DOI:10. 3969/j. issn. 1674-1951. 2020. 08. 009

基于可信计算和区块链的配电物联网内生安全研究

Research on endogenous security of distribution Internet of Things based on trusted computing and blockchain technology

孙跃[1],杨晟[2],龚钢军[2],杨佳轩[2],周波[2]
SUN Yue[1], YANG Sheng[2], GONG Gangjun[2], YANG Jiaxuan[2], ZHOU Bo[2]

(1.国网冀北电力有限公司电力科学研究院,北京 100045; 2.北京市能源电力信息安全工程技术研究中心(华北电力大学),北京 102206)

(1.State Grid Jibei Electric Power Research Institute, Beijing 100045, China; 2.Beijing Engineering Research Center of Energy Electric Power Information Security (North China Electric Power University), Beijing 102206, China)

摘 要:随着配电网规模不断扩大、网架结构日益复杂、远程视频监控和双向实时交互等新型业务的大幅增加,亟须结合配电物联网的实际运行场景、不同的业务类型、不同的安全需求和不同的动态接入特性来研究配电网物联网动态安全防护体系。可信计算与区块链作为信息安全防护方面的新兴技术,能够保障配电物联网中安全可信的运行环境与管理机制。在设计"云-边-端"架构的配电物联网主站端和边缘端的分级可信免疫管控策略的基础上,搭建了基于区块链的配电物联网分布决策和协同自治模型,并建立了配电物联网的"可管可控、精准防护、可视可信、智能防御"安全防护模型,全面提升了配电网的信息安全防御水平。

关键词:区块链;可信计算;配电物联网;内生安全;分布决策;协同自治;"云-边-端"架构;安全防护模型

中图分类号:TP 311.13:TP 301.6:TM 73 **文献标志码**:A **文章编号**:1674-1951(2020)08 - 0061 - 07

Abstract: With the continuous expansion of the distribution network, complex grid structure, perceptible mounting of new services such as remote video monitoring and two-way real-time interaction , it is urgent to combine the actual operation scenarios of the distribution Internet of Things (IoT), different services, different security needs with different dynamic access characteristics in studying the dynamic security protection system of the distribution IoT. As an emerging technology in information security protection, trusted computing and blockchain can provide a secured and credible operating environment and management mechanism for power distribution IoT. Therefore, based on a hierarchical credibility immune management and control strategy for the master station and the terminals of the distribution IoT with a "cloud-edge-user" architecture, a distributed decision-making and collaborative autonomy model for the distribution IoT taking blockchain technology is established, and a "manageable, controllable, precisely protected, visual, trusted and intelligent " security protection model for the distribution IoT is made. The model can comprehensively improve the information security defense level of distribution network.

Keywords: blockchain; trusted computing; distribution Internet of Things; endogenous security; distributed decision making; collaborative autonomy; "cloud-edge-user" architecture; security protection model

0 引言

为了加快构建清洁、高效、安全、可持续的现代能源体系,国家积极推进能源互联网试点示范,鼓励各企业探索新技术、新模式、新业态。2019 年,国家电网有限公司对建设电力物联网作出全面部署,开启电网战略转型之路。受当前技术和投资的限制,以主动配电网支撑的区域能源互联网是现阶段能源互联网落地的最佳选择[1-5]。区域能源互联网主要基于 110 kV 电压等级以下的配电网,并依据配电物联网支撑实现能源互联、信息共享、业务互动,因此,区域能源互联网应是"主动配电网+配电物联网"的综合有机体。

随着配电网源-荷两端随机性的增强,配电网

收稿日期:2020-06-28;**修回日期**:2020-08-08
基金项目:国家电网有限公司科技项目(52018K190024)

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的结构和潮流方向均发生了显著变化，电网也由传统单一的电能传输分配角色转变为集电能收集、电能传输、电能分配和电能存储于一体的新型电力交换系统，亟须通过物联网技术实现主动控制。泛在电力物联网在运行方式、拓扑形态等方面可以很好地支撑主动配电网的建设[6-8]，但配电网运行环境复杂，既要基于配电物联网来实现泛在物联和全景感知，又要面对由于物联网灵活多样的接入环境和方式、数量庞大的终端带来的配电网结构和边界的动态多变，同时还要面临更高的安全风险，因此，有必要开展攻防结合、里外兼顾、多维融合的配电网信息安全纵深防护体系的研究。

本文针对配电网的互补耦合和扁平化管理结构需求，以及现有能源电力信息安全“重边界，轻内部”的被动式和预防性的防御现状，研究如何从配电网物联网的体系结构和内部机制方面提升主动配电网的信息安全防御能力，实现配电物联网自身环境可信、运行机制可信和数据可信等3个维度的内生安全管理，全面提升配电网的信息安全防御水平。

1 主动配电网的信息安全研究现状

近几年来，伴随着能源互联网和智能电网建设的全面推进，配电互联网的发展面临诸多挑战，如分布式能源、电动车、控制负荷等电网新要素的出现以及新要素的动态、大规模接入等，都对配电网络的能源高效配置、灵活调度有了更高的要求。因此，主动配电网将成为传统配电网的转变方向。2008年国际大电网会议C6.11项目组提出了主动配电网这一概念，主动配电网采用灵活的网络拓扑结构，可以有效地控制潮流，为局部分布式发电提供主动控制和主动管理。随着微网技术的日益成熟和新型智能负荷的大规模引入，配电网呈现出拓扑结构和边界动态变化的新特征，能量类型逐步多样化，不同类型能量使用性能也存在着差异。因此，通过以微网为载体的形式将分布式能源和新型负荷接入配电网，实现了灵活、高效的配电网管理。

随着主动配电网的发展，用电侧的能量流和信息流交互需求愈加频繁，用户侧安装了具备多种功能的新型智能电表；同时，为了给用户侧提供更好的能量流和信息流的交互服务，开放的通信网络也是必需的。开放的通信网络以及各种新型智能电表等的灵活接入，无形中增加了潜入路径和威胁接入点。针对配电终端侧，随着用户侧的需求越来越高，各类终端装置的功能越来越多，新型负荷装置需要与电力系统产生更加深入的交互。面对越来越高的功能需求，配电终端及配用电侧负荷的信息安全也变得至关重要，如果负荷被非授权用户恶意占用或非法使用，造成的后果将会是极其严重的。除此之外，配电网的智能监控系统就是配电自动化系统，它负责对配电网运行进行监测与控制，其信息安全不仅关乎自身系统的运行，更关乎于整个配电网的正常运行。而配电自动化系统稳定可靠运行的重要条件是数据的真实、有效和实时。因此，针对配电自动化系统各层次的信息安全防护研究也是主动配电网信息安全防护研究的重点之一。

智能电网和能源互联网的重要基础是主动配电网，它有效地保证了对用电侧负荷的高效感知和主动控制，为电网的稳定运行起到了关键的支撑作用，因此保护其信息数据安全尤其重要。目前，主动配电网的研究成果主要集中在能源智能化协调控制、超短期负荷预测和分布式电网实时监测等方面，针对信息安全的研究较为匮乏，关于双向需求互动用电的信息安全关键技术尤其欠缺，信息安全建设的相关标准也有待完善。因此，对于主动配电网信息安全防护体系的研究尤为重要。

主动配电网中用户与电网的信息流交互集中在用户侧，随着电力用户参与的不断深入和信息通信技术开放性、互动性的增强，网络信息安全事故发生率不断升高。因此，电力系统信息安全问题备受关注，国内外相关研究机构纷纷着手于安全标准制定、安全风险分析与评估等。其中IEC 62351安全国际标准最为典型，该标准提出在通信系统不同层面采取不同措施以保证信息安全。北美电力可靠性协会制定了《关键设施保护》标准，以保护电网不受访问控制存在的控制缺陷、软件漏洞或其他控制系统漏洞造成的信息安全事件威胁。国际电工委员会提出关于双向需求互动用电的安全需求，强调同期研究安全需求的解决方案和智能电网高级量测体系的其他功能。同时，信息化是发展国家电网有限公司提出的“坚强智能电网”的基础和保障，要始终把自主、可控放在重要位置。

2 可信计算与区块链技术

2.1 可信计算

随着计算机及网络的普及，信息安全问题愈发突出，排在前3位的安全威胁为恶意代码攻击、信息非法窃取、数据和系统非法破坏，其中，以用户私密信息为目标的恶意代码攻击超过传统病毒成为最大的安全威胁。这些安全威胁的根源在于没有从体系架构上建立计算机的恶意代码攻击免疫机制。

可信计算就是在此背景下提出的一种技术理

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

念,它通过建立一种特定的完整性度量机制,使计算平台运行时具备分辨可信程序代码与不可信程序代码的能力,从而对不可信的程序代码建立有效的防治措施。

可信计算是以密码芯片为可信根,建立计算平台安全功能体系,解决计算平台核心安全问题[9-11],其技术原理如图 1 所示(图中:BIOS 为基本输入输出系统;OS 为操作系统)。

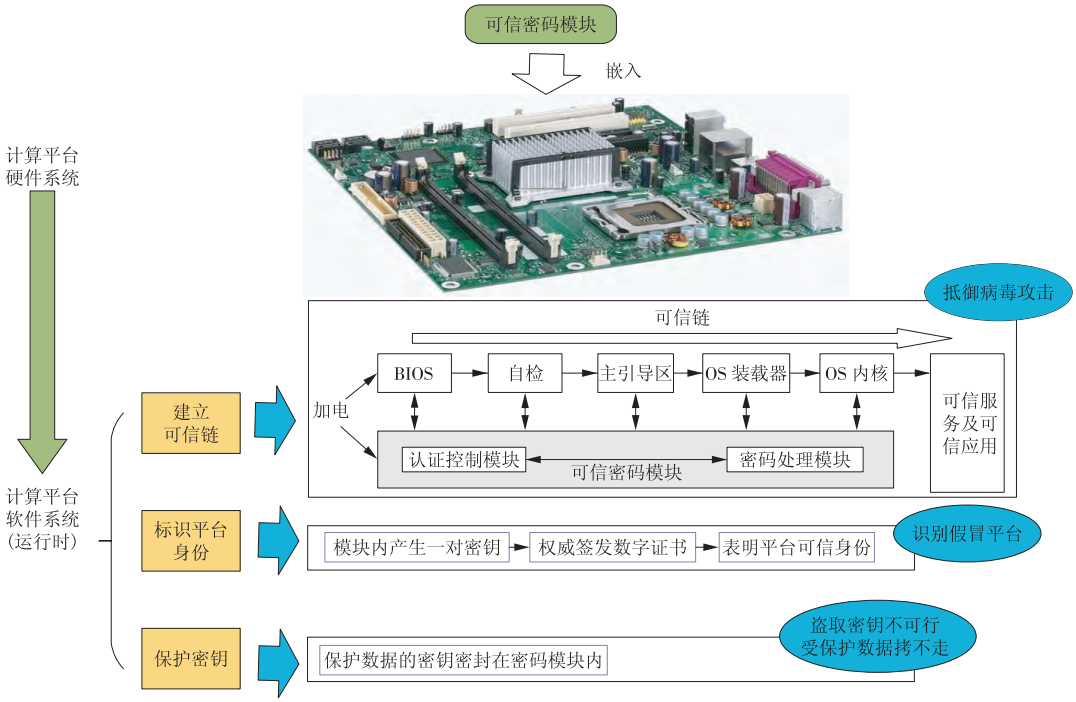

图 1　可信计算技术原理

Fig. 1　Principles of trusted computing technology

可信计算平台通过以下 3 类机制实现平台安全功能。

(1)以可信度量根为起点,计算系统平台完整性度量值,建立计算机系统平台信任链,确保系统平台可信,抵御病毒等恶意代码攻击。

(2)可信报告根标志平台身份的可信性,具有唯一性,以可信报告根为基础,实现平台身份证明和完整性证明,从而识别假冒平台。

(3)基于可信存储根,实现密钥管理、平台数据安全保护功能,提供相应的密码服务,从而确保受保护数据不会被非法拷贝。

2.2　区块链技术

比特币之父中本聪在 2008 年发表的《比特币:一个 P2P 电子现金系统》一文中提到了比特币背后的核心技术——区块链技术,区块链的去中心化、对等等特点迅速吸引众多学者探究其在各个领域应用的可能性。

金融行业最先掀起区块链的应用浪潮,比特币诞生后,以太币、莱特币等数字货币也先后面世。与此同时,纽交所、纳斯达克等大型金融集团陆续以创业投资的方式加入区块链领域,在众多项目中,作为分布式账本初创公司的 R3CEV 提出的区块链金融项目,已有汇丰、高盛、摩根大通等 25 家大型银行集团表示出浓厚的兴趣。

良好的数据透明性和可靠性是区块链能够从单一的货币应用逐渐拓展到更多领域的关键。现如今,我国能源体制改革尚处于起步阶段,而区块链在建立和维护信用等方面低成本的特点与能源互联网的发展趋势十分吻合,由此可见,区块链技术在能源行业的应用前景十分广阔。

区块链作为一个分布式的数据库和去中心化的对等(P2P)网络,具有智能合约、分布决策、协同自治、防篡改的高安全性和公开透明等特征,在运行方式、拓扑形态、安全防护等方面与配电物联网有相似之处[12-14],可基于区块链技术将配电物联网概念升级到配电物联网 2.0 时代,即配电区块链时代。

3　基于可信计算和区块链的配电物联网内生安全

3.1　“云-边-端”架构的配电物联网主站端和边缘端的分级可信免疫管控策略

配电物联网具有广泛接入、交互互联等特点,因此信息安全隐患也越来越多,传统被动式防御策略对针对电网内部的攻击效果甚微。近年来出现

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

的震网(Stuxnet)病毒事件、乌克兰电网遭黑客攻击事件、以色列国家电网大规模网络攻击事件等造成重大影响的安全事件，不仅危及电网，还涵盖了天然气、石油、汽油以及供水系统。由此可见，多数攻击事件的攻击对象是关键基础设施(即终端)，如果能在终端接入电网前就保证其安全可信，就从根源上降低了恶意攻击事件发生的可能性。此外，网络传输过程中的安全可信认证机制也是安全防护的重要内容之一。因此，本文基于配电物联网架构，分析针对内部终端的主动可信防护薄弱点，研究其进行主动防御的可信计算环境。

目前，电力二次系统安全防护总体策略可概括为安全分区、网络专用、横向隔离、纵向认证4个部分[15-16]，针对内部终端的主动可信防护薄弱点显而易见：配电物联网终端数量多，部署环境开放，易被攻击，缺乏对配电终端和物联网终端的安全可信认证；终端入网的连接可信性不能保障，终端入网环节仍有可能被攻击者恶意利用。

可信计算技术通过“计算＋保护”的双体系结构，有效弥补了计算平台本体的安全漏洞，可保障配电物联网系统内部操作系统、业务程序、操作逻辑的完整性，使其免受恶意代码和操作的干扰，达到类似生物体的安全免疫系统功效[17-18]。

因此，本文基于泛在电力物联网的“云-边-端”架构与边缘计算技术，减轻配电主站端的处理负荷，从而构建配电物联网主站端和边缘端的分级可信免疫管控策略，保证配电物联网的安全稳定，如图2所示(图中：RTU为远程终端单元；DTU为配电终端单元；FTU为馈线终端设备；TTU为配电变压器远方终端)。

可信计算一般分为节点可信、网络连接可信和应用可信3个层次：节点可信层为整个主动免疫系统提供信任起点，是主动免疫系统的源头；网络连接可信层承担节点之间交互的免疫，是网络可信的关键部分；应用可信层为节点和网络提供免疫支持和服务，更新安全策略，增强节点的免疫能力。

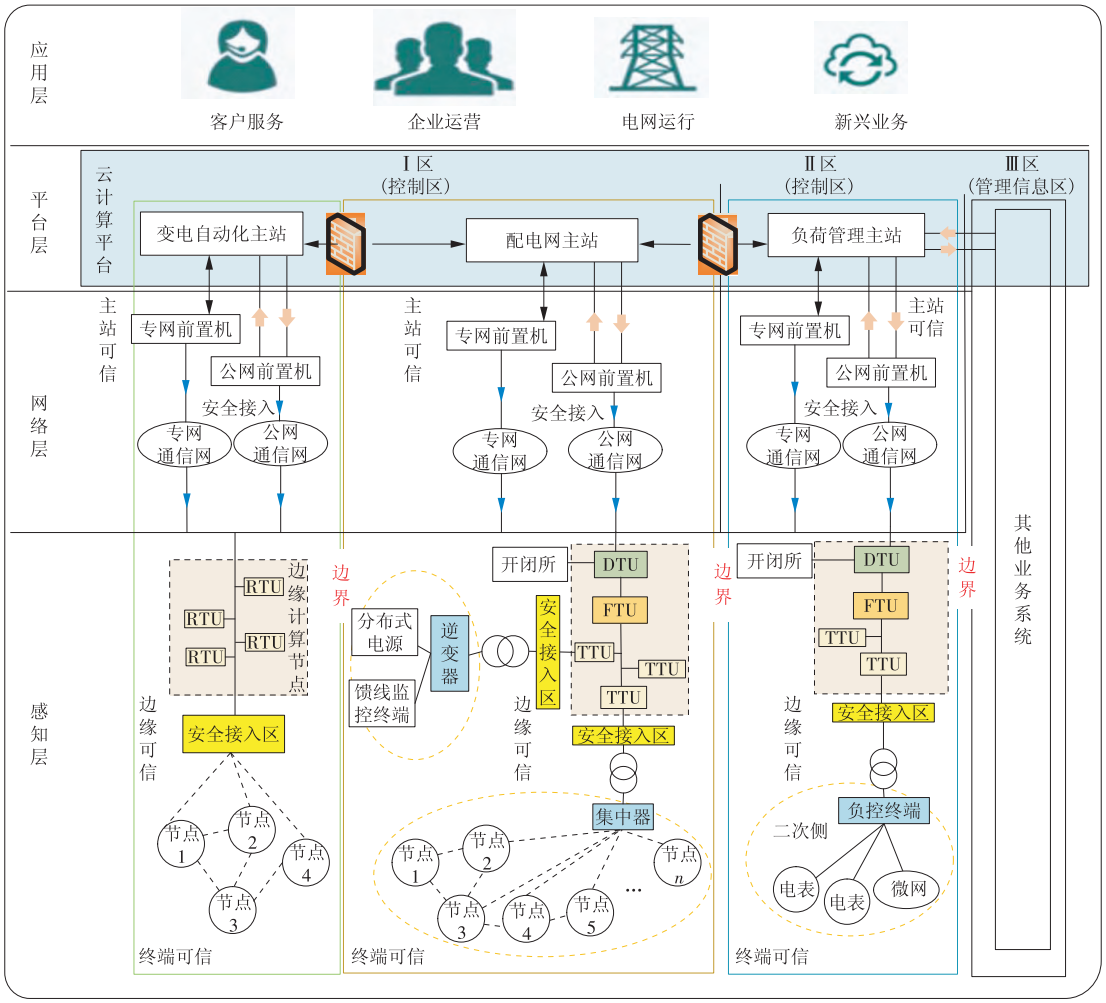

图2 “云-边-端”架构的配电物联网主站端和边缘端的分级可信免疫管控策略

Fig. 2 Hierarchical credibility immune management and control strategy for the master station and the terminals of the distribution IoT with a "cloud-side-user" architecture

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

本文构建的配电物联网主站端和边缘端的分级可信免疫管控策略每一级分别实现可信计算的节点可信、网络连接可信和应用可信3个层次的功能，将安全接入区和可信管控下放至边缘侧，利用边缘计算技术实现计算、分析与安全控制的本地化和就地化，提升处理效率和响应速率，减轻主站端的处理负荷，支撑远程和本地化处理协同与优化管理。

3.2　基于区块链的配电物联网节点映射模型

区块链技术在运行方式、拓扑形态、双边协商、安全防护等方面与配电物联网有相似之处，因此，本文开展区块链和配电物联网的物理、逻辑、功能、协议等对应映射模型的研究，以区块链技术支撑配电物联网对等互联式的数据安全交互与分享，确保配电物联网的分布决策和协同自治管理机制的安全可信以及数据防篡改和可追溯。

区块链技术去中心化和去信任的特点使得网络中的每个节点均参与相关工作，例如数据交互及记录管理等，但网络中的节点差异性较大，其计算能力不尽相同，故难以要求全部节点都负担安全防护的任务，因此将节点类型分为2类：(1)全节点，具有完整的区块结构与链上数据，每个节点配置有区块链中的所有功能；(2)轻节点，节点只保留链上的部分数据，不为整体网络提供算力，依托全节点的功能参与网络中的简单验证[19-20]。

本文参照区块链节点类型并依据配电物联网中各节点的计算能力、安全防护能力和数据的重要性，将配电物联网各节点映射为2类区块链节点：(1)分布电源、电网、配电终端、大用户负荷、储能装置、物联网网关等类节点为全节点或主节点，其计算、存储和安全防护能力最强，具有保存完整区块、路由、查询和安全验证等完整功能；(2)物联网终端节点为轻节点或从节点，该类节点算力输出和存储空间均不足以保留完整的区块链，仅具有保存区块链、路由、查询及简单安全验证等基础功能。

3.3　基于可信计算和区块链的配电物联网内生安全防护模型

可信计算技术实现了配电物联网的节点可信、网络连接可信和应用可信的安全可信运行环境，即自身安全可信的维度管控；而区块链实现了配电物联网的分布决策和协同自治管理机制的可管和可信，即运行管理机制安全可信的维度管控。因此，本文在构建配电物联网主站端和边缘端的分级可信免疫管控策略的基础上，在每一级分别实现可信计算的节点可信、网络连接可信和应用可信等3个层次功能，并将配电网和配电物联网中各节点的计算能力、安全防护能力和数据重要性等特点分别映射为全节点或主节点、轻节点或从节点，从而结合配电业务感知设备和网络安全管理的需求，搭建基于区块链的配电物联网分布决策和协同自治模型，并建立配电物联网的“可管可控、精准防护、可视可信、智能防御”安全防护模型，如图3所示。

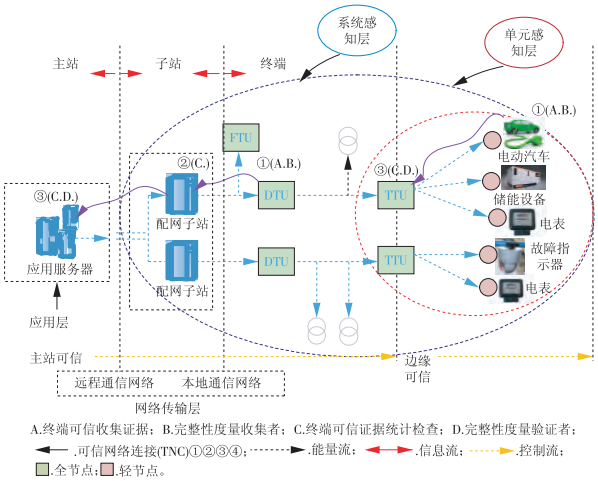

图3　基于可信计算和区块链的能源互联网内生安全防护模型

Fig. 3　Endogenous security protection model for energy internet based on trusted computing and blockchain

配电物联网运行前，各级节点之间进行逐级的可信认证与连接，双方通过公钥与私钥进行非对称加密互验身份后建立起临时的通信信道，通过传递可信报告并与白名单进行对比确定其是否处于安全可信的状态。可信认证逐级进行，信任链从主站端逐渐传递到边缘端；同时，主站、子站、智能终端之间搭建的联盟链进一步保证了链上数据的不可篡改性与可溯源性。

4　结束语

本文基于区块链与可信计算深入探究了配电物联网的内生安全，在设计“云-边-端”架构的配电物联网主站端和边缘端的分级可信免疫管控策略的基础上，搭建了基于区块链的配电物联网分布决策和协同自治模型，并建立配电物联网的“可管可控、精准防护、可视可信、智能防御”安全防护模型，实现了配电物联网自身环境可信、运行机制可信和数据可信等3个维度的内生安全管理，全面提升了配电网的信息安全防御水平。

参考文献：

[1]原凯，李敬如，宋毅，等.区域能源互联网综合评价技术综述与展望[J].电力系统自动化，2019，43(14)：41-52，64.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

YUAN Kai, LI Jingru, SONG Yi, et al. Summary and prospect of comprehensive evaluation technology of regional energy internet[J]. Automation of Electric Power Systems, 2019,43(14):41-52,64.

[2]郭创新,王惠如,张伊宁,等.面向区域能源互联网的"源-网-荷"协同规划综述[J].电网技术,2019,43(9):3071-3080.
GUO Chuangxin, WANG Huiru, ZHANG Yining, et al. Overview of "source-net-dutch" collaborative planning for regional energy internet[J].Grid Technology,2019,43(9):3071-3080.

[3]杨小巳,陶新磊.综合能源技术路线研究[J].华电技术,2019,41(11):22-25.
YANG Xiaosi, TAO Xinlei. Research on integrated energy technical route[J]. Huadian Technology, 2019, 41(11):22-25.

[4]喻小宝,谭忠富,屈高强.基于能源互联网的电力商业模式及关键技术研究[J].智慧电力,2019,47(2):9-14,36.
YU Xiaobao, TAN Zhongfu, QU Gaoqiang. Research on power business model and key technologies based on energy internet[J].Smart Electricity,2019,47(2):9-14,36.

[5]韩峰,张衍国,严矫平,等.综合能源服务业务和合作模式[J].华电技术,2019,41(11):1-4.
HAN Feng,ZHANG Yanguo,YAN Jiaoping,et al.Integrated energy service and cooperation modes [J]. Huadian Technology, 2019, 41(11): 1-4.

[6]孙毅,黄婷,崔晓昱,等.互联网视角下的泛在电力物联网[J].电力科学与技术学报,2019,34(4):3-12.
SUN Yi, HUANG Ting, CUI Xiaoyu, et al. Ubiquitous power Internet of Things from the Internet perspective[J]. Journal of Electric Power Science and Technology,2019,34(4):3-12.

[7]王申华,何湘威,方小方,等.基于泛在电力物联网多源信息的电网动态风险评估系统[J].中国电力,2019,52(12):10-19.
WANG Shenhua, HE Xiangwei, FANG Xiaofang, et al. Grid dynamic risk assessment system based on ubiquitous power Internet of Things multi-source information[J].China Electric Power,2019,52(12):10-19.

[8]陈家璘,贺易,李磊,等.泛在电力物联网传输网优化关键技术研究[J].中国电力,2019,52(12):20-26.
CHEN Jialin, HE Yi, LI Lei, et al. Research on key technologies for ubiquitous power IoT transmission network optimization[J].China Electric Power,2019,52(12):20-26.

[9]王晓,张建标,曾志强.基于可信平台控制模块的可信虚拟执行环境构建方法[J].北京工业大学学报,2019,45(6):554-565.
WANG Xiao, ZHANG Jianbiao, ZENG Zhiqiang. Building method of trusted virtual execution environment based on trusted platform control module [J]. Journal of Beijing University of Technology,2019,45(6):554-565.

[10]李晔锋,公备,徐达文,等.可信计算环境下的数据库强制行为控制研究[J].计算机应用与软件,2018,35(8):66-72.
LI Yefeng, GONG Bei, XU Dawen, et al. Research on database mandatory behavior control in trusted computing environment [J]. Computer Applications and Software, 2018,35(8):66-72.

[11]裴志江,邹起辰,谢超.基于可信计算的工业控制系统[J].计算机工程与设计,2018,39(5):1283-1289.
PEI Zhijiang, ZOU Qichen, XIE Chao. Industrial control system based on trusted computing [J]. Computer Engineering and Design,2018,39(5):1283-1289.

[12]龚钢军,杨晟,王慧娟,等.综合能源服务区块链的网络架构、交互模型与信用评价[J/OL].中国电机工程学报,2020,40(6):1-17[2020-06-25].
GONG Gangjun, YANG Sheng, WANG Huijuan, et al. Network architecture, interactive model and credit evaluation of integrated energy service blockchain[J/OL]. Proceedings of the CSEE, 2020, 40(6): 1-17[2020-06-25].

[13]龚钢军,王慧娟,杨晟,等.区块链技术下的综合能源服务[J].中国电机工程学报,2020,40(5):1397-1409.
GONG Gangjun, WANG Huijuan, YANG Sheng, et al. Comprehensive energy service under blockchain technology [J]. Proceedings of the CSEE,2020,40(5):1397-1409.

[14]龚钢军,张桐,魏沛芳,等.基于区块链的能源互联网智能交易与协同调度体系研究[J].中国电机工程学报,2019,39(5):1278-1290.
GONG Gangjun, ZHANG Tong, WEI Peifanget al. Research on energy internet intelligent transaction and collaborative scheduling system based on blockchain[J]. Proceedings of the CSEE,2019,39(5):1278- 1290.

[15]黄秀丽,马媛媛,费稼轩,等.配电自动化系统信息安全防护设计[J].供用电,2018,35(3):47-51.
HUANG Xiuli, MA Yuanyuan, FEI Jiaxuan, et al. Information security protection design of distribution automation system[J].Power Supply,2018,35(3):47-51.

[16]臧琦,邹婧,郭娟莉,等.电网调度自动化二次系统安全防护实践[J].电子设计工程,2011,19(20):47-49.
ZANG Qi, ZOU Jing, GUO Juanli, et al. Security protection practice of the secondary system of power grid dispatching automation[J].Electronic Design Engineering, 2011,19(20):47-49.

[17]张亚健,杨挺,孟广雨.泛在电力物联网在智能配电系统应用综述及展望[J].电力建设,2019,40(6):1-12.
ZHANG Yajian, YANG Ting, MENG Guangyu. Summary and prospect of ubiquitous power Internet of Things in intelligent power distribution system [J]. Electric Power Construction,2019,40(6):1-12.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[18]江秀臣，刘亚东，傅晓飞，等．输配电设备泛在电力物联网建设思路与发展趋势[J]．高电压技术，2019，45(5)：1345-1351.
JIANG Xiuchen, LIU Yadong, FU Xiaofei, et al. Construction ideas and development trends of ubiquitous power Internet of Things for transmission and distribution equipment [J]. High Voltage Technology, 2019, 45 (5): 1345-1351.

[19]刘格昌，李强．基于可搜索加密的区块链数据隐私保护机制[J]．计算机应用，2019，39(S2)：140-146.
LIU Gechang, LI Qiang. Blockchain data privacy protection mechanism based on searchable encryption [J]. Computer Applications, 2019, 39(S2): 140-146.

[20]甘俊，李强，陈子豪，等．区块链实用拜占庭容错共识算法的改进[J]．计算机应用，2019，39(7)：2148-2155.
GAN Jun, LI Qiang, CHEN Zihao, et al. Improvement of blockchain practical Byzantine fault tolerant consensus algorithm [J]. Computer Applications, 2019, 39(7): 2148-2155.

（本文责编：刘芳）

作者简介：

孙跃(1990—)，男，河北任丘人，工程师，工学硕士，从事电力系统通信技术、区块链技术、能源互联网安全技术和网络与信息安全防护技术等方面的研究(E-mail：641348552@qq.com)。

杨晟(1995—)，男，河北张家口人，在读硕士研究生，从事综合能源服务与区块链等方面的研究(E-mail：yangsheng18hebut@163.com)。

龚钢军(1974—)，男，河南济源人，副教授，工学博士，从事区块链技术应用、能源电力信息安全等方面的研究(E-mail：gong@ncepu.edu.cn)。

“边缘计算在能源互联网中的应用”专刊征稿启事

2020年，国家正式组织实施新型基础设施建设工程，重点发展新兴产业。能源互联网作为未来可能接入设备最多的物联网生态圈，产业发展空间巨大。在能源领域，新型电气信息技术的出现对能源互联网的发展起到了重要的支撑作用，同时也带来了诸如安全性、网络负载及异构设备融合等问题，边缘计算具有靠近数据源、实时性好、低时延、响应快等特征，可以在一定程度上缓解这些问题。《华电技术》作为行业科技创新、技术交流平台，特推出“边缘计算在能源互联网中的应用”专刊，并邀请华北电力大学李彬教授担任特约主编，欢迎业内同仁踊跃投稿。

一、征文范围（包括但不限于）

拟围绕边缘计算在能源领域的国内外发展现状与趋势综述、边缘计算在能源互联网中的应用场景、典型应用案例分析、产品化及实践案例、边缘计算+能源互联网架构模型、新技术融合等内容，主要征集以下方向论文：

(1)边缘计算在能源互联网中的技术发展前景和趋势分析；
(2)边缘计算相关标准化工作；
(3)边缘计算在能源领域5G网络中的应用；
(4)边缘计算与能源区块链、人工智能等交叉领域研究；
(5)边缘计算在能源互联网中的智能数据分析服务；
(6)边缘计算在能源互联网中的信息安全问题；
(7)边缘计算在能源互联网中所衍生的商业模式；
(8)区域边缘计算中心建设及部署方案；
(9)能源互联网中边缘计算与云计算的协同优化技术及相关架构；
(10)边缘计算的落地应用场景以及解决方案和产品；
(11)能源互联网中的边缘计算的项目实践案例；
(12)基于边缘计算的能源行业中的业务应用，如：智能巡检、安防监控、智能配用电、电动汽车车联网、光伏云网等；
(13)其他相关研究。

二、时间进度

专刊拟于2020年9月30日截稿，2020年10期(10月25日)后择期出版。

三、征文要求

(1)专刊只收录未公开发表的论文，拒绝一稿多投。作者对论文内容真实性和客观性负责。
(2)按照《华电技术》论文格式要求使用Word软件排版，请登录《华电技术》在线采编系统(http://www.hdpower.net)下载论文模板。
(3)请保留论文中图片、曲线和表格的原始格式文件，并在投稿时按规定提交。
(4)论文作者应遵守相关学术不端规定。

四、投稿方式

(1)在线投稿(推荐)：登录《华电技术》在线采编系统(http://www.hdpower.net)，完成在线全文投稿。
(2)邮箱投稿：direfish@163.com(李教授)；hdjs-chd@vip.163.com(编辑部)
(3)咨询联系：刘 芳　0371-58501060　13838002988；杨满成　010-63918755　13801175292

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net