



量子密钥分发技术在智能变电站中的研究

杨晓朋¹, 陈海涛², 梅力宸³, 王鹏展⁴

(1. 河南电力实业集团有限公司, 河南 郑州 450000;

2. 国网河南省电力公司信阳供电公司, 河南 信阳 464000;

3. 阿里云计算有限公司, 浙江 杭州 310000;

4. 济南恒道信息技术有限公司郑州分公司, 河南 郑州 450000)

摘要: 为了提高电力系统通信数据的安全性, 结合量子密钥分发技术和智能变电站监控系统发展的状况, 分析论证了量子密钥分发技术在智能变电站监控系统应用的可行性; 提出了量子密钥分发与智能变电站辅助监控系统相结合的技术方案; 在利用现有电力通信系统框架的前提下, 给出了变电站辅助监控系统与量子密钥分发技术的组网思路——“量子密钥+电力纵向加密认证网关”, 并对组网方案进行了验证分析, 证明了该组网方案在实际应用中的稳定性和可行性。因此, 不需要大规模调整现有通信网络框架, 即可实现规模化的应用。

关键词: 量子密钥; 监控系统; 电力纵向加密认证网关; 量子密钥分配终端

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018248

Research on quantum key distribution technology in intelligent substation

YANG Xiaopeng¹, CHEN Haitao², MEI Lichen³, WANG Pengzhan⁴

1. Henan Electric Power Industry Group Co., Ltd., Zhengzhou 450000, China

2. Xinyang Power Supply Company of State Grid Henan Electric Power Company, Xinyang 464000, China

3. Alibaba Cloud Computing Co., Ltd., Hangzhou 310000, China

4. Zhengzhou Branch of Ji'nan Heng Dao Information Technology Co., Ltd., Zhengzhou 450000, China

Abstract: In order to improve the security of the communication data of the power system, the feasibility of the application of quantum key distribution technology in the monitoring system of the intelligent substation was analyzed and demonstrated by combining the state of quantum key distribution technology and intelligent substation monitoring system. The technical scheme, intelligent substation monitoring system combined with quantum key distribution was put forward. On the premise of using the existing power communication system framework, the networking idea of intelligent substation monitoring system and quantum key distribution technology was presented, which was “quantum key + power vertical encryption authentication gateway”. And the network scheme was verified and analyzed, which proved the stability and feasibility of the networking scheme in practical application. Therefore, no need to adjust the existing communication network framework, the application scheme can be realized on a large scale.

Key words: quantum key, monitoring system, power vertical encrypted authentication gateway, quantum key distribution terminal



1 引言

基于量子力学基本原理的量子密钥分发技术能在通信双方之间建立无条件安全的密钥。随着量子通信在光纤中传输的兼容性得到解决和传输距离的延长^[1-2]以及量子通信组网成品、量子密钥分发产品的成功研制,基于量子密钥分发的技术已经可以投入实际生产当中^[3-6]。参考文献[7]是对实际的传输距离对量子密钥分发的影响和应用进行了分析,这些成果在理论上保证了量子密钥分发在实际应用中的安全性和可行性。同时,参考文献[8]给出了量子密钥网络与政务网结合的案例,利用量子密钥来保护文本文件、语音文件等的安全性,这为利用量子密钥在变电站视频监控中的应用提供了借鉴的基础。

智能变电站辅助监控技术是实现变电站无人值守的手段,它不但能够为变电站的多个辅助系统的集成化管理,而且能够实现变电站站端站控层的高级应用提供支撑^[9]。国内一些学者针对智能变电站监控系统的进行了相关研究,但是仅分析和解决了该系统在应用便捷性和站端实用性方面的问题,没有给出保证监控数据在传输中的安全性的具体方法。因此,对于站端和市级电力调度中心(以下简称“市调”)通信双方之间的信息,特别是控制一次设备的控制信息和一些电力数据的机密信息仍存在着被窃听的风险^[10-11]。本文将对智能变电站辅助监控系统设计原则和通信安全的重要性进行分析,并介绍量子密钥分发与智能变电站监控系统融合实现的方案及可行性。

2 智能变电站监控系统

2.1 智能变电站监控系统数据传输

智能变电站监控系统采用标准化、网络化、分布式的系统结构,可以将变电站的安防系统、消防系统、工业环境参数、灯光空调等远程控制设备、视频智能分析系统、视频图像、变电站的

物理区域数据、一次设备与二次设备的布置数据等内容整合成一个统一的数据平台,实时上传地区监控中心(地区中心主站),并接收监控中心的各种指令,实现各种系统功能。该系统数据的传输是依据电力系统全球通用标准 IEC61850 下的通信标准进行的,在数据通信传输的标准中,其数据都不能避免被窃听的风险,这就不可能保证在调度中心的每一个指令准确地到达站端。例如目前常用的电力通信 SIP(session initiation protocol)无法检测窃听,SSL(secure sockets layer)协议的安全性依赖于密钥技术,而这些协议安全性都同样依赖于复杂的数学计算,面临量子计算的攻击,不能保证信息的安全性,为了实现更可靠的安全性,需要更高级别的加密方式^[12-13]。

2.2 电力数据安全传输的重要性

电力系统具有独立运行的通信专网,即作为电网二次系统重要组成部分的电力通信网,为电力的生产、调度、经营和管理提供不可或缺的各项安全服务^[14]。而智能变电站监控系统传输的数据涉及常用的电力业务、管理、指令下达等数据,对整个变电站的安全生产起着重要作用,因此对其数据传输的安全性要求也比较高^[15]。

数据的安全性主要由用户管理权限、服务器系统安全、传输过程安全以及数据加密等方式控制。用户管理权限保证重要数据只能由具有相关的管理和访问权限的用户才能读取。在智能变电站监控系统中,能合法访问的授权用户为局方相关人员;服务器系统安全包括服务器物理位置的安全和服务器系统应用的安全。而在智能变电站监控系统中,服务器系统安全源于用户的安全操作和正常维护,传输过程的安全即能够监测到非法窃听者。而在智能变电站监控系统中,利用目前的技术不能确定在数据传输过程中是否存在窃听者,这也是目前智能变电站监控系统中数据通信传输的一个弊端。

3 量子密钥分发技术

量子密钥通信技术能够实现绝对安全的保密通信, 基于量子力学的未知量子态不可克隆原理、量子态测量原理、量子不确定性原理三大基本原理。在经典的通信方式中, “一次一密” 是已被证明最安全的密码机制, 而将随机生成无条件安全密钥的量子密钥分发技术与“一次一密” 结合起来, 可以实现无条件的绝对安全保密通信。

目前应用的量子密钥分发组网方式主要有点对点型和全时全通型两种。点对点型量子网络主要是在两节点分别建立收/发独立型的量子安全密钥系统, 节点之间直接部署量子安全密钥系统, 实现点与点之间的安全通信。点对点型量子网络如图 1 所示。

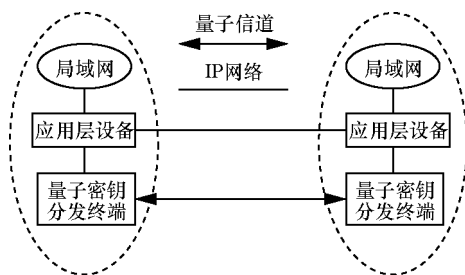


图1 点对点型量子网络

全时全通型量子网络, 每个节点为收发一体化的量子安全密钥系统, 节点之间通过量子路由器实现节点上量子安全密钥系统的互联互通, 任意两节点可实时实现量子加密信息的互通, 实现数据高度安全加密传输。全时全通型量子网络如图 2 所示。

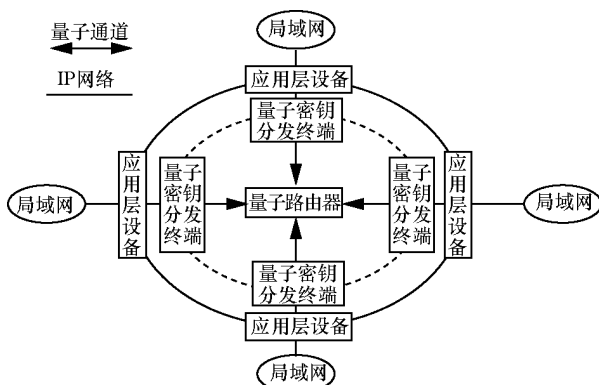


图2 全时全通型量子网络

4 量子密钥的分发在智能变电站监控系统中的实施

4.1 组网结构

量子密钥分发技术在智能变电站监控系统中部署实施中, 与传统的电力纵向加密技术有很大的不同, 主要体现在需要在量子密钥分发系统结构中加入量子通信设备用于身份认证和信息交换的会话管理模块——量子密钥分发终端设备。基于量子密钥分发的智能变电站监控系统主要的结构体系如下。

4.1.1 RJ45 接口

作为独立的内网接口, 该接口用于电力纵向加密认证网关和量子密钥分发服务器相连接, 向量子密钥分发服务器请求量子密钥。

4.1.2 波分信道

为了实现光纤资源的复用, 降低投入成本, 提高裸光纤的利用率, 采用经典—量子波分复用技术, 将业务信道、交互信道、量子信道通过波分技术整合的一个裸光纤中。

4.1.3 全通型量子网络

该网络结构通过使用量子路由器实现各个节点上的量子安全密钥系统互联互通, 实现站端和调度中心之间数据高安全加密传输, 保障数据传输的安全性。

由此可以看出, 量子密钥分发系统加入智能变电站监控系统, 并未改变监控系统的网络结构, 只是在该网络结构扩展了电力纵向加密认证网关的接口, 提高了信道的利用率, 改变了密钥的加密方式。

按照传统的电力通信加密原则, 只在上下级之间建立加密通信的隧道, 在智能变电站监控系统中, 量子密钥分发系统向纵向加密认证网关提供密钥, 对下属的几个变电站之间的通信数据进行加解密处理, 如图 3 所示。

4.2 量子密钥分发通信

市调控制对各个变电站信息通信网络, 其中长距离通信可以增设中继。这样, 市调可以在量

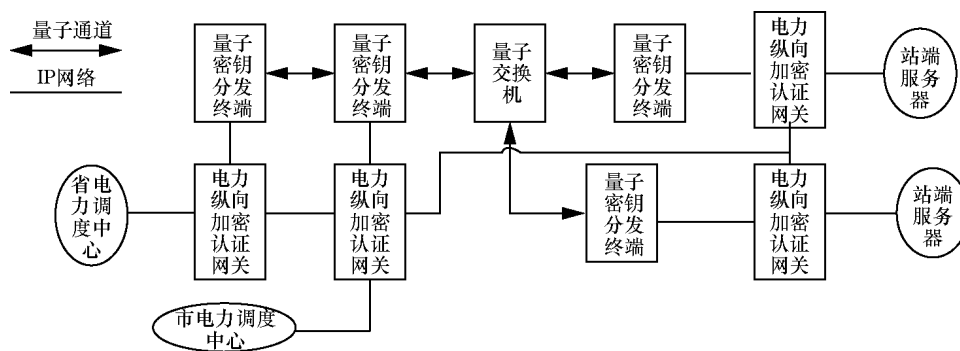


图3 基于量子密钥分发的智能变电站监控系统结构

子密钥分发技术的作用下实现与各个变电站站端进行相互安全通信。其通信流程如下。

4.2.1 量子密钥加密流程

市调与各个变电站站端量子密钥分发共享是在上层控制服务器统一的协调下进行的。

(1) 信息协商

市调和站端根据所需传送数据的安全等级，协商加密算法、量子密钥的使用形式以及密钥的更新频率。

(2) 量子密钥的请求与分发

电力纵向加密认证网关向量子密钥服务器发送请求传送密钥数据的信息。量子密钥服务器根据信息协商的结果，接受请求，同时确认发送量子密钥的更新时间，并按照协商更新时间的要求对密钥进行更新。

量子密钥服务器根据量子密钥的需求量启动量子密钥的分发，当量子密钥需求量大于量子密钥服务器中的密钥存储量时，启动量子密钥的分发。量子密钥的分发是通过量子信道进行传送的，因此可以实现绝对的通信安全。

(3) 获取量子密钥和密钥更新

量子密钥服务器向电力纵向加密认证网关发送密钥数据。同时根据协商信息，定期用量子密钥更换制定的量子密钥。

(4) 数据安全传输

在完成量子密钥的安全替换之后，直接使用替换的密钥进行数据加密，完成了量子密钥的分

发和使用。

4.2.2 站端向调度中心加密流程

站端向市调传送数据，其首先需要电力纵向加密装置与市调共享量子密钥，对通信的数据进行加密处理，然后通过IP网络发送给市调。市调接收到站端传输来的加密数据之后，利用共享的量子密钥进行数据的解密，这样站端到市调的数据传输就完成了。

4.2.3 市调向站端加密流程

当市调向站端发送动作指令时，同样用电力纵向加密认证网关与市调共享量子密钥进行数据加密，然后在站端用量子密钥对动作指令进行解密，完成市调向站端的数据传输和指令的传达过程。

如果相关数据需要向省级电力调度中心（以下简称“省调”）传输，需要在省调增设电力纵向认证网关，实现省调与市调的量子密钥共享。如果传输距离较远，可在中间增加中继站，实现量子密钥中继的收发。

4.3 实际应用分析

为了评估该系统的性能，对作为量子信道的不同光纤线路进行损耗量和量子密钥成码率测试，同时在市调和距市调17 km的站端对不同加密算法对系统的数据传输性能的影响和系统稳定性进行了测试。

4.3.1 线路损耗和成码率

针对4种不同距离的裸纤进行本测试，并记

录其稳定成码后 0.5 h 的曲线, 如图 4 所示。

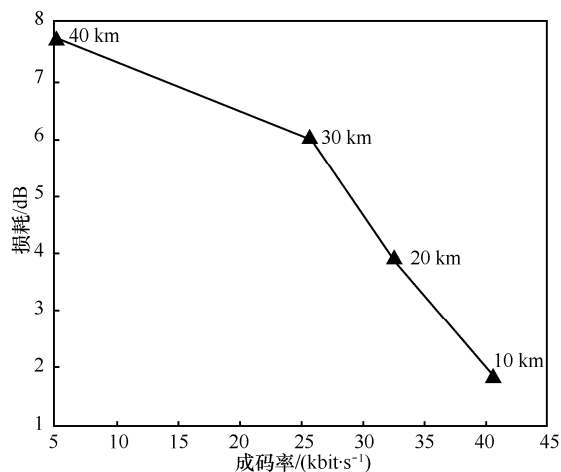


图 4 距离损耗测试

由图 4 可知, 随着光纤距离的增长其成码率逐渐降低, 损耗逐渐增大。40 km 以后成码率极低。根据量子保密通信系统正常运行需满足: 量子信道衰减 < 13 dB, 量子密钥平均成码率 > 2 kbit/s 的条件, 本系统从市调到站端的距离 17 km 左右, 能满足量子密钥分发的传输需求。

4.3.2 数据传输性能

该系统对数据传输性能的影响, 是通过采用网络性能测试仪测试电力纵向加密认证网关的不同加密算法对数据加密传输时系统的传输性能参数而评定的。采用的加密算法有 SM4、AES128、AES192、AES256, 分别和量子密钥组成加密方式, 其结果如图 5 所示。

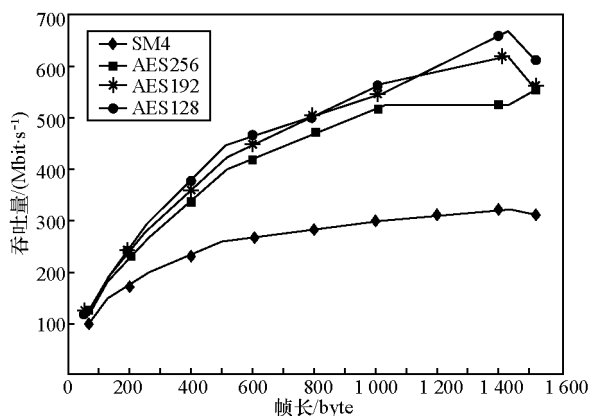


图 5 不同加密算法下系统性能测试结果

在 4 种加密算法中, AES 算法明显优于 SM4 算法; 而 AES 算法采用的 3 种密钥长度, 数据帧长的增加与算法吞吐量、系统的传输性能呈正相关。AES256 在帧长为 1 518 byte 吞吐量达到最大, AES128 和 AES192 在帧长 1 428 byte 吞吐量达到最大。总体上, 不同密钥长度的 AES 加密的量子密钥系统, 其系统传输性能具有很好的稳定性, 完全可以满足在电力系统内数据保密性要求相对较低的辅助监控系统中应用。但是考虑到电网调度数据等高保密性要求和国密算法 SM4 的传输性能, 电网调度数据传输应用需要进一步研究论证。

4.3.3 系统稳定性

系统稳定性测试是在系统实际运行的环境下, 对系统的量子密钥成码率进行了 10 天的跟踪记录, 其结果如图 6 所示。

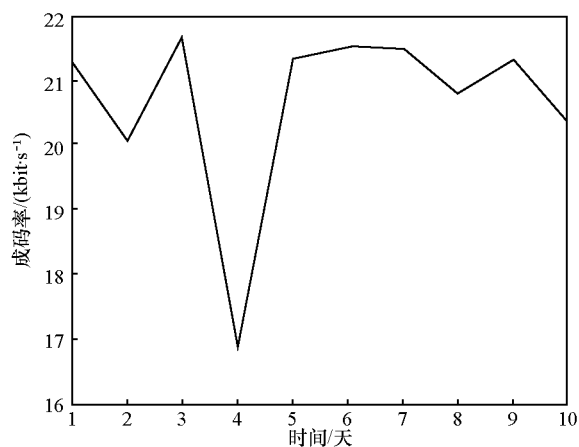


图 6 10 天稳定性测试

该系统的量子密钥成码率基本维持在 21 kbit/s 左右, 第 4 天成码率为 16.9 kbit/s (> 2 kbit/s), 存在着大的波动, 其原因是 3 级左右的风引起成码率降低。在 10 天的实际应用中, 系统可以长期满足量子密钥成码的要求, 运行流畅, 网管数据上报正常, 能够确保基于量子密钥分发的智能变电站监控系统可长时间稳定运行。

4.3.4 应用前景

基于量子密钥分发的智能变电站监控系统的初步应用和测试, 该系统在数据传输性能、系统



稳定性等方面已满足目前监控系统的使用要求。

电力系统专用光纤。量子信道对光纤的要求较高,而电力系统专网可以加快量子保密通信技术在电网内部的推广。

组网结构简单。在目前的网络架构中,省调和市调之间骨干传输层中的电力纵向加密认证网关并行增加用量子信道连接的量子密钥分发终端,在与站端的量子密钥分发传输中,增设与电力纵向加密认证网关并行的使用量子信道通信的量子密钥分发终端,即可完成网络架构的组建。

对于当前存在的线路衰减问题,在实际应用中,可以综合考虑衰减情况和传输距离,增设量子中继点;对于该系统中 AES 算法优于 SM4 加密算法的影响需要在该系统的软硬件协同方面提高对国密算法的支持,以尽快推进基于量子密钥分发技术的保密通信在电力系统中的深层次应用。

5 结束语

针对量子保密通信技术在电力系统内部推广应用的问题,本文对量子密钥分发技术在智能变电站监控系统中组网方案 and 实际应用的效果进行了分析和验证。组网方案采用电力系统独有的网络资源和“量子密钥+电力纵向加密认证网关”的设计思路,在传统变电站监控系统结构的基础上,加入了量子密钥分发系统,扩展了电力纵向加密认证网关接口,实现监控数据的加密传输。

通过对线路损耗、数据传输性能、稳定性 3 方面的测试分析,可知:在对数据安全传输要求相对较低的监控系统,该技术方案可以满足短距离数据传输的要求,具有规模化推广价值。而对于电网调度、容灾备份等保密要求高的业务数据,除在长距离传输需要增设量子中继外,还需对加密算法与量子保密通信系统的软硬件协同性和恶劣气候条件下的应对措施做进一步研究。

参考文献:

- [1] 朱卫民, 吕洪君, 解光军. 3 种光纤在 BB84 协议模型中的兼容性问题[J]. 合肥工业大学学报(自然科学版), 2016, 39(1): 90-93.
ZHU W M, LV H J, JIE G J. Compatibility problem of three kinds of optical fiber in BB84 protocol model[J]. Journal of Hefei University of Technology(Natural Science), 2016, 39(1): 90-93.
- [2] 李剑, 陈彦桦, 潘泽世, 等. 量子 BB84 协议在联合旋转噪声信道上的安全性分析[J]. 物理学报, 2016, 65(3): 25-31.
LI J, CHEN Y H, PAN Z S, et al. Security analysis of BB84 protocol in the collective-rotation noise channel[J]. Acta Physica Sinica, 2016, 65(3): 25-31.
- [3] WANG S H, CHEN W, GUO J F, et al. 2 GHz clock quantum key distribution over 260 km of standard telecom fiber[J]. Optics Letters, 2012, 37(6): 1008-1010.
- [4] 岳孝林, 王金东, 魏正军, 等. 一种新的单光源多波长双向量子密钥分发系统[J]. 物理学报, 2012, 61(18): 1-7.
YUE X L, WANG J D, WEI Z J, et al. A new multi-wavelength two-way quantum key distribution system with a single optical source[J]. Acta Physica Sinica, 2012, 61(18): 1-7.
- [5] WANG S H, CHEN W, YIN Z Q, et al. Field test of wavelength-saving quantum key distribution network[J]. Optics letters, 2010, 35(14): 2454-2456.
- [6] 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.
- [7] 吴佳楠, 魏荣凯, 韩家伟, 等. 传输距离对实际量子密钥分发系统的影响[J]. 吉林大学学报(理学版), 2014, 52(5): 1014-1017.
WU J N, WEI R K, HAN J W, et al. Influence of actual transmission distance on quantum key distribution system[J]. Journal of Jilin University(Science Edition), 2014, 52(5): 1014-1017.
- [8] 许方星, 陈巍, 王双, 等. 多层级量子密码城域网[J]. 科学通报, 2009, 54(16): 2277-2283.
XU F X, CHEN W, WANG S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network[J]. Chinese Science Bulletin, 2009, 54(16): 2277-2283.
- [9] 杨奇逊, 孟建平. 变电站综合自动化系统的体系结构[J]. 电网技术, 1996(6): 63-65.
YANG Q S, MENG J P. Systematic structure of substation composite automation[J]. Power System Technology, 1996(6): 63-65.
- [10] 周国亮, 吕凛杰, 王桂兰. 电力大数据全景实时分析关键技术[J]. 电信科学, 2016, 32(4): 159-168.
ZHOU G L, LV L J, WANG G L. Key technology of power big data for global real-time analysis [J]. Telecommunications Science, 2016, 32(4): 159-168.

- [11] 姜红红, 张涛, 赵新建, 等. 基于大数据的电力信息网络流量异常检测机制[J]. 电信科学, 2017, 33(3): 134-141.
JIANG H H, ZHANG T, ZHAO X J, et al. A big data based flow anomaly detection mechanism of electric power information network[J]. Telecommunications Science, 2017, 33(3): 134-141.
- [12] 杨光, 聂敏, 杨武军. SIP 协议量子身份认证与密钥协商方案[J]. 四川大学学报(自然科学版), 2016, 53(1): 87-92.
YANG G, NIE M, YANG W J. Quantum authentication and key agreement scheme for SIP protocol[J]. Journal of Sichuan University(Natural Science Edition), 2016, 53(1): 87-92.
- [13] 刘东, 王双, 周静, 等. 量子密钥在电网 SSLVPN 中的应用[J]. 电网技术, 2014, 38(2): 544-548.
LIU D, WANG S, ZHOU J, et al. Application of quantum keys in SSL VPN of power grid[J]. Power System Technology, 2014, 38(2): 544-548.
- [14] 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.
- [15] 沐连顺, 崔立忠, 安宁. 电力系统云计算中心的研究与实践[J]. 电网技术, 2011, 35(6): 171-175.
MU L S, CUI L Z, AN N. Research and practice of cloud computing center for power system[J]. Power System Technology, 2011, 35(6): 171-175.

[作者简介]



杨晓朋(1977-), 男, 河南电力实业集团有限公司高级工程师, 主要研究方向为光纤通信、专网通信、信息技术。



陈海涛(1968-), 男, 国网河南省电力公司信阳供电公司高级工程师, 主要研究方向为变电站辅助设施的智能化控制及高级应用。



梅力宸(1989-), 男, 阿里云计算有限公司工程师, 主要研究方向为智慧城市、数字交通。

王鹏展(1985-), 男, 济南恒道信息技术有限公司郑州分公司工程师, 主要研究方向为光纤通信、量子通信。