第 48 卷 第 11 期：4413-4426　　高电压技术　　Vol.48, No.11: 4413-4426
2022 年 11 月 30 日　　High Voltage Engineering　　November 30, 2022
DOI: 10.13336/j.1003-6520.hve.20220300

基于人工智能的电力系统网络攻击检测研究综述

张　博[1]，刘　绚[1]，于宗超[1]，王文博[1]，金倩倩[2]，李炜键[2]
（1. 湖南大学电气与信息工程学院，长沙 410082；2. 南京南瑞信息通信科技有限公司，南京 210000）

摘　要：随着电力系统中信息域与物理域的深度融合和新型电力系统建设的快速推进，网络攻击已对电力系统安全稳定运行构成巨大威胁，亟需发展电力系统网络攻击检测技术。人工智能技术在数据特征提取、复杂系统建模、非线性问题求解等方面的优势，使其成为了电力系统网络攻击检测的主流方法。论文首先概述了新型电力系统在结构复杂性、信息物理耦合、智能化程度 3 个方面的特征，并分析了新型电力系统在物理层、网络层和应用层可能遭受的网络安全威胁。然后从物理层终端设备、网络层流量、应用层报文和应用层业务系统 4 个方面对基于人工智能的网络攻击检测方法进行了详细综述。最后讨论了新型电力系统中攻击检测、攻击阻断、事后恢复 3 者之间的耦合关系和主动防御技术当前急需解决的问题，并对未来研究方向进行了展望。
关键词：人工智能；新型电力系统；网络攻击；攻击检测；主动防御

Review on Artificial Intelligence-based Network Attack Detection in Power Systems

ZHANG Bo[1], LIU Xuan[1], YU Zongchao[1], WANG Wenbo[1], JIN Qianqian[2], LI Weijian[2]
(1. College of Electrical and Information Engineering, Hunan University, Changsha 410082, China;
2. Nanjing NARI Information & Communication Technology Co., Ltd., Nanjing 210000, China)

Abstract: With the deep integration of cyber domain and physical domain and the fast development of new power systems, cyber attacks pose a severe threat to the safe and reliable operation of power systems, thus it is essential to develop detection methods for cyber attacks. Artificial Intelligence (AI) is recognized as a popular method to detect cyber attacks because of its advantages in extracting data characteristic, modeling complex systems and solving nonlinear systems. This paper first investigates three characteristics of structure complicacy, cyber physical coupling and intelligence in new power systems, and reveals the possible cyber threats that new power systems might encounter in the physical, network and application layers. After that, the AI-based detection methods for cyber attacks in new power systems are reviewed from the perspectives of terminal devices of the physical layer, network layer traffic, packets and business systems in the application layer. Finally, the coupling relationships among attack detection, attack blocking and ex-post recovery are studied, some key technologies of active defense to cyber attacks are discussed, and the corresponding future work are also given.
Key words: artificial intelligence; new power systems; network attacks; attack detection; active defense

0　引言

当前信息侧与物理侧高度耦合的新型电力系统已成为我国能源转型过程中的重要组成部分，同时也是电力系统未来的必然发展趋势[1-3]。新型电力系统具有大量智能终端接入、高新能源供能占比、信息物理高度融合等特点，在促进能源系统低碳化、智能化的同时，也给新型电力系统的安全稳定运行带来了诸多问题。例如，大量智能终端的接入提高了系统智能化水平，同时也给攻击者提供了更多的攻击入口；当高比例新能源系统遭受网络攻击时，分布式电源的随机性、间歇性和波动性将增加连锁故障的发生几率和范围；信息系统与物理系统耦合程度的加深，将增加跨域攻击途径并提高风险传播速度。以上问题不仅严重威胁着系统安全，也给攻击检测带来了较大挑战。人工智能技术因其在数据解析、特征学习、计算速度等方面的优势，成为了当前电力系统网络攻击检测的主流方法。

人工智能技术应用于电力领域始于 20 世纪 80 年代，初期被应用于处理电力系统暂态问题[4-7]，随着网络攻击技术的发展和人工智能技术的进步，已逐渐应用于电力系统网络攻击检测中。人工智能技术在电力系统攻击检测中具有以下优势：1）处理海量异构检测数据时，人工智能技术具有较强的数据降维和非线性拟合能力，能够避免维数灾的出现；2）当攻击样本较少、训练样本不均衡时，人工智能技

术的迁移学习和深度学习能力能够有效提取攻击行为的重要特征；3）针对未知攻击行为难以建模的问题，人工智能技术将复杂的模型看作一个黑箱，通过拟合输入与输出之间的关系，摆脱了繁琐的建模过程，使模型具备检测未知攻击行为的能力。

目前，已有大量基于人工智能技术的电力系统网络攻击检测研究成果，但少有文献对相关研究进行梳理和总结。鉴于此，本文对基于人工智能的攻击检测方法进行了分类综述，并对电力系统主动防御技术进行了展望。本文首先结合新型电力系统的特征，分析了当前电网所面临的网络攻击威胁；然后对人工智能在终端异常检测、流量异常检测、协议报文异常检测、业务系统异常检测 4 个方面的相关研究进行了综述；最后对电力系统网络安全主动防御技术未来的研究方向进行了分析与展望。

1 新型电力系统特征及攻击威胁分析

1.1 新型电力系统特征

构建新型电力系统，其主要目的是支撑“碳达峰、碳中和”目标的实现，是“双碳”目标在电力系统中的具体体现。在新型电力系统构建的过程中，新能源发电占比逐渐增大。同时，为实现电力系统智能化，信息系统与物理系统之间的耦合程度将逐渐增加，新型通信技术和智能技术在系统中的应用范围也将进一步扩大，使得新型电力系统具有以下特征[8]：

1）新型电力系统是含有大量智能终端的复杂巨系统。新能源发电单元单体容量较小，因此在电力系统中数量庞大，目前我国大型新能源厂站超过 4 000 个、分布式发电系统约 170 万个。由于数百万个发电单元的存在，导致与其配套的可编程逻辑控制器(programmable logic controller，PLC)、分散控制系统(distributed control system，DCS)、远程终端单元(remote terminal unit，RTU)、开闭所终端设备(data transfer unit，DTU)等智能终端设备被大量接入到电力系统中。未来，全国集中式和分布式新能源发电单元将达数千万个，运行控制层级也会进一步增多，同时信号数量也将达到数十亿，因此新型电力系统将成为一个多时空尺度、多层级、多智能终端的复杂巨系统。

2）新型电力系统是信息域与物理域高度耦合的信息物理系统。电力系统利用信息网络实现源、网、荷、储之间的互通互联，并通过信息流对功率流的传输进行控制。新型电力系统中新能源的随机性、间歇性和波动性，使得信息域与物理域之间的多个环节和多个过程需要通过高频互动，才能保证系统的安全稳定运行。同时，电力系统向综合能源系统过渡的过程中，电力系统与人类社会活动及其他能源系统之间进行交织耦合，使得新型电力系统演变成为一种高度耦合的信息物理系统，该系统具有信息–物理–社会系统属性。

3）新型电力系统是多种智能技术参与的智慧能源系统。新型电力系统参与智慧能源体系构建的主要目的是应对系统复杂性带来的系统建模难、数据处理能力弱等问题，因此在系统的应用层利用大数据、云计算、人工智能、移动互联、人机交互等新一代信息技术，对能源的全生命周期进行主动监测、智能分析、优化管控、互动共享，实现了能源的安全、高效、绿色、智慧应用。应用层中多种智能技术的参与使得新型电力系统具有多源异构数据挖掘、综合能源管理、供需灵活互动等功能，多种智能技术的应用使新型电力系统成为了智慧能源系统中的重要组成部分。

1.2 新型电力系统攻击威胁分析

新型电力系统中高比例新能源的接入，大量智能终端的使用，信息层与物理层的深度融合以及多种智能技术的介入，虽然能够达到低碳化、智能化的目的，但智能终端的增多，信息流与功率流的频繁交互，应用层与外界交互渠道的增多，也给电力系统带来了终端入侵、网络层入侵、应用层入侵等网络攻击风险。

智能终端的接入给电力系统带来了物理层终端入侵风险。随着新能源厂站数量越来越多，大量非受控智能终端设备被接入到电力系统中，由于非受控智能终端的计算资源受限，因此安全防御能力相对薄弱，为攻击者提供了大量的攻击入口。2014 年，网络安全研究人员成功破解了西班牙电力公司在智能电表中广泛应用的 AES-128(advanced encryption standard-128)加密算法，研究表明智能电表被入侵后，攻击者可以任意修改电表内的所有数据，同时还能以该智能终端为跳板对其他相邻智能终端进行攻击。因此，在智能终端本体安全防御技术没有取得较大进步的情况下，电力系统中智能终端设备的种类更多、数量更大，给电力系统带来的终端入侵的风险也更大。

信息流与功率流的频繁交互，给电力系统带来

了网络层攻击入侵风险。信息域与物理域的深度耦合，源−网−荷−储的频繁交互，控制业务的泛在开放，将导致信息域的网络风险极易跨域传导到物理系统中，进而导致严重的停电事故。2015 年乌克兰大停电的主要原因是黑客通过网络层入侵信息域主控电脑，然后向物理域一次设备发送大量恶意跳闸指令，数小时的大面积断电给乌克兰造成了巨大经济损失。同样，攻击者也可以从物理域反向渗透到信息域中，理论上以网络层为攻击入口或利用网络层频繁连接信息流与功率流的特性，可实现所有层级之间的跨域攻击或邻域攻击。因此，信息系统与物理系统之间的耦合程度越深，交互越频繁，系统网络层遭受攻击入侵的风险就越大。

新型智能技术的应用，增加了电力系统应用层与外界之间互联互通的机会，给电力系统带来了应用层攻击入侵的风险。应用层中大数据、云计算、移动互联、人机交互等新一代信息技术的应用，使得电力系统中的业务系统更加开放，网络暴露面更广；加之部分关键技术的基础理论和体系架构尚不完善，给攻击者提供了更多入侵应用层业务系统的通道。例如，某厂商空调应用程序(application，APP)曾被曝出存在安全漏洞，黑客可以通过该 APP 入侵聚合负荷云平台，从而导致智能空调大批量反复启停等恶性事件发生。此外，以大数据、云计算为技术支撑的智能系统同样会遭受网络攻击，2021 年 10 月攻击者通过智能支付平台进入美国科罗拉多州电力系统的应用层，使得应用层中大部分系统瘫痪并窃取了 25 年的历史数据。因此，电力系统在利用新型智能技术的同时，如果不同步发展相应的网络安全防御技术，就会给系统带来更多的安全隐患。

存在风险即伴随着被网络攻击的可能，如图 1 所示，攻击者可以通过对电力系统物理层、网络层、

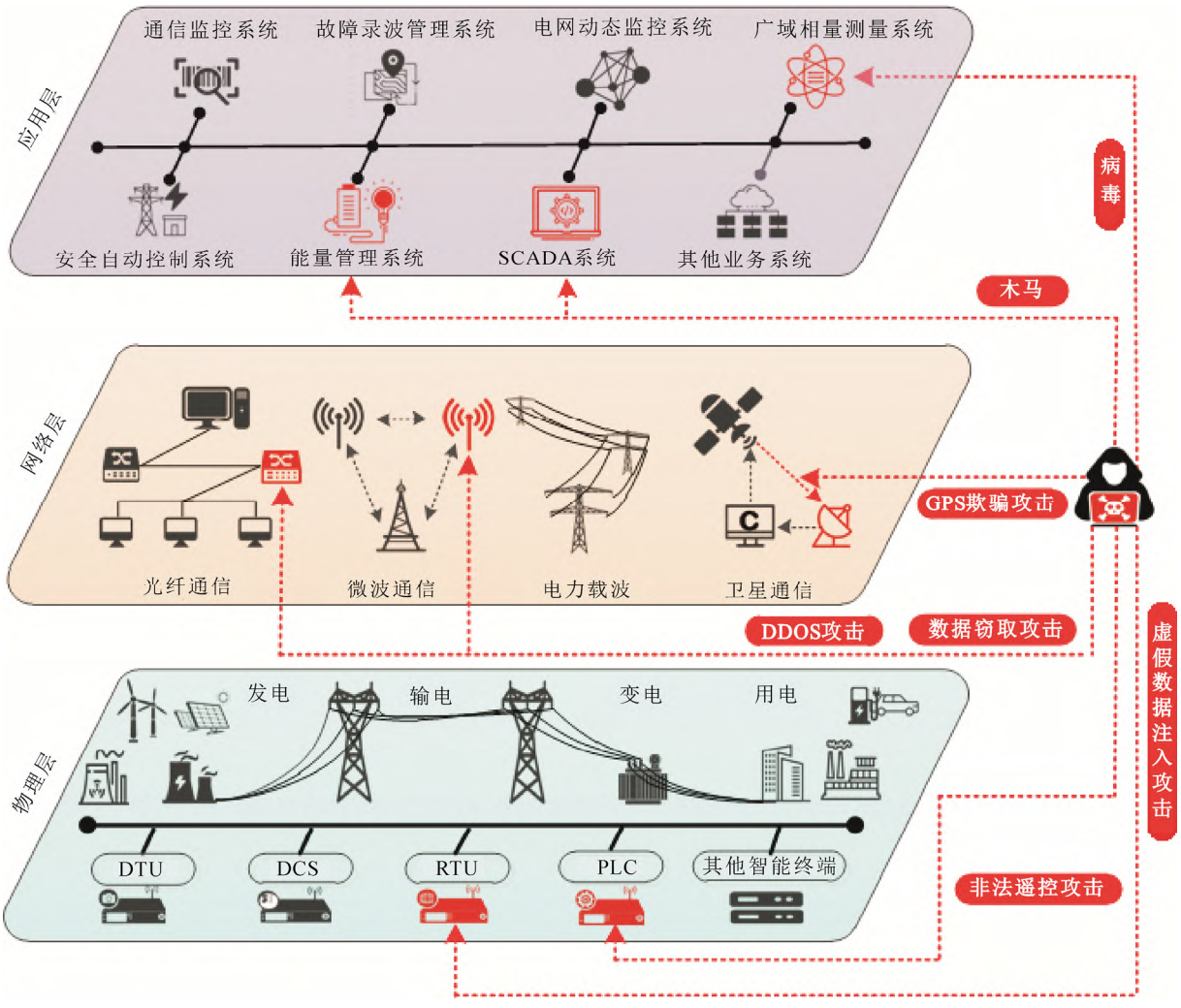

图 1　电力系统网络攻击示意图

Fig.1　Diagram of power system cyber attacks

应用层的入侵实现其攻击目的。物理层的主要攻击对象是各种非受控智能终端设备，由于智能终端设备安全防御能力弱，因此经常被攻击者选为攻击突破口。对网络层的攻击主要通过堵塞信息通路或篡改通信内容间接实现其攻击目的。应用层系统具有较强的防御能力，但其被攻击后对系统的危害最大，因此应用层往往是攻击者最终攻击的目的地。为应对网络攻击，研究人员提出了各种电力系统网络攻击检测方法，其中基于人工智能的检测方法应用最广泛。

2 基于人工智能的攻击检测综述

20 世纪 80 年代人工智能技术开始应用于电力系统，随后分别在能源预测、电力系统及综合能源系统规划、电力系统运行优化及稳定控制、电力信息物理系统网络安全等领域取得了较好的应用效果。尤其在网络安全方面，人工智能技术所具有的应对高维、时变、非线性等问题的强优化处理能力和强大的学习能力，可有效解决电力系统网络攻击检测面临的各种挑战[9]。首先，新型电力系统是结构复杂度高、技术涉及领域广、设备种类繁多的复杂综合能源系统，单纯的建模分析方法已经无法满足综合能源系统对网络攻击检测的要求；人工智能技术具有较强的自学习和迁移学习能力，能够对复杂系统进行精准分析，为解决该问题提供了有效途径。其次，为保障系统运行稳定、经济节能和智能化管理，越来越多的智能终端被应用于电力系统中，形成了类型广、体量大、维度高的攻击检测数据资源。分析处理多源异构数据，并挖掘隐藏在海量数据背后的攻击逻辑，需要通过人工智能技术中的数据降维、特征提取等功能来实现。最后，人工智能技术对模型依赖程度低，可用于未知攻击行为的检测。

综上，人工智能技术已在电力系统网络攻击检测领域得到了广泛应用。人工智能技术能够根据终端设备的监测数据、网络层流量的统计特征、应用层传输报文内容和应用层业务系统状态，对系统是否遭受网络攻击进行精准判断。本文根据攻击切入点的不同，将基于人工智能的电力系统网络攻击检测方法分为物理层智能终端攻击检测、网络层流量攻击检测、应用层协议攻击检测和应用层业务系统攻击检测 4 类，并对这 4 类检测方法进行了详细综述，检测方法分类如表 1 所示。

表 1 检测方法分类

Table 1 Classification of detection methods

攻击切入点	检测方法/对象分类	文献
物理层终端设备	非法接入攻击	[10-13]
	时间同步攻击	[14-17]
	无线攻击	[18-20]
	窃电攻击	[21-23]
	其他类攻击	[24-25]
网络层网络流量	神经网络	[26-29]
	支持向量机	[30-32]
	聚类分析	[33-36]
	其他机器学习方法	[37-39]
应用层通信协议	有监督	[41-47]
	半监督	[48-53]
	无监督	[54-58]
应用层业务系统	WAMS 系统	[59-61]
	SCADA 系统	[62-67]
	AGC 系统	[68-74]
	其他业务系统	[75-76]

2.1 物理层终端设备攻击行为检测

智能终端设备作为电力系统物理层的重要组成部分，承载着数据实时测量、设备精准遥控(遥调)等功能。随着能源互联网建设的快速推进，各种智能终端设备被接入到电力系统中，在提高信息交互的同时，也给系统网络安全带来了以下问题：

1）智能终端设备数量庞大，且部分设备数据传输实时性要求高，难以应用加密措施保护数据。

2）智能终端设备分布广，终端设备分布于各种业务系统中，难以实现统一安全防护。

3）智能终端设备种类多，多源异构的智能终端设备接入系统后会增加系统的漏洞种类和数量，给攻击者提供了更多的攻击入口。

由于以上风险的存在，电力终端设备经常遭受非法接入攻击、时间同步攻击、无线攻击、窃电攻击等各类攻击，针对这些攻击行为，研究人员也提出了一系列基于人工智能的终端设备攻击检测方法。

针对智能终端设备的非法接入，文献[10]应用前馈人工神经网络，对数据库非法链接行为进行检测，并与文献[11]和文献[12]的检测结果进行了比较，对比结果表明，文献[10]中所提方法的检测精度优于对比文献，且该方法在部分类型数据库攻击检测中的准确率可进一步提升。虽然智能终端都位于内网，与外网进行了严格的物理隔离，但部分终端的运维依然需要远程操作，而远程外联极容易将病毒、非法文件传入安全区。文献[13]针对设备运

维时的非法外联攻击，利用改进深度置信网络对电力系统智能终端外联数据进行实时监测，可实现对远程非法外联攻击的快速识别。文献[10-13]针对智能终端遭受的本地非法接入攻击和远程非法外联攻击进行了快速且准确的检测，可避免攻击者以智能终端为直接攻击对象影响系统业务，或以智能终端为跳板入侵上级控制系统而造成更大的系统危害。

除了非法接入攻击，电力终端还面临着时间同步攻击的巨大威胁。由于终端设备所接收的时间同步信号源来自全球定位系统(global positioning system，GPS)/北斗卫星的非加密民码时间同步报文，极容易被攻击者截获、解析和伪造，导致终端设备时间错误[77]。电网终端设备应用时间同步技术的初期，国内外技术标准仅对时间同步装置(系统)的电气性能、抗环境干扰能力等基本性能提出了要求，并未考虑终端设备遭受时间同步攻击后对系统运行的影响[78-80]。文献[14]利用蒙特卡洛模拟法，验证了 0.2 μs 的时间同步攻击输出可以使雷电定位装置的定位误差扩大至正常误差的 3.16 倍。文献[15]利用伪基站以电缆和空气为传输介质对同步相量测量装置(phasor measurement unit，PMU)中的时间接收机进行 GPS 欺骗攻击，结果表明应用低成本攻击设备就可以完成电力终端设备参考时间的更改，同时还可以使上级系统出现状态估计混乱的问题。文献[14]和文献[15]从攻击者的角度验证了时间同步攻击对电力系统造成破坏的可能性和经济性，同时说明了对该类攻击检测方法研究的重要意义。为实现时间同步攻击的检测，文献[16]提出一种基于超平面聚类的 PMU 时间同步攻击检测方法，利用超平面聚类将相位差集合进行分类，并将计算电抗值与实际电抗值进行比较，从而判断被攻击的 PMU 节点。当相角误差较大时，该方法对时间同步攻击检测的准确率和算法收敛性均优于 K 均值聚类算法(K-means clustering algorithm，K-means)和模糊 C 均值聚类算法，但相角误差较小时，该方法对正常数据与攻击数据的区分能力变弱。为了适用于更多的检测环境，文献[17]提出一种能应用于三相不平衡系统的时间同步攻击检测模型，该模型解决了传统方法在三相不平衡系统中对设备进行时间同步攻击检测不适用的问题，提升了人工智能技术在终端设备时间同步攻击检测中的应用潜力。

随着 5G 技术的逐渐成熟和大量电力物联网终端的接入，无线通信将成为配网侧主要的信息传输方式之一[81-82]。电力系统中的大量配网终端采用无线虚拟专网进行通信，因此电力终端存在被非法无线入侵的风险。文献[18]根据电力终端与无线通信基站的空间坐标相对固定且两者之间信号强度具有稳定的时间特性和空间特性这一特点，应用密度聚类方法对终端与真/伪基站之间的历史信号强度数据进行检测，可快速计算出伪基站的攻击坐标。文献[19]利用双隐马尔可夫模型识别无线终端的攻击行为，该模型解决了使用单个隐马尔科夫模型的入侵检测系统中高维数据计算复杂的难题。由于电力终端设备普遍具有计算资源受限的特性，因此以上方法仅能应用于具有较高数据处理能力的终端设备中。为解决人工智能在终端攻击检测中的普适性问题，文献[20]利用无线发射装置与电力终端之间的通信互异性，将终端设备需要完成的检测学习任务转移到基站中完成，降低了对终端设备算力、储存、能耗等方面的要求，扩大了人工智能技术在无线攻击检测领域中的应用范围。在攻击者的身份识别方面该方法也具有较高的精确度。

窃电攻击是造成电网非技术性经济损失的主要原因[83-85]，传统窃电攻击主要通过线路绕行、手动篡改电表数据等方式进行，智能电表的普及为窃电攻击提供了新的途径。早期窃电检测方法存在对先验知识依赖度高、检测精度低等缺点，为了摆脱先验知识的束缚并提高检测精度，部分研究人员提出了利用人工智能技术进行窃电攻击行为检测的想法[86]。文献[21]利用宽度卷积神经网络和深度卷积神经网络分别对长期数据和短期数据特性进行 2 维学习，该模型综合了宽度分量和深度分量的优点，具有良好的盗电检测性能。文献[22]利用长短期记忆网络和多层感知器构建混合深度神经网络窃电检测模型，摆脱了对先验知识的束缚，应用少量历史数据就可以完成高精度模型的训练。除负荷节点存在被网络攻击风险以外，分布式发电节点的智能终端同样存在被窃电攻击的可能，攻击者通过入侵智能电表，更改分布式电源向电网输送电能的质量参数，从而向电网索取更高的费用。为解决该问题，文献[23]通过深度卷积−循环神经网络对分布式智能电表、气象报告和数据采集与监视控制系统(supervisory control and data acquisition，SCADA)测点的各种数据经行训练，可以达到检出率(99.3%)和误报率(0.22%)的高精度窃电攻击检测。

除以上攻击外，电力终端在特定情况下还会遭

受谐振攻击、软件攻击等。负荷频率控制器被网络入侵后，会造成电力系统谐振，文献[24]搭建了攻击环境，验证了谐振攻击的可能性，并发现谐振攻击可以在一个区域内传播到其他相互连通的区域，但该文献未提出谐振攻击的检测办法。文献[25]针对软件攻击提出了一种基于长短期记忆神经网络的终端软件监测方法，能够对电力物联网中充电桩的应用程序进行正常状态和攻击状态的识别。

以上文献研究表明，应用于电力系统终端设备攻击检测的人工智能技术，不仅实现了对多种攻击行为的精准识别，还克服了终端设备算力小、分布广、数量大、异构性强等原因造成的攻击检测难题。与其他方法相比，人工智能技术在实际应用中的数据挖掘能力更强、适用范围更广、发展潜力更大。

2.2 网络层流量攻击行为检测

当电力系统遭受网络攻击时，网络流量会出现突增、突减、延迟等异常现象。基于网络层流量特征的异常检测方法，主要利用历史流量的峰值、均值、包最大(小)间隔、频率等特征建立网络层流量基线模型，并将当前流量特征与训练好的正常模型或异常模型进行比较，以检测当前系统是否遭受网络攻击。根据报文的流量特征进行攻击检测，避免了对业务流量解析的繁琐步骤和过多先验知识的限制，因此基于流量特征的攻击检测方法具有实时性高、迁移性好的优点。

但是，随着通信流量越来越大，各系统之间的交互机理越来越复杂，传统异常流量检测方法存在检测率低的问题，已无法满足新型电力系统对攻击检测的需求。为了提高异常流量检测精度，研究人员将人工智能技术应用于异常流量检测领域中，目前主要包括神经网络、支持向量机、聚类 3 种人工智能算法，本节将对这 3 种主流方法和部分其他方法进行综述。

神经网络具有较好的学习能力，因此被较早地应用于电力工控系统网络流量异常检测中。文献[26]利用神经网络对正常流量和分布式拒绝服务攻击(distributed denial of service attack，DDOS)攻击流量进行训练，获得了正常基线模型和攻击模型，该方法对 DDOS 攻击具有较高的检测率。随后，研究人员又将深度学习应用于流量异常检测中，文献[27]研究了深度学习算法在入侵检测系统中的适用性，与卷积神经网络、自编码器、循环神经网络等浅层神经网络方法相比，深度学习在流量异常检测方面的优势更明显。在深度学习的基础上，文献[28]进一步提出了一种基于深度交叉学习的入侵检测方法，通过并行交叉卷积神经网络的 2 个分支神经网络，可实现在训练样本较少情况下的流量特征学习，提高了少样本情况下的攻击检测率。文献[26-28]利用神经网络对流量异常攻击行为进行检测，能够保证在样本差异较大的情况下完成高精度检测，但所检测的攻击均为已知攻击类型，当网络层遭受新型未知攻击时，以上方法对新型攻击的检测能力会变弱甚至消失。文献[29]利用迁移学习，实现了短时间内对未知攻击的检测，弥补了其他神经网络方法无法检测新型攻击的不足。

与神经网络几乎同时应用于电力系统网络流量异常检测的人工智能方法还有支持向量机。文献[30]利用支持向量机中的风险函数和损失函数，将回归值与正常值之间的残差放大，处理后的残差集合能较明显地反映异常报文与正常报文之间的差异。为了提高支持向量机算法的检测精度，文献[31]利用优化后的支持向量机模型对智能变电站中各路由器端口的输入输出流量进行分类，该方法对拒绝服务(denial of service，DOS)、U2R(user to root)、Probing、R2L(remote to local)攻击和部分未知攻击的检测率高于支持向量机模型。为进一步提高支持向量机的特征提取能力，文献[32]先利用小波包分解等方法对流量进行时域和频域的特征提取，再利用人工蜂群优化的支持向量机算法对异常流量和正常流量进行识别分类，该方法在攻击检测前对流量数据进行变换处理，能深度挖掘攻击时流量的潜在特征，既可以提高攻击检测的准确率，又可以缩短攻击检测时间。

除神经网络与支持向量机以外，聚类分析同样被广泛应用于电力系统流量异常检测中。文献[33]应用密度聚类方法区分正常流量和异常流量，该方法在初值选取较好的情况下具有较高的攻击检测率，但初值选取不当会出现分类异常的情况。为解决聚类算法对初值敏感的问题，文献[34]将流量特征的属性值转换为熵，然后利用改进初值选取方法的 *K*-means 聚类对属性的熵值进行分类，该方法能够减小聚类分析对初值的敏感程度。同样以流量属性熵值为输入，文献[35]则利用聚类分析与支持向量机的混合模型完成异常流量的检测，该模型对已知攻击行为检测的准确率和未知攻击行为的检出能力均优于传统 *K*-means 聚类算法，为聚类算法适用

于攻击检测提供了新的解决方案。文献[33-35]对所提方法的有效性进行评估时，其主要指标均为准确率和检出率，忽略了过长检测时间对防御效果的影响。文献[36]侧重于检测方法的实时性，为了能够快速检测攻击，先应用统计分析检测出异常频率的流量，然后再应用聚类检测异常流量的属性并判断异常类型，该方法误报率低，实时性高，但检出率较低。

除以上主流方法外，部分学者还提出了其他基于人工智能的网络层流量异常检测方法。文献[37]和文献[38]分别利用经验模态分解算法和深度迁移模型完成异常流量检测，2 种方法均能在训练样本较少的情况下实现攻击检测的高准确率和高检出率。文献[39]提出一种基于信息物理融合的差分序列检测法，用以实现新型智能变电站过程层网络异常流量的检测，该方法充分考虑了智能变电站信息系统与物理系统的融合特性，适用场景具有较强的针对性。

以上文献研究表明，应用于网络层流量攻击行为检测的人工智能技术，以神经网络、支持向量机和聚类为主。3 类方法中神经网络的计算复杂度最高，可适用于算力较强的检测环境，其他 2 类算法的计算复杂度因模型参数的选择而不同，可根据具体应用环境合理选择。与基于专家知识的传统方法相比，人工智能技术对流量特征的提取能力更强、对先验知识的依赖性更低，在流量异常检测中有较好的研究前景。

2.3　应用层通信协议攻击行为检测

利用网络层的流量统计特征进行攻击检测，对专家知识要求低且方法兼容性较好，但由于对流量的解析深度不足，因此对虚假数据注入类攻击，尤其是高隐身虚假数据注入攻击的检测能力较弱。不同于网络层流量异常检测方法，基于应用层通信协议的异常流量检测，能够实现对报文的深度分析并提取报文的应用层特征，实现流量的深度检测。但该类方法对先验知识和训练数据集的完整性、真实性要求较高，因此初期应用于应用层报文异常检测的人工智能方法多为有监督学习，随着对攻击机理和人工智能算法的深入研究，检测方法已完成从有监督学习向半监督学习的过渡，并且部分学者已致力于研究高检测精度、高实时性的无监督检测方法。

初期，研究人员应用人工解析的方法提取报文中字段之间的耦合关系，文献[40]基于对面向对象变电站通用事件(generic object oriented substation event，GOOSE)、采样值(sampled value，SV)报文的解析可以准确地检测出异常报文。但基于人工协议解析的检测方法需要较强的专业知识才能建立正常报文模型和异常报文模型，且人工提取报文中字段特征时会出现字段耦合关系提取不全、字段耦合错误等情况。因此，研究人员试图应用基于监督学习的人工智能方法进行协议字段关系的提取，进而判断电力系统是否遭受网络攻击。基于有监督学习的检测方法仅需将每帧报文进行简单打标，无需深度解析就能提取报文之间的耦合关系。文献[41]将同步相量测量装置(phasor measurement unit，PMU)报文和日志输入随机森林模型中，通过该模型进行攻击检测能达到 93.91%的正确率和 93.6%的检测率。文献[42]利用深度置信网络对 IEC61850、IEC104、IEC103 等电力传输协议报文进行攻击检测，该方法在多种攻击和大量噪音影响的情况下，依然具有较高的检测率。为了进一步提高攻击检测率和正确率，部分研究试图摆脱单一算法建模的方式，将 2 种算法混合，旨在得到更精准的检测模型。文献[43]将决策树与长短期记忆神经网络相结合，提出一种基于序列分解重构的双层神经网络架构，能精确寻找 PMU 数据中的攻击数据并清除。文献[44]先将协议报文进行小波分解提取更多的协议特征，然后再用深度神经网络对所提取特征进行学习，该方法从时间特征和空间特征 2 个方面对攻击行为进行挖掘，对高隐身虚假数据注入攻击的识别能力优于传统深度学习方法。

以上方法具备较高准确率和检测率的前提是，拥有完整且大量的训练数据集，但从实际运行的电力系统中得到完整的攻击报文比较困难。文献[45]考虑到正常样本、故障样本和攻击样本之间可能存在的数据不平衡情况，利用基于集成学习的极端梯度增强分类器来提高数据的平衡性，该方法在攻击样本较少的情况下依然具有较好的检测性能。然而，将攻击检测方法应用到实际电力系统中除了需要克服训练样本不均衡问题，还需要考虑系统对检测实时性要求高和攻击溯源等问题。文献[46]利用基于贝叶斯的近似滤波器减少了通信开销和时间复杂度，提高了监控系统网络攻击检测的实时性和免疫力。为了寻找准确的攻击注入位置，文献[47]提出了一种基于深度学习的攻击位置检测模型，该模型可以实时检测虚假数据注入的精确位置。文献

[45-47]为克服训练样本不均衡、攻击检测实时性要求高、攻击注入点难以精确定位等问题，均采用有监督的人工智能方法进行攻击检测，该类方法对专家知识有极强的依赖性，不利于大范围推广。

为了减少有监督学习对先验知识的依赖，部分学者将半监督学习引入到电力系统网络攻击检测中。文献[48]搭建了基于协议分析仪和 RTU 硬件的半监督检测算法的网络攻击仿真实验平台，并验证了半监督学习在攻击检测中的可行性，为半监督学习在应用层通信协议攻击行为检测中的应用提供了重要参考依据。文献[49]将半监督支持向量机算法与状态向量估计方法进行攻击检测比较，结果表明该方法对数据的稀疏程度具有更强的鲁棒性，同时说明了半监督学习在稀疏数据处理中的优势。文献[50]提出一种基于集成学习的半监督攻击检测模型，该模型由有监督分类器和无监督分类器组成，充分利用了 2 种分类器的优势，在保证检测精度不变的同时降低了对经验知识的依赖。文献[48-50]虽然能在高检测率下利用半监督学习减少打标量，但依然不能完全摆脱打标质量对检测结果的影响。文献[51]利用半监督的 *K*-means 聚类对不同攻击模式信息进行学习和在线应用时发现，检测率和攻击类型识别的成功率严重依赖于原始训练样本的打标质量。为了向训练样本不打标的目标靠近，文献[52]提出的半监督深度学习方法只需要对少量的标注数据和大量的未标注数据进行训练，就能实现对网络攻击行为的高精度检测。文献[48-52]均以交流系统为研究背景，并未考虑直流系统特性对攻击检测的影响，文献[53]提出了一种基于混合高斯分布的半监督学习模型，用于检测直流输电系统中的网络攻击与状态估计。与支持向量机等 3 种智能算法相比，该混合模型训练时间较长，但在检测精度和检测速度方面均具有较强优势。

基于有监督学习和半监督学习的人工智能算法，其训练和测试数据集在静态环境中共享相同的分布和相同的类标签。当系统动态变化时，数据打标方式也会发生变化，因此利用打标方式训练过的检测模型可能不再适用于复杂的攻击场景。基于无监督的攻击检测方法[87-88]可以摆脱标签的束缚，自主完成报文之间逻辑关系的学习。为实现对通信协议报文的无监督学习，文献[54]提出一种对抗迁移学习框架，在报文与系统参数之间建立了映射关系，借助系统参数和拓扑结构实现对攻击特征的无监督学习。文献[55]先采用主成份分析来减少数据集的维数，然后利用模糊 C 均值聚类算法实现对攻击报文的无监督检测，该方法在拓扑变化后也能检测到网络攻击行为。虽然文献[54]和文献[55]实现了对报文的无监督学习，但是依然需要系统参数和拓扑结构作为辅助检测信息。为实现无监督学习的纯数据驱动，文献[56]和文献[57]利用局部离群因子分析技术，实现了在不需要系统模型信息情况下的网络攻击无监督检测。摆脱对打标签和系统参数依赖的无监督检测方法，普遍存在计算复杂度高的特性，为了降低检测过程中数据的计算和存储成本，文献[58]提出了一种基于隔离森林的攻击数据和低质量数据的无监督检测方法，该方法在一定程度上减少了在线检测时的计算压力。

以上文献研究表明，应用于应用层通信协议攻击行为检测的人工智能技术，已从初期的有监督学习为主过渡到以半监督学习为主。减少对专家知识的依赖可增加算法的移植性和对高隐身攻击的检测能力，目前部分学者对基于无监督学习的攻击检测方法进行了初步探索，未来基于无监督学习的人工智能算法将取代半监督学习，成为应用层协议攻击检测的主流方法。

2.4 应用层业务系统攻击行为检测

基于应用层协议异常的检测方法可以完成对绝大部分针对应用层发起的网络攻击检测，但随着攻击技术的发展，电力系统遭受的网络攻击已出现针对应用层业务系统的定制化攻击特征。应用层业务系统虽然安全防御等级较高，但依然存在安全漏洞，应用层系统一旦被攻击，将给电力系统带来严重危害。目前研究人员对广域测量系统(wide area measurement system，WAMS)系统、SCADA 系统和自动发电控制系统这 3 类业务系统的攻击检测方法研究成果较多，因此本节重点综述这 3 类系统的攻击检测方法。

WAMS 系统中的设备数量庞大且异构特征明显，大量的异构设备经常出现自然故障，导致系统难以区分网络攻击和自然故障。文献[59]应用规则学习算法可以实现 WAMS 系统异常后对网络攻击和系统自然故障的区分，同时该方法还可以处理 WAMS 系统的大型异构数据集，具有较高的分类精度、较低的误报率和较高的实时性。与文献[59]不同，文献[60]应用决策树来实现 WAMS 系统中网络攻击和系统自然故障的区分，其二分类准确率可达

98%，同时对 45 种网络攻击可实现高精度的多分类。该模型具有内存占用少、评估速度快的优点，可实现 WAMS 系统网络攻击行为的在线实时检测。文献[61]提出了一种基于递归贝叶斯滤波器的解决方案，该方案可以在部分数据丢失的情况下完成 WAMS 系统的攻击检测。

近年来，电力 SCADA 系统经历了多次升级，由最初的独立运行到现在的联网运行，更智能化的同时也给 SCADA 系统带来了更大的网络安全威胁。SCADA 系统主要完成遥测、遥信、遥控、遥调 4 项功能，攻击者的目的是破坏其 4 遥功能，以影响电力系统正常运行。

针对遥测和遥信功能的攻击主要为虚假数据注入攻击，攻击者通过改变 SCADA 系统中或即将传入系统的遥测、遥信数据来扰乱主站对系统和控制节点的状态估计。2009 年文献[62]首次提出了虚假数据注入攻击的概念，并对虚假数据注入攻击对系统状态估计的影响机理进行了详细阐述。文献[63]考虑到历史数据不受虚假数据注入攻击的影响，利用无迹卡尔曼滤波对负荷进行预测，可以显著降低虚假数据注入对系统状态估计的影响。文献[63]仅考虑了如何降低虚假数据对状态估计的影响，但未考虑在检测攻击的同时确定攻击的注入点。文献[64]首次将图神经网络应用到虚假数据注入攻击检测中，该方法利用拓扑与测量数据的空间相关性，能精准地确定虚假数据注入攻击的攻击位置。文献[63]和文献[64]针对虚假数据注入攻击的准确检测和攻击位置的精准识别进行了较为深入的研究，但对高隐身虚假数据注入攻击的检测能力不足问题，尚需进一步加强。

对遥控功能的攻击主要是对遥控指令进行篡改和破坏，或者直接伪造虚假指令，从而干扰和破坏遥控业务的执行。文献[65]分别将朴素贝叶斯、支持向量机和 K 近邻算法应用于遥控攻击检测中，研究结果表明在同等环境下，基于朴素贝叶斯的检测方法在准确率和检出率方面均优于其他算法。但该方法仅在单条线路被攻击时有较好的应用效果，为克服该局限性，文献[66]将前馈神经网络与贝叶斯算法相结合，并通过优化模型进行有效的边际推理，解决了由于指数级中断假设而导致的计算复杂度高的难题，实现了对多条线路中断的准确识别。

遥调指令攻击主要通过更改 SCADA 系统中的调整指令对变压器档位、设备参数等进行恶意调节，从而对系统的运行产生不利影响。目前已有少量针对变压器非法调档的攻击检测，文献[67]以支路或节点注入电流与终端电压的比值为指标，对移相变压器进行网络攻击检测。相关文献对虚假遥调指令攻击行为的检出率较高，但在准确率方面表现较差，主要原因是现有方法无法对自然故障和攻击行为进行精准的区分。目前针对基于人工智能技术的虚假遥调指令攻击检测的相关研究较少，所以人工智能技术在该领域的研究潜力尚需挖掘。

自动发电控制系统(automatic generation control，AGC)是电力系统中较少人为干预的闭环控制系统之一[89]，该系统主要通过终端智能设备的量测值和调度中心的控制指令计算区域控制偏差量(area control error，ACE)，进而调整发电机组输出功率，使系统处于功率平衡的稳定状态。由于系统输入数据均需网络传输，因此 AGC 存在被网络攻击的风险，当 AGC 的输入数据和传递函数被网络攻击后，会导致 AGC 对发电机组发出错误的控制指令，从而严重破坏电力系统的安全稳定运行[90-92]。当前针对 AGC 的攻击检测方法主要分为 ACE 预测和 AGC 状态估计 2 类。

在 ACE 预测方面，文献[68]和文献[69]以 ACE 历史数据为输入，利用长短期记忆神经网络来预测下一时间窗口的 ACE 数值，以此判断 AGC 是否遭受网络攻击，该方法利用系统本身存储的 ACE 数据进行预测，避免了传统 ACE 值预测方法对精准负荷预测值的依赖。

在 AGC 状态估计方面，文献[70]提出了一种基于卡尔曼滤波的针对 AGC 的检测方法，该方法基于估计残差实现攻击检测，但该方法将攻击向量作为已知量进行残差估计，而实际操作中攻击量往往是未知量。基于此，文献[71]将攻击向量当作未知量输入卡尔曼滤波模型中，得到了攻击信号和 AGC 系统状态的最小方差无偏估计，并根据估计值调整机组出力平衡系统功率，该方法同时实现了攻击检测与偏差调整。

除以上 2 种主流方法外，部分学者还提出了其他检测方法，文献[72]将 ACE 预测与 AGC 状态估计联合，提出一种数据驱动的双层入侵检测模型，该模型能在多种攻击场景中保持 95%以上的检测精度，在复杂攻击场景中比单层模型的适用性更强。文献[73]对 AGC 可能遭受的各种攻击进行风险评估，然后利用博弈论模型在检测策略库中选取最优

攻击检测方案和防御方案。文献[74]利用层次密度空间聚类方法，训练各种攻击状态下的 AGC 数据模型，从而实现常见攻击的快速检测。当前针对其他业务系统的网络攻击应用人工智能检测的方法研究成果较少，但已对电力市场[75]、安稳控制系统[76]等业务系统的攻击检测进行了初步探索。

以上文献研究表明，系统因业务差异会遭受不同种类的网络攻击，因此应用于业务系统攻击行为检测的人工智能技术需根据业务系统实际特性对检测模型进行定制化处理，通过该处理使得人工智能算法对特定攻击行为的检测针对性更强，在减少计算支出的同时，提升了系统防御能力。应用人工智能技术对业务系统进行定制化的攻击检测，将成为新型电力系统纵深防御体系的重要组成部分。

3 亟需研究的内容及展望

攻击检测技术是电力系统主动防御技术的重要组成部分，与攻击行为应急处置、攻击事后恢复之间具有强耦合关系，其中，高准确率的攻击检测技术可以提高应急处置方案的合理性。同时，准确的应急处置可以加快攻击后电力系统的恢复速度，将系统快速调整至稳态，同时减轻攻击检测压力，提高攻击检测的正确率和检出率。因此，任何一项技术的发展都会推动其他 2 项技术的进步。虽然基于人工智能的网络安全主动防御技术已经取得了一定的研究成果，但攻击技术的不断演变和进化，给电力系统网络安全带来了更多新的挑战。基于前文对当前电力系统网络攻击检测工作的分析，本章对主动防御技术中的攻击行为检测、攻击行为应急处置和攻击事后恢复未来的研究方向进行了展望。

3.1 攻击行为检测

现有基于人工智能技术的攻击行为检测方法，难以区分自然故障和网络攻击，通常将异常统一归算为网络攻击。由于两者的形成机理不同，因此对不同故障的处理手段也存在一定的差异，若不能对两者进行明确区分，将导致防御措施失效的情况出现。单一考虑信息侧数据无法对 2 种故障进行明确区分，因此后续关于检测的研究工作需要充分考虑物理系统与信息系统之间的关联关系，借助物理系统的状态表征参数和运行特性，弥补单一层面检测方法的不足，提高对自然故障和网络攻击的识别能力。

同时，现有方法对于应用层报文的检测深度不足，难以辨识针对应用层精心构造的高隐身攻击向量。攻击者对电力系统实施的高隐身攻击具有高度定制化的特点，其注入的攻击报文所有字段均在正常阈值范围内，能够避开状态估计检测。高隐身攻击的发起者通常具有较丰富的电力专业知识，因此可以对系统的薄弱点发起精准打击，对电力系统安全稳定运行造成巨大损害。所以必须研究针对高隐身攻击的检测方法，避免该类攻击威胁电力系统的的稳定运行。当前无法检测高隐身攻击的主要原因是，现有方法对报文仅能做到网络层和浅应用层解析，对报文之间的深层关系和特征无法识别。因此，后续研究工作中应该利用深度特征提取方法对业务报文进行深层特征提取，然后应用人工智能技术对不同特征进行学习，以实现对高隐身攻击的高精度检测。例如，利用新一代人工智能技术中的迁移学习技术，可以将计算机领域中用于高隐身攻击的成熟检测模型迁移至电力领域中，以提升电力系统对高等级攻击的检测能力。

除以上两点外，现有攻击检测方法还存在对设备数据处理能力要求较高和无法全方位覆盖配网侧的问题，因此后续研发配网侧攻击检测装置时，应充分考虑配网设备计算资源受限的弊端，在保证高准确率的情况下，尽量减少检测算法的计算复杂度，或者采用计算移植等方式减少配网设备的计算开支，以实现高准确率的攻击检测方法在配网中的全覆盖。

3.2 攻击行为应急处置

电力系统现有防御体系中缺少针对攻击行为的差异性应急处置方法，现有针对物理故障的三道防线，由于其继保动作、切机切负荷、系统解列的动作标准完全依赖于物理系统中电压、电流、功率、频率偏差大小等物理参数，因此现有三道防线无法有效阻止网络攻击。同时，信息域的一键查杀式网络封堵不仅会阻断正常节点的运行，还会因为封堵范围不当而导致攻击行为持续渗透。

后续研究中，一方面应参考物理域故障阻断的思想，研究针对网络攻击的多级阻断技术，结合网络攻击过程中攻击行为的时序特性，利用物理域与信息域之间的协同关系，杜绝一键查杀式的封堵技术对正常业务的影响。另一方面，还应将提高攻击预测方法的准确率作为重要研究方向。准确的攻击行为预测是进行多级阻断的重要依据，现有应用于电力系统的攻击预测方法均由 IT 领域网络攻击预测方法迁移而来，这些方法仅考虑了攻击过程中的

网络特性，并未考虑攻击过程中电力信息网络与物理网络之间的交互过程，所以检测的准确率较低。因此，应充分考虑电力系统网络攻击特性，建立融合电力业务特征的网络攻击预测模型，以提高预测精度。

3.3　攻击事后恢复

当电力系统遭受网络攻击后会导致大面积停电甚至系统崩溃，大停电后如果不能进行快速有序的恢复供电，将增加停电带来的经济损失和政治影响，甚至引发社会恐慌。虽然大停电事故后可以实施黑启动方案，但现有的串行恢复方案和并行恢复方案在实施过程中，会出现线路合环困难、配电系统并网失败、继电保护装置多次合闸操作不成功等问题。此时，急需通信系统提供及时且可靠的系统参数，帮助物理系统快速恢复供电。但是，由网络攻击导致的大停电与物理故障造成的停电机理不同，网络攻击会直接影响系统状态的可观性和控制设备的可控性。数据的不可观和设备的不可控，将直接导致自启动失败、错失最佳恢复时间、设备的重复性启动损伤、人员安全威胁等问题出现。

同时，在攻击恢复过程中，节点的恢复顺序将直接影响电力系统进入稳态的速度和稳定程度。恢复顺序应根据节点对系统稳态影响的程度来确定，而该节点重要度的计算方法不能仅以节点所承载的业务为指标，还应该充分考虑攻击特性和系统中信息域与物理域的耦合特性，综合得出最优节点恢复顺序，使系统快速达到鲁棒性较强的稳定状态。

因此，未来关于网络攻击引起的大停电事后恢复，应充分考虑通信网络的恢复对物理网络恢复的影响，具体研究应侧重于以下几个方面：

1）信息网络与物理网络协同恢复过程中交互机理的研究。

2）信息网络恢复过程中，最优恢复路径选择方法的研究。

3）物理系统恢复过程中，一次设备最佳合闸时间和最佳并网时间的研究。

4）节点恢复过程中，考虑最优恢复顺序的节点重要度计算方法研究。

只有对信息网和物理网进行协同的最优恢复，才能得到最佳的事后供能恢复效果。

4　结论

针对人工智能技术在电力系统网络攻击检测中的应用，本文从终端设备、网络流量、协议报文、业务系统 4 个方面对现有研究成果进行了综述，并得出以下结论：

1）本文根据新型电力系统具有智能终端设备繁多、信息域与物理域耦合程度较深、多种智能技术参与的 3 大特征，从物理层、网络层和应用层 3 个层级对系统面临的攻击威胁进行了分析。其中大量智能终端的接入，给攻击者提供了更多进入物理层的通道；双域的深度耦合，不仅增加了网络层传输的负担，同时也给攻击者提供了更多数据窃取的机会；多种新型智能技术在应用层中的应用，给新型网络攻击提供了新的攻击场景。

2）本文首次将电力领域中基于人工智能技术的网络攻击检测方法分为物理层终端设备攻击行为检测方法、网络层流量攻击行为检测方法、应用层通信协议攻击行为检测方法和应用层业务系统攻击行为检测方法 4 类。根据攻击切入点的不同，对检测方法进行分类，不仅能够从攻击者视角清晰地区分检测方法，还能保证现有方法总体框架的完整性。该分类思想为电力系统攻击检测方法提供了新的分类思路。

3）本文除对已知检测方法进行综述外，还对现存问题和未来研究方向进行了展望。文中指出了现有方法在自然故障和网络攻击区分、高隐身攻击检测、配网检测算法优化 3 个方面存在的问题，同时还强调了攻击行为检测与攻击行为应急处置、攻击事后恢复之间的强耦合关系，以及后两者技术发展对攻击检测技术的影响。由此可知，人工智能检测算法应该不断优化更新，以应对更复杂的工作环境和更多的新型网络攻击。

参考文献　References

[1] 辛保安，单葆国，李琼慧，等. “双碳”目标下“能源三要素”再思考[J]. 中国电机工程学报，2022，42(9)：3117-3125.
XIN Baoan, SHAN Baoguo, LI Qionghui, et al. Rethinking of the “three elements of energy” toward carbon peak and carbon neutrality[J]. Proceedings of the CSEE, 2022, 42(9): 3117-3125.

[2] 黄雨涵，丁　涛，李雨婷，等. 碳中和背景下能源低碳化技术综述及对新型电力系统发展的启示[J]. 中国电机工程学报，2021，41(增刊 1)：28-51.
HUANG Yuhan, DING Tao, LI Yuting, et al. Decarbonization technologies and inspirations for the development of novel power systems in the context of carbon neutrality[J]. Proceedings of the CSEE, 2021, 41(Supplement1): 28-51.

[3] 康重庆，姚良忠. 高比例可再生能源电力系统的关键科学问题与理论研究框架[J]. 电力系统自动化，2017，41(9)：2-11.
KANG Chongqing, YAO Liangzhong. Key scientific issues and theoretical research framework for power systems with high proportion of renewable energy[J]. Automation of Electric Power Systems, 2017, 41(9): 2-11.

[4] YIN X F, ZHU Y M, HU J K. A subgrid-oriented privacy-preserving microservice framework based on deep neural network for false data injection attack detection in smart grids[J]. IEEE Transactions on Industrial Informatics, 2022, 18(3): 1957-1967.
[5] MUSLEH A S, GUO C, ZHAO Y D. A survey on the detection algorithms for false data injection attacks in smart grids[J]. IEEE Transactions on Smart Grid, 2020, 11(3): 2218-2234.
[6] 汤 奕，崔 晗，李 峰，等. 人工智能在电力系统暂态问题中的应用综述[J]. 中国电机工程学报，2019，39(1)：2-13.
TANG Yi, CUI Han, LI Feng, et al. Review on artificial intelligence in power system transient stability analysis[J]. Proceedings of the CSEE, 2019, 39(1): 2-13.
[7] AKIMOTO Y, TANAKA H, YOSHIZAWA J, et al. Transient stability expert system[J]. IEEE Transactions on Power Systems, 1989, 4(1): 312-320.
[8] 郭剑波. 新型电力系统特征与发展挑战[R]. 兰州：国家电网有限公司，2021.
GUO Jianbo. Characteristics and development challenges of new power systems[R]. Lanzhou, China: State Grid Corporation of China, 2021.
[9] 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.
[10] 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.
[11] VALENZUELA J, WANG J H, BISSINGER N. Real-time intrusion detection in power system operations[J]. IEEE Transactions on Power Systems, 2013, 28(2): 1052-1062.
[12] MOUSAVIAN S, VALENZUELA J, WANG J H. Real-time data reassurance in electrical power systems based on artificial neural networks[J]. Electric Power Systems Research, 2013, 96: 285-295.
[13] LÜ Z N, HU Z H, NING B F, et al. Non-intrusive runtime monitoring for power system intelligent terminal based on improved deep belief networks (I-DBN)[C]//Proceedings of the 2019 4th International Conference on Power and Renewable Energy. Chengdu, China: IEEE, 2019: 361-365.
[14] 刘 亮，苏 盛，陈晓国，等. 时间同步攻击对雷电定位系统的影响与分析[J]. 高电压技术，2020，46(12)：4319-4325.
LIU Liang, SU Sheng, CHEN Xiaoguo, et al. Influence and analysis of time synchronization attack on lightning location system[J]. High Voltage Engineering, 2020, 46(12): 4319-4325.
[15] SHEPARD D P, HUMPHREYS T E, FANSLER A A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks[J]. International Journal of Critical Infrastructure Protection, 2012, 5(3/4): 146-153.
[16] XUE A C, LENG S, LI Y C, et al. A novel method for screening the PMU phase angle difference data based on hyperplane clustering[J]. IEEE Access, 2019, 7: 97177-97186.
[17] DELCOURT M, SHEREEN E, DÄN G, et al. Time-synchronization attack detection in unbalanced three-phase systems[J]. IEEE Transactions on Smart Grid, 2021, 12(5): 4460-4470.
[18] 肖 勇，钱 斌，蔡梓文，等. 电力物联网终端非法无线通信链路检测方法[J]. 电工技术学报，2020，35(11)：2319-2327.
XIAO Yong, QIAN Bin, CAI Ziwen, et al. Malicious wireless communication link detection of power internet of thing devices[J]. Transactions of China Electrotechnical Society, 2020, 35(11): 2319-2327.
[19] WU K H, LI J W, ZHANG B. Abnormal detection of wireless power terminals in untrusted environment based on double hidden Markov model[J]. IEEE Access, 2020, 9: 18682-18691.
[20] 刘 铭，刘 念，韩晓艺，等. 一种基于射频指纹的电力物联网设备身份识别方法[J]. 中国电力，2021，54(3)：80-88.
LIU Ming, LIU Nian, HAN Xiaoyi, et al. A RF fingerprint based EIOT device identification method[J]. Electric Power, 2021, 54(3): 80-88.
[21] 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.
[22] 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.
[23] 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.
[24] WU Y D, WEI Z, WENG J, et al. Resonance attacks on load frequency control of smart grids[J]. IEEE Transactions on Smart Grid, 2018, 9(5): 4490-4502.
[25] 厉彦杰. 基于机器学习的电力物联网终端设备安全监测技术研究[D]. 杭州：浙江大学，2021：61-66.
LI Yanjie. Research on security monitoring technology of power IoT terminals based on machine learning[D]. Hangzhou, China: Zhejiang University, 2021: 61-66.
[26] CHEN Y D, MA X L, WU X Y. DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory[J]. IEEE Communications Letters, 2013, 17(5): 1052-1054.
[27] NASEER S, SALEEM Y, KHALID S, et al. Enhanced network anomaly detection based on deep neural networks[J]. IEEE Access, 2018, 6: 48231-48246.
[28] ZHANG Y, CHEN X, GUO D, et al. PCCN: parallel cross convolutional neural network for abnormal network traffic flows detection in multi-class imbalanced network traffic flows[J]. IEEE Access, 2019, 7: 119904-119916.
[29] WANG W P, WANG Z R, ZHOU Z F, et al. Anomaly detection of industrial control systems based on transfer learning[J]. Tsinghua Science and Technology, 2021, 26(6): 821-832.
[30] 王 雷，张瑞青，盛 伟，等. 基于支持向量机的回归预测和异常数据检测[J]. 中国电机工程学报，2009，29(8)：92-96.
WANG Lei, ZHANG Ruiqing, SHENG Wei, et al. Regression forecast and abnormal data detection based on support vector regression[J]. Proceedings of the CSEE, 2009, 29(8): 92-96.
[31] 刘 见，赵震宇，裴茂林，等. 智能变电站过程层网络异常流量检测[J]. 计算技术与自动化，2021，40(3)：184-188.
LIU Jian, ZHAO Zhenyu, PEI Maolin, et al. Abnormal flow detection of process layer network in intelligent substation[J]. Computing Technology and Automation, 2021, 40(3): 184-188.
[32] 杨 挺，侯昱丞，赵黎媛，等. 基于时−频域混合特征的变电站通信网异常流量检测方法[J]. 电力系统自动化，2020，44(16)：79-86.
YANG Ting, HOU Yucheng, ZHAO Liyuan, et al. Abnormal traffic detection method of substation communication network based on time-frequency domain mixed features[J]. Automation of Electric Power Systems, 2020, 44(16): 79-86.
[33] LIU S Y, HU J, HAO S N, et al. Improved EM method for internet traffic classification[C]//Proceedings of the 2016 8th International Conference on Knowledge and Smart Technology. Chiang Mai, Thailand: IEEE, 2016: 13-17.
[34] 钟志琛. 基于网络流量异常检测的电网工控系统安全监测技术[J]. 电力信息与通信技术，2017，15(1)：98-102.
ZHONG Zhichen. Security monitoring technology of power grid industrial control system based on network traffic anomaly detection[J]. Electric Power Information and Communication Technology, 2017, 15(1): 98-102.
[35] 刘亚丽，孟令愚，丁云峰. 电网工控系统流量异常检测的应用与算法改进[J]. 计算机系统应用，2018，27(3)：173-178.
LIU Yali, MENG Lingyu, DING Yunfeng. Application and algorithm improvement of abnormal traffic detection in smart grid industrial control system[J]. Computer Systems & Applications, 2018, 27(3): 173-178.
[36] FU L D, ZHANG W B, TAN X B, et al. An algorithm for detection of traffic attribute exceptions based on cluster algorithm in industrial internet of things[J]. IEEE Access, 2021, 9: 53370-53378.
[37] 赵 博，张华峰，张 驯，等. 基于 EMD 的电厂网络流量异常检测方法[J]. 计算机科学，2019，46(11A)：464-468.
ZHAO Bo, ZHANG Huafeng, ZHANG Xun, et al. EMD-based anomaly detection for network traffic in power plants[J]. Computer Science, 2019, 46(11A): 464-468.

[38] YANG T, HOU Y C, LIU Y C, et al. WPD-ResNeSt: substation station level network anomaly traffic detection based on deep transfer learning[J]. CSEE Journal of Power and Energy Systems, 2021, doi: 10.17775/CSEEJPES. 2020.02850.

[39] 张嘉誉，章坚民，杨才明，等. 基于信息物理融合的智能变电站过程层网络异常流量检测[J]. 电力系统自动化，2019，43(14)：173-181.
ZHANG Jiayu, ZHANG Jianmin, YANG Caiming, et al. Abnormal traffic detection on process layer network of smart substation based on cyber physical fusion[J]. Automation of Electric Power Systems, 2019, 43(14): 173-181.

[40] 丁修玲，张延旭，蔡泽祥，等. 基于报文解析的变电站过程层网络信息流异常保护方法[J]. 电力系统保护与控制，2013，41(13)：58-63.
DING Xiuling, ZHANG Yanxu, CAI Zexiang, et al. A protection method of abnormal information flow in process layer network based on packet analysis[J]. Power System Protection and Control, 2013, 41(13): 58-63.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] HU C M, YAN J, WANG C. Advanced cyber-physical attack classification with extreme gradient boosting for smart transmission grids[C]//Proceedings of 2019 IEEE Power & Energy Society General Meeting. Atlanta, USA: IEEE, 2019: 1-5.

[46] 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.

[47] 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.

[48] PARIZAD A, HATZIADONIU C. A laboratory set-up for cyber attacks simulation using protocol analyzer and RTU hardware applying semi-supervised detection algorithm[C]//Proceedings of 2021 IEEE Texas Power and Energy Conference. College Station, USA: IEEE, 2021: 1-6.

[49] OZAY M, ESNAOLA I, VURAL F T Y, 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.

[50] 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.

[51] WANG P Y, GOVINDARASU M, ASHOK A, et al. Data-driven anomaly detection for power system generation control[C]//Proceedings of 2017 IEEE International Conference on Data Mining Workshops. New Orleans, USA: IEEE, 2017: 1082-1089.

[52] 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.

[53] FOROUTAN S A, SALMASI F R. Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method[J]. IET Cyber-Physical Systems: Theory & Applications, 2017, 2(4): 161-171.

[54] ZHANG Y X, YAN J. Domain-adversarial transfer learning for robust intrusion detection in the smart grid[C]//Proceedings of 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. Beijing, China: IEEE, 2019: 1-6.

[55] 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.

[56] 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.

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

[58] WU T, ZHANG Y J A, TANG X Y. Isolation forest based method for low-quality synchrophasor measurements and early events detection[C]//Proceedings of 2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids. Aalborg, Denmark: IEEE, 2018: 1-7.

[59] 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.

[60] 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.

[61] CHAKRABARTY S, SIKDAR B. Detection of hidden transformer tap change command attacks in transmission networks[J]. IEEE Transactions on Smart Grid, 2020, 11(6): 5161-5173.

[62] LIU Y, NING P, 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. Chicago, USA: ACM, 2009: 21-32.

[63] 刘鑫蕊，常 鹏，孙秋野. 基于 XGBoost 和无迹卡尔曼滤波自适应混合预测的电网虚假数据注入攻击检测[J]. 中国电机工程学报，2021，41(16)：5462-5475.
LIU Xinrui, CHANG Peng, SUN Qiuye. Grid false data injection attacks detection based on XGBoost and unscented Kalman filter adaptive hybrid prediction[J]. Proceedings of the CSEE, 2021, 41(16): 5462-5475.

[64] BOYACI O, NARIMANI M R, DAVIS K R, et al. Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks[J]. IEEE Transactions on Smart Grid, 2022, 13(1): 807-819.

[65] IBRAHIM A M, EZZAT M, ABDELAZIZ A Y. Performance comparison of classification methods for line outage detection[C]//Proceedings of the 2016 Eighteenth International Middle East Power Systems Conference. Cairo, Egypt: IEEE, 2016: 26-32.

[66] 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.

[67] CHAKRABARTY S, SIKDAR B. Detection of malicious command injection attacks on phase shifter control in power systems[J]. IEEE Transactions on Power Systems, 2020, 36(1): 271-280.

[68] ZHANG F L, LI Q H. Deep learning-based data forgery detection in automatic generation control[C]//Proceedings of 2017 IEEE Conference on Communications and Network Security. Las Vegas, USA: IEEE, 2017: 400-404.

[69] JEVTIC A, ZHANG F L, LI Q H, et al. Physics- and learning-based detection and localization of false data injections in automatic generation control[J]. IFAC-PapersOnLine, 2018, 51(28): 702-707.

[70] KHALAF M, YOUSSEF A, EL-SAADANY E. Detection of false data injection in automatic generation control systems using Kalman filter[C]//Proceedings of 2017 IEEE Electrical Power and Energy Conference. Saskatoon, Canada: IEEE, 2017: 1-6.

[71] 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.

[72] ALI M Q, YOUSEFIAN R, AL-SHAER E, et al. Two-tier data-driven intrusion detection for automatic generation control in smart grid[C]//Proceedings of 2014 IEEE Conference on Communications and Network Security. San Francisco, USA: IEEE, 2014: 292-300.

[73] LAW Y W, ALPCAN T, PALANISWAMI M. Security games for risk minimization in automatic generation control[J]. IEEE Transactions on Power Systems, 2015, 30(1): 223-232.

[74] WANG P Y, GOVINDARASU M. Anomaly detection for power system generation control based on hierarchical DBSCAN[C] //

Proceedings of 2018 North American Power Symposium. Fargo, USA: IEEE, 2018: 1-5.
[75] ESMALIFALAK M, SHI G, HAN Z, et al. Bad data injection attack and defense in electricity market using game theory study[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 160-169.
[76] WEN B, LI P. Risk assessment of security and stability control system against cyber attacks[C]//Proceedings of the 2021 IEEE 2nd China International Youth Conference on Electrical Engineering. Chengdu, China: IEEE, 2021: 1-5.
[77] 钱 斌，蔡梓文，肖 勇，等. 电力系统时间同步攻击研究综述[J]. 电网技术，2020，44(10)：4035-4045.
QIAN Bin, CAI Ziwen, XIAO Yong, et al. Review on time synchronization attack in power system[J]. Power System Technology, 2020, 44(10): 4035-4045.
[78] IEEE. IEEE standard for synchrophasors for power systems: C37.118—2005[S]. New York, USA: IEEE, 2006.
[79] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 电力系统的时间同步系统检测规范：GB/T 26866—2011[S]. 北京：中国标准出版社，2011.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration. Testing specifications of time synchronism systems for power system: GB/T 26866—2011[S]. Beijing, China: China Standards Press, 2011.
[80] 国家能源局. 电力系统的时间同步系统 第 1 部分：技术规范：DL/T 1100.1—2009[S]. 北京：中国电力出版社，2009.
National Energy Administration. Time synchronism systems of power system part 1: technical specifications: DL/T 1100.1—2009[S]. Beijing, China: China Electric Power Press, 2009.
[81] 张 宁，杨经纬，王 毅，等. 面向泛在电力物联网的 5G 通信：技术原理与典型应用[J]. 中国电机工程学报，2019，39(14)：4015-4024.
ZHANG Ning, YANG Jingwei, WANG Yi, et al. 5G communication for the ubiquitous internet of things in electricity: technical principles and typical applications[J]. Proceedings of the CSEE, 2019, 39(14): 4015-4024.
[82] 黄彦钦，余 浩，尹钧毅，等. 电力物联网数据传输方案：现状与基于 5G 技术的展望[J]. 电工技术学报，2021，36(17)：3581-3593.
HUANG Yanqin, YU Hao, YIN Junyi, et al. Data transmission schemes of power internet of things: present and outlook based on 5G technology[J]. Transactions of China Electrotechnical Society, 2021, 36(17): 3581-3593.
[83] 金 晟，苏 盛，薛 阳，等. 数据驱动窃电检测方法综述与低误报率研究展望[J]. 电力系统自动化，2022，46(1)：3-14.
JIN Sheng, SU Sheng, XUE Yang, et al. Review on data-driven based electricity theft detection method and research prospect for low false positive rate[J]. Automation of Electric Power Systems, 2022, 46(1): 3-14.
[84] 金 晟，苏 盛，曹一家，等. 基于格兰杰归因分析的高损台区窃电检测[J]. 电力系统自动化，2020，44(23)：82-89.
JIN Sheng, SU Sheng, CAO Yijia, et al. Electricity-theft detection for high-loss distribution area based on granger causality analysis[J]. Automation of Electric Power Systems, 2020, 44(23): 82-89.
[85] 陈启鑫，郑可迪，康重庆，等. 异常用电的检测方法：评述与展望[J]. 电力系统自动化，2018，42(17)：189-199.
CHEN Qixin, ZHENG Kedi, KANG Chongqing, et al. Detection methods of abnormal electricity consumption behaviors: review and prospect[J]. Automation of Electric Power Systems, 2018, 42(17): 189-199.
[86] 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.
[87] 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.
[88] 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.
[89] 徐飞阳，薛安成，常乃超，等. 电力系统自动发电控制网络攻击与防御研究现状与展望[J]. 电力系统自动化，2021，45(3)：3-14.
XU Feiyang, XUE Ancheng, CHANG Naichao, et al. Research status and prospect of cyber attack and defense on automatic generation control in power system[J]. Automation of Electric Power Systems, 2021, 45(3): 3-14.
[90] HUANG T, SATCHIDANANDAN B, KUMAR P R, et al. An online detection framework for cyber attacks on automatic generation control[J]. IEEE Transactions on Power Systems, 2018, 33(6): 6816-6827.
[91] SRIDHAR S, GOVINDARASU M. Model-based attack detection and mitigation for automatic generation control[J]. IEEE Transactions on Smart Grid, 2014, 5(2): 580-591.
[92] AMELI A, HOOSHYAR A, EL-SAADANY E F, et al. Attack detection and identification for automatic generation control systems[J]. IEEE Transactions on Power Systems, 2018, 33(5): 4760-4774.

张 博
1992—，男，博士生
主要研究方向为电力信息物理系统网络安全
E-mail: bozhang@hnu.edu.cn

ZHANG Bo
Ph.D. candidate

刘 绚(通信作者)
1985—，男，博士，教授，博导
主要研究方向为电力网络信息物理安全、大数据及人工智能在电力系统中的应用
E-mail: xliu@hnu.edu.cn

LIU Xuan
Ph.D., Professor
Corresponding author

于宗超
1996—，男，博士
主要研究方向为大数据及人工智能在电力系统中的应用
E-mail: zongchaoyu@hnu.edu.cn

YU Zongchao

王文博
1998—，男，硕士生
主要研究方向为电力信息物理系统网络安全
E-mail: wwb1998@hnu.edu.cn

WANG Wenbo

收稿日期 2022-03-10 修回日期 2022-07-11 编辑 何秋萍