基于5G配电网差动保护安全防护策略研究

张 泰[1],杨 雪[2],汪晓帆[2]
(1. 国网四川省电力公司电力科学研究院, 四川 成都 610041;
2. 国网四川省电力公司眉山供电公司,四川 眉山 620010)

摘 要:对5G承载配电网差动保护的网络安全防护策略进行了讨论。首先,给出了配电网差动保护的架构和实现原理;其次,对比分析了5G和4G的安全防护策略和机制,并在此基础上结合5G的自身安全挑战,分析了基于5G配电网差动保护安全防护需求,首次提出了两种5G独立组网和非独立组网模式下基于5G配电网差动保护的安全防护策略和目标;最后,根据配电网差动保护业务数据流向和边界条件给出了基于5G配电网差动保护的安全风险点和应对措施。

关键词:5G;差动保护;网络安全防护
中图分类号:TM77 **文献标志码**:A **文章编号**:1003-6954(2020)06-0060-06

Research of Security Protection Strategy for Differential Protection of 5G-based Distribution Network

Zhang Tai[1], Yang Xue[2], Wang Xiaofan[2]
(1. State Grid Sichuan Electric Power Research Institute, Chengdu 610041, Sichuan, China;
2. State Grid Meishan Electric Power Supply Company, Meishan 620010, Sichuan, China)

Abstract: The security protection strategy for differential protection of 5G-based distribution network is discussed. Firstly, the architecture and implementation principle of differential protection of distribution network are given. Secondly, the security of 5G and 4G networks is compared and analyzed. Combined with the security challenges of 5G, the security protection requirements for 5G-based distribution network are analyzed, and then two security protection goals for differential protection of 5G-based distribution network with SA and NSA are proposed. Finally, the security risk points and countermeasures are given based on the data flow and boundary conditions of the differential protection. The results demonstrate that the proposed security protection strategy is effective.

Key words: 5G; differential protection; security protection of network

0 引 言

配电网是国民经济和社会发展的重要公共基础设施,担负着保障国家经济发展和居民生活质量的重要使命。当前,随着分布式电源、柔性负荷大量接入以及供需互动用电不断深入,配电网的故障特性发生了显著改变,给配电网的安全可靠运行带来了新的挑战。此外,配电网分布广、拓扑结构复杂、中性点接地方式多样,发生故障时,故障点查找、隔离与恢复极为困难,如不能及时排除,将威胁人身及设备安全,甚至引发大面积停电事故。

随着配电网逐渐往主动配电网过渡[1-3],新的构建模式使得配电网的运行面临新的挑战:1)分布式电源的引入将电网由单端辐射型网络变成了多源异构复杂网络,电网可能面临传统三段式电流保护失去选择性和灵敏性降低的风险;2)分布式电源类型复杂,短路电流难以准确计算,传统三段保护之间的级差配合困难;3)当变电站出线断路器跳闸,将导致后级多条线路均被纳入故障停电范围;4)故障发生后,当前恢复送电策略使恢复供电时间较长。因此,传统的过流保护作为配电网线路的主保护存在无法兼顾快速性和选择性要求以及定值困难等问题,其诱发越级跳闸和大范围停电事件的风险越来

越高,难以满足用户对供电可靠性不断提高的要求。配电网差动与区域保护具有可以实现故障区间的快速定位与隔离、定值易整定等优点,但光纤通信敷设的纵联通道方案,存在成本高、难度大、通道利用率低等问题,无法适应分布式电源日益增多的接入电网需求。

随着全球能源互联网的建设推进,大量电厂、电网、用电侧的设备接入国家电网公司网络。在主网通信接入网建设方面,主要依赖光纤组网方式满足保护、安控等控制类业务的通信传输需求。在配电网的通信建设方面,在 A + 、A 类供电区域,为确保电力的可靠供应,与之配套的电力通信网往往采用光纤专网的方式进行,但建设成本居高不下,运行维护压力巨大,无法满足配电网对通信传输可靠性的要求。此外,A + 、A 类供区,城市建设快、市政施工频繁导致配电网引起的光纤中断后无法快速恢复,配电网自动化只能采用盲调方式,严重制约配电网自动化的运行效率。随着配电自动化的建设推进,在 B、C、D 类供电区域,如果仍然采用光纤专网的方式将给公司带来巨大的经营压力,组网及维护成本过高等问题始终难于解决。

2019 年 6 月 6 日,工业和信息化部正式向中国电信、中国移动、中国联通、中国广电四家运营商发放 5G 商用牌照,这标志着中国正式进入 5G 商用元年。5G 技术的低时延、高可靠、海量连接特征,与国家电网公司电网状态全息感知、数据全面连接、业务全程在线、服务全新体验的“能源互联网”建设目标高度吻合。5G 主要在 4G 技术体系基础上的终端接入速率、基站终端连接容量和业务基础时延方面显著提升,在电网中的主要应用场景[4-6]包括:1)增强型移动宽带(enhanced mobile broadband, eMBB),在人口密集区为用户提供 1 Gbps 用户体验速率和 10 Gbps 峰值速率,较 4G 接入速率提升 10 倍,适用于高清视频监控、无人机巡检、维修培训等对带宽的需求非常高的业务。2)超高可靠与低延迟的通信(ultra reliable low latency communications, URLLC),提供毫秒级的端到端时延和接近 100% 的业务可靠性保证,适用于配电自动化、精准控制等对时延的要求高的业务。3)大规模机器类通信(massive machine type of communication, mMTC),提供具备超千亿网络连接支持能力,适用于电网信息的采集、状态检测等海量连接和数据采集应用场景。此外,5G 通信技术具有高带宽、低时延及安全可靠的特点,可以满足配电网差动保护与区域保护纵联通道数据传输时间的要求。利用 5G 通信技术承载配电网纵联保护通道,可在较低成本投入下实现保护快速准确动作,并兼顾保护间的优化配合,可快速隔离故障区间,最大程度缩小故障停电范围和停电时间。

1 基于 5G 配电网差动保护架构

目前,配电网保护可采用过流保护、差动保护和基于 GOOSE 的网络拓扑保护,主流方式仍然是采用基于过流速断的级差保护机制,均通过光纤连接实现。现阶段,尚无 10 kV 线路站内开关过流 I 段设置级差的最佳方案,10 kV 城网线路无法实现故障区域的快速和最小范围隔离。随着配电网络不断延伸扩容、拓扑结构日趋复杂,过流保护定值在复杂配电网配合困难、选择性差、速动性差的问题日益凸显。此外,配电通信网覆盖范围大,覆盖终端数量多,大量设备安装于户外,运行情况复杂,光纤通信线路受市政施工破坏严重,使用缺陷量大,缺陷处理任务繁重。且由于 10 kV 配电网新投入运行时异动量较大,导致相应的通信接入网频繁变动,对网络结构影响大,光纤敷设难度大且成本高。基于 5G 承载配电网差动保护不仅具有良好的经济效益,且是践行国家数字新基建的具体举措。

配电网差动保护试点工程架构如图 1 所示,在保留原过流保护的基础上,增设了 10 kV 相关 5G 差动保护设备,包括 5G 保护装置(实现差动保护及相关配电网自动化功能)、客户端前置设备(customer premise equipment, CPE,实现通道 5G 数据的收发传输)、对时装置(接受北斗/GPS 卫星对时,辅助两侧保护装置实现采样同步),并采用 5G 网络进行数据传输(本次试点工程采用移动运营商网络)。

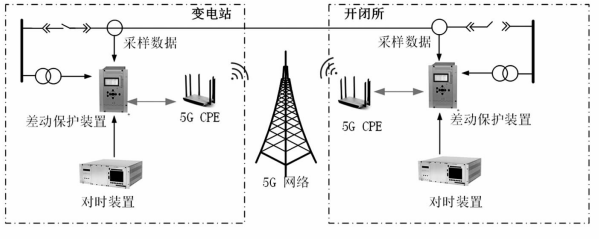

图 1 基于 5G 配电网差动保护架构

2 基于 5G 的配电网差动保护安全概述

2.1 5G 技术的安全挑战[7-8]

相比 4G 网络,5G 不仅要考虑语音和数据的安全性,更要考虑万物互联场景下垂直行业的应用安全。此外,面对各种异构网络(如 4G、WiFi 等)和设备的接入,5G 相较于过往的移动通信技术具有新的安全挑战。

首先是新的业务场景下的安全,5G 的三大场景对安全的要求不同。在 eMBB 场景下,AR/VR 的安全和行业应用安全不同;在 mMTC 场景下,存在设备认证成本高、易产生信令风暴的问题,需要群组认证机制,此外,考虑到设备的能耗,应该设计轻量级的安全算法和简单高效的安全协议;在 uRLLC 场景下,必须考虑时延和安全开销的折中,并需要考虑计入身份认证的时延、数据安全保护引入的时延、网络节点加解密引入的时延和安全上下文切换引入的时延等。

其次,作为 5G 核心网服务化架构(service based architecture, SBA),必然引入了软件定义网络(software defined network, SDN)和网络功能虚拟化(network functions virtualization, NFV)技术来实现其功能,这与传统网络中依赖设备隔离的安全防护方式截然不同,如 NFV 中虚拟化管理层的安全问题,因此存在 SDN 控制网元和转发节点的安全隔离和管理问题等;再者,网络切片被认为是 5G 保障安全的有力手段,但切片之间的安全隔离、虚拟网络的安全部署和管理问题也需要重点考虑;网络开放功能,需要核心网与第三方网元以及核心网元之间支持更高更灵活的安全能力,实现业务签发、发布和每用户每服务都有安全通道。

此外,各种接入技术有不同的安全要求,对隐私的保护程度也不同,用户数据可能穿越不同接入网络和厂商提供的功能网络实体散布在网络各处,通过数据挖掘可能分析出更多用户隐私。4G 已经暴露出泄露用户身份标识(IMSI)的漏洞,因此 5G 网络需要通过加强的安全机制对用户身份进行隐私保护。

2.2 5G 安全机制分析[9-11]

为应对上述安全挑战,5G 网络使用多种技术,使网络具备新的安全能力。

2.2.1 保护用户设备(UE)与网络之间的通信

1)独立组网(standalone, SA)安全:通过 PDCP(packet data convergence protocol),分组数据汇聚协议)保护 UE 和 gNB(5G 基站)之间的控制面和用户面数据。

2)非独立组网(non - standalone, NSA)安全:通过 NSA - MM(移动性管理)保护用户和 AMF(接入和移动管理功能)之间的 NSA 信令。

2.2.2 保护公共陆地移动网(public land mobile network, PLMN)内部网元的通信

1)回传保护。

2)核心网保护。

3)接入认证。

4)伪基站检测和防护机制。

2.2.3 保护网络之间的通信

1)运营商互联安全。

2)多层次切片安全:包括 UE 和切片间、切片内外 NF(网络功能)间安全、切片内 NF 间安全。

2.2.4 向应用提供 5G 安全能力

1)统一认证框架(EAP),适配多种安全凭证和认证方式,并且认证能力开放(AKMA)能为第三方提供认证服务和安全通道。

2)二次认证,即在用户接入网络时所做认证(被称为“主认证”)之后为接入特定业务建立数据通道而进行的认证。例如,当 5G 网络用于为高保障业务系统提供通信时,用户通过接入认证后并不能直接与业务系统建立连接,而是利用业务相关的信任凭据与用户终端进行认证,并在认证通过的情况下才允许 5G 网络为用户建立与业务系统之间的通信链路。二次认证的实质是为构建在 5G 网络之上的第三方应用提供“5G 接入认证 + 第三方应用认证”的双重认证机制,从而提升应用的接入安全性。

3)应用认证与密钥管理,通过用户身份 SUPI 加密,提升隐私保护能力,其对称算法密钥长度延长至 256 bit;

4)差异化安全保护,即用户面按需保护。

5)安全能力开放,让运营商网络安全能力深入地渗透到第三方业务生态环境中。

2.3 配电网差动保护的风险点分析

利用 5G 来承载配电网差动保护业务,面临着来源于 5G 网络和 5G 关键技术的各种恶意攻击等风险,同时也面临着配电网本身数据泄露的风险。

基于 5G 的配电网差动保护业务可能面临的风险如表 1 所示。

表 1　基于 5G 配网差动保护的安全风险

风险层面		风　险　描　述	风险等级
5G 网络安全威胁	终端安全威胁	设备及硬件威胁:硬件设备被盗,物理防护设施破坏等。	低
		操作系统威胁:操作系统漏洞利用,恶意程序入侵等。	高
		业务应用威胁:差动保护业务应用程序入侵,业务盗用等。	高
	接入网安全威胁	空口信道威胁:阻塞攻击,干扰攻击等。	中
		接入与认证威胁:用户传输数据窃听,认证过程受到中间人攻击或钓鱼攻击等。	低
		空口密钥泄露:归属核心网生成的密钥在信令链路传输过程中泄露。	低
	核心网安全威胁	核心网非授权访问。	低
		终端侧对核心网攻击:信令风暴,拒绝服务攻击等。	低
		网络功能服务的非授权或越权访问。	低
		能力开放安全威胁:能力开放接口非授权访问,能力开放资源滥用。	低
5G 关键技术安全威胁	边缘计算(MEC)安全威胁	MEC 设备威胁:物理攻击、硬件木马攻击,侧信道攻击,身份伪造攻击等。	低
		MEC 平台威胁:虚拟化基础设施入侵,虚拟机或容器逃逸,平台配置恶意更改等。	高
		MEC 应用威胁:资源滥用,侧信道攻击,非授权访问,恶意软件植入,拒绝服务攻击等。	高
		通信层威胁:数据窃听,分组欺骗攻击,通信路由攻击。	中
	SDN 安全威胁	应用层安全威胁:恶意程序注入,隐私信息泄露。	中
		数据层安全威胁:拒绝服务攻击,控制流表篡改,数据泄露。	中
		控制器安全威胁:拒绝服务攻击,控制流表篡改恶意程序注入、安全策略绕行等。	中
		南北向接口威胁:中间人攻击,通信内容篡改、窃听,传输协议漏洞等。	中
	NFV 安全威胁	NFVI 安全威胁:虚拟机或容器逃逸,恶意软件注入,漏洞利用,侧信道攻击,拒绝服务攻击等。	中
		VNF 安全威胁:身份仿冒,非授权访问,敏感信息泄露,漏洞利用,拒绝服务攻击,恶意配置等。	中
		MANO 安全威胁:漏洞利用,非法授权使用,接口数据篡改,与 VNF 之间的通信安全威胁等。	中
	切片安全威胁	切片非法接入,资源耗尽,切片之间的通信安全威胁,切片之间的侧信道攻击,切片间隔离性破坏等。	中
数据风险		数据安全威胁:数据传输过程中的攻击篡改、窃听、中间人攻击,数据存储系统的非法访问等。	高

3　基于 5G 配电网差动保护网络安全防护策略

3.1　基于 5G 配电网差动保护安全隐患

图 2 所示为基于 5G 配电网差动保护数据流向图。

CPE 插入 USIM 卡,接入 5G 网络即完成了 CPE 与核心网的一系列网元秘钥派生的过程,秘钥长度允许 256 bit,保证了 CPE 与基站之间在空口的数据安全。数据的完整性保护可选,需要向运营商确认。中心 - 分布单元(center unit - distributed unit, CU - DU)到用户面功能(user - plane function, UPF)是通过 IPSEC 协议进行安全保护,因此,差动保护装置到 CPE 再到基站,数据安全能得到保证。但是,根据安全边界和数据流,配电网差动保护仍存在如下的安全风险。

1)风险 1:应用层业务数据的安全性风险。由于应用域安全不在 5G 安全标准规定的网络保障范围内,因此,应用层面数据存在在进入 5G 信道之前

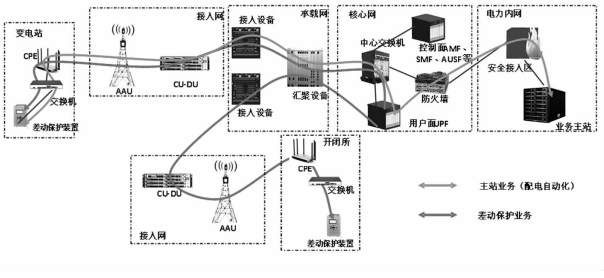

图 2　基于 5G 配电网差动保护数据流向

被篡改的风险。

解决措施:业务数据加密。

2)风险 2:CPE、DTU 存在被攻破、植入恶意代码的可能,影响业务的正常运行。

如某型号 CPE 存在漏洞(CVE - 2017 - 8155、8156),串口访问无认证,攻击者可控制该设备;协议漏洞,TR - 604 协议(LAN 侧 DSL 设备管理配置协议)漏洞导致攻击者不需要任何认证,可直接对 CPE 设备状态进行重新配置、恶意操作;病毒、木马、蠕虫、勒索软件、间谍软件、流氓软件植入;拒绝服务攻击(DDos)。

解决措施:CPE 安全防护、IPS/IDS、安全加固、漏扫。

3)风险 3:USIM 卡和通讯终端存在被盗/异常风险。

解决措施:USIM 卡位置绑定,机卡绑定。

除了上述解决措施外,还提出以下安全防护策略:

1)在 CPE 处开启安全设置,开启防护墙、防 Dos 攻击设置(ICMP_FLOOD、UDP_FLOOD、TCP_SYN_FLOOD 过滤)。

2)部署 IPS/IDS,对 CPE、DTU 的异常行为或威胁进行检测,对源地址进行检查,发现被感染的恶意终端。

3)使用加密芯片对业务数据加密,防止数据被篡改。

4)与运营商确认是否开启空口数据完整性保护。

5)要求运营商支持 USIM 卡位置绑定、支持机卡绑定认证。

6)定期进行漏洞扫描、渗透测试、安全加固、版本升级、等保评级。

7)部署认证与授权应用,提供对配电站终端的二次认证与授权机制,保证应用安全。

3.2 两种组网模式下的防护方案

考虑到目前 5G 网络建设的进程,设计在两种组网模式下,即 NSA 和 SA 的安全防护方案。NSA 非独立组网模式兼顾 4G 和 5G 网络,而 SA 独立组网模式只有 5G 网络,因此,两种模式下安全防护方案也不尽相同。

1)NSA 模式下的配电网差动保护业务整体安全防护方案如表 2 所示。

表 2 NSA 5G 配电网差动保护安全防护方案

防护目标	防护方案
认证授权	终端身份认证,终端数据与存储系统授权访问
通信加密	终端数据加密存储,通信过程中的数据加密传输
防火墙	监控进出变电站和开闭所的网络流量,防护针对终端的网络攻击行为
入侵检测系统(IDS)	主机入侵检测(HIDS):监测针对终端操作系统和应用软件的攻击或异常行为,并进行告警和处置 网络入侵检测(NIDS):采集进出终端的网络通信数据,检测其中的网络攻击行为并进行告警和处置
服务质量(QoS)监测	监测差动保护数据传输质量,对时延抖动过大、带宽异常等情况进行告警

2)SA 组网模式下基于电力专用 MEC 的配电网差动保护业务整体安全防护方案如表 3 所示。

表 3 SA 5G 配电网差动保护安全防护方案

防护内容	防护目标
认证授权	终端身份认证,终端数据与存储系统授权访问 终端与 MEC 业务系统二次认证 MEC 业务系统授权访问、业务应用认证
通信加密	终端数据加密存储,通信过程中的数据加密传输 MEC 业务系统数据加密存储,通信过程中的数据加密传输
防火墙	监控进出变电站和开闭所的网络流量,防护针对终端的网络攻击行为 监控进出 MEC 平台的网络流量,防护针对业务系统的网络攻击行为
入侵检测系统(IDS)	主机入侵检测(HIDS):监测针对终端和 MEC 业务系统的操作系统和应用软件的攻击行为,并进行告警和处置 网络入侵检测(NIDS):采集进出终端和 MEC 业务系统的网络通信数据,检测其中的网络攻击行为,并进行告警和处置
服务质量(QoS)监测	监测差动保护数据传输质量,对时延抖动过大、带宽异常等情况进行告警

IDS 系统方案的设计需考虑以下情况:

1)5G 网络边缘环境通常资源有限,系统应具备较高的资源利用率;

2)5G 网络中的安全威胁类型多、变化快,系统应具备灵活、快速部署各种检测功能的能力。

由于目前配电网差动保护尚未涉及边缘计算(multi - access edge computing, MEC)和 5G 网络切片,因此暂不考虑这两方面的安全防护策略。

4 结 语

基于 5G 的配电网差动保护能实现保护范围内的全线速动,无需与其他保护配合,具有优良的速动性、灵敏性和选择性,且不受系统方式潮流的影响,是目前为止电网保护领域特性较好的保护机制之一。但作为国家能源的重要基础设施,配电网的安全稳定运行尤为重要,因此,全面分析了基于 5G 的配电网差动保护安全隐患,提出以下安全防护策略和方案,切实保障配电网安全稳定运行:

1)给出了配电网差动保护的架构和实现原理;

2)对比分析了 5G 和 4G 网络安全性能;

3)基于 5G 的自身安全挑战分析了基于 5G 的配电网安全防护需求,继而根据差动保护的数据流向和边界条件给出了基于 5G 配电网差动保护的安全风险点和应对措施;

4)提出了两种组网模式下基于 5G 配电网差动保护的安全防护实现目标。

参考文献

[1] 潘本仁,王和春,张妍,等. 含分布式电源的主动配电网重构策略研究[J]. 电力系统保护与控制,2020,48(15):102 – 107.

[2] 白加林,高昌培,王宇恩,等. 基于数据源共享的广域智能保护及控制系统研究与应用[J]. 电力系统保护与控制,2016,44(18):157 – 162.

[3] 毛文晋,李红伟,李超. 一种考虑 DG 出力优化分配的配电网重构方法[J]. 电力系统保护与控制,2017,45(13):57 – 63.

[4] 张平,陶运铮,张治. 5G 若干关键技术评述[J]. 通信学报,2016,37(7):15 – 29.

[5] Gupta A, Jha R K. A Survey of 5G Network: Architecture and Emerging Technologies[J]. IEEE Access, 2015, 3:1206 – 1232.

[6] Agyapong P, Iwamura M, Staehle D, et al. Design Consider – ations for A 5G Network Architecture[J]. Communications Magazine, IEEE, 2014, 52(11): 65 – 75.

[7] 冯登国,徐静,兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018, 29(6): 1813 – 1825.

[8] 李晖,付玉龙. 5G 网络安全问题分析与展望[J]. 无线电通信技术,2015, 41(4): 1 – 7.

[9] 杨红梅,赵勇. 5G 安全风险分析及标准进展[J]. 中兴通讯技术 2014, 52(11): 65 – 75.

[10] Zou Y, Zhu J, Wang X, et al. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends[J]. Proceedings of the IEEE, 2016, 104(9):1727 – 1765.

[11] 李宏佳,王利明,徐震,等. 5G 安全:通信与计算融合演进中的需求分析与架构设计[J]. 信息安全学报, 2018, 3(5): 1 – 14.

作者简介:

张 泰(1982),男,博士,高级工程师,研究方向为电力通信、网络安全;

杨 雪(1985),女,硕士,高级工程师,研究方向为电力通信;

汪晓帆(1993),女,硕士,助理工程师,研究方向为电力通信。

(收稿日期:2020 – 11 – 04)

(上接第 54 页)

[12] 田宏杰. 线损分析预测在供电管理中的应用[J]. 电力系统保护与控制, 2010,38(7): 77 – 80.

[13] 孙雁斌, 刘恺, 陈亦平, 等. 异步联网的交直流输电网损在线优化方法及其在南方电网的实现[J]. 电网技术, 2016, 40(4):1018 – 1024.

[14] 王楠, 张粒子, 黄巍, 等. 电力系统安全经济调度网损协调优化方法[J]. 电网技术, 2010, 34(10): 105 – 108.

[15] 杨文锋, 王彬宇, 程卓, 等. 城市中低压配电网降损规划决策方法[J]. 电网技术, 2014, 38(9): 2598 – 2604.

[16] 陈沧杨, 胡博, 谢开贵, 等. 计入电力系统可靠性与购电风险的峰谷分时电价模型[J]. 电网技术, 2014, 38(8): 2141 – 2145.

[17] 沈红宇, 陈晋, 归三荣, 等. 新一轮电力改革对电网企业配电网规划的影响与对策[J]. 电力建设,2016, 37(3):47 – 51.

[18] 罗运虎,邢丽冬,王勤,等. 峰谷分时电价用户响应模型参数的最小二乘估计[J]. 华东电力,2009, 37(1):67 – 69.

[19] 阮文骏, 王蓓蓓, 李扬, 等. 峰谷分时电价下的用户响应行为研究[J]. 电网技术, 2012, 36(7): 86 – 92.

[20] 顾苏雯,马宏忠,王华芳,等. 基于动态多种群粒子群算法的低压配电网电压无功优化[J]. 电力电容器与无功补偿,2017,38(6):91 – 96.

[21] 郭桂静,徐道安,师秀凤. 基于 Matpower 的电力系统潮流计算[J]. 企业导报,2016(12):172 – 174.

作者简介:

况 华(1973),男,高级工程师,主要从事配电网电压、电能质量方面的研究。

(收稿日期:2020 – 10 – 29)