



基于量子保密通信及 5G 硬切片专网的配网应用研究

吴忠平¹, 王路杰², 许佳诺², 王彦博³, 章立伟¹

(1. 国网宁波供电公司信息通信分公司, 浙江 宁波 315048;

2. 中国移动通信集团浙江有限公司宁波分公司, 浙江 宁波 315048;

3. 北京交通大学, 北京 100044)

摘要: 5G 技术以其超低时延、超高带宽、超大规模连接的显著优势, 有效弥补了配网领域传统光纤通信的弊端, 为配电应用提供了一种全新的网络通信方式, 然而 5G 技术的应用带来的信息安全问题也逐渐凸显。基于此, 提出了一种基于量子保密通信及 5G 硬切片专网的配网应用方案, 该方案为配网业务定制端到端 5G 硬切片专网, 采用量子保密通信技术保障数据传输安全性, 并在实际配网业务场景中进行方案的部署验证。结果显示配网业务 5G 硬切片专网的平均时延为 16.89 ms, 下行发送和接收速率分别为 380 Mbit/s 和 371 Mbit/s, 上行发送和接收速率分别为 31.2 Mbit/s 和 30 Mbit/s, 基本满足电力配网应用的通信要求, 并且基于量子保密通信技术, 量子态误码率为 0.76%, 传输数据能够进行正常加解密, 验证了量子保密通信和 5G 硬切片技术在配网应用的可行性。

关键词: 5G; 网络切片; 量子保密通信; 配网; 信息安全

中图分类号: TN929.5

文献标志码: A

doi: 10.11959/j.issn.1000-0801.2022003

Application research of distribution network based on quantum secure communication and 5G hard-slicing private network

WU Zhongping¹, WANG Lujie², XU Jianuo², WANG Yanbo³, ZHANG Liwei¹

1. Information and Communication Company, State Grid Ningbo Electric Power Company, Ningbo 315048, China

2. Ningbo Branch of China Mobile Zhejiang Co., Ltd., Ningbo 315048, China

3. Beijing Jiaotong University, Beijing 100044, China

Abstract: With its significant advantages of ultra-low latency, ultra-high bandwidth, and ultra-large-scale connection, 5G technology effectively compensates for the shortcomings of traditional optical fiber communication in the distribution network field, and provides a new network communication method for power distribution applications. However, the information security issues brought by the applications of 5G technology have appeared gradually. Based on this, a distribution network application scheme based on quantum secure communication and 5G hard-slicing private network was proposed. An end-to-end 5G hard-slicing private network for distribution network services was customized, and ensuring data transmission security by quantum secure communication technology. And this scheme has been deployed and verified in the actual distribution service network scenario, and the results showed that the average delay of 5G hard-slicing private network was 16.89 ms, the download sending and receiving rates were 380 Mbit/s



and 371 Mbit/s, respectively, the upload sending and receiving rates were 31.2 Mbit/s and 30 Mbit/s, which meets the communication requirements of distribution network applications. Based on quantum secure communication technology, the quantum bit error rate was 0.75%, and the transmitted data can be encrypted and decrypted smoothly, which verified the feasibility of quantum secure communication and 5G hard-slicing technology in the distribution network.

Key words: 5G, network slice, quantum secure communication, distribution network, information security

0 引言

配电网作为连接发电侧和用电侧的末端环节,肩负着将电力传输给千家万户的重要使命,在保障供电稳定、优化供电质量和提升供电安全等方面具有重要作用。面向国家电网“建设具有卓越竞争力的世界一流能源互联网企业”的战略目标,打造广泛互联、智能互动、灵活柔性、安全可控的新一代电力系统已成为电力行业高质量发展的大势所趋,这对配电网的安全性和可靠性提出了更高的要求。传统配网应用主要采用部署光缆满足通信需求,然而一方面配电网末端点位繁多,若进行光缆网络配网全覆盖,部署成本高、周期长、难度大,另一方面配电网电气拓扑复杂持续提升,光纤部署的灵活性和适应性差^[1-2],制约了配电网的自动化和智能化发展水平。

5G 作为新一代蜂窝移动通信技术,在网络指标、网络定制化、部署灵活性等方面具有显著优势,满足电力行业的超低时延、超高带宽、超大规模连接的网络通信需求,为相关电力应用提供有力的通信网络支撑。可以说,5G 网络与电力行业的深度融合逐渐成为赋能未来泛在电力物联网的重要方向。作为典型的 5G 应用场景,配网侧的 5G 应用日益广泛,在配网柱上开关应用方面^[3],5G 网络的低时延特性能够为柱上开关提供实时通信保障,实现电力配网送电的精准调度;在配网相量测量装置(phasor measurement unit, PMU)业务方面^[4],5G 网络高精度授时的理论精度级别达 500 ns,完美适配 PMU 业务对于授时精度和时延的通信需求,为电力系统枢纽点的电压相位、

电流相位等相量数据提供精准的时标信息;在配电网数据采集方面^[5],5G 网络每平方千米高达百万级的连接规模,为配网终端的海量数据采集提供了有效通信手段。

5G 技术的应用一定程度上加速了配电网的信息化、智能化和自动化发展进程,但同时也带来了信息安全问题。5G 网络下安全威胁来源主要有以下几点^[6-7]。

- 在 5G 移动边缘网络架构下,边缘计算节点接入的异构终端类型和数量骤增,扩大了信息数据暴露面和安全风险点。
- 5G 网络用户多,对现有的鉴权系统压力过大,可能造成数据泄露。
- 5G 网络将承载更加丰富多样的配网应用,相应的应用终端通信协议呈多样化趋势,易遭受越权访问、软件漏洞、拒绝服务等安全攻击。

基于此,亟待寻求一种更加有效的通信加密技术提升配网防护安全性。量子保密通信是量子力学和密码学的产物,基于量子力学中的海森伯不确定性原理、未知量子态不可克隆定理和非正交量子态不可区分定理实现通信双方的量子密钥共享,目前已经被证明在理论上可以实现保密通信的“无条件安全性”^[8-10]。目前,量子保密通信已逐步在政务、金融、电力等高安全性要求的领域凸显出重要的应用价值,其中,电力行业作为保障国计民生和社会安全的基础性行业,其数据安全性直接影响着国民生产生活和社会经济发展。量子保密通信技术的应用有效弥补了传统保密通信方式的缺陷,为电力安全提供了全新的技

术手段,对电力保障、电力调度、配电网和容灾备份等业务的数据安全防护具有重要的意义^[11]。

1 关键应用技术

1.1 5G 网络切片

网络切片是 5G 移动通信时代下引入的全新网络技术。作为一种网络资源灵活配置方式,网络切片根据不同行业、不同场景和不同客户的业务通信需求,将单一物理网络端到端虚拟出多个特点各异且相互隔离的逻辑子网,从而满足 5G 网络资源的按需调配和灵活定制^[12]。所谓“端到端”,是指包含了无线网、承载网和核心网在内的整体 5G 网络架构的网络切片组合,并基于切片管理系统对端到端网络切片进行全生命周期管理。

根据端到端各环节的网络隔离性,行业内通常将网络切片分为硬切片和软切片,如图 1 所示。在无线网侧,网络切片主要通过参数配置和功能调度方式实现^[12],其中,软切片方案包括基于 QoS 保障机制的频谱资源动态调度和分配,硬切片方案包括基于频谱资源独享的无线资源块(resource block, RB)资源预留、独立载波的载频隔离和独立基站的专网专用等;在承载网侧,主要通过对网络拓扑资源按需定制多个虚拟网络以形成网络切片,其中,软切片在两层及以上,采用统计复

用的切片技术,包括基于多协议标签交换(multi-protocol label switching, MPLS)、分段路由(segment routing, SR)的隧道技术和基于虚拟专用网(virtual private network, VPN)、虚拟局域网(virtual local area network, VLAN)等的虚拟化技术,硬切片在物理层或数据链路层,主要包括灵活以太网(flex ethernet, FlexE)、光传送网(optical transport network, OTN)、波分复用(wavelength division multiplexing, WDM)等基于物理刚性管道的切片技术^[13];在核心网侧,主要基于网络功能虚拟化(network functions virtualization, NFV)平台定制逻辑网络切片,其中,软切片方案共用省级或地市级用户面功能(user plane function, UPF)网元,硬切片方案基于入驻式的独享 UPF,保障转发数据的专享专用。

1.2 量子保密通信技术

量子通信,作为当前量子论和信息论相结合的全新研究领域,是指利用量子力学原理进行信息传递的一种新型的通信方式。广义上的量子通信是指将某个物理量的量子态从一个地方传送到另一个地方,其研究分支领域包括量子保密通信、量子隐形传态和量子密集编码等^[10,14],其中,以量子密钥分发(quantum key distribution, QKD)为基础的量子保密通信是当前应用广泛且成熟的技术。

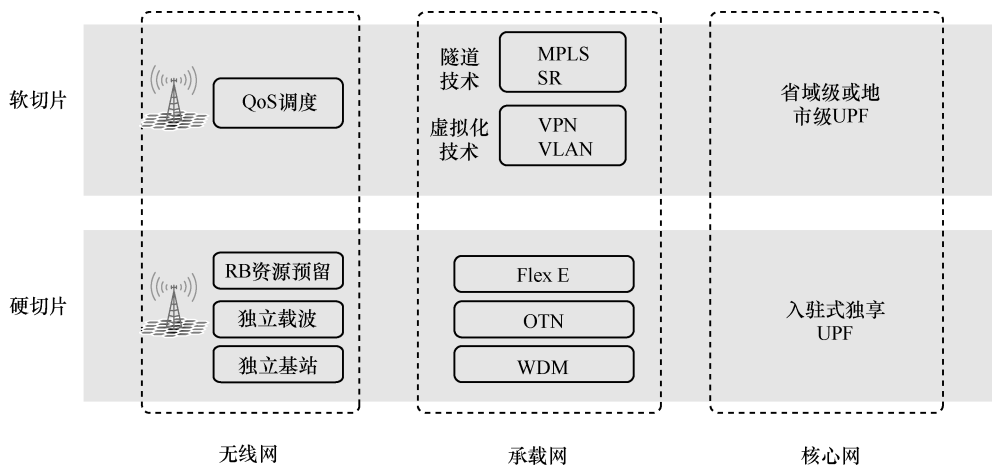


图 1 端到端网络切片分类示意图



术。QKD 技术是指一种在通信双方之间建立量子通道,并以量子态为信息载体进行信息传输,从而实现通信双方共享实时密钥的加密方法,该方法通过量子力学固有的理论特性保证安全性和可靠性。相比于传统通信模式,量子保密通信在理论上可以实现严格数学证明的无条件安全性^[15]。

1984 年, Benett 和 Brassard 提出了首个量子密钥分发协议,简称 BB84 协议。该协议采用两组共轭基和 4 个量子态作为量子信息的载体,通信双方首先利用量子信道进行量子态传输,发送方将测量基矢编码后的量子态发送给接收方,接收方随机选择测量矢量进行测量并保存测量结果;然后通信双方利用经典信道进行密钥协商,得到原始密钥;最后接收端公布原始密钥部分值,双方进行系统扰动或窃听操作判断,获得最终的安全密钥,确保在传输不被窃听的条件下完成整个密钥分发过程^[11,16],量子密钥分发工作原理如图 2 所示。BB84 协议的提出标志着量子通信保密技术开启了新的篇章,并且由于 BB84 协议具备操作性好、稳定性强的优势,其逐渐成为当前实用化程度高的量子通信协议。

2 基于量子保密技术及 5G 硬切片专网的配网应用方案

2.1 整体系统架构设计

基于 5G 的量子保密通信及硬切片专网需要承载电力生产、调度、巡检、管理等重要业务,是建设一流能源互联网企业和提升电网安全管理

要素的关键环节。量子保密通信技术与 5G 硬切片技术结合需要多维度的考虑,尤其在面对较为复杂的电力配网业务时,需要针对其特点进行多个方面的设计^[17]。

在进行整体系统架构设计时,要考虑量子保密技术与 5G 硬切片技术的能力定位,并分析配网应用与配网主站的设备类型、数据量大小、时延要求、安全要求等方面的因素,针对生产控制大区和管理信息大区业务进行相应的设计。整体系统架构如图 3 所示,量子保密技术作为数据加密手段发挥目前最安全的通信加密体系优势,5G 硬切片网络作为数据传输手段发挥解决配网“最后一公里”通信痛点的优势,通过在地市公司和配网应用终端部署量子安全设备和 5G 硬切片专用设备,实现端到端数据传输的量子安全加固,解决由于边缘节点接入异构终端增多、用户数量增多和业务应用日益丰富导致的数据安全问题。

2.2 配网量子保密通信实现方案

为实现电力配网量子密钥的远距离的安全分发,需要开发量子密钥充注机、量子密钥管理平台等软硬件设备,构建以量子密钥能力开通调度平台为中心,量子密钥充值机为通道,量子安全客户机为载体的量子保密通信网络^[11],量子通信配网应用系统架构如图 4 所示。在传输方式上,量子密钥层的量子密钥电力配网应用侧与地市供电公司大楼(发送端/接收端)之间的连接通过单独部署的单芯裸光纤,结合量子通信链路的可靠成码条件,对 QKD 与 QKD 之间的距离和光纤

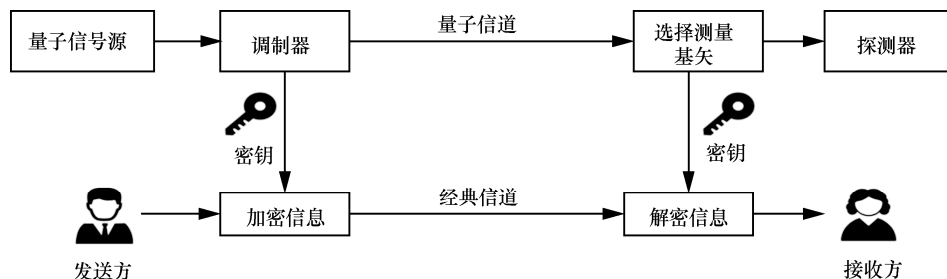


图 2 量子密钥分发工作原理

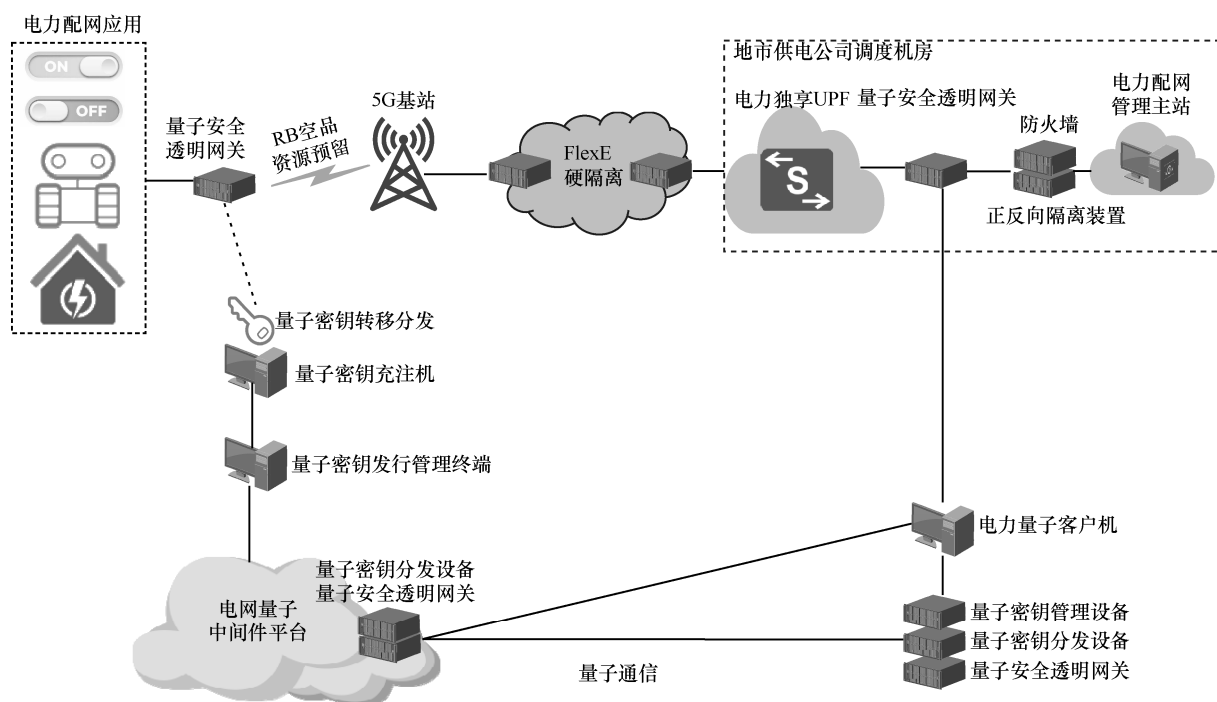


图3 基于量子通信及5G硬切片专网的配网应用系统整体架构

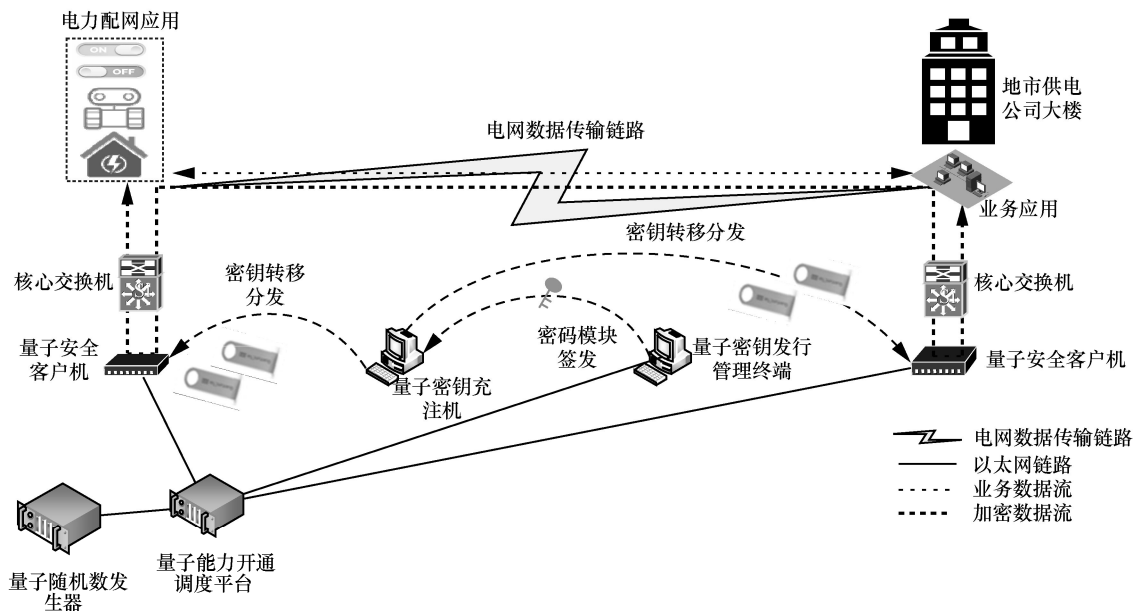


图4 量子通信配网应用系统架构

衰减也有适当的要求，建议配网应用与地市供电公司大楼距离 $<50\text{ km}$ ，光纤衰减程度 $<13\text{ dB}$ ^[18]。量子能力开通调度管理平台系统将量子随机数发生器通过密钥充注机，充注进已完成密钥介质发行的量子U盾、量子TF卡或量子软key。在申领

量子U盾等密钥介质后，插入客户端（或将软key导入终端，或将量子密钥导入连接服务端的量子增强适配设备），利用API调用密钥介质/量子增强适配设备，进行接入认证和工作密钥协商。基于工作密钥，配网应用端、主站端之间完成相



应的量子安全加密通信,从而实现量子密钥的安全存储和分发,实现配网应用的量子安全保密通信。

2.3 5G 硬切片专网架构方案

5G 硬切片专网的主要体现以下两大维度:电力与其他行业及个人用户通信业务之间的专网隔离,以及电力自身生产控制大区和管理信息大区业务之间的隔离。针对上述两大维度,可从无线电接入网、承载网和核心网 3 个方面分别设计专网隔离策略^[19],5G 硬切片配网应用系统架构如图 5 所示。

5G 无线电接入网主要体现在配网应用与 5G 基站通信方面。在进行网络切片选择时,5G 无线电接入网基于无线资源控制(radio resource control, RRC)消息中的 Temp ID 或者网络切片选择辅助信息(network slice selection assistance information, NSSAI)选择接入和移动性管理功能(access and mobility management function, AMF)。电力配网应用终端在和 AMF 建立通信时获取 AMF 所支持的切片信息,并基于预先定义的切片,进行 5G 无线网络调度。针对电力业务高标准的隔离需求,可以通过 RB 资源预留技术,在配网应用涉及的 5G 基站预留足够的空口资源,硬性保障电力业务,避免其他行业或者个人业务影响配网应用的性能表现。

5G 承载网主要体现在运营商的基站与核心网的网元通信方面。通过每个切片端到端硬管道

隔离,在传统以太网架构的基础上,引入了全新的 FlexE 技术,实现介质访问控制(media access control, MAC)子层,属于数据链路层和物理层(physical layer, PHY)的解耦。当配网业务数据流进入 5G 基站后,经过数据的捆绑(小管道合并供大数据使用)、子速率化(大管道供小数据使用)、通道化(大管道供大数据使用)形成基于 FlexE 的配网业务硬隔离专网,实现在承载网环境的其他行业或者个人业务与配网业务的物理隔离。

5G 核心网主要体现在下沉核心网的网元与调度边界安全隔离装置通信方面。5G 核心网可以分为控制面和用户面,控制面网元主要包含 AMF、会话管理功能(session management function, SMF)、网络切片选择功能(network slice selection function, NSSF)、认证服务器功能(authentication server function, AUSF)、统一数据管理(unified data management, UDM)功能、策略控制功能(policy control function, PCF)等,用户面网元主要为 UPF。其中,与配网业务转发数据高相关的网元主要为 SMF、UPF。在电力终端连接 5G 网络基本信令及通信建立后,SMF、UPF 将负责电力业务的会话管理和业务转发,具体包括 SMF 负责电力业务的 IP 地址分配管理、UPF 进行选择及策略实施、QoS 中的控制部分、计费数据采集、漫游等功能。UPF 负责电力业务的路由转发、策略实施、流量报告、QoS 处理等,

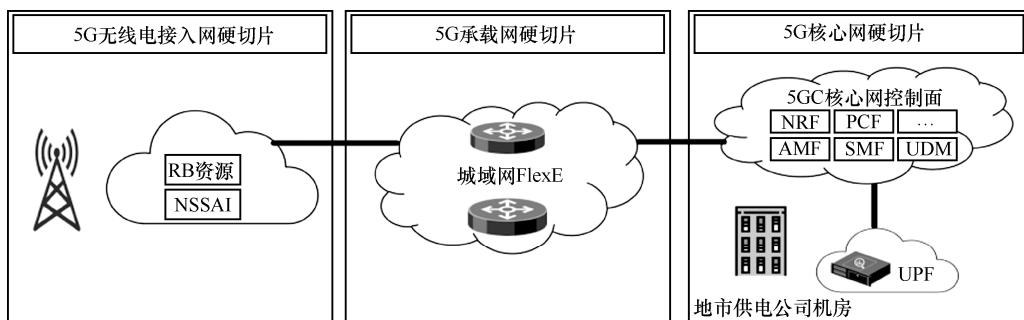


图 5 5G 硬切片配网应用系统架构

相当于电力配网业务的出口网关。根据电力管理需求,业务转发的出口网关应在本地部署,需要部署一套独享的 UPF 网元于地市供电公司调度机房,并在同一硬件资源池上虚拟出电力业务专用的逻辑核心网元,为每个独立切片包含完整的核心网控制面和用户面功能,形成服务电力配网应用的专网^[20]。

3 配网业务量子保密通信及 5G 硬切片专网验证

2021 年 5 月,国家电网、中国移动、北京交通大学、国科量子与华为在浙江宁波联合验证了配网业务量子通信及硬切片专网,验证了量子保密通信和 5G 硬切片技术在配网应用的可行性。

3.1 配网业务量子保密通信验证

为验证量子保密通信系统在配网业务中的适用性,需要验证量子保密通信信号能否在复杂配网业务环境中稳定传输,本文从量子设备对接与量子系统稳定性两方面进行评估。

首先,验证测试量子安全网关与相关设备对接功能,即两台量子安全网关可以通过底层以太网网络实现对接,进行数据正常传输及传输过程中成功加、解密。在验证过程中,如图 4 所示搭建测试系统,确保量子密钥分发子系统正常工作,能向量子安全网关输出量子密钥;其次,将量子安全网关与两端设备对接,量子安全网关底层以太网网络,使用量子密钥进行数据传输加解密;最后,在配网调度主站或模拟网络可以同量子安全网关对接及业务通信,通过网络出口设备进行流量镜像及抓包,发现有 ESP 协议即加密协议,说明量子安全网关与相关设备能够实现正常对接。

此外,针对量子通信系统在电网环节下的稳定成码性能,测试了量子通信 QKD 系统在实际电力架空线路柱上开关的量子比特误码率(发送端和接收端在选择同样测量基的情况下,接收端出现错误结果的概率)^[21]。结果显示量子信道衰减

5 dB,量子态误码率 0.76%,满足量子比特误码率小于 11%的最低理论安全成码要求,有效保证量子通信系统在电网业务中的稳定性和可用性。

3.2 5G 硬切片专网通信验证

5G 硬切片专网的验证须在无线电接入网、承载网、核心网进行端到端的测试。无线网络设备采用华为的 AAU/BBU 5G 设备,部署于配网应用地区,承载网设备采用华为的 PTN980 设备,实现基于基站到核心网的传输,核心网设备采用华为 E9000 设备,部署于地市供电公司的核心机房。部署在基站上的 AAU 设备以上下行 RB 最小比例表示切片专用 RB 资源;部署在承载网的 PTN980 设备配置两个 FlexE 分组切片,切片 2 承载电力配网专享业务,配置 1 GB 带宽;切片 1 为默认切片,承载基站 To C 业务,配置占用剩余的链路大时隙带宽;部署在地市供电公司的 E9000 设备通过防火墙、正反向隔离装置上联国网 OPEN5200 配电自动化系统,下联浙江移动核心网,并与配网业务的电力终端进行认证绑定。

5G 硬切片专网与普通用户网络资源使用对比如图 6 所示,经验证,在对电力切片配网应用硬切片业务满灌包时,普通用户可使用 30% RB 资源,硬切片业务最大可使用 70% 资源,1 Gbit/s 承载网带宽资源;配网硬切片应用不进行业务时,普通用户最高可使用 70% RB 资源。即证明 5G 硬切片专网业务最低能够使用 30% 的无线 RB 资源,1 Gbit/s 的承载网带宽资源,满足 5G 硬切片专网定义。

3.3 配网业务量子保密通信及 5G 硬切片专网的网络指标验证

在完成上述系统搭建后,进行配网业务量子保密通信及 5G 硬切片专网的关键网络指标验证。

(1) 通过测试平台模拟电力配网主站,将配网终端的 10 个遥信变位模拟信息进行量子安全加密,经 5G 硬切片网络上送测试平台,经解密后在测试平台顺利监测到遥信变位信息,并可通过测

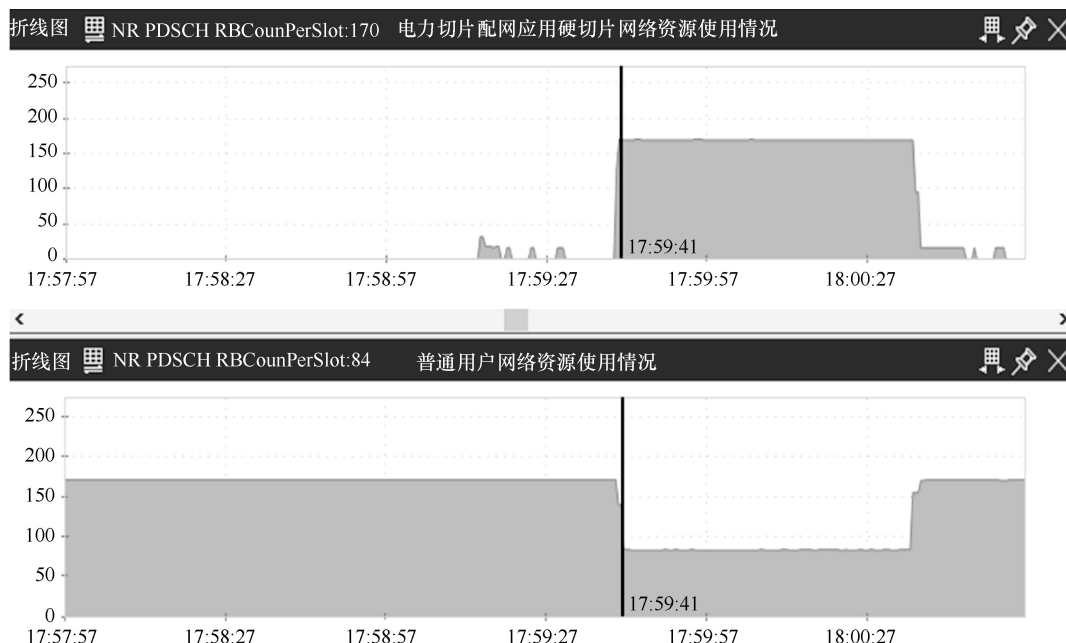


图6 5G硬切片专网与普通用户网络资源使用对比

试平台对配网终端进行遥控,即完成信源-信宿之间的传输。

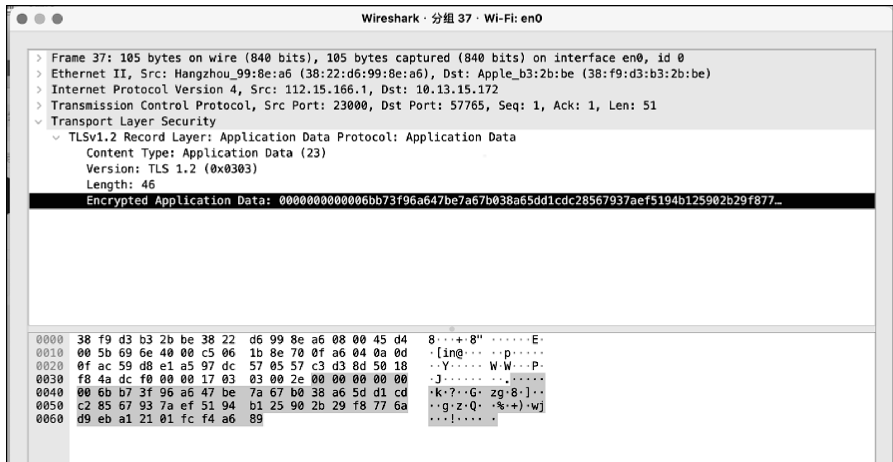
(2)在对应5G基站的传输设备PTN980进行报文监测,分别获取RSA(Ron Rivest-Adi Shamir-Leonard Adleman)算法加密的遥信报文和量子加密的遥信报文,并分别尝试破译。结果显示RSA加密的遥信报文在具有RSA密钥的情况下较容易破解,在不具有RSA密钥的情况下需大量时间破解,而采用量子加密的遥信报文由于其难以伪造性、难以否认性及难以回溯性几乎无破解可能。

(3)测试平台与配网应用终端进行连续28h的灌包测试,在平台侧生成相关测试结果模型。如图7和表1所示,测试结果表明,5G加量子保密通信的最小时延为13.11ms,最大时延为141.83ms,平均时延为16.89ms,点对点下行速率发送380Mbit/s,接收371Mbit/s,点对点上行速率发送31.2Mbit/s,接收30Mbit/s。基本满足电力配网应用的通信需求^[21],后期计划采用授时精度更加精准的5G模组,进一步优化网络性能指标,更加有效支撑电力配网业务。

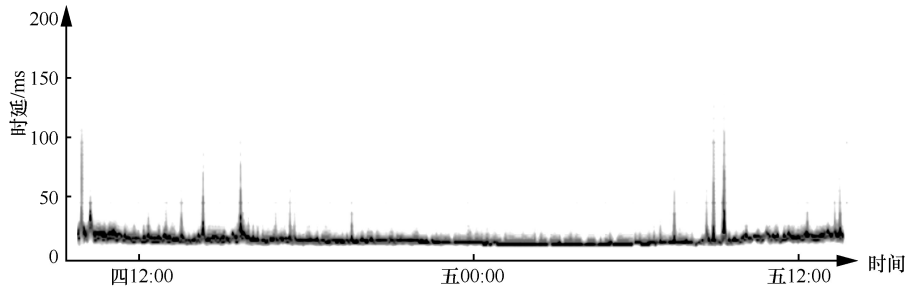
4 结束语

随着5G技术在电网应用的逐步深入,配网应用的安全性和可靠性逐渐成为电力行业研究的热点课题。量子通信作为被理论证明是无条件安全的新一代通信加密技术,对保障配电网5G专网的安全性具有重要价值。本文首先介绍了5G网络切片关键技术和量子保密通信技术的基本原理,在此基础上,提出了基于量子保密技术及5G硬切片专网的配网应用方案架构,并在浙江宁波区域配电应用中进行了实地部署和系统验证。验证结果表明,量子态误码率仅为0.76%,满足量子通信最低理论安全成码要求,同时配网业务5G硬切片专网的端到端平均时延为16.89ms,基本满足电力配网应用的时延要求,且量子通信技术能够保障传输数据进行正常加解密,破解难度极高,验证了量子保密通信和5G硬切片技术在配网应用的可行性。

本文提出的基于量子保密通信及5G硬切片专网的配网应用方案对于解决配网领域创新应用的安全性问题具有一定的指导意义,也为量子保



(a) 报文监听结果



(b) 时延测试结果

图 7 配网业务量子保密通信及 5G 硬切片网络指标测试

表 1 关键网络指标测试结果

网络指标		5G+量子保密技术	5G+RSA 保密技术
时延	最小时延	13.11 ms	14.28 ms
	最大时延	141.83 ms	140.52 ms
	平均时延	16.89 ms	17.05 ms
	时延抖动平均值	3.31 ms	3.68 ms
下行速率	发送速率	380 Mbits/s	395 Mbits/s
	接收速率	371 Mbits/s	382 Mbits/s
上行速率	发送速率	31.2 Mbits/s	31.7 Mbits/s
	接收速率	30.0 Mbits/s	321.3 Mbits/s
安全性	破解难度	极难	无密钥较难 有密钥较易

密通信技术在电力行业的拓展推广提出了可行的探索路径。

参考文献:

[1] 张辰, 林晓亮, 段凌霄, 等. 基于 5G 通信技术的配电网精准控制端到端承载方案研究[J]. 浙江电力, 2021, 40(2): 78-84.

ZHANG C, LIN X L, DUAN L X, et al. Research on the

end-to-end bearing scheme of accurate control in power distribution based on 5G communication[J]. Zhejiang Electric Power, 2021, 40(2): 78-84.

[2] 张建雨, 姜睿智, 李俊刚, 等. 基于 5G 通信的配电网差动保护技术研究[J]. 电力系统保护与控制, 2021, 49(7): 17-23.

ZHANG J Y, JIANG R Z, LI J G, et al. Research on differential protection of a distribution network based on 5G communication[J]. Power System Protection and Control, 2021, 49(7): 17-23.



- [3] 毕昊林, 王加友, 黄良栋, 等. 基于边缘计算的柱上开关状态监测研究[J]. 中国新技术新产品, 2020(6): 13-14.
BI H L, WANG J Y, HUANG L D, et al. Research on on-pole switch state monitoring based on edge computing [J]. New Technology & New Products of China, 2020(6): 13-14.
- [4] 袁通, 高厚磊, 徐彬, 等. 5G 高精度时间同步及在电网中的应用模式研究[J]. 电力信息与通信技术, 2020, 18(8): 47-53.
YUAN T, GAO H L, XU B, et al. Research on 5G high-precision time synchronization and its application mode in power grid[J]. Electric Power Information and Communication Technology, 2020, 18(8): 47-53.
- [5] 王毅, 陈启鑫, 张宁, 等. 5G 通信与泛在电力物联网的融合: 应用分析与研究展望[J]. 电网技术, 2019, 43(5): 1575-1585.
WANG Y, CHEN Q X, ZHANG N, et al. Fusion of the 5G communication and the ubiquitous electric Internet of Things: application analysis and research prospects[J]. Power System Technology, 2019, 43(5): 1575-1585.
- [6] 张滨. 5G 边缘计算安全研究与应用[J]. 电信工程技术与标准化, 2020, 33(12): 1-7.
ZHANG B. Research and application on the 5G edge computing[J]. Telecom Engineering Technics and Standardization, 2020, 33(12): 1-7.
- [7] 谢振华. 5G 移动网络安全技术分析[J]. 邮电设计技术, 2019(4): 49-52.
XIE Z H. Analysis of security technology of 5G mobile network[J]. Designing Techniques of Posts and Telecommunications, 2019(4): 49-52.
- [8] 王金东, 张智明. 量子密钥分发系统的现实无条件安全性[J]. 量子电子学报, 2014, 31(4): 449-458.
WANG J D, ZHANG Z M. Unconditional security of quantum key distribution based on practical devices[J]. Chinese Journal of Quantum Electronics, 2014, 31(4): 449-458.
- [9] 赖俊森, 吴冰冰, 汤瑞, 等. 量子通信应用现状及发展分析[J]. 电信科学, 2016, 32(3): 123-129.
LAI J S, WU B B, TANG R, et al. Analysis on the application and development of quantum communication[J]. Telecommunications Science, 2016, 32(3): 123-129.
- [10] 樊矾, 魏世海, 杨杰, 等. 量子保密通信技术综述[J]. 中国电子科学研究院学报, 2018, 13(3): 356-362.
FAN F, WEI S H, YANG J, et al. Review of quantum secret communication technology[J]. Journal of China Academy of Electronics and Information Technology, 2018, 13(3): 356-362.
- [11] 倪振华, 李亚麟, 姜艳. 量子保密通信原理及其在电网中的应用探究[J]. 电力信息与通信技术, 2017, 15(10): 43-49.
NI Z H, LI Y L, JIANG Y. Brief introduction of quantum secure communications and the application survey in state grid[J]. Electric Power Information and Communication Technology, 2017, 15(10): 43-49.
- [12] 刘义亮, 李鑫, 薄开涛. 5G 端到端网络协同关键技术[J]. 电信科学, 2020, 36(3): 144-155.
LIU Y L, LI X, BO K T. End-to-end network collaboration in 5G networks[J]. Telecommunications Science, 2020, 36(3): 144-155.
- [13] 王强, 陈捷, 廖国庆. 面向 5G 承载的网络切片架构与关键技术[J]. 中兴通讯技术, 2018, 24(1): 58-61.
WANG Q, CHEN J, LIAO G Q. Architecture and key technologies of 5G transport network slicing[J]. ZTE Technology Journal, 2018, 24(1): 58-61.
- [14] 吴华, 王向斌, 潘建伟. 量子通信现状与展望[J]. 中国科学: 信息科学, 2014, 44(3): 296-311.
WU H, WANG X B, PAN J W. Quantum communication: status and prospects[J]. Scientia Sinica (Informationis), 2014, 44(3): 296-311.
- [15] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.
- [16] 吴佳伟, 卞宇翔, 张庆, 等. 基于无线通道的电力量子密钥分发系统[J]. 电信科学, 2020, 36(2): 68-75.
WU J W, BIAN Y X, ZHANG Q, et al. Wireless quantum power distribution system based on wireless[J]. Telecommunications Science, 2020, 36(2): 68-75.
- [17] 王磊, 赵广怀, 范晓楠, 等. 量子保密通信在电网业务应用的方案研究与设计[J]. 电力信息与通信技术, 2018, 16(3): 34-38.
WANG L, ZHAO G H, FAN X N, et al. Research and design of quantum private communication in power grid service application[J]. Electric Power Information and Communication Technology, 2018, 16(3): 34-38.
- [18] BRASSARD G, LÜTKENHAUS N, MOR T, et al. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6): 1330-1333.
- [19] 李挺, 赵侠, 陈其铭, 等. 5G 网络切片在电力行业的应用[J]. 电信工程技术与标准化, 2020, 33(1): 15-18. LI T, ZHAO X, CHEN Q M, et al. Application of network slice in electric power industry[J]. Telecom Engineering Technics and Standardization, 2020, 33(1): 15-18.
- [20] 陈丰. 基于 5G 网络切片技术的智慧电网应用研究[J]. 邮电设计技术, 2020(6): 87-92.
CHEN F. Application research of smart power grid based on 5G network slicing technology[J]. Designing Techniques of Posts and Telecommunications, 2020(6): 87-92.
- [21] 刘国军, 张小建, 吴鹏, 等. 电力量子保密通信安全测试指

标体系研究[J]. 电力信息与通信技术, 2017, 15(10): 50-54.
LIU G J, ZHANG X J, WU P, et al. Research on security test index system of power quantum secure communication[J]. Electric Power Information and Communication Technology, 2017, 15(10): 50-54.

[作者简介]



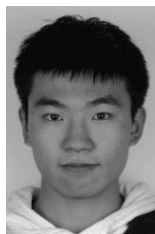
吴忠平(1970-), 男, 国网宁波供电公司信息通信分公司高级工程师, 主要研究方向为电力系统通信。



王路杰(1996-), 男, 中国移动通信集团浙江有限公司宁波分公司助理工程师, 主要研究方向为 5G 网络信息通信。



许佳诺(1995-), 女, 中国移动通信集团浙江有限公司宁波分公司助理工程师, 主要研究方向为 5G 网络信息通信。



王彦博(2000-), 男, 北京交通大学在读, 主要研究方向为建模及图像处理。



章立伟(1982-), 男, 国网宁波供电公司信息通信分公司高级工程师, 主要研究方向为电力系统通信。