelligence of power systems, the design of MTD strategies presents both challenges and opportunities. On one hand, the diversified characteristics of new power systems expand the implementation scenarios and methods of MTD strategies; on the other hand, the complex multi-energy interconnection structure imposes higher requirements on their implementation effectiveness. The systematic framework for the application and development of MTD in new power systems is presented in this study with the objective of continuously strengthening the defense capability of power systems. This goal will be achieved within future complex energy environments, ultimately ensuring the safe and stable operation of power systems. Current research primarily focuses on traditional transmission networks, which are difficult to adapt to the requirements of new power systems. This study analyzes the application potential of MTD in new power systems and proposes the corresponding key technologies. In addition, based on the characteristics of new power systems in power generation, transmission, distribution, and consumption, this study discusses the specific implementation strategy of MTD in detail. Future MTD technology should not be limited to an independent application but should operate in interaction within a multi-layer defense system, acting as a link across the detection, identification, and response stages. Through the coordinated application of multi-layer defense measures, the resilience of power systems against attacks such as FDIA can be significantly enhanced.

Key words: new power systems; false data injection attack; moving target defense; cyber-physical systems; multi-energy interconnection

（编辑　赵　婧）

引用格式: Zang Tianlei,Gong Yahui,Li Chuangzhi,et al.Research status and prospects of new power systems moving target defense against false data injection attacks[J].Advanced Engineering Sciences,2025,57(5):114–133.[臧天磊,龚亚辉,李创芝,等.应对虚假数据注入攻击的新型电力系统移动目标防御研究现状与展望[J].工程科学与技术,2025,57(5):114–133.]