能源关键基础设施网络安全威胁与防御技术综述

李建华*

(上海交通大学网络安全技术研究院 上海 200240)

(中国能源研究会能源网络安全研究中心 北京 100045)

摘 要：在信息技术飞速发展的背景下，能源关键基础设施得到了变革性的飞速发展，与人工智能、大数据、物联网等新技术深度融合。信息技术在显著优化能源关键基础设施的效率和性能的同时，也带来了更加具有持续性和隐蔽性的新型安全威胁。如何针对能源关键基础设施建立体系化、智能化的安全防御体系是亟需解决的问题。该文从能源关键基础设施本身的发展趋势入手，对其面对的传统和新型安全威胁的机理进行了分析。在此基础上，对能源关键基础设施的防御技术演进进行深入的研究和分析。

关键词：能源关键基础设施；网络安全；人工智能；高级持续威胁；软件定义网络

中图分类号：TN915.08; TP393 **文献标识码**：A **文章编号**：1009-5896(2020)09-2065-17

DOI: 10.11999/JEIT191055

Overview of Cyber Security Threats and Defense Technologies for Energy Critical Infrastructure

LI Jianhua

(*Institute of Cyber Science and Technology*, *Shanghai Jiao Tong University*, *Shanghai* 200240, *China*)

(*Research Center for Energy Security*, *China Energy Research Society*, *Beijing* 100045, *China*)

Abstract: Energy critical infrastructure has undergone transformative rapid development in the context of the rapid development of information technology, and has been deeply integrated with new technologies such as Artificial Intelligence (AI), big data, and the Internet of Things. While information technology significantly improves the efficiency and performance of energy critical infrastructure, it also brings new types of security threats that are more persistent and covert. An urgent problem is how to establish a systematic and intelligent security defense system for energy critical infrastructure. This paper starts with the development trend of energy critical infrastructure, and analyzes the mechanism of the traditional and new security threat mechanisms it faces. On this basis, insightful analysis on the research status and evolution trends of defense technologies for energy critical infrastructures is made.

Key words: Energy critical infrastructure; Cyber security; Artificial Intelligence (AI); Advanced Persistent Threat (APT); Software-defined networking

1 引言

能源，是指能够向人类生产活动提供能量的各种资源，包括风能，电能，太阳能，核能等。对于一个成熟的工业化国家，能够安全高效地利用各类能源是其长期可持续发展的先决条件。在信息时代，新能源技术与网络技术深度融合，形成了能源互联网这一全新的能源利用体系，对社会的经济发展模式与人们的生活方式带来了深远的影响。能源互联网可理解是综合运用先进的电力电子技术，信息技术和智能管理技术，将大量由分布式能量采集装置，分布式能量储存装置和各种类型负载构成的能源节点互联起来，以实现能量双向流动的能量对等交换与共享网络。作为能源互联网的重要组成部分，能源关键基础设施是指综合运用先进的互联网技术，将新型电力网络、石油网络、天然气网络等能源节点串联起来，保障国家经济正常运行，为政府和人民提供服务的重要系统。能源关键基础设施关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全和公共利益。近年来，以智能电网为代表的能源关键基础设

收稿日期：2019-12-31；改回日期：2020-08-05；网络出版：2020-08-06

*通信作者： 李建华 lijh888@sjtu.edu.cn

基金项目：国家自然科学基金(61431008)

Foundation Item: The National Natural Science Foundation of China (61431008)

施逐渐成为了现阶段的研究热点。智能电网是在传统电力系统基础上，通过集成先进传感技术、信息通信技术、控制技术、智能技术、新能源、新材料和储能技术等形成的新一代电力系统，具有高度信息化、自动化、互动化、智能化等特征，可以更好地实现电网安全、可靠、经济、高效、自治运行[1]。在以往传统电网结构下，大量采用机械式电力结构、人工操作结构，对电网的控制能力较弱，对电网用电需求的峰值波动没有很好的处理办法。随着电网承载的能量越来越大，中心化发电，通过远程输电配电的传统电网发展成熟，替代了早期工厂的本地建设发电设备的模式，成为主流的电网结构。

由于先进信息技术的引入，在传统电网的结构基础上，大量数字设备被安装进入电网，可以通过数字技术对电网的电力资源以及负载进行数字化管理，大量采用自动化设备实现对电网的控制，从而提高了对电网的控制能力，因此，在传统电网的中心化结构下，通过数字化改造，电网进入了数字化电网时代。二十一世纪以来，随着大规模新能源的使用，例如风能、太阳能等，分布式发电结构被大量运用，同时，用户对个性化服务的需求也不断上升。因此，在数字化电网的基础上，实现扁平化结构改造，实现柔性控制，提高电网的灵活性，是智能电网时代的发展目标，通过高效的信息技术，实现能源的优化流动、管理和应用。目前，虽然各国对智能电网的定义各有侧重，但是各国建设智能电网的任务都一样，一定要保证安全，一定要使能源利用达到经济优质、高效清洁的目的[2–4]。当前，人工智能、大数据、云/雾计算等先进的信息技术已经在能源关键基础设施中得到了广泛应用，对发电、输电、配电和用电等环节的智能化和高效性起到了关键作用。但是，与此同时，先进的信息技术也给能源关键基础设施的数据、网络、设备和业务流程带来了更多的脆弱性和更大的受攻击面。以震网、BlackEnergy为代表的多样化的高级持续威胁(Advanced Persistent Threats, APT)给伊朗、乌克兰、委内瑞拉等国家的能源关键基础设施造成了毁灭性的打击，并严重危害了这些国家的安全和稳定。

在能源领域，信息安全风险总是伴随着新技术的发展进步而不断出现。在5G物联网快速发展的今天，传统信息安全技术已经难以在复杂信息物理环境下为能源互联网提供高效、精准的检测与评估能力。传统的信息安全防护基础理论与关键技术发展明显滞后于当下基于5G通信技术的能源互联网融合发展进程。主要表现在：

第一，能源控制虚拟化、计算资源切片化环境下的数据安全责任体系建设还是空白，技术上未能实现能源控制数据与网络控制数据的智能化协同处理，进而导致能源安全风险和网络安全风险的度量原则、评价依据和分级标准缺乏自适应能力。

第二，能源系统越来越处于开放的网络环境中，5G环境下的能源互联网将支持移动用户对能源生产，存储，转换周期的个性化、透明化的管理与控制，因而网络攻击日趋多样化、专业化。安全防护边界已经从传统的能源企业内外网，拓展到App、智能终端及传感器。传统安全防护技术手段缺乏先边界加固后纵深防御的理念，远远不能满足新形势下高危复杂多变的能源生产安全稳定应用需求。

第三，智能传感器、分析软件、云服务等新型技术在能源互联网里的广泛应用一方面便利了行业人员进行宏观调控管理，另一方面也成为黑客新的攻击面，带来了新的安全威胁。传统防护策略下，能源智能设备的更新、升级周期大多较长，缺乏灵活性和自优化能力，不得不以当前的技术防御未知的攻击，缺乏对安全事件的深度分析能力和关联预测能力。

如何在通信技术日新月异，安全威胁不断演进的新形势下保障能源关键基础设施网络安全，越来越受到国内外学界和业界的重视。但是，总体上该领域还处于研究的起步阶段，国内外都尚未形成系统、全面、深入的研究成果。

能源关键基础设施作为国家关键基础设施的重要组成部分，其安全性直接影响到国家安全和社会稳定。本文从以电力基础设施为代表的能源关键基础设施本身的发展趋势入手，对其面对的传统和新型安全威胁的机理进行了分析，进而对能源关键基础设施的防御技术演进进行深入的分析，为我国的能源关键基础设施网络安全防御提供良好的参考。

2 能源关键基础设施的现状与发展

在全球能源危机与气候变暖背景下，能源关键基础设施将成为现代社会生产力保持高速发展的基石，而能源关键基础设施的信息安全保障将成为构建国家能源主体安全体系的重中之重。下面以智能电网为代表，介绍了能源关键基础设施研究的发展趋势。

2.1 能源关键基础设施的演进

传统电网由极其复杂且固件化的变压器、断路器、输配电线路等设施组成，这些电力设备普遍使用着专用的管理系统，并运行着大量低效率、高能耗、安全性低的应用，且各功能的运行在地理上通

常是孤立的、非协作的。如此封闭式的电网架构越来越难以满足当今社会中企业、运营商以及用户日益灵活多变的用电需求。

针对传统电网的种种弊端，国内外纷纷开展了智能电网的研究工作。文献[5]针对国际上智能电网相关主要研究项目进行了详细分析。美国能源部(Department Of Energy, DOE)于2001年组建了工作组专门负责提供分布式能源的通信技术与控制技术方案以图改造传统电网模式。2007年，DOE在其发布的GridWise中描绘了向智能电网变革的前景[6]。同年，美国联邦政府通过两个议会法案：(1)智能电网规划与安全法案；(2)美国复苏与再投资法案，对智能电网未来发展分别提供了有效的政策支持和大量的资金支持[7]。2012年，Fang等人[8]通过对全球智能电网支持项目、标准化研究进展和相关领域的创新学术成果进行调研，对包括发电、输电、配电以及微电网等在内的智能电网基础设施，包括智能抄表、实时状态监控、数据聚合分析建模等智能电网信息管理系统，以及包括无线自组织网络、蜂窝网络、认知无线电、IEEE802.1x、卫星通信、微波通信、光通信和电力线通信等在内的先进通信技术进行了详细的综合分析，并指出智能电网信息安全威胁防御将成为未来智能电网发展过程中亟需突破的难题。近年来，在政府政策和企业基金的大力支持下全球智能电网又取得新的发展，尤其是在信息与通信技术突飞猛进的今天，云计算、物联网、新型通信网络、边缘计算、大数据、人工智能的出现正在有力的推动着电网信息物理系统孤岛之间的互连、互通、互操作，全球智能电网正在走向成熟化、实用化[9–14]。

Embix已经与英特尔欧洲实验室联合开展一项名为‘COOPERATE’的研究项目，该项目基于欧洲(CEN-CENELEC-ESI)和美国(NIST)的最新的国际互操作性标准，致力于节能社区方面的研究，得到了欧盟第七框架计划的资金支持。在全球范围内，阿尔斯通电网已经参与了超过30个智能电网试点示范项目。从这些项目积累的经验中可以总结出智能电网与传统电网的本质区别，双向的信息和能量流动使智能电网无缝地融入了智慧城市的健康发展。智能电网兼容传统电网的同时，又能够灵活、安全、高效地接纳智慧城市中各种新技术的出现，并适应了新场景的能源需求。

近年来，我国借鉴欧美以智能电网为代表的能源关键基础设施项目的研究经验，对我国智能电网的未来发展、技术组成以及实现步骤等进行了统一规划和研究[15]。在“十一五”期间，电力信息化建设已纳入国家电网发展的总体战略，电力工业的软件系统也逐步升级。进入“十一五”之后，国家电网公司开始实施以电网信息化为主题的“SG186”信息化工程。2011年发布的《国民经济和社会发展第十二个五年规划纲要》提出的“十二五”期间电力行业转型升级、提高产业核心竞争力的总体任务是“适应大规模跨区输电和新能源发电并网的要求，加快现代电网体系建设，依托信息、控制和储能等先进技术，推进智能电网建设，切实加强城乡电网建设与改造，增强电网优化配置电力能力和供电可靠性。目前，《电力发展“十三五”规划2016～2020》为绿色、高效、协调、节约的共享性电力需求供应系统的建设指明了方向和总体路线。

经过近二十年的发展，能源生产，能源运输，能源使用等各个环节的能源关键基础设施能够以智能电网的形式实现互联互通，通过现代化的ICT技术逐渐构建了基于物联网的能源状态信息采集系统、电能质量检测系统、自动化配电系统、设备状态检测系统、动态能源交易系统等，如图1所示。其主要特征包括：可视化、双向流动、去中心化、数字化、网络化和移动支持等。

2.2 能源关键基础设施网络安全成为学术界和产业界的关注热点

以智能电网为例，智能电网通过把传统电网孤立而封闭的变电站、输配系统、电力市场、需求侧管理以及多样化的新能源系统等通过先进的传感测量技术、自动化控制技术、高速双向的通信技术(如5G等)和高级决策优化技术(如云计算、大数据分析、人工智能等)进行大规模的互连，从而实现更加安全、可靠、灵活、高效、经济、自适应、生态友好的电力资源管控。智能电网将成为下一代电网架构变革的主流趋势。然而，智能电网正在面临着前所未有的信息安全威胁挑战。随着电网系统的智能化发展，国内外学术界和产业界对智能电网及其安全的研究越来越重视。在当前的学术领域，由IEEE Power and Energy Society, IEEE Communications Society, IEEE Computer Society主办的国际顶级会议如SmartGridComm, INFOCOM, ICC, SIGCOMM等会议和IEEE Trans. on Smart Grid, IEEE Trans. on Industrial Informatics, IEEE Trans. on Mobile Computing等SCI期刊，以及国内EI期刊《电力系统自动化》，《计算机学报》，《中国电机工程学报》中，智能电网及其信息安全已经成为国内外学者关注的新热点。国外(尤其是美国)针对当前智能电网架构的信息安全保障方面

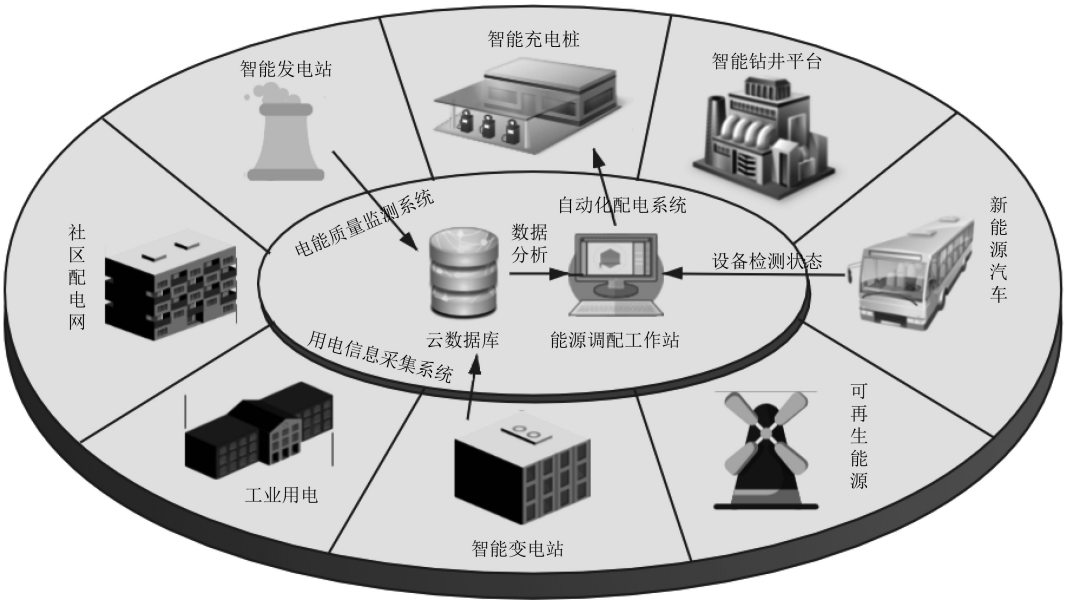

图 1 能源关键基础设施基本架构

的研究已经逐渐深入到电网攻击检测与建模[16–18]、电网状态数据的安全采集和存储[19]、智能电网安全通信协议的设计与分析[20–22]，智能电网用户身份识别与访问控制[23]等内容上；而国内针对智能电网信息安全的研究明显落后于国外，尚处于对智能电网及其信息安全威胁的认知阶段。中国电力科学研究院在文献[24,25]中分别分析了在将分布式能源集成电网主干系统过程中输配电电压的协同调控问题和微电网的配置与优化问题，并基于国内现有基础设施条件提出了有效的调度优化算法；清华大学成立了能源互联网创新研究院，研究方向主要包括能源战略与运筹、能源仿真与调控、直流电网、电力电子器件及其高端应用、大容量储能、新能源发电及电工新材料、能源传感及网络通讯、能源大数据分析等多个能源互联网核心技术，力争攻克关键前沿科技难题、取得突破性创新研究成果，为我国建立基础设施智能化、生产消费互动化、信息流动充分化的新型能源体系；国家电网公司信息化“SG186”工程通过评审，“SG186”工程安全防护总体方案对电网管理信息系统安全防护的对象、方案、技术实施要点和产品需求给出了详细的规划和建议，目前国内电网信息系统防护大多采用该方案进行部署，是我国电网安全防护从单纯的物理防护向信息-物理交叉防护的重要标志。

与此同时，国内外产业界也逐渐加大资金投入以加快针对智能电网及其信息安全保障产品开发和规模化使用。根据ZionResearch的市场调研，2020年全球智能电网市场价值将达到1200亿美元，且透明度市场调研公司(transparency market research)的报告预测全球智能电网的安全市场将从2016年的43.5亿美元增至2025年的105.8亿美元，期间年复合增率达10.5%。目前，国际知名企业如Intel, Siemens, Symantec, IBM, Cisco, Honeywell International, Maxim, ABB等已经成为全球智能电网及其安全产品的关键参与者，并积极发布了相关智能电网安全战略发展规划。其中，思科发布了Cisco Smart Grid能够支持电力行业的单位建立基于标准的安全网络，从而有效满足发电、配电、能源储备和消耗的需求；ABB推出的新型智能外置无线传感器能够实时监测电机的运行状态，将相应的状态数据通过互联网传输到安全的云服务器上，从而保证发电厂电机运行的安全性；Maxim公司推出的MAX36025能够为智能电网的数据集中器增设安全加密功能。据称，仅ABB推出的新型智能外置无线传感器能够使工作人员通过用户终端安全地获取电机运行的趋势数据、运行时间以及负载数据等，进而帮助智能电网用户降低近70%的电机故障停工时间，并延长30%的电机使用寿命，同时将减少近10%的能耗。2013年，包括国家电网公司、思源电气和西南电气等在内的智能电网领跑者在“十二五期间”对特高压输电、电力需求侧管理技术、电网资源优化技术等电网输配电系统进行了升级[26,27]，但从公开资料调研发现，“十二五”期间我国企业单位并没有针对智能电网信息安全防护开展产品研发。我国在智能电网信息安全威胁防御产品的研发与生产领域尚处与空白阶段。

国际上对智能电网相关信息技术及其信息安全技术的标准化研究也在步步推进[28]。2011年由美国

国家标准与技术研究院(NIST)提出并制定的IEEE P2030智能电网标准和互通原则《IEEE P2030 能源技术和信息技术与电力系统(EPS)、最终应用及负荷的智能电网互操作性指南》[29]正式获批，对企业了解如何以及在何处发展智能电网系统及其应用提供了理论依据。该指南还描述了未来智能电网发展所需要建立的其他相关标准。目前智能电网信息安全相关的标准如表1所示。其中，美国国家标准与技术研究院(NIST)从智能电网的安全策略需求、工业系统安全控制、大电力系统安全控制、工控系统保护文件等多个方面分别制定了建议规范；而IEEE在IEEE 1686-2007规范中对智能电网关键基础设施智能电子设备安全进行了标准化，IEC制定了智能电网中数据及数据传输安全的IEC 62351标准，该标准规范了适合在智能电网环境下防止敏感信息泄露、关键数据篡改的加密技术和认证技术。

近几年，我国国家重点研发计划、自然科学基金等对智能电网的相关基础理论研究加大了投入，但对智能电网信息安全威胁防御基础理论和方法应用研究立项还很少。然而，根据前期调研，国际上对全面评估智能电网信息安全威胁并开展智能电网攻击防御体系构建是保障未来智能电网安全运行的前提保障已经达成共识，且单纯依赖传统的数据加密、签名技术，漏洞挖掘技术，防火墙技术，入侵检测技术等开展被动的信息安全防御难以适应未来智能电网环境所面临的新型信息安全威胁。

3　能源关键基础设施面临的网络安全威胁

3.1　能源关键基础设施面临的传统安全威胁

先进通信网络技术的引进，给能源关键基础设

表 1　国内外现有智能电网安全相关标准与规范

国际标准与规范	
标准、建议、规定、指南	制订单位
Smart Grid Cyber Security Strategy and Requirements (DRAFT NIST 7628)	National Institute of Standards and Technology (NIST)
IEEE 21451 -- Standard for a Smart Transducer Interface for Sensors, and Actuators	Shanghai Jiao Tong University (NIST)
Good Practice Guide, Process Control and SCADA Security	Centre for the Protection ofNational Infrastructure (CPNI)
ANSI/ISA-99 Manufacturing and Control Systems Security' Part 1: Concepts, Models and Terminology (2007) Part2: Establishing a Manufacturing and Control Systems Security Program (2009)	The International Society of Automation (ISA)
21 steps to Improve Cyber Security of SCADA Networks	U.S. Department of Energy (DOE)
Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82)	National Institute of Standards and Technology (NIST)
Recommended Security Controls for Federal Information Systems (including those for Bulk Power System) (NIST SP 800-53)	National Institute of Standards and Technology (NIST)
Advanced Metering Infrastructure (AMI) System Security Requirements	Advanced Security Acceleration Project (ASAP) – Smart Grid
Security Profile for Advanced Metering Infrastructure	Advanced Security Acceleration Project (ASAP) – Smart Grid
Utility AMI Home Area Network System Requirements Specification	Utility AMI
IEC 62351 1-8, Power System Control and Associated Communications – Data and Communication Security	International Electrotechnical Commission (IEC)
IEEE 1686-2007, IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities	IEEE
CIP-002, 003-009	North American Electric Reliability Corporation (NERC)
Cyber Security Procurement Language for Control Systems	Department of Homeland Security (DHS)
System Protection Profile - Industrial Control Systems	National Institute of Standards and Technology (NIST)
Catalog of Control Systems Security: Recommendations for Standards Developers	Department of Homeland Security (DHS)
Wireless Standards (ISA SP100)	ISA
国内标准与规范	
电力监控系统安全防护规定	发改委
信息安全技术安全可控信息系统电力系统安全指标体系	中国电力科学研究院
电力系统管理及其信息交换数据和通信安全	全国电力系统管理及其信息交换标准化技术委员会

施的运行和管理带来了极大的方便，同时也给传统和能源关键基础设施带来了巨大的安全隐患。当前能源关键基础设施遭受的传统信息安全威胁，主要包括发电系统攻击[30]、相量同步测量单元(Phasor Measurement Units, PMU)攻击[31]、状态估计攻击[32]、封锁攻击[33]、负载重分配攻击[34]、信息物理交换攻击[35]、分布式系统和用户侧攻击[36]、虚假数据注入攻击[37]、电力市场攻击[38]、变电站攻击[39]以及传统网络攻击等。在输电系统中，比较具有代表性的攻击为封锁攻击(interdiction attacks)，其为输电系统在大规模恶意攻击情况下第一个被研究的脆弱性问题。封锁表示在输电系统中的线路、变压器、变电站、总线等等出现跳脱[40]。在实践中，封锁攻击可以直接通过恶意的控制命令或者间接的通过错误的测量数据实现。而在消费者端，客户方攻击体现在高级测量体系(Advanced Metering Infrastructure, AMI)系统下数以百万计的智能电表随时受到安全威胁，由于受到成本和性能的限制，大多数的智能电表都使用轻量级的安全机制，因此，也会被当成大量的恶意攻击的攻击目标。其中虚假数据注入攻击也是一种常见的客户方攻击，与此同时，该攻击也会向数据采集与监视控制系统(Supervisory Control And Data Acquisition, SCADA)中注入虚假数据。其目的是为了攻击能源关键基础设施系统中的状态估计，通过在用户端注入虚假数据，从而使得状态估计出现偏差，从而获得错误的控制命令，完成攻击。另外，能源关键基础设施中的大量的数据信息和控制信息都会通过公开的互联网进行传输，因此，在传统网络中存在的攻击威胁，同样也会发生在能源关键基础设施中。

3.2 能源关键基础设施面临的新型安全威胁

近年来，出现了一系列不同于传统攻击的新型威胁，绕过了能源关键基础设施中已有的防御体系，造成了巨大影响。就近几年发生的多起工控安全事件而言，攻击者都是对能源关键基础设施发起高级持续威胁(Advanced Persistent Threat, APT)。APT的原理相对于其他攻击形式更为高级和先进，攻击者通常利用隐蔽和复杂的攻击手段对工控进行有针对性地长期持续性网络攻击的攻击和渗透。

3.2.1 能源关键基础设施面临的新型安全威胁介绍

当威胁从传统的漏洞挖掘与利用向新型APT演进的时候，能源关键基础设施比传统能源设施更容易受到影响，如图2所示。(1)能源关键基础设施系统中存在大量分布式的可再生能源发电设备，系统通过数百万个智能测量设备提供了在能源关键基础设施中的双向、实时的通信系统，实现了优化的能量管理以及用户激励，这些复杂能源业务与信息系统深度融合。APT往往跨能源关键基础设施业务和信息系统，利用其跨空间脆弱性实施攻击，跨空间风险因素难以识别给APT防御带来了极大的困难；(2)与传统攻击相比，APT具有强针对性、潜伏性、隐蔽性的特点，从威胁情报的角度，当前依然缺乏有针对性地对APT的弱信号、低关联、慢时变威胁情报进行有效分析；(3)在对APT跨空间风险进行识别和针对性威胁建模之后，必须对APT的攻击行为和攻击路径进行形式化建模，才能进行有效的APT防御，但是目前在能源关键基础设施中依然缺乏对APT建模的有效方法；(4)在能源关键基础设施中，由于APT利用水坑攻击，远程执行等技术，导致其具有动态性、长期纠缠性、随机性，使得传统的检测、隔离防御方法失效。如何有针对性地实施新的防御，是亟需解决的问题。

综上，能源关键基础设施作为国家重要能源基础设施，关系着国家安全和社会全民安全的命脉，一旦受到网络攻击威胁，将对整个国家及社会带来不可估量的损失和安全隐患。因此，研究针对能源关键基础设施信息安全威胁防御技术已经成为能源关键基础设施发展亟需解决的首要问题。目前，由于能源关键基础设施中数据采集与存储的时空分散性、异常定位分析与响应的超低时延要求、主动输配电调控的强动态性、新能源系统接入的间歇性、移动用户即插即用之需求的时空不确定性以及跨时空状态管理与风险估计的复杂性使得攻击者能够利用能源关键基础设施中广泛存在的脆弱节点(如大规模部署的传感器等)以更隐蔽的方式发起新型APT[41]。另一方面，传统的安全防护仅仅依靠部署于边界或特殊节点的防火墙、入侵防御系统(Intrusion Prevention System, IPS)、入侵检测系统(Intrusion Detection System, IDS)等安全设备进行的静态控制，实行以特征检测为主的网络安全监控，这种被动式防御已不再适用于在能源关键基础设施中面向新型APT的防御。因此，如何有效实现面向能源关键基础设施新型APT的有效防御，已成为目前国内外学术界和工业界亟需解决的问题。

3.2.2 能源关键基础设施面临的新型安全威胁的现状

2010年6月，伊朗“震网”病毒席卷全球，对以能源基础设施为代表的核电站、智能电网、水坝实施蠕虫病毒，对伊朗布什尔核电站造成了严重影响。此外，2014年3月，韩国国防部高调宣布正在

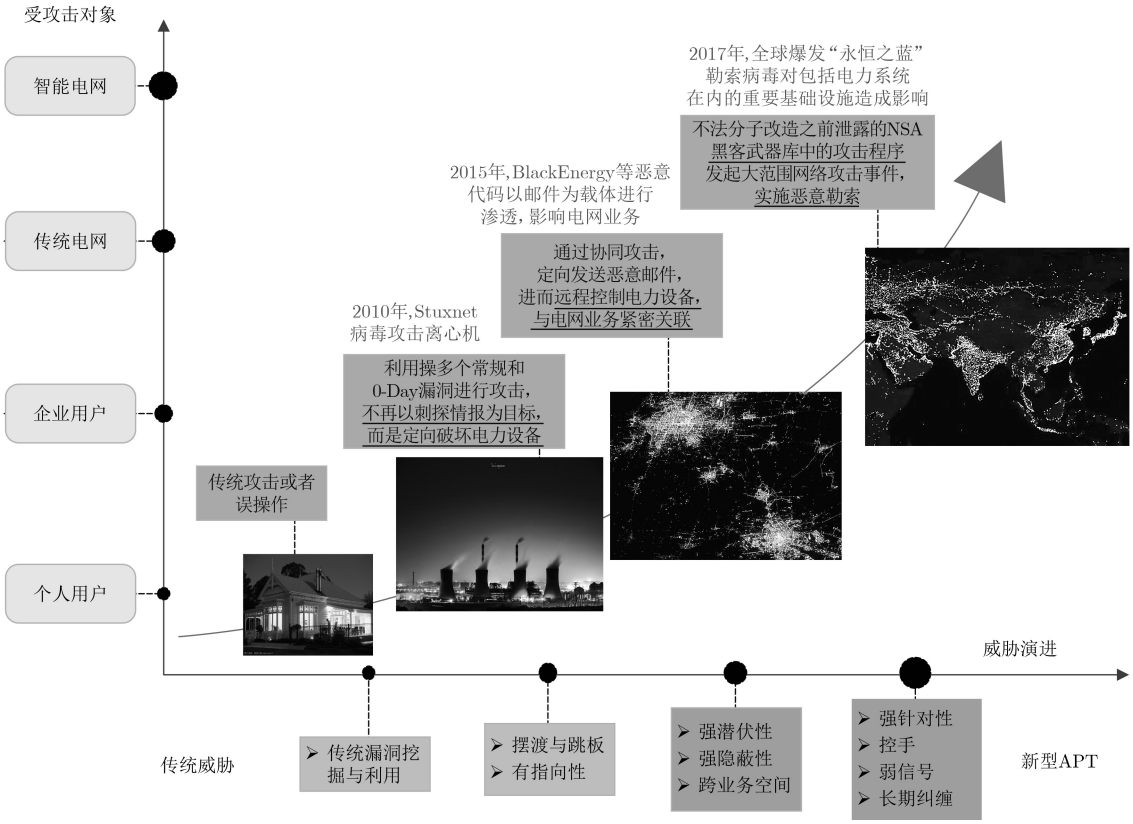

图 2 能源关键基础设施的网络安全威胁演进

对朝鲜实施“网络战”，以成功攻击伊朗核设施的“超级工厂病毒”(stuxnet)为蓝本，研发一种类似的网络病毒，旨在对朝鲜核设施造成物理性破坏。另外，极光攻击(aurora attack)直指[42]发电系统，利用了自动增益控制系统(AGC)的初始控制器的脆弱性实现的，攻击者通过快速开关发电机的电路的断路器，使得发电机无法同步，最终被摧毁。2015年12月，乌克兰国家电网受到“BlackEnergy”恶意组件的攻击，通过协同攻击，定向发送恶意邮件，进而远程控制关键电力设备，导致大面积长时间停电，数十万户居民的生活受到了影响[43,44]。

与传统能源设施不同，能源关键基础设施中使用了大量的计算机软件来代替人工实现对电能资源的调控，在这些软件开发过程中，漏洞往往会在代码的架构、设计或编写过程中引入。例如引入了安全程度较低的或恶意的第三方代码库，使用了不受信任的开发框架，都可能导致漏洞或恶意代码出现在终端的运行软件中。在运行维护工作中，如果不及时更新系统和相关软件补丁，也容易导致漏洞攻击的发生。2017年5月12日，黑客借助由美国国家安全局泄露出的漏洞攻击工具，利用高危漏洞Eternal Blue (永恒之蓝)在世界范围内传播Wanna Cry勒索病毒致使Wanna Cry勒索病毒大爆发。据相关报道，包括美国、英国、中国等在内的150多个国家地区近30万台设备均受到其攻击。其影响涉及教育、金融、能源和医疗等众多行业，造成了严重的信息安全问题[45]。在我国，部分校园网用户受害严重，实验室数据和毕业设计被锁定加密，部分大型企业由于应用系统和数据库文件被加密后无法正常工作，影响巨大。在信息化发展如此迅猛的今天，其带来的危害及影响相当严重[46]。勒索病毒Wanna Cry与以前的勒索软件有非常明显的区别，它具有蠕虫性质，具有传播速度更快、传播范围更广，全程自动化、攻击行为更隐蔽，感染无法补救、危害程度深等特点。勒索病毒利用“永恒之蓝(Eternal Blue) ”SMB漏洞攻击工具，穿透网络边界进入内部网络区域对目标主机进行端口扫描，目标主机被成功攻陷后会从攻击机下载Wanna Cry木马进行感染，木马母体为mssecsvc.exe，运行后会扫描随机IP的互联网机器，也会扫描局域网相同网段的机器进行感染传播，此外还会释放敲诈者编制的程序tasksche.exe，对磁盘文件进行加密勒索[47]。

以乌克兰电网APT事件为例来分析，攻击者通过鱼叉式钓鱼邮件或其他手段，首先向“跳板机”植入BlackEnergy，建立据点，然后向其他主机进行渗透，包括办公区的主机、便携设备以及电网控制层的关键主机作为跳板，从而攻击获得SCADA系统的关键主机的控制权限。另外，不排除攻击者

在攻击实施前，已经通过长期渗透完成对电力系统的环境预置。在攻击者获得SCADA系统的控制能力后，通过下达断电指令导致电力系统断电。另外同时破坏了SCADA对上层的故障回馈和显示能力，导致工作人员无法定位故障，有效恢复电力。另外，在攻击电力系统的同时，攻击者通过线下的DDoS攻击，使得电力客服中心瘫痪，从而无法定位断电用户区域，从而更长期拖延电力恢复的时间。其攻击流程如图3所示。

3.2.3 能源关键基础设施的安全脆弱性

以高级持续威胁(Advanced Persistent Threat, APT)为代表的弱信号、低关联、慢时变的攻击方式严重威胁着能源关键基础设施安全运行[48,49]。然而，也正是能源关键基础设施对于ICT技术的强依赖性，能源关键基础设施安全将面临来自信息系统及信息物理融合方面的诸多新威胁。目前，针对能源关键基础设施安全威胁来源方面的研究比较分散，还没有形成全面而明确的能源关键基础设施安全威胁来源分析框架。通过对现阶段研究的资料的整理，本文总结出能源关键基础设施中存在以下3种常见的新型信息安全威胁来源：

(1) 能源关键基础设施中传感测量等设备的脆弱性：

能源关键基础设施中传感测量设备的大量部署导致数据采集与存储在时空上呈现强分散性。大量缺乏信息安全防护的传感测量设备为攻击者以更隐蔽、更低代价的方式搜集并发现系统中存在的脆弱点提供便利的同时，增加了攻击定位、溯源、拒止的难度[50]。

基于Zigbee的家庭网络中能源关键基础设施通信的安全威胁主要来自于节点的脆弱性如内存溢出、能量耗尽、网管失效等[51]；而能源关键基础设施中的AMI的数据安全性威胁主要集中在用户用电习惯、地址等隐私的信息保护方面[52]；文献[53]提出了一种针对能源关键基础设施的能量转换节点的攻击策略，该攻击策略将能够导致能源关键基础设施级联的失效，并导致大规模停电；实时地发电调节与能源关键基础设施负载管理和传输状态监管由相位测量单元PMU感知并经SCADA系统/能源管理系统(Energy Management System, EMS)等进行管理，PMU与SCADA/EMS系统的数据及数据交换过程中数据的机密性存在安全风险，攻击者可能稀疏的隐蔽在分布式的仪表，难以通过流量审计等常规方法进行检测[54]；此外，在用户侧，资源有限的智能电表及其通信也将面临网络攻击威胁，其日志记录、用户权限等敏感信息泄露可能成为攻击者发起二次攻击的重要参考[55]。

(2) 能源关键基础设施通信网络的脆弱性：

相比传统能源关键基础设施，用于智能电子设备互连互通的网元(无线接入点、工业交换机、路由器、网管服务器等)成为新型能源关键基础设施的重要组成部分。能源关键基础设施中对电力服务

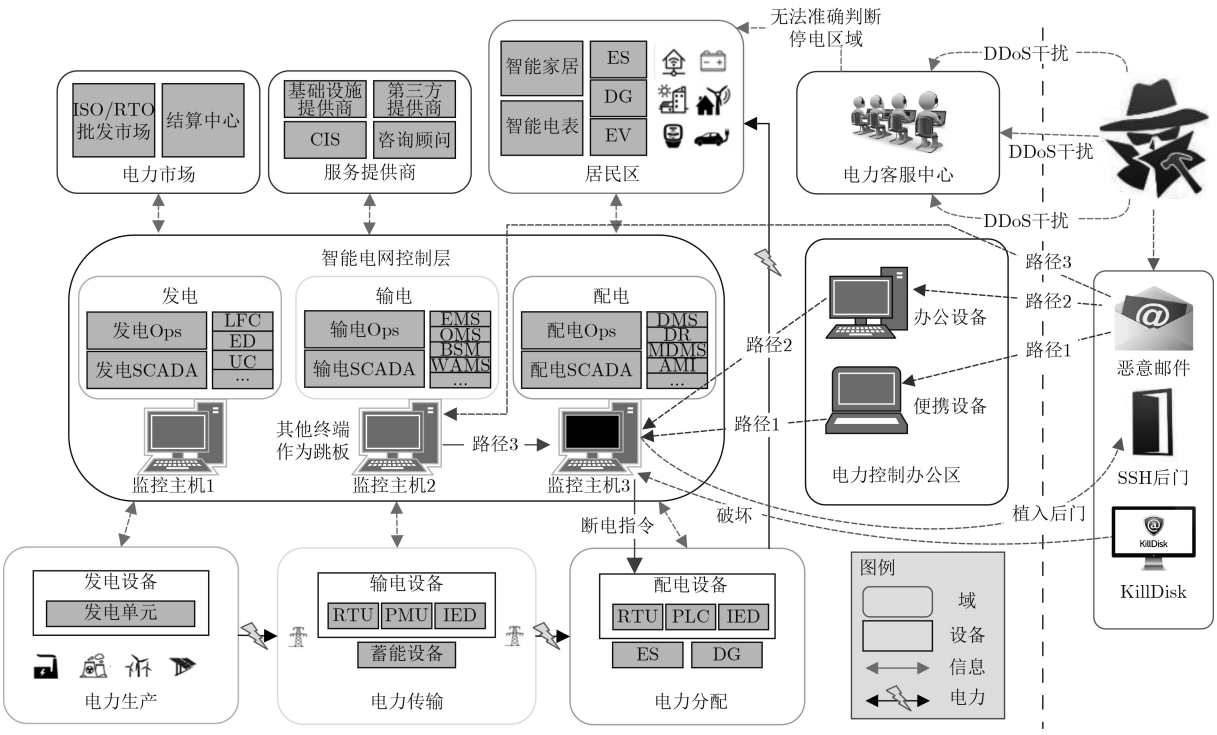

图 3 BlackEnergy的APT攻击流程

需求响应的超低时延要求也将可能成为攻击者的利用对象，通过网络基础设施降低一些关键网络节点的通信性能从而延迟控制命令、状态数据上报等，进而到达时电压控制失衡进而导致能源关键基础设施物理设施被摧毁的目的[56]。攻击者还可以利用主动配电调控的强动态性发起攻击，攻击者通过虚假IP地址伪装用电终端，诱使能源关键基础设施预先在不需要太多电能的区域或时段配置较多的电能，从而导致电力调度失衡，造成大面积停电，文献[57]利用软件定义网络对主动配能源关键基础设施的通信节点进行统一监管。

此外，新能源发电因受环境因素(风能发电受天气影响很大)影响很大而具有间歇性，新能源接入能源关键基础设施将对设施稳定造成一定的影响[58]，那么攻击者将可以通过攻击新能源的通信系统如篡改风力等级测量数据等开展针对能源关键基础设施的攻击；能源关键基础设施允许如电动车等移动储能设备的接入[59]，电动车即插即用需求在时空上具有较强的不确定性，且大规模电动车的位置移动将影响城市用电的分布情况，以V2G/V2H为代表的新型技术的通信网络需要新型的安全认证[60]，密钥分发[61]，通信模式[62]。同时，微电网的安全稳定运行也将直接受到网络攻击的威胁[63]。

(3) 能源关键基础设施业务的脆弱性：

传统攻击方式不同，智能攻击的攻击者将首先从网络上搜集能源关键基础设施业务信息等作为社工数据，然后通过智能的分析算法(如博弈论、机器学习等)对发现能源关键基础设施业务漏洞。为了分析连续网络拓扑攻击环境下能源关键基础设施信息物理系统存在的安全风险，文献[54]提出了基于Q-Learning智能能源关键基础设施脆弱性分析方法，经该方法检测后攻击者再针对脆弱点发起持续拓扑攻击可以使攻击成功率得到显著提升；文献[64]中介绍了几种针对能源关键基础设施通信的智能攻击与对抗策略，通过两阶段的零和博弈可以使攻击效果最大化。

总之，能源关键基础设施信息安全威胁来源正在朝着多样化、复杂化、隐形化、智能化方向发展。攻击者几乎可以从任意位置发起攻击，并利用地址变化在能源关键基础设施中通行无阻。面对日益增加的能源关键基础设施状态数据，威胁来源的低关联性、慢时变性、信号强度弱等特点使低时延的集中搜集并实时处理能源关键基础设施状态数据并实时对基础设施状态进行有效控制变得越来越困难，这给为以能源的互连、互通、互操作为宗旨的能源关键基础设施构建跨时空系统状态管理与风险估计体系带来了诸多困难[59]。

4　能源关键基础设施网络安全防御技术的现状与发展

面对日益严重的能源关键基础设施信息安全威胁，本文旨在构建面向能源关键基础设施的新型信息安全威胁主动防御体系。本节首先分析了现有的能源关键基础设施信息安全威胁防御技术；其次，分析了防御能源关键基础设施新型信息安全威胁的技术需求；最后分析了现有的新型信息安全防御技术应用于能源关键基础设施的优缺点。

4.1　现有的能源关键基础设施网络安全防御技术

数字化能源关键基础设施主要通过数据收集与监控(Supervisory Control And Data Acquisition, SCADA)系统来对能源关键基础设施运行状态进行管理和控制。SCADA系统通常由专门的计算机、通信系统和传感测量设备相结合，通过对从传感器上搜集的状态数据进行深度分析生成来对物理设备进行控制的决策[65]。随着能源设备的自动化以及通信技术的高速发展，通过网络与SCADA系统互连的电力控制设备逐渐增多。现有能源关键基础设施信息安全防御技术主要包括：(1)网络隔离技术；(2)访问控制技术；(3)入侵检测技术。网络隔离技术目前已经发展至第5代，实现原理是通过专用通信设备、专有安全协议和加密验证机制及应用层数据提取和鉴别认证技术，进行不同安全级别网络之间的数据交换，彻底阻断了网络间的直接TCP/IP连接，同时对网间通信的双方、内容、过程施以严格的身份认证、内容过滤、安全审计等多种安全防护机制，从而保证了在不同网络之间进行数据交换的安全、可控，杜绝由操作系统和网络协议自身漏洞带来的安全风险。广泛使用的网络隔离技术包括物理隔离和逻辑隔离两种，分别以设置DMZ和部署MPLS-VPN [66]为代表。防火墙技术[67]是实现两个网络间访问控制的重要手段，也属于一种特殊的隔离技术。访问控制技术的主要目的是网络资源不被非法使用和访问，简单的访问控制技术包括口令、生物识别等，基于角色的访问控制(RBAC)是与现代商业应用相结合的产物，在能源关键基础设施中也经常使用；入侵检测/防御系统(Intrusion Detection/ Prevention Systems, IDS/IPS)[68–70]。通过对数据包的深度解析，能够有效阻止蠕虫、病毒、DOS攻击等，部分厂商的IDS/IPS具有主动防御功能，但设计十分复杂。以上方法仅适用于避免控制中心遭受网络攻击，对于由传感测量设备、通信网络、用户终端自身脆弱性带来的安全威胁几乎没有任何作用；而且基于能源关键基础设施业务脆弱性分析的智能攻击将能够有效的绕过入侵防御系

统的检测和拦截。针对能源关键基础设施中以上传统的信息安全威胁，国内外科研人员也提出了异常检测[39]、木马检测[40]、脆弱性分析[42]等方案和措施，起到了较好的防御作用。

4.2 新型能源关键基础设施网络安全防御技术

在工业信息化的今天，关键能源基础设施安全从未像现在这样面临原理创新、理论创新、技术创新和应用创新等如此之多的挑战。在这种背景下，传统能源关键基础设施网络向新型能源关键基础设施网络过渡已是必然趋势。未来的能源关键基础设施网络的安全防护将具备智能化、自适应化、可定义化等诸多特性，不断演化出纵深防御、人工智能防御、基于云、雾计算防护等模式。来自传感测量设备、通信网络、用户终端等自身脆弱性和基于数据分析的智能攻击等新型信息安全威胁对信息安全防御技术提出了新的需求。图4给出了能源基础设施的信息安全防御技术的示意图。

目前，能源基础设施网络安全防护发展的几个主要的形态已经成为工业安全演进的重要基础，对工业物联网的发展带来了不可估量的影响。(1)在网络安全方面，第5代移动通信系统(简称5G)，有着很多其他移动网络不可比拟的优越性，比如能够传输高质量视频图像，支持高速上传和下载，具有更高的频谱利用率和智能化等，大大降低了工业传感器和安全监测设备通信的时延，提高了实时性；(2)在数据安全方面，随着大数据概念逐渐普及，如何保护数据也成为新的难题。差分隐私和虚假数据注入[71]等攻击对工业安全带来新的挑战。大数据在引入安全问题的同时，也是解决信息安全问题的有效手段；(3)在系统安全方面，纵深式，分布式的防御架构和移动目标防御，拟态防御等技术为安全防护系统的设计提供了新的思路，完全改变了传统能源基础设施中的安全防护策略；(4)在新兴技术方面，人工智能是信息全球化背景下的新技术革命，将机器学习和工业生产二者有机结合。基于深度神经网络的异常检测技术和态势感知技术使得人们能更及时的检测出能源基础设施中的漏洞；另外，云计算概念的兴起也从根本上改变了原有能源基础设施的工作模式，云计算通过使计算分布在大量的分布式计算机上，而非集中在本地计算机或远程服务器中。同时，通过数据中心传送可信赖的服务和创建在服务器上的不同层次的虚拟化技术是关键。这使得计算资源能被切换到需要的应用上，根据需求访问计算机和存储系统。这种计算和服务模式，极大优化和提升了能源基础设施的工作质量和效率。

(1) 分布式纵深防御：为了对能源关键基础设施的安全稳定运行进行全方位监控，通常需要在能源关键基础设施内部或附近大规模的部署各类分布式部署的传感器以实时搜集电机运行参数、用户需求、市场动态等能源数据。然而由于传感节点的电池能量、存储能力、计算能力十分有限，传统的信息安全防御技术将难以有效保障这些能源数据在传感设备及通信节点的安全性。目前，面向传感数据安全性保障的信息安全技术主要包括数据脱敏[72]、细粒度访问控制[73]、轻量级加解密机制[74,75]等。在云计算架构下，数据通常要聚集到云计算中心，那么就保证数据在采集和传输过程中的安全性[76]. 但是上述方法都不能保证数据在传感测量设备中存储

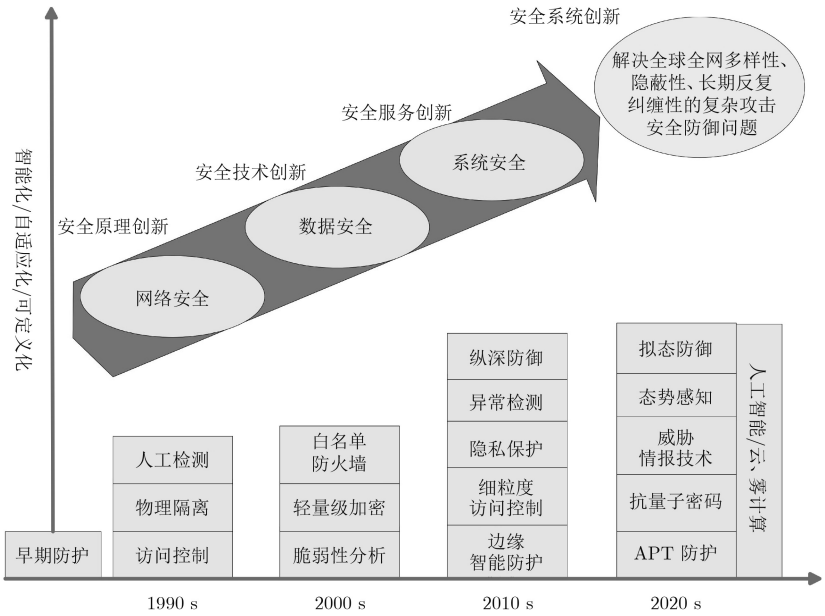

图 4 能源基础设施的信息安全防御技术

时的安全性。为了适应资源有限的传感器、执行器、用户终端对安全性的需求，安全功能的去中心化部署已经引起广泛关注。早在2001年就在网络边缘设计了防火墙架构，但技术的局限性，使边缘部署防火墙的成本和效益都不是十分乐观[77]。由于虚拟化技术迅速发展和云计算应用的巨大成功，将虚拟化网络功能动态的部署到网络边缘已经不再是技术上的难题，且部署效率和成本都将是可接受的。2015年之后，文献[78,79]分别设计了以用户为中心的安全部署方案，这些方案将虚拟的安全功能动态、灵活、主动地部署在靠近用户的网络边缘，从而提高了用户端(包括移动终端)的安全性。2017年，文献[80]通过调研现阶段边缘计算的发展，综合分析了在边缘部署安全策略的需求和挑战，并指出在边缘计算架构下，peer-to-peer的数据传输带来的边缘流量的发现、审计、过滤亟需增强。考虑到能源关键基础设施中越来越多的点对点能量交换，如车辆到车辆(V2V)、车辆到电网(V2G)、车辆到基础设施(V2G)等，在网络边缘进行的能量交换、数据交换的安全性需要一种能够支持具有分布式纵深防御功能的信息安全威胁防御技术。

(2) 自适应的智能化防御：能源关键基础设施的调度决策离不开对大规模数据的分析和处理，而能源关键基础设施的信息安全威胁防御更离不开对大规模安全威胁情报的挖掘和分析。利用能源关键基础设施中广泛搜集的状态数据，挖掘能源关键基础设施中隐蔽存在的安全威胁，动态评估能源关键基础设施整体安全态势，并利用人工智能算法自适应的调整防御策略，文献[81]提出了一种新颖的基于深度学习的系统安全评估特征提取框架，以自动提取有效的训练特征，这些特征可以通过分类器轻松进行分类。在时空上智能化部署防御策略也是未来能源关键基础设施信息安全威胁防御技术发展的重要需求之一。

(3) 可定义化的主动防御：汇聚能源数据对通信性能的需求主要包括QoS保障[82,83]以及网络中的阿安全密钥分发[84]等。能源关键基础设施允许风能、太阳能等分布式能源的接入，并向电动车等移动能源存储设备提供双向能量流动接口，大大增加了能源调度的复杂性。包括微电网在内的能源关键基础设施业务的多样化和复杂化，跨网络域(车联网、无线传感网络、移动通信网络等异构网络)的调度控制安全对能源关键基础设施通信的实时性、可扩展性和稳定性提出了更高的要求。目前，能源关键基础设施通信也开始向新型通信网络演进，新型通信网络主要包括软件定义网络(SDN)。然而，尽管SDN解决了一些传统网络的安全问题，但由于受到包括高开放性及动态性、用户服务需求、通信设备的性能、和恶意攻击等因素的影响，SDN自身安全性还有待进一步研究，但SDN对底层网络的动态重构给能源关键基础设施信息安全威胁的主动防御技术带来了新的契机。为了防御能源关键基础设施新型信息安全威胁，利用SDN可以对能源关键基础设施通信基础设施进行重定义、对能源关键基础设施业务进行动态编排、并在包括传感测量设备在内的能源关键基础设施中主动部署安全管控策略[85]。

(4) 大数据的环境感知防御：现有的智能电网安全方案大多集中在安全保护和检测上。安全态势感知仍然是智能电网中尚未解决的问题，文献[86]提出了一种进行网络物理安全评估(CPSA)的新型集成的网络物理安全协同模拟器工具，文献[87]引入博弈论和强化学习，提出了一种基于大数据分析的智能电网安全态势感知机制。在网络空间安全态势越来越复杂的趋势下，威胁情报的研究对能源关键基础设施的安全有至关重要的意义。参与威胁情报感知、共享和分析的各方结合自身业务流程与安全需求，针对核心资产增强威胁情报感知能力，积极融合云计算、大数据等前沿技术，建立威胁与漏洞深度分析系统，在深度挖掘与关联融合的基础上做好安全态势评估及风险预警，动态调整安全策略，部署快速可行的安全响应战略，确保关键资产的安全[88]。

(5) 基于新型密码技术的数据保护：密码是网络安全的基础设施，利用密码技术能够有效实现身份认证、访问控制、数据加密和信任管理，构建基于密码的安全防护体系是确保能源互联网安全发展的核心任务。由于能源互联网信息和结构的复杂性以及新信息技术的融入，常用的密码技术在满足其安全需求上略显不足，需要研发新的密码体系来适应能源基础设施安全的新需求。容侵是信息安全领域的一种新策略，它使系统在遭受攻击时，仍能为合法用户提供预期的有效服务。文献[89]提出了一种全新的、基于容侵技术的CA方案，该方案在完成对证书签名的同时，保证了CA私钥的机密性和可用性，并能够容忍一定数量的入侵，达到了容侵的目的。随着计算机计算能力的不断增强，尤其是量子计算机概念的提出，对于公钥密码RSA, ECC等密码体制形成了严重的威胁，这些体制所基于的大整数分解离散对数等问题的困难性，在量子计算下已不再是一个难题。研究后量子时代的密码加密机制，保障数据和通信安全成为密码学领域的一个重要方向。基于格的密码体制基于格上的困难问题

SVP, CVP等，被证明可以有效抵御量子计算攻击。自1996年，文献[90]提出基于格上困难问题的构建密码方案的可能性之后，二十多年来基于格密码改进的抗量子密码方案不断出现，包括散列函数、公钥加密方案、数字签名方案等[91]。随着密码体制研究的深入和物联网建设的推进，新的密码技术将在能源关键基础设施安全中起到至关重要的作用。

4.3 能源关键基础设施防御技术发展方向

目前国内外研究人员对众多新型的安全技术都进行了一定的研究，主要包括拟态安全[92]、移动目标防御[93]、威胁情报技术[88]、SDN安全防护及服务[85,94]、基于大数据的攻击态势感知[87]。针对传统网络的APT防御问题也得到了一定研究，主要集中在云系统的APT防护[95,96]、数据驱动的攻击检测[97,98]、基于独立访问的命令与控制检测[99]、攻击潜伏与预测分析[100–102]。但是，体系化、多层次的APT纵深分析与主动防御方法依然有待进一步研究。同时，由于传统网络与能源关键基础设施通信在协议、架构、业务等方面的巨大差异，适用于传统网络的防御方法并不适用于能源关键基础设施场景。因此，为了有效防御能源关键基础设施中各种新型和复杂的信息安全威胁，适应能源关键基础设施未来发展趋势，亟需研究一套针对能源关键基础设施系统和业务所面临的新型信息安全威胁的攻击防御理论。

近几年，我国也对能源关键基础设施的工控通信网络安全相关基础理论研究加大了投入，目前的关注点集中在能源关键基础设施安全的脆弱性评估、变电站入侵检测、安全数据融合、嵌入式设备安全等方向上。在这些研究的基础上，面对不断演进的安全威胁，本文将新型的信息与通信技术、网络安全技术与能源关键基础设施系统及业务特点深度融合，在方法论层面形成面向能源关键基础设施新型信息安全威胁的主动防御方法，为能源关键基础设施关键基础设施和重要业务的安全保障提供理论和技术支撑。

5 结束语

现有的能源关键基础设施信息安全威胁防御技术仍然存在如下问题：(1)缺乏针对能源关键基础设施中新型关键基础设施(如智能电表、智能电子设备、智能传感器、通信基站等)的脆弱性主动分析理论，现有的集中式、被动式防御方法难以应对针对能源关键基础设施开展的以APT为代表的新型攻击威胁；(2)现有脆弱性分析技术缺乏对能源关键基础设施及其通信架构演进的考虑，且没有方法描述分布式能源、微电网、移动能源(V2G)等新型能源关键基础设施应用场景的安全需求，且难以评估网络功能虚拟化、通信流量与计算方式边缘化进程中的安全需求演进趋势。(3)缺乏针对能源关键基础设施信息安全威胁的有效特征提取模型和检测理论，不能很好地从大规模能源关键基础设施数据中发现和感知弱信号、低关联、慢时变的信息物理叠加风险；(4)结合能源关键基础设施系统和业务特点的智能安全策略部署也还没有得以彻底解决，需要一种符合能源关键基础设施脆弱性分布特征的主动安全策略部署机制。

综上所述，要对能源关键基础设施新型网络安全威胁进行深入的研究，首先需要建立一套能源关键基础设施演变规律及结构模型，在此基础上可以对能源关键基础设施的脆弱性评估建立理论模型，其次根据脆弱性评估结果在安全事件发生之前，帮助管理员识别出系统中存在的孤立脆弱点及脆弱点之间相互利用带来的组合漏洞，并提供科学合理的安全解决方案。此外，对所采取安全策略之后网络安全态势进行跟踪学习，将能够建一套完整的能源关键基础设施脆弱性分布趋势预测体系。这样不仅可以发现存在的安全漏洞和隐患，还有助于建立具有预警功能的能源关键基础设施信息安全保障机制。但是，目前，对能源关键基础设施架构的演进脉络、能源关键基础设施信息安全威胁来源的演进趋势以及新型防御技术的发展趋势等方面的研究工作还没有形成系统的模型方法和分析机制，对能源关键基础设施环境下数据处理范式、通信网络的革新、基于大数据的业务决策机理等缺乏全面的认知，对防御能源关键基础设施新型信息安全威胁的技术需求特征不十分明确。

下一步研究需要基于现有的能源关键基础设施系统的特性模型和网络空间安全领域中已有的技术基础，针对能源关键基础设施APT来源的隐蔽性、潜伏性、长期纠缠性等等特点，有针对性地融合复杂网络理论、本体论、软件定义、在线强化学习等先进的理论知识，创新性的建立一套完整的面向能源关键基础设施新型APT的主动防御理论，其成果将为能源关键基础设施系统的设计、性能评估及安全保障提供科学的理论依据和指导。

参 考 文 献

[1] SATO T, KAMMEN D M, DUAN B, *et al*. Smart Grid Standards: Specifications, Requirements, and Technologies[M]. Singapore: John Wiley & Sons, 2015.

[2] AKINGENEYE I and WU Jingxian. Low latency detection of sparse false data injections in smart grids[J]. *IEEE Access*, 2018, 6: 58564–58573. doi: 10.1109/ACCESS.2018.

2873981.

[3] 张钧, 黄翰, 张义斌. 国外智能电网顶层技术路线对比分析[J]. 华北电力大学学报: 社会科学版, 2015(4): 25–30.
ZHANG Jun, HUANG Han, and ZHANG Yibin. Comparative analysis of foreign smart grid top-level roadmaps[J]. *Journal of North China Electric Power University: Social Sciences*, 2015(4): 25–30.

[4] WANG Kuan, LI Jianhua, WU Jun, *et al*. QoS-predicted energy efficient routing for information-centric smart grid: A network calculus approach[J]. *IEEE Access*, 2018, 6: 52867–52876. doi: 10.1109/ACCESS.2018.2870929.

[5] LIGHTNER E M and WIDERGREN S E. An orderly transition to a transformed electricity system[J]. *IEEE Transactions on Smart Grid*, 2010, 1(1): 3–10. doi: 10.1109/TSG.2010.2045013.

[6] RADOGLOU-GRAMMATIKIS P I and SARIGIANNIDIS P G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems[J]. *IEEE Access*, 2019, 7: 46595–46620. doi: 10.1109/ACCESS.2019.2909807.

[7] BUSH G W. Address to a joint session of congress and the American people[R]. 2001: xviii.

[8] FANG Xi, MISRA S, XUE Guoliang, *et al*. Smart grid—The new and improved power grid: A survey[J]. *IEEE Communications Surveys & Tutorials*, 2012, 14(4): 944–980.

[9] BERA S, MISRA S, and RODRIGUES J J P C. Cloud computing applications for smart grid: A survey[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(5): 1477–1494. doi: 10.1109/TPDS.2014.2321378.

[10] TANYINGYONG V, OLSSON R, CHO J W, *et al*. IoT-grid: IoT communication for smart DC grids[C]. 2016 IEEE Global Communications Conference, Washington, USA, 2016: 1–7.

[11] YOUSSEF N E H B, BAROUNI Y, KHALFALLAH S, *et al*. Mixing SDN and CCN for content-centric Qos aware smart grid architecture[C]. The 25th IEEE/ACM International Symposium on Quality of Service, Vilanovaila Geltru, 2017: 1–5.

[12] LI Gaolei, WU Jun, GUO Longhua, *et al*. SDN based dynamic and autonomous bandwidth allocation as ACSI services of IEC61850 communications in smart grid[C]. 2016 IEEE Smart Energy Grid Engineering, Oshawa, 2016: 342–346.

[13] KUMAR N, ZEADALLY S, and RODRIGUES J J P C. Vehicular delay-tolerant networks for smart grid data management using mobile edge computing[J]. *IEEE Communications Magazine*, 2016, 54(10): 60–66. doi: 10.1109/MCOM.2016.7588230.

[14] AHSAN U and BAIS A. Distributed big data management in smart grid[C]. The 26th Wireless and Optical Communication Conference, Newark, 2017: 1–6.

[15] LIU Keyan, SHENG Wanxing, LIU Yuan, *et al*. Optimal sitting and sizing of DGs in distribution system considering time sequence characteristics of loads and DGs[J]. *International Journal of Electrical Power & Energy Systems*, 2015, 69: 430–440.

[16] AMIN S, LITRICO X, SASTRY S S, *et al*. Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models[J]. *IEEE Transactions on Control Systems Technology*, 2013, 21(5): 1679–1693. doi: 10.1109/TCST.2012.2211874.

[17] NTALAMPIRAS S. Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling[J]. *IEEE Transactions on Industrial Informatics*, 2015, 11(1): 104–111. doi: 10.1109/TII.2014.2367322.

[18] LIU Xuan and LI Zuyi. Trilevel modeling of cyber attacks on transmission lines[J]. *IEEE Transactions on Smart Grid*, 2017, 8(2): 720–729.

[19] NI Jianbing, ALHARBI K, LIN Xiaodong, *et al*. Security-enhanced data aggregation against malicious gateways in smart grid[C]. 2015 IEEE Global Communications Conference, San Diego, 2015: 1–6.

[20] 伊胜伟, 张翀斌, 谢丰, 等. 基于Peach的工业控制网络协议安全分析[J]. 清华大学学报: 自然科学版, 2017, 57(1): 50–54.
YI Shengwei, ZHANG Chongbin, XIE Feng, *et al*. Security analysis of industrial control network protocols based on Peach[J]. *Journal of Tsinghua University: Science and Technology*, 2017, 57(1): 50–54.

[21] OOZEER M I and HAYKIN S. Cognitive risk control for mitigating cyber-attack in smart grid[J]. *IEEE Access*, 2019, 7: 125806–125826. doi: 10.1109/ACCESS.2019.2939089.

[22] ALOUL F, AL-ALI A R, AL-DALKY R, *et al*. Smart grid security: Threats, vulnerabilities and solutions[J]. *International Journal of Smart Grid and Clean Energy*, 2012, 1(1): 1–6.

[23] GUAN Zhitao, LI Jing, ZHU Liehuang, *et al*. Toward delay-tolerant flexible data access control for smart grid with renewable energy resources[J]. *IEEE Transactions on Industrial Informatics*, 2017, 13(6): 3216–3225. doi: 10.1109/TII.2017.2706760.

[24] SHENG Wanxing, LIU Keyan, CHENG Sheng, *et al*. A trust region SQP method for coordinated voltage control in smart distribution grid[J]. *IEEE Transactions on Smart Grid*, 2016, 7(1): 381–391. doi: 10.1109/TSG.2014.2376197.

[25] ABHINAV S, MODARES H, LEWIS F L, *et al*. Synchrony in networked microgrids under attacks[J]. *IEEE*

Transactions on Smart Grid, 2018, 9(6): 6731–6741. doi: 10.1109/TSG.2017.2721382.

[26] 吴聪, 唐巍, 白牧可, 等. 基于能源路由器的用户侧能源互联网规划[J]. 电力系统自动化, 2017, 41(4): 20–28.
WU Cong, TANG Wei, BAI Muke, *et al*. Energy router based planning of energy internet at user side[J]. *Automation of Electric Power Systems*, 2017, 41(4): 20–28.

[27] 孟晓丽, 高君, 盛万兴, 等. 含分布式电源的配电网日前两阶段优化调度模型[J]. 电网技术, 2015, 39(5): 1294–1300.
MENG Xiaoli, GAO Jun, SHENG Wanxing, *et al*. A day-ahead two-stage optimal scheduling model for distribution network containing distributed generations[J]. *Power System Technology*, 2015, 39(5): 1294–1300.

[28] WANG Yufei, ZHANG Bo, LIN Weimin, *et al*. Smart grid information security - a research on standards[C]. 2011 International Conference on Advanced Power System Automation and Protection, Beijing, China, 2011: 1188–1194.

[29] BASSO T, HAMBRICK J, and DEBLASIO D. Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards[C]. 2012 IEEE PES Innovative Smart Grid Technologies, Washington, USA, 2012: 1–7.

[30] SRIKANTHA P and KUNDUR D. Denial of service attacks and mitigation for stability in cyber-enabled power grid[C]. 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, Washington, USA, 2015: 1–5.

[31] ZHANG Zhenghao, GONG Shuping, 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. doi: 10.1109/TSG.2012.2227342.

[32] LIU Yao, NING Peng, and 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): 13.

[33] YAN Jun, HE Haibo, ZHONG Xiangnan, *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.

[34] XIANG Yingmeng, DING Zhilu, ZHANG Yichi, *et al*. Power system reliability evaluation considering load redistribution attacks[J]. *IEEE Transactions on Smart Grid*, 2017, 8(2): 889–901.

[35] LIU Shan, KUNDUR D, ZOURNTOS T, *et al*. Coordinated variable structure switching attack in the presence of model error and state estimation[C]. The 3rd IEEE International Conference on Smart Grid Communications, Tainan, China, 2012: 318–323.

[36] SANKAR L, RAJAGOPALAN S R, MOHAJER S, *et al*. Smart meter privacy: A theoretical framework[J]. *IEEE Transactions on Smart Grid*, 2013, 4(2): 837–846. doi: 10.1109/TSG.2012.2211046.

[37] XU Ruzhi, WANG Rui, GUAN Zhitao, *et al*. Achieving efficient detection against false data injection attacks in smart grid[J]. *IEEE Access*, 2017, 5: 13787–13798. doi: 10.1109/ACCESS.2017.2728681.

[38] YE Hongxing, GE Yinyin, LIU Xuan, *et al*. Transmission line rating attack in two-settlement electricity markets[J]. *IEEE Transactions on Smart Grid*, 2016, 7(3): 1346–1355. doi: 10.1109/TSG.2015.2426418.

[39] TEN C W, HONG J, and LIU C C. Anomaly detection for cybersecurity of the substations[J]. *IEEE Transactions on Smart Grid*, 2011, 2(4): 865–873. doi: 10.1109/TSG.2011.2159406.

[40] SALMERON J, WOOD K, and BALDICK R. Analysis of electric grid security under terrorist threat[J]. *IEEE Transactions on Power Systems*, 2004, 19(2): 905–912. doi: 10.1109/TPWRS.2004.825888.

[41] ALSHAMRANI A, MYNENI S, CHOWDHARY A, *et al*. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities[J]. *IEEE Communications Surveys & Tutorials*, 2019, 21(2): 1851–1877.

[42] SRIVASTAVA A, MORRIS T, ERNSTER T, *et al*. Modeling cyber-physical vulnerability of the smart grid with incomplete information[J]. *IEEE Transactions on Smart Grid*, 2013, 4(1): 235–244. doi: 10.1109/TSG.2012.2232318.

[43] 李中伟, 佟为明, 金显吉. 智能电网信息安全防御体系与信息安全测试系统构建乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化, 2016, 40(8): 147–151.
LI Zhongwei, TONG Weiming, and JIN Xianji. Construction of cyber security defense hierarchy and cyber security testing system of smart grid: Thinking and enlightenment for network attack events to national power grid of Ukraine and Israel[J]. *Automation of Electric Power Systems*, 2016, 40(8): 147–151.

[44] STELLIOS I, KOTZANIKOLAOU P, and PSARAKIS M. Advanced persistent threats and zero-day exploits in industrial internet of things[M]. ALCARAZ C. Security and Privacy Trends in the Industrial Internet of Things. Cham: Springer, 2019: 47–68.

[45] BERRUETA E, MORATO D, MAGAÑA E, *et al*. A survey on detection techniques for cryptographic ransomware[J]. *IEEE Access*, 2019, 7: 144925–144944. doi: 10.1109/ACCESS.2019.2945839.

[46] AL-RIMY B A S, MAAROF M A, and SHAID S Z M.

Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions[J]. *Computers & Security*, 2018, 74: 144–166.

[47] LEE K, LEE S Y, and YIM K. Machine learning based file entropy analysis for ransomware detection in backup systems[J]. *IEEE Access*, 2019, 7: 110205–110215. doi: 10.1109/ACCESS.2019.2931136.

[48] PAUDEL S, SMITH P, and ZSEBY T. Attack models for advanced persistent threats in smart grid wide area monitoring[C]. The 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, Pittsburgh, 2017: 61–66.

[49] SKOPIK F, FRIEDBERG I, and FIEDLER R. Dealing with advanced persistent threats in smart grid ICT networks[C]. ISGT 2014, Washington, 2014: 1–5.

[50] WANG Zhiwei. An identity-based data aggregation protocol for the smart grid[J]. *IEEE Transactions on Industrial Informatics*, 2017, 13(5): 2428–2435. doi: 10.1109/TII.2017.2705218.

[51] FOUDA M M, FADLULLAH Z M, and KATO N. Assessing attack threat against ZigBee-based home area network for smart grid communications[C]. 2010 International Conference on Computer Engineering & Systems, Cairo, Egypt, 2010: 245–250.

[52] ISMAIL Z, LENEUTRE J, BATEMAN D, *et al*. A game theoretical analysis of data confidentiality attacks on smart-grid AMI[J]. *IEEE Journal on Selected Areas in Communications*, 2014, 32(7): 1486–1499. doi: 10.1109/JSAC.2014.2332095.

[53] FARRAJ A K, HAMMAD E M, AL DAOUD A, *et al*. A game-theoretic control approach to mitigate cyber switching attacks in smart grid systems[C]. 2014 IEEE International Conference on Smart Grid Communications, Venice, Italy, 2014: 958–963.

[54] GIANI A, BITAR E, GARCIA M, *et al*. Smart grid data integrity attacks[J]. *IEEE Transactions on Smart Grid*, 2013, 4(3): 1244–1253. doi: 10.1109/TSG.2013.2245155.

[55] KOSUT O, JIA Liyan, THOMAS R J, *et al*. Malicious data attacks on the smart grid[J]. *IEEE Transactions on Smart Grid*, 2011, 2(4): 645–658. doi: 10.1109/TSG.2011.2163807.

[56] MASTER N, MOUNZER J, and BAMBOS N. Distributed smart grid architecture for delay and price sensitive power management[C]. 2014 IEEE International Conference on Communications, Sydney, 2014: 3670–3675.

[57] AYDEGER A, AKKAYA K, CINTUGLU M H, *et al*. Software defined networking for resilient communications in smart grid active distribution networks[C]. 2016 IEEE International Conference on Communications, Kuala Lumpur, Malaysia, 2016: 1–6.

[58] RANA M M, LI Li, and SU S W. An adaptive-then-combine dynamic state estimation considering renewable generations in smart grids[J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(12): 3954–3961. doi: 10.1109/JSAC.2016.2611963.

[59] ROSSEBØ J E Y, WOLTHUIS R, FRANSEN F, *et al*. An enhanced risk-assessment methodology for smart grids[J]. *Computer*, 2017, 50(4): 62–71. doi: 10.1109/MC.2017.106.

[60] ZHANG Shanghua, LI Qiang, WU Jun, *et al*. A security mechanism for software-defined networking based communications in vehicle-to-grid[C]. 2016 IEEE Smart Energy Grid Engineering, Oshawa, 2016: 386–391.

[61] 谢永,李香,张松松.一种可证安全的车联网无证书聚合签名改进方案[J]. 电子与信息学报, 2020, 42(5): 1125–1131. doi: 10.11999/JEIT190184.

XIE Yong, LI Xiang, ZHANG Songsong, *et al*. An improved provable secure certificateless aggregation signature scheme for vehicular Ad Hoc NETworks[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1125–1131. doi: 10.11999/JEIT190184.

[62] LI Gaolei, WU Jun, LI Jianhua, *et al*. Battery status sensing software-defined multicast for V2G regulation in smart grid[J]. *IEEE Sensors Journal*, 2017, 17(23): 7838–7848. doi: 10.1109/JSEN.2017.2731971.

[63] 邵苏杰, 郭少勇, 邱雪松, 等. 基于加权队列的无线智能电网通信网采集数据流量调度算法[J]. 电子与信息学报, 2014, 36(5): 1209–1214.

SHAO Sujie, GUO Shaoyong, QIU Xuesong, *et al*. Traffic scheduling algorithm based on weighted queue for meter data collection in wireless smart grid communication network[J]. *Journal of Electronics & Information Technology*, 2014, 36(5): 1209–1214.

[64] CHEN Pinyu, CHENG S M, and CHEN K C. Smart attacks in smart grid communication networks[J]. *IEEE Communications Magazine*, 2012, 50(8): 24–29. doi: 10.1109/MCOM.2012.6257523.

[65] JOHNSON R E. Survey of SCADA security challenges and potential attack vectors[C]. 2010 International Conference for Internet Technology and Secured Transactions, London, 2010: 1–5.

[66] YANG Yi, XU Haiqing, GAO Lei, *et al*. Multidimensional intrusion detection system for IEC 61850-based SCADA networks[J]. *IEEE Transactions on Power Delivery*, 2017, 32(2): 1068–1078. doi: 10.1109/TPWRD.2016.2603339.

[67] DO V L, FILLATRE L, NIKIFOROV I, *et al*. Security of SCADA systems against cyber–physical attacks[J]. *IEEE Aerospace and Electronic Systems Magazine*, 2017, 32(5): 28–45. doi: 10.1109/MAES.2017.160047.

[68] ZHANG Jiexin, GAN Shaoduo, LIU Xiaoxue, *et al*. Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis[C]. 2016 IEEE Symposium on Computers and Communication, Messina, Italy, 2016: 318–325.

[69] PAN Zhiwen, HARIRI S, and PACHECO J. Context aware intrusion detection for building automation systems[J]. *Computers & Security*, 2019, 85: 181–201.

[70] YILMAZ E N and GÖNEN S. Attack detection/prevention system against cyber attack in industrial control systems[J]. *Computers & Security*, 2018, 77: 94–105.

[71] LIANG Gaoqi, ZHAO Junhua, LUO Fengji, *et al*. A review of false data injection attacks against modern power systems[J]. *IEEE Transactions on Smart Grid*, 2017, 8(4): 1630–1638. doi: 10.1109/TSG.2015.2495133.

[72] YU Shucheng, REN Kui, and LOU Wenjing. FDAC: Toward fine-grained distributed data access control in wireless sensor networks[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2011, 22(4): 673–686. doi: 10.1109/TPDS.2010.130.

[73] WU Jun, DONG Mianxiong, OTA K, *et al*. Cross-domain fine-grained data usage control service for industrial wireless sensor networks[J]. *IEEE Access*, 2015, 3: 2939–2949. doi: 10.1109/ACCESS.2015.2504541.

[74] KIM Y, KOLESNIKOV V, and THOTTAN M. Resilient end-to-end message protection for cyber-physical system communications[J]. *IEEE Transactions on Smart Grid*, 2018, 9(4): 2478–2487. doi: 10.1109/TSG.2016.2613545.

[75] ELATTAR M. Reliable Communications Within Cyber-Physical Systems Using the Internet (RC4CPS)[M]. Berlin, Heidelberg: 2020.

[76] GUAN Zhitao, LI Jing, WU Longfei, *et al*. Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid[J]. *IEEE Internet of Things Journal*, 2017, 4(6): 1934–1944. doi: 10.1109/JIOT.2017.2690522.

[77] MARKHAM T and PAYNE C. Security at the network edge: A distributed firewall architecture[C]. DARPA Information Survivability Conference and Exposition II. DISCEX'01, Anaheim, 2001, 1: 279–286.

[78] MONTERO D, YANNUZZI M, SHAW A, *et al*. Virtualized security at the network edge: A user-centric approach[J]. *IEEE Communications Magazine*, 2015, 53(4): 176–186. doi: 10.1109/MCOM.2015.7081092.

[79] MONTERO D and SERRAL-GRACIÀ R. Offloading personal security applications to the network edge: A mobile user case scenario[C]. 2016 International Wireless Communications and Mobile Computing Conference, Paphos, Cyprus, 2016: 96–101.

[80] ESPOSITO C, CASTIGLIONE A, POP F, *et al*. Challenges of connecting edge and cloud computing: A security and forensic perspective[J]. *IEEE Cloud Computing*, 2017, 4(2): 13–17. doi: 10.1109/MCC.2017.30.

[81] SHAH G A, GUNGOR V C, and AKAN O B. A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications[J]. *IEEE Transactions on Industrial Informatics*, 2013, 9(3): 1477–1485. doi: 10.1109/TII.2013.2242083.

[82] SUN Mingyang, KONSTANTELOS I, and STRBAC G. A deep learning-based feature extraction framework for system security assessment[J]. *IEEE Transactions on Smart Grid*, 2019, 10(5): 5007–5020. doi: 10.1109/TSG.2018.2873001.

[83] ZAFAR S, JANGSHER S, BOUACHIR O, *et al*. QoS enhancement with deep learning-based interference prediction in mobile IoT[J]. *Computer Communications*, 2019, 148: 86–97. doi: 10.1016/j.comcom.2019.09.010.

[84] 关志涛, 徐月, 伍军. 传感器网络中基于三元多项式的密钥管理方案[J]. 通信学报, 2013, 34(12): 71–78. doi: 10.3969/j.issn.1000-436x.2013.12.008.
GUAN Zhitao, XU Yue, and WU Jun. Ternary polynomial based key management scheme for wireless sensor network[J]. *Journal on Communications*, 2013, 34(12): 71–78. doi: 10.3969/j.issn.1000-436x.2013.12.008.

[85] LUO Shibo, DONG Mianxiong, OTA K, *et al*. A security assessment mechanism for software-defined networking-based mobile networks[J]. *Sensors*, 2015, 15(12): 31843–31858. doi: 10.3390/s151229887.

[86] SAXENA N, CHUKWUKA V, XIONG Leilei, *et al*. CPSA: A cyber-physical security assessment tool for situational awareness in smart grid[C]. The 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Dallas, 2017: 69–79.

[87] WU Jun, OTA K, DONG Mianxiong, *et al*. Big data analysis-based security situational awareness for smart grid[J]. *IEEE Transactions on Big Data*, 2018, 4(3): 408–417. doi: 10.1109/TBDATA.2016.2616146.

[88] 李建华. 网络空间威胁情报感知、共享与分析技术综述[J]. 网络与信息安全学报, 2016, 2(2): 16–29. doi: 10.11959/j.issn.2096-109x.2016.00028.
LI Jianhua. Overview of the technologies of threat intelligence sensing, sharing and analysis in cyber space[J]. *Chinese Journal of Network and Information Security*, 2016, 2(2): 16–29. doi: 10.11959/j.issn.2096-109x.2016.00028.

[89] 柴争义, 白浩, 张浩军. 一种容侵的CA私钥签名方案[J]. 河北师范大学学报: 自然科学版, 2008, 32(3): 310–312.
CHAI Zhengyi, BAI Hao, and ZHANG Haojun. An

intrusion tolerant signature scheme of CA private key[J]. *Journal of Hebei Normal University: Natural Science Edition*, 2008, 32(3): 310–312.

[90] AJTAI M. Generating hard instances of lattice problems (extended abstract)[C]. The 28th Annual ACM Symposium on Theory of Computing, Philadelphia, 1996: 99–108.

[91] CHEN L, JORDAN S, LIU Yikai, *et al*. Report on post-quantum cryptography[R]. NISTIR 8105, 2016.

[92] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7): 2–7. doi: 10.3969/j.issn.1000-0801.2014.07.001.

WU Jiangxing. Meaning and vision of mimic computing and mimic security defense[J]. *Telecommunications Science*, 2014, 30(7): 2–7. doi: 10.3969/j.issn.1000-0801.2014.07.001.

[93] HEYDARI V, KIM S I, and YOO S M. Scalable anti-censorship framework using moving target defense for Web servers[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(5): 1113–1124. doi: 10.1109/TIFS.2016.2647218.

[94] HUANG Lina, LI Gaolei, WU Jun, *et al*. Software-defined QoS provisioning for fog computing advanced wireless sensor networks[C]. 2016 IEEE SENSORS, Orlando, 2016: 1–3.

[95] XIAO Liang, XU Dongjin, XIE Caixia, *et al*. Cloud storage defense against advanced persistent threats: A prospect theoretic study[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(3): 534–544. doi: 10.1109/JSAC.2017.2659418.

[96] 张浩, 王丽娜, 谈诚, 等. 云环境下APT攻击的防御方法综述[J]. 计算机科学, 2016, 43(3): 1–7, 43. doi: 10.11896/j.issn.1002-137X.2016.03.001.

ZHANG Hao, WANG Lina, TAN Cheng, *et al*. Review of defense methods against advanced persistent threat in cloud environment[J]. *Computer Science*, 2016, 43(3): 1–7, 43. doi: 10.11896/j.issn.1002-137X.2016.03.001.

[97] 付钰, 李洪成, 吴晓平, 等. 基于大数据分析的APT攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1–14. doi: 10.11959/j.issn.1000-436x.2015184.

FU Yu, LI Hongcheng, WU Xiaoping, *et al*. Detecting APT attacks: A survey from the perspective of big data analysis[J]. *Journal on Communications*, 2015, 36(11): 1–14. doi: 10.11959/j.issn.1000-436x.2015184.

[98] HONG K F, CHEN C C, CHIU Y T, *et al*. Ctracer: Uncover C&C in advanced persistent threats based on scalable framework for enterprise log data[C]. 2015 IEEE International Congress on Big Data, New York, 2015: 551–558.

[99] WANG Xu, ZHENG Kangfeng, NIU Xinxin, *et al*. Detection of command and control in advanced persistent threat based on independent access[C]. 2016 IEEE International Conference on Communications, Kuala Lumpur, Malaysia, 2016: 1–6.

[100] 刘彩霞, 胡鑫鑫, 刘树新, 等. 基于Lowe分类法的5G网络EAP-AKA'协议安全性分析[J]. 电子与信息学报, 2019, 41(8): 1800–1807.

LIU Caixia, HU Xinxin, LIU Shuxin, *et al*. Security analysis of 5G network EAP-AKA' protocol based on Lowe's taxonomy[J]. *Journal of Electronics & Information Technology*, 2019, 41(8): 1800–1807.

[101] 张小松, 牛伟纳, 杨国武, 等. 基于树型结构的APT攻击预测方法[J]. 电子科技大学学报, 2016, 45(4): 582–588. doi: 10.3969/j.issn.1001-0548.2016.04.011.

ZHANG Xiaosong, NIU Weina, YANG Guowu, *et al*. Method for APT prediction based on tree structure[J]. *Journal of University of Electronic Science and Technology of China*, 2016, 45(4): 582–588. doi: 10.3969/j.issn.1001-0548.2016.04.011.

[102] 姚苏, 关建峰, 潘华, 等. 基于APT潜伏攻击的网络可生存性模型与分析[J]. 电子学报, 2016, 44(10): 2415–2422. doi: 10.3969/j.issn.0372-2112.2016.10.020.

YAO Su, GUAN Jianfeng, PAN Hua, *et al*. Modeling and analysis for network survivability of APT latent attack[J]. *Acta Electronsica Sinica*, 2016, 44(10): 2415–2422. doi: 10.3969/j.issn.0372-2112.2016.10.020.

李建华：男，1965年生，教授，博士生导师，研究方向为网络安全技术与应用.

责任编辑：陈　倩