第46卷 第9期 2022年5月10日
DOI：10.7500/AEPS20210613001
电力系统自动化
Automation of Electric Power Systems
Vol. 46 No. 9 May 10，2022

机器学习在电力信息物理系统网络安全中的应用

彭 莎[1]，孙铭阳[1]，张镇勇[1,2]，邓瑞龙[1]，程 鹏[1]
（1. 浙江大学控制科学与工程学院，浙江省杭州市 310027；2. 贵州大学计算机科学与技术学院，贵州省贵阳市 550025）

摘要：随着信息化程度的不断深入，传统电力系统逐渐发展成为典型的信息物理系统(CPS)。开放的信息系统环境使得电力系统的安全运行面临着各种潜在网络攻击的威胁。近年来，机器学习方法迅猛发展，并已广泛应用于电力CPS网络安全领域。一方面，电力CPS中数据的爆炸式增长以及硬件运算能力的提升为机器学习的应用创造了良好条件；另一方面，相比于传统的基于机理的建模分析方法，基于数据的机器学习方法具有模型构建以及实时性需求2个方面的优势。文中从攻防2个角度对机器学习在电力CPS网络安全领域的应用进行了归纳总结。其中，攻击者角度主要包括拓扑信息推断、攻击资源优化以及攻击构建3个方面；防守者角度主要包括安全保护、攻击检测以及攻击缓解3个方面。最后，分析展望了电力CPS网络安全领域存在的挑战以及未来的研究方向。

关键词：电力系统；信息物理系统；网络安全；机器学习

0 引言

随着控制、通信和计算机等信息技术的发展，传统电力系统广泛引入了传感、网络和计算等技术，逐步发展成为信息系统与物理系统深度融合并广泛交互的信息物理系统(cyber-physical system，CPS)[1]。电力CPS是关系国民经济和国家安全的重大关键基础设施。随着信息化程度的不断深入，电力CPS的安全运行面临着各种潜在网络攻击的威胁[2]。为保障电力系统的安全稳定运行，面向电力CPS网络安全的研究受到了学术界和工业界的广泛关注。

近年来，机器学习技术在计算速度以及学习能力方面发展迅速，在计算机视觉、医学诊断以及异常检测等领域的应用表现可圈可点[3-5]。各领域都在进行技术革新，向智能化时代迈进。在电力CPS领域，各项信息技术的深度融合使得电力系统数据量显著增长，为数据驱动的机器学习方法应用提供了便利。将机器学习方法应用于电力CPS网络安全领域，能够有效提高数据解析度，克服电力系统的日益庞大以及网络攻击的复杂多变引入的无法准确构建模型的难题。同时，一些机器学习方法还能满足电力系统的实时性需求[6]。

目前，已有大量文献对机器学习在电力CPS网络安全领域的应用进行了探索[2,6-10]，但现有的电力CPS领域的综述文章并未对这一研究课题进行归纳总结。一部分文章关注于机器学习相关技术在整个电力系统中的应用，对网络安全部分的探讨不够具体和深入[6-8]；另一部分文章对电力CPS网络安全中的关键技术进行了调研，但缺少具体阐明机器学习技术在网络安全各环节的应用情况[2,9-10]。鉴于此，本文对机器学习在电力CPS网络安全中的应用进行了全面分类与总结。

本文首先对电力CPS网络安全进行了概述，介绍了电力CPS网络安全要求以及面临的挑战，接着简要介绍了各类机器学习方法，并总结了机器学习方法应用于电力CPS网络安全领域的契机与优势。然后，从攻防2个角度分别出发，具体阐述了电力CPS网络安全研究中面临的问题，全面调研了机器学习应用于电力CPS网络安全的现有文献。其中，攻击角度的应用包括拓扑信息推断、攻击资源优化以及攻击构建，防御角度的应用包括攻击前的保护、攻击时的检测以及缓解。最后，对该研究领域存在的挑战以及未来的研究方向进行了分析与展望。

1 电力CPS网络安全

电力CPS的物理系统与信息系统深度融合并广泛交互，系统中各设备的相互作用由系统的动态特性以及协调系统运行的规则决定。电力CPS的

收稿日期：2021-06-13；修回日期：2021-11-18。
上网日期：2022-02-16。
国家自然科学基金资助项目(62073285)；浙江省自然科学基金重点项目(LZ21F020006)。

具体结构如图1所示。物理系统由与物理世界直接连接的一次设备组成，主要涉及发电、输电、配电系统中的设备，包括光伏板、发电机、变压器以及输/配电路等。这些设备通过量测设备、执行器以及信息系统进行交互，控制电能的生产、传输和分配。信息系统由二次设备（信息通信单元）组成，包括路由器、交换机和集线器等通信网络组件、控制系统主机等计算组件及数据库等设备。这些设备使用公共通信协议在数字链路上互联、共享、存储并处理来自物理系统的数据，执行广域监测、控制和保护[1]。具体来说，物理系统的运行情况由量测设备进行采集，采集得到的实时量测数据通过通信网络传输给控制中心，控制中心基于所接收的数据进行计算，更新控制策略，控制器根据控制策略输出适当的控制指令并传输给执行器，执行器通过被控介质控制物理系统的运行。与直接对物理设备产生影响的物理安全问题不同，电力CPS的网络安全问题是指利用电力信息系统的安全漏洞，破坏数据的机密性、完整性和可用性，导致错误的规划判断、财产损失和用户隐私泄露等，间接影响物理系统的安全问题[2]。随着物理系统与信息系统的耦合逐渐深入，信息物理耦合交互过程更为复杂，电力CPS的运行过程对信息系统更具依赖性。然而，信息系统的通信环境较为开放，为电力CPS增加了更多的攻击面，使得电力CPS面临着越来越多网络攻击的威胁。因此，增强电力CPS网络安全至关重要。

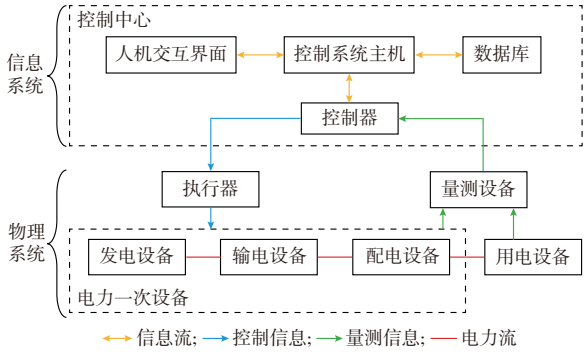

图1　电力CPS结构

Fig. 1　Framework of cyber-physical power system

电力CPS网络安全旨在确保电力系统的健壮性、安全性以及抵御攻击的弹性，为此电力CPS需要满足以下3点要求[11]。

要求1：攻击检测以及自愈。在信息系统运行代码维度方面，攻击检测是保障电力CPS安全稳定运行的关键环节。电力CPS需要及时掌握系统运行状态、预测运行趋势、快速检测与识别攻击导致的异常事件。此外，从物理系统设备维度出发，需要保障电力基础设施的可用性，因此，电力CPS需要弹性运行，具有自愈能力，检测出攻击后能够自动干预，快速隔离攻击并及时自我修复[12]。

要求2：身份认证以及访问控制。在信息系统协议维度方面，电力CPS需要提供可靠的身份认证以及访问控制等机制来防止未经授权的访问，以保证信息系统中的电子信息设备以及相关数据的安全。

要求3：安全的通信协议以及架构。为确保信息系统网络维度的安全，电力CPS需要将防御策略集成到网络协议和体系结构中，使得电力CPS能够实现安全高效的通信。

当前，针对电力CPS网络安全的研究也围绕上述3点要求展开。由于要求2和3与电力系统物理特性关联较弱，可以直接迁移或扩展其他领域的相关方法或架构，例如针对要求2的现有研究通常将信息安全和计算机安全领域的相关工作迁移到电力CPS领域[13-14]；针对要求3的网络架构开发设计大多也由现有的架构改进而来[15-16]。因此，电力CPS网络安全相关研究大部分关注要求1。针对要求2和3的研究大都致力于设计合适的加密机制和通信架构，较少应用机器学习方法，所以本文主要关注要求1。针对要求1，传统的机理建模方法利用电力系统的物理特性以实现攻击检测和自愈[17-19]。然而，随着电力CPS规模的日益庞大以及网络攻击种类的增加，机理建模方法面临建模困难和计算复杂度高等挑战。因此，学术界开始广泛探索应用机器学习方法以满足该安全要求。

2　机器学习方法概述

机器学习是利用经验来提升性能或做出准确预测的计算方法[20]。其中，“经验”通常以“数据”形式存在，每条数据由关于一个对象的多个特征组成，特征反映了该对象在某方面的表现或性质。在机器学习中，数据的集合称为数据集。一个完整的数据集通常被划分为训练集与测试集，机器学习基于训练集训练模型，通过测试集评价模型效果。基于模型对新的数据进行判断的过程称为预测，预测任务分为分类、回归以及决策等。根据所需数据集类型的不同，可以将机器学习分为无监督学习、监督学习、半监督学习和强化学习。

2.1　无监督学习

无监督学习所需数据集为未标记数据集，其基于未标记数据训练模型，试图挖掘出这些数据中隐含的共同特征[21]。根据训练方式的不同，无监督学习可分为不同的子类，常见子类包括降维与度量学

习(例如主成分分析[22]、独立成分分析[23])、聚类(例如K均值聚类[24]、局部异常因子法[25])和神经网络(例如自组织映射网络[26]、自编码器[27])等。

2.2 监督学习

监督学习所需数据集为标记数据集,其基于标记数据训练模型,学习数据与对应的标记之间存在的特定关系[21]。监督学习根据训练方式的不同可分为不同的子类,常见子类包括神经网络(例如前馈神经网络[28]、长短期记忆(long short-term memory, LSTM)人工神经网络[29])、回归(例如线性回归[30]、逻辑回归[31])、决策树[32]和贝叶斯方法[33]等。

2.3 半监督学习

在半监督学习所需数据集中,少量数据为标记数据,其余均为无标记数据,2类数据一起训练得到模型[34]。半监督学习假设未标记数据与标记数据从同样的数据源独立同分布采样而来,该假设说明未标记数据揭示的数据分布信息与标记数据是相关联的,所以可以在仅使用标记数据的监督学习中加入无标记数据提升模型性能,由此产生了半监督学习。典型的半监督学习算法包括半监督核均值漂移聚类[35]和半监督支持向量机[36]等。

2.4 强化学习

强化学习所需数据通过与环境交互产生,智能体在环境中不断尝试和试验来获取数据并优化动作策略[37]。动作策略是状态到动作的映射,最优策略描述了在给定状态下采取何种动作将获得最大的长期累积回报。强化学习用于解决序列决策问题。传统的强化学习方法,例如Q学习[38]用表格的形式表示值函数,只适用于状态和动作空间较小的情况。为克服这一局限性,将深度神经网络强大的表达能力与强化学习的决策能力相结合的深度强化学习算法被广泛研究应用,例如异步优势行动者-评论家(asynchronous advantage actor-critic, A3C)算法[39]。

3 机器学习在电力CPS中应用的优势

随着大数据时代的来临,机器学习已被广泛应用于各个领域[3-5]。在电力CPS领域,一方面,控制、通信和计算机等信息技术的深度融合使得与电力系统运行相关的数据量呈指数趋势增长[6,40],为机器学习的应用提供了数据基础;另一方面,高性能计算正以远超摩尔定律的速度快速发展[41],其高速处理数据和执行复杂计算的能力为机器学习的应用提供了硬件基础。这2个方面为机器学习在电力CPS中的应用创造了良好条件。

此外,相较于传统的机理建模方法,机器学习方法具有模型构建以及实时性需求2个方面的优势。首先,随着电力CPS的规模日益扩大、信息物理耦合的不断深入以及大规模可再生能源的接入,电力系统的模型构建日渐复杂,且网络攻击的复杂多变也为机理模型的建立引入了新的难题,使得无法准确构建模型已成为机理建模方法在电力CPS网络安全领域的应用瓶颈。机器学习方法将复杂的机理模型看作一个黑箱,通过拟合黑箱输入与输出间的映射关系实现数据驱动的求解方案,不仅摆脱了烦琐的建模环节以及模型建立不准确对电力CPS网络安全研究带来的影响[6],还能够捕捉电力系统数据的时空相关性,实现基于数据维度的多方位网络攻击检测。其次,电力CPS网络安全至关重要,需要及时对各类网络攻击进行检测、识别、缓解以及隔离等,以免造成整个系统的崩溃。因此,电力CPS网络安全领域的应用通常对实时性有着较高的要求。然而,实际的电力系统模型复杂庞大,网络攻击种类繁多,传统的机理建模分析方法计算过程时间复杂度较高[42]。虽然由于应用场景和所选择算法的不同,并非所有机器学习方法都具有实时性优势,但在电力CPS网络安全领域,机器学习方法的应用往往考虑了实时性需求。机器学习方法对物理模型依赖程度较低,通过数据拟合简化电力CPS问题[43-44],一定程度上降低了计算复杂度,且部分机器学习方法的模型训练过程可以离线进行,减轻了实时计算负担[20]。因此,在电力CPS网络安全领域,机器学习方法在满足实时性需求方面更有优势,优势的大小与具体场景和算法选择有关。

综上所述,电力CPS的网络安全问题研究存在诸多理论制约和技术瓶颈,需要探索应用新的方法帮助其摆脱困境。在外在的条件支持以及内在的问题需求的双向驱动下,利用数据进行快速预测的机器学习技术凭借其多方面的优势,在电力CPS网络安全领域逐渐崭露头角,已应用于自动电压控制[45]、频率控制[46]、数据采集与监控(supervisory control and data acquisition, SCADA)系统[47-48]、广域测量系统(wide area measurement system, WAMS)[49-50]、状态估计[51-53]、高级量测体系(advanced metering infrastructure, AMI)[54-55]以及电力市场[56-58]等方面。

4 机器学习在电力CPS潜在攻击威胁分析中的应用

为确保电力CPS网络安全,提升攻击检测以及自愈能力,现有研究从攻、防2个角度展开。攻击角度研究的主要目的是分析电力CPS面临的潜在攻击威胁,为防御设计提供指导。潜在攻击威胁分析

主要包括拓扑信息推断、最小化攻击资源、攻击资源优化以及攻击构建等方面。目前，机器学习主要应用于拓扑信息推断、攻击资源优化以及攻击构建3个方面。

4.1　拓扑信息推断

针对电力CPS的网络攻击手段繁多，例如拒绝服务攻击、中间人攻击、重放攻击、旁路控制等[2]。实施这些攻击不需要任何与电力系统相关的拓扑以及线路参数等物理信息，难以对电力物理系统造成影响，攻击效果有限。如果攻击者掌握相关物理信息，便可根据这些信息设计出对电力系统更具破坏力的攻击，例如虚假数据注入攻击（false data injection attack，FDIA）[59]。当前，针对电力CPS的潜在攻击威胁分析大都集中于此类需要相关物理信息的攻击中。然而，这些信息通常被严格管理，攻击者难以直接获取。在电力CPS中，信息系统环境较为开放，传输或存储于信息系统中的电力系统日常运行数据较为容易获取。因此，当前研究都以此为突破口，从较易获取的量测数据中推导攻击所需的电力系统拓扑信息[60]。为易于推导，该问题通常被表述为信号处理领域的盲源分离问题[61]。

机器学习方法能够有效揭示数据间潜在的机理联系，而不利用任何机理信息，为盲源分离问题提供可行解。无监督学习中的降维与度量学习方法——独立成分分析以及主成分分析，常用于解决盲源分离问题。部分仅需无标记数据的神经网络方法也已被应用于电力系统物理信息挖掘。另外，无监督聚类方法可以识别出与当前拓扑更相关的量测数据，帮助攻击者更为准确地进行拓扑信息推断。

一些研究利用主成分分析或独立成分分析推导攻击所需的电力系统信息。文献[62-64]使用主成分分析将量测数据投影到前n个主成分上，其中n为状态变量的个数，投影所得矩阵即为电力系统拓扑矩阵。若攻击者能推导证明量测数据是若干个相互独立的分量的线性组合，则使用独立成分分析解混量测数据将更具合理性与准确性，因为独立成分分析假设源数据彼此独立且不为高斯分布，目标为最大化独立性，而主成分分析对数据分布不做任何假设。线性独立成分分析已被应用于推导攻击所需关键信息[56]。然而，上述研究存在诸多局限之处，首先，上述研究都是基于直流（direct current，DC）潮流模型，在交流（alternating current，AC）潮流模型下算法准确性将大大降低；其次，基于矩阵分解的无监督学习方法计算复杂度较高，不适用于大规模系统。为此，可以考虑将神经网络应用于电力系统物理信息推导，其强大的非线性特征提取能力可以较为准确地提取出基于AC潮流模型的系统物理信息，并且大多神经网络算法可采用离线训练，在线使用的方式，极大减轻了实时计算负担，可适用于大规模系统。文献[65]利用此思路，引入自注意生成式对抗网络，基于攻击区域的历史量测数据以及攻击区域与非攻击区域之间的结线信息获取电力系统相关物理信息。

然而，由于用于推断的历史量测数据往往与某个特定的拓扑相关联，因此上述方案仅在电力系统拓扑和相关参数固定时有效，难以应对通过主动改变电力系统参数值来防御FDIA的移动目标防御策略[66]。为对抗该防御策略，可以从历史数据中挑选出与当前拓扑更相关的量测数据用于推断。文献[67]使用具有噪声的基于密度的空间聚类（density-based spatial clustering of applications with noise，DBSCAN）方法识别出与当前拓扑更相关的量测数据，再通过独立成分分析推导系统拓扑信息。然而，聚类和独立成分分析过程所需计算时间较长，特别是聚类过程需要识别分类大规模系统的大范围量测数据。因此，该研究方案在实时操作中存在瓶颈。

综上所述，目前关于电力系统拓扑信息推断的研究较少，且在大规模复杂系统上的性能表现以及实时操作存在局限性。为此，电力CPS研究者可以从算法选择上探索该问题的解决方案。近年来，关于非线性盲源分离问题的研究发展迅速，基于贝叶斯集合学习、基于自组织映射以及基于核的非线性盲源分离算法等都实现了较好的应用效果[68-70]。电力CPS研究者可以根据电力系统量测数据的特点，选择合适的非线性盲源分离问题算法，探索更为高效准确的实时拓扑信息推断策略。

电力系统拓扑信息推导研究表明，海量的电力CPS量测数据蕴含了许多关键信息，攻击者可利用这些信息构造出极具破坏力的攻击。因此，量测数据的机密性对保障电力CPS安全不可忽视。

4.2　攻击资源优化

攻击者掌握的攻击资源往往有限，如何优化攻击资源的使用仍需要探讨。由于电力CPS中各个设备的功能、拓扑位置以及与其他设备的安全互相关性不同，因此攻击不同设备对电力CPS造成的影响有强弱之分[19]。为最大化攻击造成的影响，攻击者需要在攻击实施前合理分配攻击资源，确定攻击目标。电力CPS的结构与运行方式较为复杂，如果仅利用传统的机理建模方法，通过时域仿真手段计算每种攻击目标组合策略对电力系统造成的影响，计算量将十分庞大。另外，当攻击目标的数量大于一时，攻击者需要发起多次攻击。一般来说，多次攻

击可分为连续攻击和并发攻击[71]。连续攻击所需的并发资源相对较少,但其对电力系统造成的影响可能与并发攻击相当甚至更严重。然而,由于连续攻击的攻击序列组合数较多,因此计算量将更为庞大。通常,可以将连续攻击的攻击序列确定问题看作一个序列决策问题进行求解。

相比传统的机理建模方法,机器学习在模型构建以及实时性需求方面更具优势,可以利用电力系统海量的数据进行训练,快速获取最优攻击策略,最大限度利用攻击资源。不同机器方法依照其不同的特性,被应用于攻击资源优化的不同方面,其中,无监督学习主要用于攻击目标的选择,其应用优势在于能够挖掘电力CPS设备间的潜在联系,对设备进行预分类,加速目标选择过程;强化学习主要用于攻击序列的设计,其应用优势在于免去了烦琐的电力CPS建模过程,并能实现在线序列决策,满足实时性需求。

无监督学习中的聚类学习可以将数据分组为多个由具有相似特征的对象组成的子集。利用聚类方法,可将电力系统各元件按照其某些特征划分为若干不相交的子集,用于攻击目标的选择。如文献[72]依照总线坐标,采用K均值聚类将电力系统各总线划分为不同总线组,再选取每个总线组中功率最大的总线作为攻击目标,其攻击方式假设为攻击者可以通过网络入侵(例如钓鱼攻击、分布式拒绝服务攻击以及蛮力攻击等)致使线路切换。然而,聚类方法无法对连续攻击问题的攻击序列给出建议。

强化学习擅长解决顺序决策问题,已应用于设计电力CPS连续攻击策略。文献[71]考虑电路切换攻击,提出了一个电力系统攻防双方零和博弈模型,并利用Q学习求解最优攻击序列。目前,利用强化学习设计连续攻击策略的研究仅在小规模系统上进行了实验验证,大规模系统的状态-动作空间较大,有效性难以考证。此外,在电力CPS中,攻防双方会根据当前的系统状态及时调整攻防策略,即双方的策略在博弈过程中是动态的且具有耦合性,而当前研究往往假设防守方的防守策略在每次博弈开始前已确定且整个博弈过程中不再改变,简化了实际场景。

基于上述已有研究可知,当前研究还存在对攻击效果影响因素考虑不全,将攻防场景过于简化等问题,导致当前各研究方案的通用性及说服力较弱。为此,电力CPS研究者需要在设计攻击资源优化方案时将更多因素纳入考虑,例如文献[72]仅依据坐标对总线进行聚类,而忽略了各总线的流量限制等其他物理特性。此外,当前研究往往假设攻击方式为线路切换攻击,因为不同的线路所连接的节点重要性不同,所以攻击不同的线路造成的级联影响通常具有强弱之分,使得选择攻击线路以及确定攻击顺序尤为重要。而针对其他一些攻击方式(例如通过网络攻击造成发电器或者变压器异常)的攻击资源优化问题,目前尚缺乏基于机器学习的研究对此进行探索。

针对攻击资源优化的研究对揭示电力CPS的脆弱性,找出电力CPS较薄弱的部分具有重要意义。电力系统操作人员可据此提前发现问题,采取适当的方案对脆弱部分加以保护。

4.3 攻击构建

当前,基于机理建模方法构建攻击的方案通常是离线的,需要攻击者较为准确地提前评估攻击的表现以及隐蔽性[59,73]。在线攻击方法通过与环境实时交互,获取环境的即时反馈,免去了对攻击效果的预判。恰当的在线攻击方法能够实时调整攻击策略,使得攻击在实现攻击效果的同时,又能满足隐蔽性要求。

相较机理建模方法,一方面,机器学习方法不需要对电力系统机理建模,不要求攻击者掌握任何电力系统拓扑参数信息;另一方面,大部分机器学习方法能够实现快速在线预测。这两方面的优势为机器学习方法应用于电力CPS在线攻击方案的设计提供了可能。强化学习方法通过与环境交互来学习和优化动作策略,已应用于电力CPS在线攻击的构建。

电力系统的状态转换过程可以看作一个马尔可夫链,为强化学习的应用提供了基础。文献[45]将FDIA的构建问题转化为一个部分可观察的马尔可夫决策过程,并通过Q学习求解。该研究将动作设定为对原始量测值调整的百分比,奖励由目标总线前后电压变化差值确定。然而,目前基于强化学习的序列攻击构建方案停留于静态攻击策略求解层面,没有考虑攻防双方的动态博弈过程。

相比于离线攻击构建方案[59,73],在线攻击构建方案的关键优势在于对动态环境的及时响应。为此,电力CPS研究者需要探索如何准确刻画电力系统环境的动态特性以及环境中各动态变量的耦合性,以提高在线攻击构建方案的性能表现。

探索攻击构建方案的本质是加强并完善攻击检测方法等电力CPS防御措施。电力系统操作人员可根据构建攻击的原理反向推导,设计合适的防御方法。

目前,机器学习在电力CPS潜在攻击威胁分析中的应用分类如图2所示。

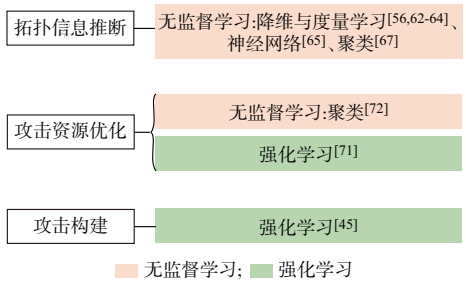

图2　机器学习在潜在攻击分析中的应用分类
Fig. 2　Classification of applications of machine learning in potential attack analysis

5　机器学习在电力CPS安全防御中的应用

防御角度可分为4个部分：攻击前的保护、攻击时的检测、攻击时的缓解和攻击后的恢复。目前，各研究工作主要集中于前3个部分，即安全保护、攻击检测和攻击缓解。

5.1　安全保护

电力CPS网络安全保护研究是指在电力CPS安全规划阶段，分析系统最重要以及面对网络攻击最脆弱的部分，以便对这些部分加强保护力度，防止网络入侵。当前，该部分研究主要集中于脆弱性分析问题。

脆弱性分析是指找出电力系统中最脆弱的节点。这些节点遭受网络攻击后将对电力CPS产生较大的影响，因此需要防御者在攻击发生前对这些节点进行保护，防患于未然。脆弱性分析研究等价于4.2节中介绍的攻击资源优化研究，只是分别以防御者和攻击者的角度对问题进行剖析，因此这两类问题使用的机理建模方法以及这些方法面临的瓶颈也基本相同，即难以建立精确的系统模型以及计算复杂度过高。

为解决上述瓶颈问题，机器学习方法凭借其在模型构建以及实时性需求方面的优势，已应用于电力CPS脆弱性分析领域。与机器学习方法在攻击资源优化问题上的应用类似，无监督学习中的聚类方法能够挖掘出数据间的内在关联，主要应用于识别电力CPS最脆弱的节点；强化学习作为一种序列决策工具，主要应用于连续攻击防御领域。

针对最脆弱节点的识别，文献[74]提出了一个基于自组织映射神经网络的聚类方案。文献[55]应用K均值聚类确定在不同程度的FDIA下各节点的脆弱程度。相比K均值聚类方案，基于自组织映射神经网络的聚类方案对非线性关系的拟合能力更强，更适合拥有复杂节点关系的电力CPS。

针对连续攻击的防御研究，文献[75]应用强化学习识别导致大停电的关键节点序列。目前，该类研究的局限之处在于没有考虑攻防双方的动态博弈过程。

综上所述，电力CPS脆弱性分析研究与攻击资源优化研究面临的不足之处类似，即对防御效果影响因素考虑不全、将攻防场景过于简化等问题。为此，电力CPS研究者在设计防御方案时需要考虑更多可变因素，例如节点间的相关性、攻击者的攻击行为变化等，使防御策略更具实用性。

5.2　攻击检测

攻击检测是保障电力CPS安全稳定运行的重要一环，及时准确的检测方案能将攻击带来的影响最小化。面对复杂化的电力物理系统以及多元化的电力信息系统，基于机理建模的检测方法存在诸多理论制约和技术瓶颈。第一，电力CPS网络庞大且结构复杂，针对电力CPS的网络攻击种类繁多，机理建模方法难以准确构建系统故障与攻击特征之间的关联关系；第二，当电力系统安全稳定运行时，相邻时刻的运行数据一般变化较小，因此运行数据在时间尺度上发生突变意味着该时刻发生攻击的可能性较高，而多数机理建模方法无法在时间尺度上构建量测数据的相关性，一定程度上影响了检测准确率；第三，攻击检测算法的实时性至关重要，然而机理建模方法的检测过程较为耗时，难以满足实时安全的要求。

机器学习方法克服了上述难题，其免去了烦琐的建模步骤，利用海量数据揭示电力CPS各尺度上的关联关系，在线进行攻击检测[76]。

目前，应用机器学习检测电力CPS网络攻击的文献主要关注一些常见的以及对电力系统影响较大的网络攻击，其具体可分为四大类：异常检测、FDIA检测、断路攻击检测和窃电检测。此外，还有一些研究关注电力CPS中其他网络攻击的检测问题。

5.2.1　异常检测

异常检测用于检测量测数据中的离群点，并不针对某一类特定的网络攻击。无监督学习和监督学习作为各领域常用的异常检测方法，已被广泛应用于电力CPS网络安全领域。此外，强化学习方法也已被应用于该领域。

文献[77]和文献[78]分别采用局部异常因子法以及独立森林算法检测同步相量测量单元(phasor measurement unit，PMU)数据是否遭受攻击。文献[79]应用主成分分析方法得到PMU数据的核心子空间，通过判断核心子空间是否发生改变进行攻击检测。上述检测方案均假设训练数据和测试数据的分布相同，若数据分布改变，则模型需要重新训练。然而电力CPS环境是动态的，其物理层和网络层均

面临持续的变化，导致数据分布发生改变。电力CPS攻击检测任务相关性较强，迁移学习方法可将已训练好的检测模型的相关参数迁移到新的检测模型中。文献[80]提出了一个基于深度神经网络的迁移学习框架，用于攻击检测。

相比无监督学习方法，监督学习方法拥有数据标记作为指导，可更准确地识别各种攻击。检测结果的可解释性对电力CPS较为重要，因此一些文献采用具有较高可解释性的基于规则的机器学习方法检测攻击[81]。然而规则的生成耗时耗力，为克服这一缺陷，有研究采用兼顾可解释性与消耗时间的决策树进行实时网络攻击检测[49]。神经网络的可解释性虽然欠佳，但具有较强的非线性特征提取能力，已被广泛应用于电力CPS异常检测领域[82-84]。集成学习由多个弱分类器构成一个强分类器，以期在某些情况下提高检测性能，极端梯度提升[85]以及自适应增强[86]等集成学习算法已应用于电力CPS网络攻击检测。

攻击检测问题也可设计为马尔可夫决策问题并利用强化学习求解。文献[87]将如何在误报率最小的情况下最快检测到电力CPS网络攻击的问题设计为马尔可夫决策问题，并基于强化学习求解。相比其他机器学习方法，强化学习方法关注于每一步动作所能得到的长期累计回报，通过合理设置奖励函数可实现误报率与检测速度间的平衡。

5.2.2 FDIA检测

遭受FDIA的数据仍遵循物理定律，可以绕过传统的坏数据检测方法。监督学习、半监督学习、无监督学习以及强化学习方法已应用于FDIA检测研究。

监督学习方法是最早应用于FDIA检测的机器学习方法。早期主要应用了一些浅层、相对简单的监督学习算法检测FDIA，主要包括K最近邻分类[88-89]、支持向量机[57,88-89]、稀疏逻辑回归[88]、感知机[89]、自适应增强算法[89]、多核学习[89]以及贝叶斯推理[90]等。这些方法各具优势，其中K最近邻分类和支持向量机分别在小规模系统和大规模系统中表现更佳，稀疏逻辑回归在稀疏系统中的表现优于前两者，感知机对系统大小敏感性较低，自适应增强算法和多核学习对系统大小和数据稀疏性的变化更具鲁棒性，贝叶斯推理方法的可解释性较高。随着计算能力以及系统运行数据量的攀升，基于深度神经网络的攻击检测方案开始崭露头角，深度置信网络(deep belief network, DBN)[58]、深度前馈神经网络[91]、循环神经网络(recurrent neural network, RNN)[51]、卷积神经网络(convolutional neural network, CNN)[52]等算法已应用于FDIA检测，由于深度学习方法具有强大的非线性特征提取能力，RNN还能捕获连续系统状态下数据的时间相关性，深度神经网络的检测性能普遍优于前述浅层机器学习算法，但同时也牺牲了可解释性。另外，还有一些文献使用集成学习算法检测FDIA，例如文献[92]分别集成了决策树、朴素贝叶斯、逻辑回归、神经网络以及支持向量机等多种分类器，并将它们的性能与单一分类器的性能进行了对比分析。

监督学习需要大量的标记数据，但与电力CPS安全相关的标记数据往往难以获得。半监督学习利用少量的标记数据和大量的无标记数据进行学习。文献[89]利用半监督支持向量机检测FDIA，是半监督学习方法在此领域的首次应用。深度学习算法也可以采用半监督的方式进行训练，并已有研究将其应用于FDIA检测领域[53]，该研究结合自编码器与生成对抗网络，将自编码器的编码部分作为生成对抗网络的产生器。

与电力CPS网络安全相关的标记数据往往较少，因此许多研究应用无监督学习方法检测FDIA。主成分分析可以恢复由低秩分量和稀疏分量叠加而成的矩阵中的每个分量[93]。电力系统状态在短时间内变化较小，实际量测值矩阵通常是低秩的；而攻击矩阵由于攻击者倾向于以最小的代价发起攻击且一些量测数据可能受到保护，往往是稀疏的。因此，可以采用主成分分析恢复观测矩阵中的每个分量，以检测FDIA[47]。然而该方法的计算复杂度较高，难以实际应用。相较而言，聚类方法的时间复杂度更低，常用于异常分离，文献[94]和文献[48]分别使用模糊C均值聚类以及局部异常因子法进行攻击检测。擅于提取非线性表达的自编码器也可通过比较输入与输出间的重构误差的方式检测FDIA[95]。

文献[96]将FDIA检测问题描述为局部可观马尔可夫决策过程，并采用深度强化学习技术求解。与传统的强化学习方案相比，深度强化学习方案利用深度神经网络拟合未知状态，更适用于状态-动作空间较大的电力CPS环境。

5.2.3 断路攻击检测

传统的机理建模方法已能较为准确地检测断路攻击，然而随着电力系统的规模日益增大，计算量较大的机理建模方法难以满足实时检测的要求，因此一些研究开始探索基于机器学习的检测方法。目前该类研究较少，且仅有监督学习的方法应用于该领域。

文献[97]和文献[98]分别使用支持向量机和线性回归检测断路攻击。文献[99]研究并比较了支持

向量机、朴素贝叶斯和K最近邻分类算法用于检测断路攻击的性能表现，实验结果表明基于朴素贝叶斯的检测方案性能最佳。然而上述研究[97-99]只能检测单条线路中断，文献[50]克服了这一局限性，结合贝叶斯推理以及前馈神经网络的思想，可实时检测多条线路中断。

5.2.4　窃电检测

异常检测、FDIA检测以及断路攻击检测的数据集通常来自远程终端单元(remote terminal unit，RTU)或PMU，而窃电检测的数据集通常来自提供用户用电数据的电表。一般情况下，窃电不会导致电力系统的不安全或不稳定，但会给电力公司造成一定的经济损失。目前监督学习、无监督学习、半监督学习均已应用于窃电检测研究。

通常，普通用户的数量远超窃电用户，使得训练数据集不平衡。支持向量机可通过为正、反例分配不同的权值处理不平衡数据集，已应用于窃电检测[100]。文献[101]采用可处理不平衡数据集的随机欠采样自适应增强集成学习方法检测窃电。电表数据蕴含的信息较多，神经网络可准确、高效地学习自变量和因变量之间复杂的非线性关系，在窃电检测领域应用十分广泛，多层前馈神经网络[54]、卷积神经网络[102]、LSTM网络[103]均有所应用。其中，卷积神经网络主要用于提取一天内不同时刻的电表数据与用户是否窃电的关系；而LSTM网络擅长学习数据间的时间特性，被用于学习用电数据的长期依赖性。为同时捕获顺序数据的长短期特征，一些研究将LSTM网络与卷积神经网络的思想相结合用于窃电检测[104]。

对于某个给定用户，窃电样本有时很少甚至不存在，因此一些研究利用无监督学习方法进行窃电检测。文献[105]使用规则归纳创建基于各类用户特征的窃电检测模型，但规则生成过程极具挑战性且十分耗时。为克服此缺陷，一些研究使用聚类方法检测窃电[106-108]。

虽然窃电样本较少，但半监督学习方法可最大限度利用这些样本。基于自编码器的半监督学习模型已被应用于窃电检测[109]。

5.2.5　其他攻击检测

电力CPS网络攻击种类繁多，一些文献对其他网络攻击检测进行了研究。例如，基于支持向量机的分布式入侵检测系统被用于检测电力通信系统网络层的攻击[110]。监督学习方法被应用于电力CPS时间同步攻击[111]的检测[46]。部分文献利用机器学习算法检测数据源标识混合攻击，例如多粒度级联森林算法[112]和前馈神经网络算法[113]等。极限学习机技术被用于识别网络入侵中被破坏的仪表[114]。朴素贝叶斯分类器被用于检测针对负荷预测数据的网络攻击[115]。

上述各类针对不同攻击的机器学习检测算法优缺点各异，需要根据实际应用背景与应用需求选择合适的算法。例如，各类无监督学习算法免去了成本较高的人工类别标注过程，但检测精度往往低于监督学习算法；半监督学习算法能将少量的标注样本利用起来以提高检测精度；强化学习算法适用于求解序列决策问题，但将其应用于攻击检测领域需要将检测问题重新定义为序列决策问题，过程较为复杂且难以带来检测性能的提高。在攻击检测算法的具体选择上，也需要考虑各机器学习算法的特性，例如，朴素贝叶斯算法有较强的数学基础，可解释性强、对数据缺失不敏感，但其需要计算先验概率且对输入样本的表达形式较敏感；K最近邻算法检测准确度高且能提取非线性特征，但其计算量较大且不适用于样本集不平衡的情况；支持向量机算法可处理不平衡样本集且检测准确率较高，但其对缺失数据较敏感且核函数的选取较难；神经网络可充分拟合复杂的非线性关系，检测准确度高，但其需要大量的模型参数且可解释性较差等。此外，各类攻击检测问题在实际应用中面临着可用样本数量较少、样本集不均衡、检测准确率与模型泛化能力难以兼顾以及模型可解释性较差等难题。因此，电力CPS研究者需要根据实际应用背景下的难点所在以及关于模型检测精度、检测速度、泛化能力、可解释性等方面的应用需求，综合考虑各机器学习算法的优缺点，以挑选出合适的机器学习算法。

5.3　攻击缓解

目前，利用机理建模方法或机器学习方法缓解针对电力CPS网络攻击的研究相对较少。现有研究利用博弈论[116]或语义分析[117]的方法以缓解攻击对电力系统带来的影响，但这些方法面临着模型构建困难以及计算资源消耗较多等局限性。近年来，部分研究将机器学习方法应用于攻击缓解领域，这些研究主要集中于攻击缓解中的数据恢复部分。

攻击向量移除指移除被攻击量测值中的攻击注入部分，将量测数据恢复到未攻击状态，以减轻数据完整性攻击对电力CPS的影响。对于该问题，机理建模方法无法挖掘数据间的深层联系以及时间关联性，难以实现电力数据恢复。

机器学习方法拥有强大的数据挖掘能力，使恢复被攻击数据成为可能。目前无监督学习和监督学习方法已应用于该问题。

矩阵分解是数据恢复领域的常用方法[118]。为

移除攻击向量，可采用无监督的矩阵分解技术，例如鲁棒主成分分析[93]，恢复低秩量测值矩阵和稀疏攻击矩阵叠加而成的观测矩阵中的各分量，从而得到实际量测矩阵[47]。但基于矩阵分解的方法计算复杂较高，且矩阵稀疏度会影响恢复精度。一些无监督神经网络算法，例如降噪自动编码器[119]以及生成对抗网络[120]可重建受FDIA影响的量测值，以消除攻击所致的偏差。然而上述方法均会使未受攻击的量测部分被替换。

一些研究将监督学习方法应用于攻击向量移除中。文献[121]采用贝叶斯状态估计实时去除不可靠的量测值，并使用多层前馈神经网络降低贝叶斯估计的计算复杂度。然而，贝叶斯技术需要系统先验知识，对高度动态化的电力CPS适应能力较差。卷积神经网络在图像去噪任务中具有较高的有效性[122]。为此，文献[123]应用卷积神经网络剔除被攻击的量测值，然而该方法也会使未受攻击的量测部分被替换。

当前，移除攻击向量的研究主要面临的难题是如何保证量测数据中未被攻击部分的完整性，求解该难题的前提在于准确定位量测数据中被攻击的部分。随后，需要最大限度保护未被攻击部分在攻击向量移除过程中不被改动，以使恢复得到的量测数据更接近原始量测数据。

目前，机器学习在电力CPS安全防御中的应用分类如图3所示。

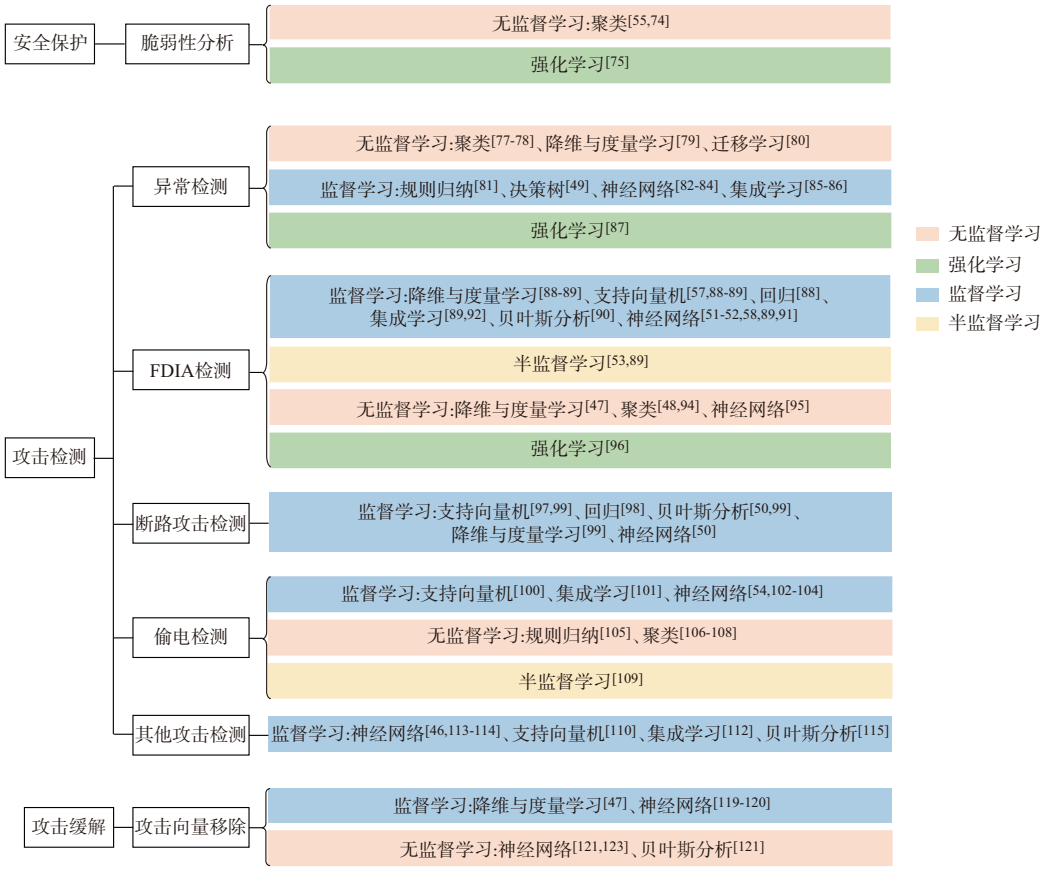

图3　机器学习在安全防御中的应用分类

Fig. 3　Classification of applications of machine learning in defense

6　展望

与较为健壮的电力一次系统相比，电力CPS网络安全较薄弱，研究起步较晚。目前，该领域仍面临着许多挑战，包括但不局限于如下4个方面：

1)最小化攻击资源：攻击者在发动攻击前，需要考虑攻击实施成功的可能性，确定发动攻击所需的最小攻击资源。例如，文献[124]表明在CPS中，若超过一半的传感设备被攻击，则CPS操作者将不能精确恢复系统状态，而在电力CPS网络安全领域，对于某种网络攻击，攻击者需要多少攻击资源才能达到攻击目的的研究仍为欠缺。最小攻击资源的确定是攻击资源、攻击效果以及攻击隐蔽性三者的权衡问题，将该问题表述为优化问题求解可作为研究思路之一。

2）网络安全评估：网络安全评估指估计不同种类网络攻击对电力CPS造成的影响，将这些攻击按影响大小排序，以便设计防御措施。网络安全评估问题与稳定评估问题相似，不同的是，稳定评估根据系统当前运行状态对重要故障进行筛选，并据此对当前状态做$N-k$故障分析，分析不同故障对当前运行状态的影响程度。而网络安全评估用于分析不同网络攻击对当前运行状态的影响，不考虑攻击造成的故障种类。当前，已有许多研究关注稳定评估问题[125]，而对网络安全评估的研究工作仍较匮乏。针对电力CPS的网络攻击种类繁多，该问题的难点之一在于如何使评估方案具有通用性或可迁移性。由于针对电力CPS的网络攻击相关性较强，因此可以考虑利用迁移学习方法将针对某种网络攻击的评估方案迁移到针对新的网络攻击的评估方案中。目前，迁移学习在电力CPS网络攻击检测中已取得较好的表现[80]。

3）防御资源规划：不同的网络攻击具有不同的特征（例如频率、可发现性以及再现性等），对电力CPS整体安全性的影响有强弱之分。由于防守方的防御资源往往有限，无法针对所有网络攻击实施保护措施，因此，需要根据网络攻击的影响程度及其相应的特征合理部署防御资源，建立电力CPS网络安全首道防线。防御资源规划是防御成本与防御性能之间的权衡问题。该问题建立在已明确各网络攻击对电力CPS的影响的基础上，由影响强弱判断电力CPS对各网络攻击的容忍度，并以此为基准分配防御资源。电力CPS各设备间存在物理连接或通信关系，因此，网络安全具有整体、全面、协同的特点，在分配防御资源时，需要考虑合并针对不同网络攻击的防御策略产生的并发影响。该问题的解决方案之一是利用多智能体强化学习[126]，使每个智能体维护一个关于不同网络攻击的防御策略和一个局部值函数，所有智能体的总目标是使电力CPS更为安全。目前，在微电网领域，多智能体强化学习算法已有较多应用[127]。

4）恢复策略评估：电力CPS网络攻击防御由攻击前的保护、攻击时的检测、攻击时的缓解和攻击后的恢复4个部分组成。然而现存文献大多关注前3个部分。电力CPS与国家安全以及国民经济发展息息相关，快速消除攻击影响，及时恢复电力系统的安全平稳运行，以保障电力可用性尤为重要。根据攻击发生的时间段以及电力使用场景的不同，需要采取不同的防御措施，以达到恢复成本与恢复所需时长的平衡，例如，城市商圈白天断电相比学校区域夜晚断电要求更短的恢复时长。文献[128]利用深度强化学习方法确定因网络攻击而跳闸的输电线路的最佳合闸时间，该研究为机器学习在恢复策略设计中的应用提供了范例，更多的应用尚待挖掘探索。

7　结语

本文首先介绍了电力CPS网络安全的要求及挑战，然后从数据基础及硬件基础、模型构建及实时性需求角度分别分析了机器学习应用于电力CPS网络安全领域的契机与优势，接着从攻防两个角度阐述了电力CPS网络安全面临的难点问题并归纳了机器学习在各问题上的应用，最后分析展望了该领域存在的挑战以及未来的研究方向。

机器学习方法具有强大的线性及非线性关系拟合能力，对于电力CPS网络安全面临的各类挑战均有应用的可能。例如对于最小化攻击资源问题，可根据电力系统当前的状态、预期达到的攻击效果以及要求的攻击隐蔽性，端到端输出最小需要的攻击资源，也可利用机器学习加速该优化问题的求解速度，以达到实时性要求。由此可见，电力CPS网络安全领域还有许多亟待解决的问题，机器学习在该领域的应用尚待进一步探索。

参考文献

[1] 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 modelling and evaluation [J]. Automation of Electric Power Systems, 2019, 43(9): 9-21.

[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] 张顺，龚怡宏，王进军.深度卷积神经网络的发展及其在计算机视觉领域的应用[J].计算机学报，2019，42(3)：453-482.
ZHANG Shun, GONG Yihong, WANG Jinjun. The development of deep convolution neural network and its applications on computer vision [J]. Chinese Journal of Computers, 2019, 42(3): 453-482.

[4] 田娟秀，刘国才，谷珊珊，等.医学图像分析深度学习方法研究与挑战[J].自动化学报，2018，44(3)：401-424.
TIAN Juanxiu, LIU Guocai, GU Shanshan, et al. Deep learning in medical image analysis and its challenges[J]. Acta Automatica Sinica, 2018, 44(3): 401-424.

[5] 席亮，刘涵，樊好义，等.基于深度对抗学习潜在表示分布的异常检测模型[J].电子学报，2021，49(7)：1257-1265.
XI Liang, LIU Han, FAN Haoyi, et al. Deep adversarial

learning latent representation distribution model for anomaly detection[J]. Acta Electronica Sinica, 2021, 49(7): 1257-1265.

[6] 杨挺,赵黎媛,王成山.人工智能在电力系统及综合能源系统中的应用综述[J].电力系统自动化,2019,43(1):2-14.
YANG Ting, ZHAO Liyuan, WANG Chengshan. Review on application of artificial intelligence in power system and integrated energy system [J]. Automation of Electric Power Systems, 2019, 43(1): 2-14.

[7] 周念成,廖建权,王强钢,等.深度学习在智能电网中的应用现状分析与展望[J].电力系统自动化,2019,43(4):180-191.
ZHOU Niancheng, LIAO Jianquan, WANG Qianggang, et al. Analysis and prospect of deep learning application in smart grid [J]. Automation of Electric Power Systems, 2019, 43(4): 180-191.

[8] IBRAHIM M S, DONG W, YANG Q. Machine learning driven smart electric power systems: current trends and new perspectives[J]. Applied Energy, 2020, 272: 115237.

[9] SUN C C, HAHN A, LIU C C. Cyber security of a power grid: state-of-the-art [J]. International Journal of Electrical Power & Energy Systems, 2018, 99: 45-56.

[10] 李泽科,陈泽文,王春艳,等.电力监控系统的网络安全威胁溯源技术研究[J].电力工程技术,2020,39(2):166-172.
LI Zeke, CHEN Zewen, WANG Chunyan, et al. Network security threat tracing technology of power monitoring system [J]. Electric Power Engineering Technology, 2020, 39(2): 166-172.

[11] WANG W Y, LU Z. Cyber security in the smart grid: survey and challenges[J]. Computer Networks, 2013, 57(5): 1344-1371.

[12] 国家自然科学基金委员会,中国科学院.未来10年中国学科发展战略——数学[M].北京:科学出版社,2012.
National Natural Science Foundation of China, Chinese Academy of Sciences. China's disciplinary development strategy for the next 10 years—mathematics [M]. Beijing: Science Press, 2012.

[13] 骆钊,谢吉华,顾伟,等.基于SM2密码体系的电网信息安全支撑平台开发[J].电力系统自动化,2014,38(6):68-74.
LUO Zhao, XIE Jihua, GU Wei, et al. SM2-cryptosystem based information security supporting platform in power grid[J]. Automation of Electric Power Systems, 2014, 38(6): 68-74.

[14] 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.
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.

[15] 李祝红,赵灿明,闫龙,等.智能电网中电力线通信网络负载均衡的机会路由协议[J].计算机应用,2019,39(3):812-816.
LI Zhuhong, ZHAO Canming, YAN Long, et al. Load balancing opportunistic routing protocol for power line communication network in smart grids[J]. Journal of Computer Applications, 2019, 39(3): 812-816.

[16] HUSSAIN S M S, USTUN T S, KALAM A. A review of IEC 62351 security mechanisms for IEC 61850 message exchanges [J]. IEEE Transactions on Industrial Informatics, 2020, 16(9): 5643-5654.

[17] 金能,梁宇,邢家维,等.提升配电网线路保护可靠性的远方保护及其与就地保护优化配合方案研究[J].电工技术学报,2019,34(24):5221-5233.
JIN Neng, LIANG Yu, XING Jiawei, et al. Research on remote protection and the optimized coordination scheme of local-remote protection to enhance the protection reliability of the line in distribution network [J]. Transactions of China Electrotechnical Society, 2019, 34(24): 5221-5233.

[18] KHALAF M, YOUSSEF A, EL-SAADANY E. Joint detection and mitigation of false data injection attacks in AGC systems[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 4985-4995.

[19] LIU C S, LIANG H, CHEN T W, et al. Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation [J]. IEEE Transactions on Power Systems, 2020, 35(2): 1468-1478.

[20] MOHRI M, ROSTAMIZADEH A, TALWALKAR A. Foundations of machine learning [M]. Cambridge, USA: MIT Press, 2018.

[21] 谢娟英,丁丽娟,王明钊.基于谱聚类的无监督特征选择算法[J].软件学报,2020,31(4):1009-1024.
XIE Juanying, DING Lijuan, WANG Mingzhao. Spectral clustering based unsupervised feature selection algorithms [J]. Journal of Software, 2020, 31(4): 1009-1024.

[22] 李磊,严正,冯冬涵,等.结合主成分分析及生产函数的电网智能技术评价探讨[J].电力系统自动化,2014,38(11):56-61.
LI Lei, YAN Zheng, FENG Donghan, et al. Discussion on intelligent technology evaluation of electrical power grid based on principal component analysis and production function [J]. Automation of Electric Power Systems, 2014, 38(11): 56-61.

[23] 樊继聪,王友清,秦泗钊.联合指标独立成分分析在多变量过程故障诊断中的应用[J].自动化学报,2013,39(5):494-501.
FAN Jicong, WANG Youqing, QIN S Joe. Combined indices for ICA and their applications to multivariate process fault diagnosis[J]. Acta Automatica Sinica, 2013, 39(5): 494-501.

[24] JAIN A K. Data clustering: 50 years beyond *K*-means [J]. Pattern Recognition Letters, 2010, 31(8): 651-666.

[25] 张志鹏,李勇,曹一家,等.通信和电网联合仿真的配电网局部异常因子故障辨识算法[J].电力系统自动化,2016,40(17):44-50.
ZHANG Zhipeng, LI Yong, CAO Yijia, et al. A local outlier factor fault identification algorithm based on the co-simulation between cyber and power system for distribution network [J]. Automation of Electric Power Systems, 2016, 40(17): 44-50.

[26] 於东军,吴小俊,HANCOCK Edwin R,等.广义SOM及其在人脸性别识别中的应用[J].计算机学报,2011,34(9):1719-1725.
YU Dongjun, WU Xiaojun, HANCOCK E R, et al. Generalized SOM with application to facial gender identification [J]. Chinese Journal of Computers, 2011, 34(9): 1719-1725.

[27] KUSNER M J, PAIGE B, HERNÁNDEZ-LOBATO J M. Grammar variational autoencoder [C]// International Conference on Machine Learning, August 6-11, 2017, Sydney, Australia: 1945-1954.

[28] 唐滢淇，董树锋，朱承治，等．基于Tri-Training-LASSO-BP网络的静态电压稳定裕度在线预测方法[J]．中国电机工程学报，2020，40(12)：3824-3835.
TANG Yingqi, DONG Shufeng, ZHU Chengzhi, et al. Online prediction method of static voltage stability margin based on Tri-Training-LASSO-BP network [J]. Proceedings of the CSEE, 2020, 40(12): 3824-3835.

[29] 陆继翔，张琪培，杨志宏，等．基于CNN-LSTM混合神经网络模型的短期负荷预测方法[J]．电力系统自动化，2019，43(8)：131-137.
LU Jixiang, ZHANG Qipei, YANG Zhihong, et al. Short-term load forecasting method based on CNN-LSTM hybrid neural network model [J]. Automation of Electric Power Systems, 2019, 43(8): 131-137.

[30] SEBER G A F, LEE A J. Linear regression analysis [M]. Hoboken, USA: John Wiley & Sons, 2003.

[31] HOSMER D W, LEMESHOW S, STURDIVANT R X. Applied logistic regression [M]. Hoboken, USA: John Wiley & Sons, 2013.

[32] 张棪，曹健．面向大数据分析的决策树算法[J]．计算机科学，2016，43(增刊1)：374-379.
ZHANG Yan, CAO Jian. Decision tree algorithms for big data analysis [J]. Computer Science, 2016, 43 (Supplement 1): 374-379.

[33] 朱军，胡文波．贝叶斯机器学习前沿进展综述[J]．计算机研究与发展，2015，52(1)：16-26.
ZHU Jun, HU Wenbo. Recent advances in Bayesian machine learning [J]. Journal of Computer Research and Development, 2015, 52(1): 16-26.

[34] 刘建伟，刘媛，罗雄麟．半监督学习方法[J]．计算机学报，2015，38(8)：1592-1617.
LIU Jianwei, LIU Yuan, LUO Xionglin. Semi-supervised learning methods [J]. Chinese Journal of Computers, 2015, 38(8): 1592-1617.

[35] ANAND S, MITTAL S, TUZEL O, et al. Semi-supervised kernel mean shift clustering [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2014, 36(6): 1201-1215.

[36] 郭虎升，王文剑，潘世超．基于组合半监督的增量支持向量机学习算法[J]．模式识别与人工智能，2016，29(6)：504-510.
GUO Husheng, WANG Wenjian, PAN Shichao. Combinatorial semi-supervised incremental support vector machine learning algorithm [J]. Pattern Recognition and Artificial Intelligence, 2016, 29(6): 504-510.

[37] SUTTON R S, BARTO A G. Reinforcement learning: an introduction [J]. IEEE Transactions on Neural Networks, 1998, 9(5): 1054.

[38] 瞿凯平，张孝顺，余涛，等．基于知识迁移Q学习算法的多能源系统联合优化调度[J]．电力系统自动化，2017，41(15)：18-25.
QU Kaiping, ZHANG Xiaoshun, YU Tao, et al. Knowledge transfer based Q-learning algorithm for optimal dispatch of multi-energy system [J]. Automation of Electric Power Systems, 2017, 41(15): 18-25.

[39] MNIH V, BADIA A P, MIRZA M, et al. Asynchronous methods for deep reinforcement learning [C]// International Conference on Machine Learning, June 19-24, 2016, New York, USA: 1928-1937.

[40] 左松林，陈伟，付真斌，等．基于EKF算法的分布式光伏发电异常数据排查技术[J]．电力工程技术，2020，39(5)：120-125.
ZUO Songlin, CHEN Wei, FU Zhenbin, et al. Abnormal data inspection technology of photovoltaic power generation based on EKF algorithm [J]. Electric Power Engineering Technology, 2020, 39(5): 120-125.

[41] DE FINE LICHT J, BESTA M, MEIERHANS S, et al. Transformations of high-level synthesis codes for high-performance computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(5): 1014-1029.

[42] LIU Y, SUN K, YAO R, et al. Power system time domain simulation using a differential transformation method [J]. IEEE Transactions on Power Systems, 2019, 34(5): 3739-3748.

[43] AZMAN S K, ISBEIH Y J, MOURSI M S E, et al. A unified online deep learning prediction model for small signal and transient stability [J]. IEEE Transactions on Power Systems, 2020, 35(6): 4585-4598.

[44] 李常刚，李华瑞，刘玉田，等．大电网动态安全风险智能评估系统[J]．电力系统自动化，2019，43(22)：67-75.
LI Changgang, LI Huarui, LIU Yutian, et al. Intelligent assessment system for dynamic security risk of large-scale power grid [J]. Automation of Electric Power Systems, 2019, 43(22): 67-75.

[45] CHEN Y, HUANG S W, LIU F, et al. Evaluation of reinforcement learning-based false data injection attack to automatic voltage control [J]. IEEE Transactions on Smart Grid, 2019, 10(2): 2158-2169.

[46] LOU X, TRAN C, TAN R, et al. Assessing and mitigating impact of time delay attack: a case study for power grid frequency control [C]// Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, April 16-18, 2019, Montreal, Canada: 207-216.

[47] HAO J P, PIECHOCKI R J, KALESHI D, et al. Sparse malicious false data injection attacks and defense mechanisms in smart grids [J]. IEEE Transactions on Industrial Informatics, 2015, 11(5): 1-12.

[48] KONSTANTINOU C, MANIATAKOS M. A data-based detection method against false data injection attacks [J]. IEEE Design & Test, 2020, 37(5): 67-74.

[49] ADHIKARI U, MORRIS T H, PAN S Y. Applying Hoeffding adaptive trees for real-time cyber-power event and intrusion classification [J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4049-4060.

[50] ZHAO Y, CHEN J S, POOR H V. A learning-to-infer method for real-time power grid multi-line outage identification [J]. IEEE Transactions on Smart Grid, 2020, 11(1): 555-564.

[51] YU J J Q, HOU Y H, LI V O K. Online false data injection attack detection with wavelet transform and deep neural networks [J]. IEEE Transactions on Industrial Informatics, 2018, 14(7): 3271-3280.

[52] WANG S Y, BI S Z, ZHANG Y J A. Locational detection of the false data injection attack in a smart grid: a multilabel classification approach [J]. IEEE Internet of Things Journal,

2020, 7(9): 8218-8227.
[53] ZHANG Y, WANG J H, CHEN B. Detecting false data injection attacks in smart grids: a semi-supervised deep learning approach[J]. IEEE Transactions on Smart Grid, 2021, 12(1): 623-634.
[54] ISMAIL M, SHAHIN M, SHAABAN M F, et al. Efficient detection of electricity theft cyber attacks in AMI networks[C]// 2018 IEEE Wireless Communications and Networking Conference (WCNC), April 15-18, 2018, Barcelona, Spain.
[55] ANWAR A, MAHMOOD A N, TARI Z. Identification of vulnerable node clusters against false data injection attack in an AMI based smart grid[J]. Information Systems, 2015, 53: 201-212.
[56] ESMALIFALAK M, NGUYEN H, ZHENG R, et al. A stealthy attack against electricity market using independent component analysis[J]. IEEE Systems Journal, 2018, 12(1): 297-307.
[57] DENG Y Y, ZHU K, WANG R, et al. Real-time detection of false data injection attacks based on load forecasting in smart grid[C]// 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), October 21-23, 2019, Beijing, China.
[58] HE Y B, 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.
[59] LIU Y, NING P, REITER M K. False data injection attacks against state estimation in electric power grids[J]. ACM Transactions on Information and System Security, 2011, 14(1): 1-33.
[60] CHIN W L, LEE C H, JIANG T. Blind false data attacks against AC state estimation based on geometric approach in smart grid communications[J]. IEEE Transactions on Smart Grid, 2018, 9(6): 6298-6306.
[61] 赵海峰,张亚,李世中.侵彻过载信号的欠定盲源分离与特征提取[J].仪器仪表学报,2019,40(10):208-218.
ZHAO Haifeng, ZHANG Ya, LI Shizhong. Undetermined blind source separation and feature extraction of penetration overload signals[J]. Chinese Journal of Scientific Instrument, 2019, 40(10): 208-218.
[62] YU Z H, CHIN W L. Blind false data injection attack using PCA approximation method in smart grid[J]. IEEE Transactions on Smart Grid, 2015, 6(3): 1219-1226.
[63] 田继伟,王布宏,尚福特.基于鲁棒主成分分析的智能电网虚假数据注入攻击[J].计算机应用,2017,37(7):1943-1947.
TIAN Jiwei, WANG Buhong, SHANG Fute. False data injection attacks based on robust principal component analysis in smart grid[J]. Journal of Computer Applications, 2017, 37(7): 1943-1947.
[64] 李元诚,邱日轩,曾婧.基于核主成分分析的智能电网盲在线虚假数据注入攻击[J].电网技术,2018,42(7):2270-2278.
LI Yuancheng, QIU Rixuan, ZENG Jing. Blind online false data injection attack using kernel principal component analysis in smart grid[J]. Power System Technology, 2018, 42(7): 2270-2278.
[65] JIAO R H, XUN G Y, LIU X, et al. A new AC false data injection attack method without network information[J]. IEEE Transactions on Smart Grid, 2021, 12(6): 5280-5289.
[66] ZHANG Z Y, DENG R L, 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, 2020, 15: 2320-2335.
[67] HIGGINS M, TENG F, 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.
[68] 陈雷,甘士忠,张立毅,等.基于样条插值与人工蜂群优化的非线性盲源分离算法[J].通信学报,2017,38(7):36-46.
CHEN Lei, GAN Shizhong, ZHANG Liyi, et al. Nonlinear blind source separation algorithm based on spline interpolation and artificial bee colony optimization [J]. Journal on Communications, 2017, 38(7): 36-46.
[69] KABASHIMA Y, KRZAKALA F, MÉZARD M, et al. Phase transitions and sample complexity in Bayes-optimal matrix factorization[J]. IEEE Transactions on Information Theory, 2016, 62(7): 4228-4265.
[70] YE C, TOYODA K, OHTSUKI T. Blind source separation on non-contact heartbeat detection by non-negative matrix factorization algorithms[J]. IEEE Transactions on Biomedical Engineering, 2020, 67(2): 482-494.
[71] NI Z, PAUL S. A multistage game in smart grid security: a reinforcement learning solution[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 30(9): 2684-2695.
[72] PAUL S, HAQ M R, DAS A, et al. A comparative study of smart grid security based on unsupervised learning and load ranking[C]// 2019 IEEE International Conference on Electro Information Technology (EIT), May 20-22, 2019, Brookings, USA: 310-315.
[73] HINES P, COTILLA-SANCHEZ E, BLUMSACK S. Do topological models provide good information about electricity infrastructure vulnerability?[J]. Chaos, 2010, 20(3): 033122.
[74] YAN J, ZHU Y H, HE H B, et al. Multi-contingency cascading analysis of smart grid based on self-organizing map[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(4): 646-656.
[75] YAN J, HE H B, ZHONG X N, et al. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(1): 200-210.
[76] 王琦,邰伟,汤奕,等.面向电力信息物理系统的虚假数据注入攻击研究综述[J].自动化学报,2019,45(1):72-83.
WANG Qi, TAI Wei, TANG Yi, et al. A review on false data injection attack toward cyber-physical power system[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.
[77] WU M, XIE L. Online detection of low-quality synchrophasor measurements: a data-driven approach[J]. IEEE Transactions on Power Systems, 2017, 32(4): 2817-2827.
[78] WU T, ZHANG Y J A, TANG X Y. Isolation forest based

method for low-quality synchrophasor measurements and early events detection[C]// 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), October 29-31, 2018, Aalborg, Denmark.

[79] MAHAPATRA K, CHAUDHURI N R, KAVASSERI R G, et al. Online analytical characterization of outliers in synchrophasor measurements: a singular value perturbation viewpoint[J]. IEEE Transactions on Power Systems, 2018, 33(4): 3863-3874.

[80] ZHANG Y, YAN J. Domain-adversarial transfer learning for robust intrusion detection in the smart grid [C]// IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), October 21-23, 2019, Beijing, China.

[81] ADHIKARI U, MORRIS T H, PAN S Y. Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 3928-3941.

[82] WILSON D, TANG Y F, YAN J, et al. Deep learning-aided cyber-attack detection in power transmission systems [C]// 2018 IEEE Power & Energy Society General Meeting (PESGM), August 5-10, 2018, Portland, USA.

[83] 杨智伟,刘灏,毕天姝,等.基于长短期记忆网络的PMU不良数据检测方法[J].电力系统保护与控制,2020,48(7):1-9.
YANG Zhiwei, LIU Hao, BI Tianshu, et al. PMU bad data detection method based on long short-term memory network[J]. Power System Protection and Control, 2020, 48(7): 1-9.

[84] ANWAR A, MAHMOOD A, RAY B, et al. Machine learning to ensure data integrity in power system topological network database[J]. Electronics, 2020, 9(4): 693.

[85] HU C M, YAN J, WANG C. Advanced cyber-physical attack classification with extreme gradient boosting for smart transmission grids[C]// 2019 IEEE Power & Energy Society General Meeting (PESGM), August 4-8, 2019, Atlanta, USA.

[86] WANG D F, WANG X J, ZHANG Y, et al. Detection of power grid disturbances and cyber-attacks based on machine learning[J]. Journal of Information Security and Applications, 2019, 46: 42-52.

[87] KURT M N, OGUNDIJO O, LI C, et al. Online cyber-attack detection in smart grid: a reinforcement learning approach [J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5174-5185.

[88] OZAY M, ESNAOLA I, YARMAN VURAL F T, et al. Smarter security in the smart grid [C]// 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), November 5-8, 2012, Tainan, China: 312-317.

[89] OZAY M, ESNAOLA I, YARMAN VURAL F T, et al. Machine learning methods for attack detection in the smart grid [J]. IEEE Transactions on Neural Networks and Learning Systems, 2016, 27(8): 1773-1786.

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

[91] ASHRAFUZZAMAN M, CHAKHCHOUKH Y, JILLEPALLI A A, et al. Detecting stealthy false data injection attacks in power grids using deep learning [C]// 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), June 25-29, 2018, Limassol, Cyprus: 219-225.

[92] ASHRAFUZZAMAN M, DAS S, CHAKHCHOUKH Y, et al. Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning[J]. Computers & Security, 2020, 97: 101994.

[93] CANDÈS E J, LI X D, MA Y, et al. Robust principal component analysis? [J]. Journal of the ACM, 2011, 58(3): 1-37.

[94] MOHAMMADPOURFARD M, SAMI A, SEIFI A R. A statistical unsupervised method against false data injection attacks: a visualization-based approach [J]. Expert Systems With Applications, 2017, 84: 242-261.

[95] KUNDU A. Deep learning techniques for detection of false data injection attacks on electric power grid [D]. Texas, USA: Texas A&M University, 2019.

[96] AN D, YANG Q Y, LIU W M, et al. Defending against data integrity attacks in smart grid: a deep reinforcement learning-based approach[J]. IEEE Access, 2019, 7: 110835-110845.

[97] ABDELAZIZ A Y, MEKHAMER S F, EZZAT M, et al. Line outage detection using support vector machine (SVM) based on the phasor measurement units (PMUs) technology [C]// 2012 IEEE Power and Energy Society General Meeting, July 22-26, 2012, San Diego, USA.

[98] GARCIA M, CATANACH T, WIEL S V, et al. Line outage localization using phasor measurement data in transient state [J]. IEEE Transactions on Power Systems, 2016, 31(4): 3019-3027.

[99] IBRAHIM A M, EZZAT M, ABDELAZIZ A Y. Performance comparison of classification methods for line outage detection [C]// 2016 Eighteenth International Middle East Power Systems Conference (MEPCON), December 27-29, 2016, Cairo, Egypt: 26-32.

[100] 康宁宁,李川,曾虎,等.采用FCM聚类与改进SVR模型的窃电行为检测[J].电子测量与仪器学报,2017,31(12):2023-2029.
KANG Ningning, LI Chuan, ZENG Hu, et al. Electric larceny detectionusing FCM clustering and improved SVR model [J]. Journal of Electronic Measurement and Instrumentation, 2017, 31(12): 2023-2029.

[101] AVILA N F, FIGUEROA G, CHU C C. NTL detection in electric distribution systems using the maximal overlap discrete wavelet-packet transform and random undersampling boosting [C]// 2019 IEEE Power & Energy Society General Meeting (PESGM), August 4-8, 2019, Atlanta, USA.

[102] ZHENG Z B, YANG Y T, NIU X D, et al. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids [J]. IEEE Transactions on Industrial Informatics, 2018, 14(4): 1606-1615.

[103] BUZAU M M, TEJEDOR-AGUILERA J, CRUZ-ROMERO P, et al. Hybrid deep neural networks for detection of non-technical losses in electricity smart meters[J]. IEEE Transactions on Power Systems, 2020, 35(2): 1254-1263.

[104] ISMAIL M, SHAABAN M F, NAIDU M, et al. Deep learning detection of electricity theft cyber-attacks in renewable distributed generation[J]. IEEE Transactions on Smart Grid, 2020, 11(4): 3428-3437.

[105] LEON C, BISCARRI F, MONEDERO I, et al. Variability and trend-based generalized rule induction model to NTL detection in power companies[J]. IEEE Transactions on Power Systems, 2011, 26(4): 1798-1807.

[106] VIEGAS J L, ESTEVES P R, VIEIRA S M. Clustering-based novelty detection for identification of non-technical losses[J]. International Journal of Electrical Power & Energy Systems, 2018, 101: 301-310.

[107] 王桂兰,周国亮,赵洪山,等.大规模用电数据流的快速聚类和异常检测技术[J].电力系统自动化,2016,40(24):27-33.
WANG Guilan, ZHOU Guoliang, ZHAO Hongshan, et al. Fast clustering and anomaly detection technique for large-scale power data stream[J]. Automation of Electric Power Systems, 2016, 40(24): 27-33.

[108] 杜章华,苏盛,刘正谊,等.基于生产经营状态识别的低误报率窃电检测二次筛查方法[J].电力系统自动化,2021,45(2):97-104.
DU Zhanghua, SU Sheng, LIU Zhengyi, et al. Second inspection method for electricity theft detection with low false alarm rate based on identification of production and operation status[J]. Automation of Electric Power Systems, 2021, 45(2): 97-104.

[109] LU X Q, ZHOU Y, WANG Z D, et al. Knowledge embedded semi-supervised deep learning for detecting non-technical losses in the smart grid[J]. Energies, 2019, 12(18): 3452.

[110] ZHANG Y C, WANG L F, SUN W Q, et al. Distributed intrusion detection system in a multi-layer network architecture of smart grids[J]. IEEE Transactions on Smart Grid, 2011, 2(4): 796-808.

[111] ZHANG Z H, GONG S P, DIMITROVSKI A D, et al. Time synchronization attack in smart grid: impact and analysis[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 87-98.

[112] CUI Y, BAI F F, LIU Y L, et al. Spatio-temporal characterization of synchrophasor data against spoofing attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5807-5818.

[113] LIU S Y, YOU S T, YIN H, et al. Model-free data authentication for cyber security in power systems[J]. IEEE Transactions on Smart Grid, 2020, 11(5): 4565-4568.

[114] KHANNA K, PANIGRAHI B K, JOSHI A. AI-based approach to identify compromised meters in data integrity attacks on smart grid[J]. IET Generation, Transmission & Distribution, 2018, 12(5): 1052-1066.

[115] CUI M J, WANG J H, YUE M. Machine learning-based anomaly detection for load forecasting under cyberattacks[J]. IEEE Transactions on Smart Grid, 2019, 10(5): 5724-5734.

[116] CHEN G, DONG Z Y, HILL D J, et al. Exploring reliable strategies for defending power systems against targeted attacks[J]. IEEE Transactions on Power Systems, 2011, 26(3): 1000-1009.

[117] 麻建中,胡凯波,於立峰.工控运维中基于语义分析的智能电网控制攻击防御[J].中国电力,2020,53(9):214-220.
MA Jianzhong, HU Kaibo, YU Lifeng. Smart grid control attack defense based on semantic analysis in industrial control operation and maintenance[J]. Electric Power, 2020, 53(9): 214-220.

[118] HAO Y S, WANG M, CHOW J H, et al. Modelless data quality improvement of streaming synchrophasor measurements by exploiting the low-rank Hankel structure[J]. IEEE Transactions on Power Systems, 2018, 33(6): 6966-6977.

[119] AHMED S, LEE Y, HYUN S H, et al. Mitigating the impacts of covert cyber attacks in smart grids via reconstruction of measurement data utilizing deep denoising autoencoders[J]. Energies, 2019, 12(16): 3091.

[120] LI Y C, WANG Y Y, HU S Y. Online generative adversary network based measurement recovery in false data injection attacks: a cyber-physical approach[J]. IEEE Transactions on Industrial Informatics, 2020, 16(3): 2031-2043.

[121] MESTAV K R, LUENGO-ROZAS J, TONG L. Bayesian state estimation for unobservable distribution systems via deep learning[J]. IEEE Transactions on Power Systems, 2019, 34(6): 4910-4920.

[122] 盖杉,鲍中运.基于深度学习的高噪声图像去噪算法[J].自动化学报,2020,46(12):2672-2680.
GAI Shan, BAO Zhongyun. High noise image denoising algorithm based on deep learning[J]. Acta Automatica Sinica, 2020, 46(12): 2672-2680.

[123] GE Q Y, JIAO C Q. Mitigating the impacts of false data injection attacks in smart grids using deep convolutional neural networks[C]// 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC), July 17-19, 2020, Beijing, China: 174-177.

[124] FAWZI H, TABUADA P, DIGGAVI S. Secure estimation and control for cyber-physical systems under adversarial attacks[J]. IEEE Transactions on Automatic Control, 2014, 59(6): 1454-1467.

[125] YAN R, GENG G C, JIANG Q Y, et al. Fast transient stability batch assessment using cascaded convolutional neural networks[J]. IEEE Transactions on Power Systems, 2019, 34(4): 2802-2813.

[126] BUSONIU L, BABUSKA R, DE SCHUTTER B. A comprehensive survey of multiagent reinforcement learning[J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2008, 38(2): 156-172.

[127] 沈珺,柳伟,李虎成,等.基于强化学习的多微电网分布式二次优化控制[J].电力系统自动化,2020,44(5):198-206.
SHEN Jun, LIU Wei, LI Hucheng, et al. Reinforcement learning based distributed secondary optimal control for multiple microgrids[J]. Automation of Electric Power Systems, 2020, 44(5): 198-206.

[128] WEI F R, WAN Z Q, HE H B. Cyber-attack recovery strategy for smart grid based on deep reinforcement learning [J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2476-2486.

彭　莎(1998—),女,博士研究生,主要研究方向:智能电网安全、机器学习。E-mail:pengsha_mail123@163.com

孙铭阳(1988—),男,博士,研究员,主要研究方向:人工智能与电力大数据、低碳能源系统优化运行与规划、能源互联网安全。E-mail:mingyangsun@zju.edu.cn

张镇勇(1991—),男,副教授,主要研究方向:工业控制系统安全、智能电网安全、人工智能技术应用安全、移动计算。E-mail: zyzhangnew@gmail.com

邓瑞龙(1987—),男,通信作者,博士,研究员,主要研究方向:工控安全、智能电网、通信网络。E-mail:dengruilong@zju.edu.cn

(编辑　杨松迎)

Application of Machine Learning in Cyber Security of Cyber-Physical Power System

PENG Sha[1], *SUN Mingyang*[1], *ZHANG Zhenyong*[1,2], *DENG Ruilong*[1], *CHENG Peng*[1]

(1. College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China;
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China)

Abstract: With the deepening of informationization, the traditional power system has been transformed into a typical cyber-physical system (CPS). Considering the open cyber system environment, the security operation of the cyber-physical power system (CPPS) faces threats from various potential cyberattacks. In recent years, machine learning approaches have been developing rapidly and have been widely used in CPPS cyber security. On the one hand, the explosive growth of data in the CPPS and the improvement of hardware computing power create the right conditions for applying machine learning approaches. On the other hand, compared with the traditional model-based approaches, the data-based machine learning approaches has advantages in two aspects: modeling and real-time requirements. This paper summarizes the application of machine learning in CPPS cyber security from the perspectives of attack and defense, respectively. The perspective of attack mainly includes three aspects: topology inference, attacking resource optimization, and attack construction. The perspectives of defense mainly include three aspects: security protection, attack detection, and attack mitigation. Finally, the challenges and future research directions in the field of CPPS cyber security are proposed.

This work is supported by National Natural Science Foundation of China (No. 62073285) and Key Program of Zhejiang Provincial Natural Science Foundation of China (No. LZ21F020006).

Key words: power system; cyber-physical system (CPS); cyber security; machine learning