智能电网的网络安全风险及应对策略

岳芳[1,2],王雪珍[3],姜山[4*]

1. 中国科学院武汉文献情报中心,武汉 430071
2. 科技大数据湖北省重点实验室,武汉 430071
3. 中国科学院宁波材料技术与工程研究所,宁波 315201
4. 甬江实验室,宁波 315202

摘要 智能电网将网络和信息技术与电网融合以增强电力系统的可靠性、安全性和效率,但在高度信息化和互联环境下,智能电网面临着日益复杂多变的网络安全风险。概述了智能电网的概念和架构,指出其双向可交互性是与传统电网最大的区别。总结了智能电网的安全漏洞和面临的网络攻击,主要分为机密性攻击、完整性攻击和可用性攻击3类。总结回顾了机器学习、区块链、量子计算等增强智能电网网络安全的新策略,机器学习算法可增强电网故障检测和攻击识别的准确性和灵敏度,区块链技术通过其去中心化和防篡改特性为智能电网提供身份验证、数据安全、隐私保护等解决方案,量子计算在电网故障诊断和数据传输安全方面有巨大应用潜力。提出了未来的主要挑战和研究方向。

关键词 智能电网;网络攻击;机器学习;区块链;量子计算

随着气候变化形势日益严峻,电力系统向清洁、高效转型成为应对气候危机的关键路径。智能电网将网络和信息技术与电网融合,实现电力和信息的双向流动,更高效地整合发电资源、储能设施和电力消费者,提升电网的自主化、可预测性和可操作性,从而增强整个电力系统的可靠性、安全性和效率。美国能源部认为:“智能电网提供了前所未有的机遇,将能源部门带入更高可靠性、可用性和效率的新时代。[1]”

世界各国均高度重视构建智能化的现代电力网络,将智能电网作为助力电力系统清洁高效转型的关键基础。美国能源部在2015年就启动“电网

收稿日期:2023-11-13;修回日期:2024-03-15

基金项目:中国科学院A类战略性先导科技专项(XDA29010500);中国科学院战略研究与决策支持系统建设专项(GHJ-ZLZX-2023-06)

作者简介:岳芳,副研究员,研究方向为能源科技战略情报,电子信箱:yuef@whlib.ac.cn;姜山(通信作者),副研究员,研究方向为先进制造战略,电子信箱:shan-jiang@ylab.ac.cn

引用格式:岳芳, 王雪珍, 姜山. 智能电网的网络安全风险及应对策略[J]. 科技导报, 2024, 42(9): 6-16;
doi: 10.3981/j.issn.1000-7857.2023.11.01692

现代化计划”[2],旨在建立灵活、安全、可靠的未来电网,2022年又推出了“建设更好电网倡议”[3],以加强输电规划,促进全国范围内大容量输电线路的改造升级。欧洲能源研究联盟(EERA)2016年开始启动“智能电网联合行动计划”[4],组织大学和公共研发机构开展跨学科合作以加速欧洲智能电网的开发部署。2023年,欧盟委员会提出了“欧盟电网行动计划”[5],通过对欧盟市场的全面整合推动电网基础设施现代化,以构建更强大、互联、数字化和弹性的电网体系。日本经济产业省早在2010年就发布《智能电网国际化标准路线图》,提出了发展智能电网的重点攻关技术领域[6]。中国从“八五”开始加强电网相关基础设施建设,“十二五”以来持续将发展智能电网写入历次国民经济发展规划。国家能源局2023年发布《关于加快推进能源数字化智能化发展的若干意见》[7],提出“以数字化智能化电网支撑新型电力系统建设”。在国家政策支持和引导下,中国电网集团积极推动智能电网建设。国家电网公司在2009年就提出了“坚强智能电网”概念及建设规划,推动构建以特高压电网为骨干网架、各级电网协调发展的统一坚强智能电网[8],并在2024年进一步提出“打造数智化坚强电网”,增加了“大云物移智链”等现代信息技术、数字化智能化绿色化发展等关键要素[9]。南方电网公司2019年开始全面启动数字化转型,以新一代数字技术贯通源网荷储全环节[10]。随着建设的深入,中国电网智能化水平逐步提升,源网荷储协调互动能力日益增强。目前,国家电网公司已建成全球规模最大的新能源云平台,为新能源提供一站式接网服务,累计接入风光场站超过530万座[11];打造了国内最大能源区块链公共服务平台“国网链”,支撑开展绿色电力交易。南方电网公司已将995家新能源场站信息全部接入新能源调度运行管理平台,自主研发了“夸父”新能源高精度功率预测系统,预测准确率可在国家标准要求基础上提升3%~7%[12]。

然而,随着“云大物移智链”等新技术深度融入智能电网建设,智能设备接入增多,数据信息高度互联,电网受攻击面扩大,却有可能导致极为严峻的后果。电网安全技术对于最大限度地预防与减轻网络攻击及网络安全事件的危害,保障电网安全高效、持续运行具有极其重要的意义。本文讨论智能电网的概念和架构,总结智能电网的漏洞以及可能面临的网络攻击,针对机器学习、区块链、量子计算等增强智能电网网络安全的新策略进行回顾,提出未来的主要挑战和研究方向。

1　智能电网概念及架构

目前国际上对于智能电网尚无统一定义。美国国家标准与技术研究院(NIST)对智能电网的定义是:一个现代化的电网,可实现能量的双向流动,并使用双向通信和控制功能,从而带来一系列新的功能和应用[13]。电气与电子工程师协会(IEEE)称智能电网为“一项革命性的事业,需要新的通信和控制能力、能源、发电模型以及遵守司法管辖区的监管结构”[14]。国际电工委员会(IEC)指出,智能电网包括电网现代化,智能电网技术使电网变得更加灵活、更能互动,并使其能够提供实时反馈,融合了促进智能监测、控制、通信和自修复的技术和服务[15]。美国能源部将智能电网定义为一种新型的、自下而上构建的电网,通过电力供应端与消费端双向通信的数字技术和沿输电网络的传感技术使电网变得智能,以数字方式响应快速变化的电力需求[1]。

由上述定义可以看出,智能电网意味着更智能的发电、输电、配电,以及用户、运营、市场和服务供应商的集成。智能电网与传统电网最大的差别在于其双向可交互性,即电力和信息的双向流动。传统电网是单向系统,发电厂无法及时从用户侧获得反馈以调整供电策略,而智能电网是双向可调节网络,通过分析用户信息,可以制定供电策略,平抑峰谷用电,实现更高效地并入波动性可再生能源,并最大限度降低发电成本。传统电网与智能电网的区别如表1[16]所示。

智能电网的基础架构包含了传统电网中的电力生产、输配和使用环节,另外还包含信息传送的各环节。IEEE基于NIST概念模型[17],从智能电网主要业务流程出发,提出了智能电网的基本架构

表1 传统电网与智能电网对比

特征	传统电网	智能电网
通信方式	单向	双向
发电方式	集中式发电	分散式/分布式发电
控制方式	人工	自动控制与恢复
监控系统	人工	自动
监测和控制所需传感器	没有或较少	大量传感器用于监控
紧急情况应对	反应慢	反应快
用户选择	选择有限	广泛的选择
网络类型	径向	分散式/分布式
安全/隐私问题	减少安全和隐私问题	容易出现安全和隐私问题
涉及数据	数据较少	涉及海量数据
存储系统	不使用存储空间	使用存储系统

(图1[18]),由8个逻辑域、32个子域组成,如表2[18]所示。其中,各域之间均可进行信息的双向交互,而发电、输电、配电和用户域可进行信息和电力的双向流动。

智能电网的通信网络连接电网、服务供应商和用户,之间的通信通过多种不同的通道和协议进行。智能电表、传感器和控制设备在智能电网中的集成使电网更加灵活和智能化,先进计量基础设施(AMI)可连接用户和通信网络,智能电表可向供应商提供电力使用、中断和电价数据。此外,智能电网还包括各种运行管理组件,如用于输电的能源管理系统(EMS),以及用于配电的配电管理系统(DMS)等,整个传输网络通过监控和数据采集(SCADA)系统进行监测和控制。由于智能电网中

图1 IEEE智能电网架构

表2 IEEE智能电网域及子域

逻辑域	包含子域	所有子域
发电	批量发电:(1) 零散发电:(2)(3)(4)	(1)先进发电解决方案;(2)分布式能源资源;(3)分布式发电;(4)储能系统;(5)先进保护;(6)资产管理与优化;(7)微电网和纳米电网;(8)智慧城市;(9)变电站自动化;(10)输电自动化;(11)输配电规划;(12)电能质量管理;(13)用户侧支持技术解决方案;(14)需求响应;(15)电动汽车;(16)智能电表系统;(17)分布式运行;(18)现场设备运行;(19)输电运行;(20)可见性及控制;(21)市场支持技术解决方案;(22)服务供应商支持技术解决方案;(23)架构(互操作性、可用性等);(24)业务流程再造;(25)通信系统;(26)控制系统;(27)经济性论证、成本回收模型;(28)教育及培训;(29)环境影响及效率;(30)信息和数据管理;(31)策略、政策、程序和标准;(32)系统弹性(网络安全、关键基础设施保护、可靠性合规性)
输电	(5)(6)(7)(8)(9)(10)(11)	
配电	(5)(6)(7)(8)(9)(10)(11)(12)	
用户	(5)(6)(7)(8)(9)(11)(13)(14)(15)(16)	
运行	(17)(18)(19)(20)	
市场	(21)	
服务供应商	(22)	
基础支持系统	(23)(24)(25)(26)(27)(28)(29)(30)(31)(32)	

的信息流分布在电力生产至消费的广泛环节,极大地拓宽了电力系统中的“网络攻击界面”,其先进的自动化和通信功能使整个系统面临网络威胁,且存在各种安全限制和漏洞[19]。在智能电网中,SCADA系统、相量测量单元(PMU)、远程终端单元(RTU)中都可能存在漏洞,包括缺乏防火墙、配置错误、缺乏安全审计、安全措施不足以及身份验证不当等,这些都会导致整个智能电网系统的失效,成为攻击者的目标。对智能电网的攻击可能有侵入敏感用户数据、传播恶意软件、损坏通信设备、注入虚假信息、攻击或修改监测及控制设备等,这些都有可能危及电网运行,导致电力中断等,可能产生严重的社会经济后果,甚至损害国家安全。

2　智能电网的安全漏洞及网络攻击

2.1　智能电网的安全漏洞

智能电网是集物理网络、信息技术和运营技术为一体的复杂系统,并与其他基础设施交互。因此,其安全漏洞可能存在于自身电网系统以及与其相连的外部系统,主要有物理漏洞、信息技术及运营技术漏洞、数据管理漏洞、服务和应用程序漏洞等,概述如表3[20-22]。这些漏洞可能对电网安全产生直接或间接影响,导致断电、经济损失等多种后果,重则影响整个电网,造成重大损失。

表3　智能电网的安全漏洞

类型	说明	特征或影响
物理漏洞	智能电网中各类物理组件的漏洞,如监控不足、部件受损、变电站冗余约束、电网运行环境缺陷等	是传统电网就存在的问题,在智能电网环境下可能与网络攻击叠加,造成较大影响
信息技术及运营技术漏洞	随着信息和运营技术在电网的应用,相关智能设备的硬/软件存在漏洞;智能电网中使用的多种通信技术和协议也可能存在各种漏洞,成为连接外部攻击和内部运营系统的通道	随着智能电网信息和运营系统的发展而增加的漏洞,且有可能威胁整个网络
数据管理漏洞	智能电网需要收集和管理来自大量节点的实时数据,在海量数据的收集、分析、处理和维护过程中存在许多漏洞	基于广域网在各实体之间的数据交换可能是导致网络漏洞的主要原因,大多数智能电网在数据安全和隐私管理方面都存在不足,而且缺乏针对智能电网领域特定数据的专用保护技术
服务和应用程序漏洞	智能电网提供的需求侧管理、分布式发电资源管理、输配电自动化等数字化服务和应用中存在的漏洞,如操作系统版本陈旧、维护文件不正确、缺乏补丁政策和维护更新、缺乏入侵检测系统、身份验证不当、设备及系统兼容性不足等	这些漏洞是智能电网服务和应用程序所使用的信息技术的固有漏洞

2.2　智能电网网络攻击

针对智能电网的网络攻击通常会利用其漏洞发起,多数使用勒索软件和恶意软件来入侵网络,向电力公司索要巨额赔偿,或是造成电力服务中断等恶性后果。历史上首次因网络攻击造成的大规模停电事故是2015年的乌克兰电力系统网络攻击事件。2015年12月23日,乌克兰电力系统发生了一场灾难性的网络攻击,导致乌克兰西部地区停电6小时,直接影响超过8万户。黑客利用钓鱼邮件发送恶意软件BlackEnergy,入侵并控制了电力公司的SCADA系统,远程控制变电站完成断电操作,还攻击了客服中心阻止用户报告断电情况[23]。SCADA系统往往整合了先进计量基础设施、分布式能源资源、配电自动化等复杂单元,容易成为网络攻击的主要目标[24]。通过访问控制层并注入虚假信号或恶意软件,可能导致整个电网完全瘫痪。

目前,针对智能电网的恶意软件正在不断演变,有些能够隐蔽地在电网控制系统中运行,干扰

电力分配,造成能源浪费。有些能够阻断控制中心对变电站等设施的控制,达到切断电力供应的目的。尤其是,如果核电站的核反应堆控制系统被恶意攻击,可能造成更大的安全危害。2010年,伊朗纳坦兹核设施遭遇“震网”病毒攻击,直接导致1000多台离心机瘫痪,已经证明可通过攻击工业设备管理控制系统和SCADA系统对关键基础设施造成重大破坏。值得注意的是,2021年伊朗纳坦兹核设施再度遭遇网络攻击,不仅离心机被破坏,电力系统也遭到破坏且引发爆炸,表明随着设施互联性的增强,网络攻击的范围和影响都在扩大[25]。迄今为止,针对智能电网的网络攻击主要有虚假数据注入攻击(FDIA)、拒绝服务(DoS)攻击、数据帧攻击(DFA)、中间人(MITM)攻击、负载改变攻击(LAA)、虚假命令注入攻击(FCIA)、负荷重分配攻击(LRA)、协调网络物理拓扑(CCPT)攻击、重放攻击(RA)等。根据信息安全三要素(CIA),即机密性(confidentiality)、完整性(integrity)和可用性(availability),对智能电网网络攻击分类如表4[19]所示。

表4 根据CIA的智能电网网络攻击分类

网络安全目标	攻击类型
机密性	社会工程、窃听、流量分析、未经授权的访问、密码窃取、中间人、嗅探、重放、伪装、数据注入
完整性	篡改、重放、虫洞、虚假数据注入、欺骗、数据修改、中间人、时间同步、伪装、负荷下降攻击
可用性	干扰、虫洞、拒绝服务、低速DoS、缓冲区溢出、泪滴、Smurf、Puppet、时间同步、伪装、中间人、欺骗攻击

1)机密性攻击。机密性攻击试图窃取仅应在安全方之间共享或保密的信息,其并不试图改变所传输的信息,而是通过嗅探智能电网中的通信通道以获取所需的信息。例如,通过密码猜测、密码嗅探、字典攻击和社会工程等进行密码攻击以获取用户账号。在智能电网中,窃听攻击是一种被动攻击方式,通过嗅探IP数据包或拦截局域网无线传输来破坏数据机密性[26]。流量分析攻击也是一种被动攻击,通过嗅探和分析信息以获取有用信息。伪装攻击是一种主动攻击方式,其通过MAC欺骗、ARP欺骗、IP欺骗等对参数进行非法修改,伪装成合法资产以获得更多特权。身份欺骗攻击,如消息重放攻击、中间人攻击等可在不使用用户密码的情况下伪装成授权资产。PMU、TCP/IP数据包和智能电表是嗅探攻击的主要目标,如果未经加密,攻击者将可能收集到关键信息。

2)完整性攻击。完整性攻击旨在修改原始数据的内容,例如用户帐户数据、计费数据、电压和传感器数值、控制命令、设备运行状态数据等,还可能对信息进行延迟和重新排序[27]。FDIA是一种常见且威胁程度较高的完整性攻击,能够干扰智能电表测量,恶意伪造测量结果以影响状态估计结果,通过欺骗控制中心、扰乱电力市场获利。而且,FDIA具有较强的隐蔽性,能够避开电网的不良数据检测(BDD)机制。通过影响上层控制中心决策,FDIA可能导致电力系统切负荷、线路过载、电力市场破坏等,已成为现代电力系统的严重威胁[28]。根据攻击目标的不同,FDIA可分为如下方式:① 通过在状态变量中引入任意误差,同时绕过不良测量检测来攻击状态估计;② 通过拓扑篡改误导控制中心;③ 经济攻击,通过增加运营成本/损失或从电力市场非法获利;④ 攻击智能电网应用,如SCADA系统、PMU等。有研究发现,FDIA在导致目标线路断电的同时,触发级联故障促使多个线路跳闸,最终导致更大规模的断电[29];还可通过PMU数据相关断电检测来掩盖线路断电,使运营商不能及时察觉故障[30]。攻击者还有可能识别可造成最大损害或耗费最少攻击资源的最佳网络攻击序列[31]。此外,FDIA还有可能导致智能电网频率异常、停电、用电设备损坏等问题[32]。

3)可用性攻击。可用性意味着授权用户可以访问信息,可用性攻击会阻止并可能破坏智能电网中授权访问的稳定性。DoS攻击是一种常见的可用攻击[33-34],通常包括利用大量无用数据占用系统

资源使系统难以及时响应,以及操纵协议和系统中的漏洞或异常等,有时可能2种手段兼而有之。以众多分散个体为目标的DoS攻击称为分布式拒绝服务(DDoS)攻击,其使用虚假请求淹没通信服务器,以堵塞服务器并使其无法进行通信。智能电网中的智能电表、智能电器、数据聚合器、PMU、RTU、智能电子设备(IED)、可编程逻辑控制器(PLC)等智能设备由于采用了互联网标准协议,暴露出各种漏洞导致DoS攻击。此外,一些公用事业公司的网络安全管理也存在缺陷,并未将PMU网络归类为关键网络资产,这可能会导致缺乏抵御DoS等网络攻击的能力[35]。DoS攻击实现简单,但有可能在智能电网中造成重大破坏,随着智能电网系统并网规模的扩大,DoS攻击的影响可能从轻微到严重,甚至可能导致数百万用户的长时间断电[36]。

3　增强智能电网网络安全的新策略

当前已有多种技术用于智能电网网络攻击的检测和防御,随着网络攻击策略的不断更新和日益复杂化,现有技术正在不断发展和更新,机器学习、区块链、量子计算等新兴技术的发展和应用,为增强智能电网的网络安全提供了新的策略。

3.1　机器学习技术

机器学习(ML)作为一种有效的工具,能够收集和分析智能电网中产生的大量数据并做出适当决策,使电网按照预期优化运行。机器学习由各种算法和技术组成,通过指令集分析现有数据,根据数据生成决策或预测,其在智能电网中的主要应用包括预测发电量和用电量[37]、优化电力调度、自适应控制能源价格、故障检测[38]、网络攻击识别[39]等。

利用机器学习算法,能够免去繁琐的机理建模步骤,基于大量数据检测智能电网的网络攻击。使用多层感知器(MLP)深入分析FDIA对智能电网的影响发现,一定程度的伪造数据会降低智能电网决策的准确性,如果存在干扰,并且模型由于错误数据而无法预测干扰,电网可能会进入不稳定状态从而导致灾难性事件[40]。有研究以停电为例,分析了智能电网的物理变化对基于机器学习的FDIA检测的影响[41]。目前,监督学习、半监督学习、无监督学习、强化学习等方法已经用于FDIA检测[42]。研究发现,对于无监督模型,集成学习算法性能优于单一算法[43]。深度学习由于具有强大的非线性特征提取能力,具有较高灵敏度和准确度,逐渐被用于FDIA检测,如使用递归神经网络[44]、卷积神经网络[45]、混合神经网络[46]、双向循环神经网络[47]等算法。一些研究尝试使用半监督方式进行深度学习训练,将自动编码器集成到先进的生成对抗网络中,通过捕获异常测量和安全测量之间的不一致性来检测FDIA下的异常[48]。

对于DoS攻击,使用机器学习技术可增强防御策略,如蜂窝计算网络(CCN)可预测PMU丢失的信息,将自动编码器与深度极限学习机相结合可预测由于DoS攻击而丢失的数据,发出控制信号以维持系统稳定[49],利用多级自动编码器模型可检测DDoS攻击[50]。针对窃电攻击,利用集成学习算法可实时识别智能电表的错误读数,以检测窃电攻击[51];利用贝叶斯优化器对深度神经网络进行超参数优化,可提升窃电检测的准确性[52]。针对隐形网络攻击,研究者提出了结合核主成分分析(KPCA)的极端随机树(ERT)算法[53]。对于多种数据完整性攻击,使用K最近邻和决策树(DT)等算法进行攻击分类,准确率达到96.5%[54];而利用变分模态分解(VMD)和DT算法开发的网络物理异常检测系统,准确率可接近99.9%[55]。

3.2　区块链技术

区块链是一种新兴的信息技术,其基于共识机制和网络开放性,通过多种加密技术实现点对点的分布式存储网络。随着电网向智能化发展,电力系统面临智能设备接入身份认证困难、数据存储通信效率低、电力交易及节点信息不安全等问题。例如,智能电网中的大量智能设备节点需要进行动态注册和认证,传统电网的中心式认证方式效率低、成本高、跨链认证互信困难,且无法进行复杂的身份认证加密计算,难以识别恶意节点的伪造身份信息[56]。一些恶意节点可能向电网控制中心提供错误反馈,导致决策失误造成停电等后果。将区块链技术应用于电网,为身份验证、授权和数据交换提

供了新的防篡改机制,其链式数据结构、去中心化模式可实现数据的快速验证、保存、维护和传输,进而改善智能电网的安全性。

智能电网中的先进计量基础设施会生成大量与计费、能源使用等相关信息,上传至中央数据中心可能造成网络攻击等问题,利用区块链可在不信任的网络环境中对计量设施提供去中心化的访问控制,避免单点故障带来的影响。例如,将数据驱动分析与区块链技术结合,可成功检测与FDI攻击和智能电表故障相关的数据问题[57~58];基于以太坊区块链的去中心化系统可减轻针对智能电表的DDoS攻击[59]。

将区块链技术用于通过传感器和电源管理单元(PMU)监控电力设备参数,并通过信息共享进行智能管理,可以增强智能电网稳定性,监控窃电和断电情况[60]。有研究者针对受损智能电网设计了一个现实威胁模型,并提供了数据共享的激励机制,可防止运营商为了盈利而隐瞒或歪曲数据[61]。利用区块链和智能合约技术可确保能源交易安全[62],基于区块链的工业物联网能源交易方案可实现透明、可验证的公平交易[63]。此外,区块链技术还可以用于智能电网的数据隐私保护,如传感器数据[64]、能源交易数据[65]及消费数据[66]等。

3.3 量子计算技术

量子计算使用量子位作为信息处理和计算的基本单元,由于量子位可以处于0和1的叠加态,多个量子位可以同时处于不同的叠加态,且2个量子位之间存在特殊的相互关联状态(即量子纠缠),因此量子计算可利用量子叠加和量子纠缠并行处理和高效求解问题,相比经典计算机实现指数级的计算速度增长。随着智能化、信息化程度加深,电力系统每时每刻都在产生大量数据,对电力系统的规划、运行管理和调度的复杂性在不断增强,这需要更强的计算能力。因此,量子计算在这一领域具有较大应用潜力。

近年来,量子计算逐渐应用于增强智能电网的网络安全[67]。例如,利用量子计算能够克服深度学习模型复杂性导致的计算挑战,对电力系统故障诊断具有更可靠的诊断性能和更少响应时间[68]。量子密钥分发(QKD)在智能电网领域的应用相对成熟,正从实验室研究发展至商业产品[69]。密钥生成和分发对于智能电网中数据传输的安全非常重要,传统密码学基于数学算法的计算复杂度,无法察觉窃听,且智能电网智能终端设施往往计算能力有限,无法承担计算成本高昂的加密技术。QKD不依赖计算复杂性,其利用量子力学定律产生完全随机且仅双方知道的量子密钥,一旦有第三方试图窃听就会因为产生干扰而被察觉,因而可确保密钥的安全性。美国能源部致力于推广在智能电网中应用量子通信技术。2019年,美国橡树岭国家实验室(ORNL)、洛斯阿拉莫斯国家实验室(LANL)和美国电力运营商EPB公司第一次示范了具有不同底层硬件和软件组件的QKD系统,并于2020年5月在查塔努加市的电力系统成功进行了示范,用于加密控制信息以调度和控制电力输配[70]。2023年7月,EPB公司建设的美国首个商用量子网络EPB Quantum Network正式对外开放接受申请[71]。中国国家电网公司2016年开始与科大国盾量子技术股份有限公司合作布局将量子加密技术应用于电力系统,在北京市、安徽省、山东省、湖北省等多个地区示范工程项目的建设和探索[72]。2022年1月,国家电网公司宁波江北10 kV横山线主线正式投运,这是中国首条基于量子加密无线通信的全自动化架空线路[73]。

4 结论

智能电网通过电力和信息的双向流动,实现传统网络的转型升级,为构建高效、可靠的新型电力系统奠定基础。智能电网与传统电网最大的区别是双向可交互性,其基础架构包含了传统电力生产、输配和使用环节及信息传送的各环节。电网的智能化信息化也带来了一些网络安全风险,本文总结了智能电网的安全漏洞和面临的网络攻击,阐述了机器学习、区块链、量子计算等新兴技术在增强智能电网网络安全方面的可能应用和发展方向。展望未来,仍需针对这些新兴解决方案作进一步研究以应对一些关键挑战。

1）人工智能和机器学习是增强智能电网运行可靠性、电网效率和鲁棒性的可行方案,并能达到预期的服务质量要求。为了确保模型的准确性,减少智能电网中人工智能模型的过拟合及欠拟合问题,需要丰富的历史数据来训练模型。此外,还应为控制人工智能模型的决策提供保障,以符合电力系统的网络安全约束。联邦机器学习在数据隐私保护方面极具应用前景,其邀请底层设备以协作方式训练人工智能模型,通过本地化模型训练,使得每个设备的隐私都得到了保护,已被用于智能电网中的电力负荷预测、能源需求预测和大型电力系统的数据隐私保护。然而,该技术容易受到网络攻击,在大量应用前有必要考虑强大的安全措施。

2）区块链技术尚不成熟,因此有必要对安全监管框架进行具体分析。如果访问密钥保持安全,区块链技术将是确保电网安全的重要方法。可以通过组合分布式区块链网络来构建整个输电系统的区块链电网,以有效防止输电系统故障。为了在智能电网中建立安全的RTU和IED控制系统,可以利用复杂算法开发基于区块链的智能电表,将其用于分布式发电系统控制器以调节电压和电能质量。此外,考虑到区块链的数据不变性和去中心化等特性可以实现数据的永久存储,在实施智能合约时必须小心,因为任何故障或不当行为都可以在系统内被观察到。

3）尽管迄今为止量子计算已在一定程度上得以实现,但要超越经典计算仍需解决各种问题,主要与量子硬件和实现有关。目前还没有一种有保证的物理量子随机存取存储器可以有效地将信息编码成量子态,并确保量子算法的执行速度。智能电网需要大量具有高连接性的量子比特来执行大规模系统的量子算法,而且控制这些量子比特极具挑战性,因为其对温度非常敏感。因此,量子设备需要特殊的基础设施以保持低温条件。量子计算机容易受到噪声或量子退相干的影响,这也是构建大规模量子计算机的主要障碍之一,因为在退相干过程中量子比特不再保持预定的量子态,实现大量量子比特纠缠非常困难。此外,为了避免量子计算机的错误对电力系统的影响,需要开发一种通用的容错和纠错量子计算机。量子密钥协议并非用于处理大量节点,因此当通信节点数量增加时,系统复杂性和成本可能会显著增加,需要开发支持大量用户的量子-经典混合网络。考虑到智能电网可能覆盖较大的地理范围,而密钥速率随着传输距离的增加而迅速下降,为了避免在密钥传输过程中的暴露和不同步风险,需要开发一种可以建立端到端密钥的QKD协议,并支持具有短通信延迟的实时动态控制。

参考文献(References)

[1] US Department of Energy. The smart grid[EB/OL]. [2023-08-04]. https://www. smartgrid. gov/the_smart_grid/smart_grid.html.

[2] US Department of Energy. Grid modernization initiative [EB/OL]. [2024-03-02]. https://www.energy.gov/gmi/grid-modernization-initiative.

[3] US Department of Energy. Building a better grid initiative [EB/OL]. (2022-01-12)[2024-01-03]. https://www.energy.gov/oe/articles/building-better-grid-initiative.

[4] EERA. EERA IP smart grids[EB/OL]. [2024-03-02]. https://eera-smartgrids.eu/.

[5] European Commission. Grids, the missing link-An EU action plan for grids[EB/OL]. (2023-11-28) [2024-01-03]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A757%3AFIN.

[6] 张晶, 叶筠英, 李彬, 等. 智能电网标准国际化战略研究[J]. 供用电, 2020, 37(3): 3-9.

[7] 国家能源局. 国家能源局关于加快推进能源数字化智能化发展的若干意见[EB/OL]. (2023-03-28)[2024-01-03]. https://www. gov. cn/zhengce/zhengceku/2023-04/02/content_5749758.htm?eqid=da02903f00041dfd00000003645-caedc.

[8] 黄训诚, 和萍, 崔光照, 等. 中国智能电网发展述评、展望与建议[J]. 轻工学报, 2016, 31(2): 54-65.

[9] 姜义平. 构建新型电力系统 打造数智化坚强电网[EB/OL]. (2024-02-22)[2024-02-22]. http://www.cnenergynews.cn/dianwang/2024/02/22/detail_20240222148484.html.

[10] 杨彬. 南方电网数字化转型和数字电网建设的进展、未来展望[EB/OL]. (2021-12-16)[2024-02-22]. https://news.bjx.com.cn/html/20211216/1193950.shtml.

[11] 辛保安. 加快构建新型电力系统为美丽中国建设赋动能[EB/OL]. (2024-03-04) [2024-03-06]. http://dzb. rmzxb.com. cn/rmzxbPaper/pc/con/202403/04/content_58092. html

[12]《南方电网新型电力系统发展报告(2021—2023)》发布[EB/OL]. (2023-10-10)[2024-02-02]. https://news.bjx.com.cn/html/20211216/1193950.shtml.
[13] NIST. Smart grid: A beginner's guide[EB/OL]. (2012-07-12)[2023-08-04]. https://www.nist.gov/el/smart-grid/about-smart-grid/smart-grid-beginners-guide.
[14] IEEE. About IEEE smart grid[EB/OL]. [2023-08-04]. https://smartgrid.ieee.org/about-ieee-smart-grid.
[15] IEC. Bringing intelligence to the grid[R]. Geneva: IEC, 2018.
[16] Dorji S, Stonier A A, Peter G, et al. An extensive critique on smart grid technologies: Recent advancements, key challenges, and future directions[J]. Technologies, 2023, 11(3): 81-101.
[17] NIST. NIST framework and roadmap for smart grid interoperability standards, release 3.0[EB/OL]. (2014-10-01)[2023-08-04]. https://www.nist.gov/system/files/documents/smartgrid/NIST-SP-1108r3.pdf.
[18] IEEE. IEEE smart grid domains & sub-domains[EB/OL]. [2023-08-04]. https://smartgrid.ieee.org/domains.
[19] Gunduz M Z, Das R. Cyber-security on smart grid: Threats and potential solutions[J]. Computer Networks, 2020, 169: 107094.
[20] Ding J G, Qammar A, Zhang Z M, et al. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions[J]. Energies, 2022, 15(18): 6799-6835.
[21] Lázaro J, Astarloa A, Rodríguez M, et al. A survey on vulnerabilities and countermeasures in the communications of the smart grid[J]. Electronics, 2021, 10(16): 1881.
[22] Ericsson G N. Toward a framework for managing information security for an electric power utility-CIGRÉ experiences[J]. IEEE Transactions on Power Delivery, 2007, 22(3): 1461-1469.
[23] Titcomb J. Ukrainian blackout blamed on cyber-attack[EB/OL]. (2016-01-05)[2023-08-04]. https://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html.
[24] 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.
[25] 秦安. 秦安:伊朗核设施再度被"黑"有何警示[EB/OL]. (2021-04-14)[2023-08-04]. https://opinion.huanqiu.com/article/42i6mtP6qMB.
[26] Gunduz M Z, Das R. Analysis of cyber-attacks on smart grid applications[C]//Proceedings of International Conference on Artificial Intelligence and Data Processing (IDAP). Piscataway, NJ: IEEE, 2018: 1-5.
[27] Tan S, De D, Song W Z, et al. Survey of security advances in smart grid: A data driven approach[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 397-422.
[28] Shi H Z, Xie L B, Peng L. Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method[J]. Computers & Electrical Engineering, 2021, 91: 107058.
[29] Che L, Liu X, Li Z Y, et al. False data injection attacks induced sequential outages in power systems[J]. IEEE Transactions on Power Systems, 2019, 34(2): 1513-1523.
[30] Liu X, Li Z Y, Liu X D, et al. Masking transmission line outages via false data injection attacks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(7): 1592-1602.
[31] 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.
[32] Tan R, Nguyen H H, Foo E Y S, et al. Optimal false data injection attack against automatic generation control in power grids[C]//Proceedings of ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS). Piscataway, NJ: IEEE, 2016: 1-10.
[33] Yi P, Zhu T, Zhang Q Q, et al. A denial of service attack in advanced metering infrastructure network[C]//Proceedings of IEEE International Conference on Communications (ICC). Piscataway, NJ: IEEE, 2014: 10-14.
[34] Guo Y H, Ten C W, Hu S Y, et al. Modeling distributed denial of service attack in advanced metering infrastructure[C]//Proceedings of IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Piscataway, NJ: IEEE, 2015: 1-5.
[35] Attia M, Senouci S M, Sedjelmaci H, et al. An efficient Intrusion Detection System against cyber-physical attacks in the smart grid[J]. Computers & Electrical Engineering, 2018, 68: 499-512.
[36] Taft J. Assessment of existing synchrophasor networks[EB/OL]. (2018-04-30)[2023-08-04]. https://www.naspi.org/sites/default/files/reference_documents/pnnl_27557_assess_existing_synchrophasor_net.pdf.
[37] Frincu M, Chelmis C, Noor M U, et al. Accurate and efficient selection of the best consumption prediction method in smart grids[C]//Proceedings of IEEE International Conference on Big Data (Big Data). Piscataway, NJ: IEEE, 2014: 721-729.
[38] Karimipour H, Geris S, Dehghantanha A, et al. Intelligent anomaly detection for large-scale smart grids[C]//Proceedings of IEEE Canadian Conference of Electrical and Computer Engineering (CCECE). Piscataway, NJ: IEEE, 2019: 1-4.

[39] Karimipour H, Dehghantanha A, Parizi R M, et al. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids [J]. IEEE Access, 2019, 7: 80778-80788.

[40] Tufail S, Batool S, Sarwat A I. False data injection impact analysis in AI-based smart grid[C]//Proceedings of Southeast Conference 2021. Piscataway, NJ: IEEE, 2021: 1-7.

[41] Mohammadpourfard M, Weng Y, Pechenizkiy M, et al. Ensuring cybersecurity of smart grid against data integrity attacks under concept drift[J]. International Journal of Electrical Power & Energy Systems, 2020, 119: 105947.

[42] 彭莎, 孙铭阳, 张镇勇, 等. 机器学习在电力信息物理系统网络安全中的应用[J]. 电力系统自动化, 2022, 46(9): 200-215.

[43] 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.

[44] Wang Y F, Zhang Z H, Ma J H, et al. KFRNN: An effective false data injection attack detection in smart grid based on Kalman filter and recurrent neural network[J]. IEEE Internet of Things Journal, 2022, 9(9): 6893-6904.

[45] 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.

[46] Sawas A M, Khani H, Farag H E Z. On the resiliency of power and gas integration resources against cyber attacks [J]. IEEE Transactions on Industrial Informatics, 2021, 17(5): 3099-3110.

[47] Kwon S, Yoo H, Shon T. IEEE 1815.1-based power system security with bidirectional RNN-based network anomalous attack detection for cyber-physical system[J]. IEEE Access, 2020, 8: 77572-77586.

[48] 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.

[49] Li Y C, Zhang P, Ma L Q. Denial of service attack and defense method on load frequency control system[J]. Journal of the Franklin Institute, 2019, 356(15): 8625-8645.

[50] Shan A L, Li Y C. Learning multilevel auto-encoders for DDoS attack detection in smart grid network[J]. IEEE Access, 2019, 7: 108647-108659.

[51] Abdulaal M J, Ibrahem M I, Mahmoud M M E A, et al. Real-time detection of false readings in smart grid AMI using deep and ensemble learning[J]. IEEE Access, 2022, 10: 47541-47556.

[52] Lepolesa L J, Achari S, Cheng L. Electricity theft detection in smart grids based on deep neural network[J]. IEEE Access, 2022, 10: 39638-39655.

[53] Camana Acosta M R, Ahmed S, Garcia C E, et al. Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks[J]. IEEE Access, 2020, 8: 19921-19933.

[54] Ravikumar G, Govindarasu M. Anomaly detection and mitigation for wide-area damping control using machine learning[J]. IEEE Transactions on Smart Grid, 2024: 1.

[55] Singh V K, Govindarasu M. A cyber-physical anomaly detection for wide-area protection using machine learning[J]. IEEE Transactions on Smart Grid, 2021, 12(4): 3514-3526.

[56] Syed M H, Guillo-Sansano E, Wang Y, et al. Real-time coupling of geographically distributed research infrastructures: Taxonomy, overview, and real-world smart grid applications[J]. IEEE Transactions on Smart Grid, 2021, 12(2): 1747-1760.

[57] Kumari A, Patel M M, Shukla A, et al. ArMor: A data analytics scheme to identify malicious behaviors on Blockchain-based smart grid system[C]//Proceedings of GLOBECOM 2020-2020 IEEE Global Communications Conference. Piscataway, NJ: IEEE, 2020: 1-6.

[58] Samy S, Banawan K, Azab M, et al. Smart blockchain-based control-data protection framework for trustworthy smart grid operations[C]//Proceedings of IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). Piscataway, NJ: IEEE, 2021: 0963-0969.

[59] Abou E H Z, Hafid A, Khoukhi L. Blockchain meets AMI: Towards secure advanced metering infrastructures [C]//Proceedings of ICC 2020-2020 IEEE International Conference on Communications (ICC). Piscataway, NJ: IEEE, 2020: 1-6.

[60] Butt A S, Huda N U, Amin A A. Design of fault-tolerant control system for distributed energy resources based power network using Phasor Measurement Units [J]. Measurement and Control, 2023, 56(1/2): 269-286.

[61] Reijsbergen D, Maw A, Dinh T T A, et al. Securing smart grids through an incentive mechanism for blockchain-based data sharing[C]//Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy. New York: ACM, 2022: 191-202.

[62] Maw A, Adepu S, Mathur A. ICS-BlockOpS: Blockchain for operational data security in industrial control system [J]. Pervasive and Mobile Computing, 2019, 59: 101048.

[63] Li M, Hu D H, Lal C, et al. Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things[J]. IEEE Transactions on Industrial Infor-

matics, 2020, 16(10): 6564-6574.
[64] Ramanan P, Li D, Gebraeel N. Blockchain-based decentralized replay attack detection for large-scale power systems[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(8): 4727-4739.
[65] Ferrag M A, Maglaras L. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1285-1297.
[66] Samuel O, Javaid N. GarliChain: A privacy preserving system for smart grid consumers using blockchain[J]. International Journal of Energy Research, 2022, 46(15): 21643-21659.
[67] Kong P Y. A review of quantum key distribution protocols in the perspective of smart grid communication security[J]. IEEE Systems Journal, 2022, 16(1): 41-54.
[68] Ajagekar A, You F Q. Quantum computing based hybrid deep learning for fault diagnosis in electrical power systems[J]. Applied Energy, 2021, 303: 117628.
[69] Alshowkan M, Evans P G, Starke M, et al. Authentication of smart grid communications using quantum key distribution[J]. Scientific Reports, 2022, 12(1): 12731.
[70] ORNL. ORNL, LANL-developed quantum technologies go the distance[EB/OL]. (2020-05-12) [2023-08-10]. https://www.ornl.gov/news/ornl-lanl-developed-quantum-technologies-go-distance.
[71] EPB. EPB quantum network powered by qubitekk accepting applications[EB/OL]. (2023-07-25) [2023-08-10]. https://epb. com/newsroom/press-releases/epb-quantum-network-accepting-applications.
[72] 王蕙蓉. 量子破解“电力孤岛”,赋能电网系统[EB/OL]. (2022-05-15) [2023-08-10]. https://www. thepaper. cn/newsDetail_forward_17797502.
[73] 孙冉冉, 余建斌. “量子加密”助力新型电力系统[EB/OL]. (2022-01-17) [2023-08-10]. http://finance. people. com.cn/n1/2022/0117/c1004-32332535.html.

Network security risks and new countermeasures under the smart grid environment

YUE Fang[1,2], WANG Xuezhen[3], JIANG Shan[4*]

1. National Science Library (Wuhan), Chinese Academy of Sciences, Wuhan 430071, China
2. Hubei Key Laboratory of Big Data in Science and Technology, Wuhan 430071, China
3. Ningbo Institute of Materials Technology and Engineering, Chinese Academy of Sciences, Ningbo 315201, China
4. Yongjiang Laboratory, Ningbo 315202, China

Abstract The smart grid integrates network and information technologies with the grid to enhance the reliability, security, and efficiency of the power system. However, in a highly digitalized and interconnected environment, the smart grid faces increasingly complex and variable network security risks. This paper outlines the concept and architecture of the smart grid, indicating that its biggest difference from the traditional grid is bidirectional interactivity. Then, the security vulnerabilities and cyber attacks are summarized in terms of three categories, namely confidentiality attacks, integrity attacks, and availability attacks. Then, new strategies for enhancing the network security of smart grid, such as machine learning, blockchain, quantum computing are reviewed. Machine learning algorithms can improve the accuracy and sensitivity of power grid fault detection and attack identification. Blockchain technology provides solutions for identity verification, data security, and privacy protection through its decentralized and tamper-resistant features. Quantum computing has significant application potential in power grid fault diagnosis and data transmission security. Finally, the major challenges and future research directions are prsented.

Keywords smart grid; cyber attacks; machine learning; blockchain; quantum computing

（责任编辑 傅雪）