

一种新的智能变电站通信业务安全隔离技术的研究

汪强¹, 徐小兰², 张剑¹

(1. 许继昌南通信设备有限公司, 河南 许昌 461000; 2. 许继电气股份有限公司, 河南 许昌 461000)

摘要: 为了保障智能变电站通信网络的可靠性和安全性, 必须对网络中的通信业务流进行安全隔离传输。分析了智能变电站通信业务流的特点, 简述了目前常用的网络隔离技术, 着重剖析了目前智能变电站通信网络采用的业务隔离技术的应用情况和特点, 指出智能变电站通信业务流对安全隔离的迫切需求。研究了全光交换技术的分类和主流技术的主要特性指标, 探索性地提出基于全光波长和全光标签混合交换技术的电力业务安全隔离方案, 并详细介绍了方案的技术原理和实现措施。通过引入业务隔离评估模型, 以实验方式论证了该方案的可行性。

关键词: 通信网络; 安全; 光波长交换技术; 光标签交换技术; 业务隔离

A new method of smart substation communication service security isolation technology

WANG Qiang¹, XU Xiaolan², ZHANG Jian¹

(1. XJ Changnan Communication Equipment Co., Ltd., Xuchang 461000, China;

2. XJ Electric Co., Ltd., Xuchang 461000, China)

Abstract: In order to guarantee the reliability and security of the communication network of smart substation, it must carry out the safety isolation transmission of communication business network flow. This paper analyzes the features of smart substation communication business flow, expounds the present commonly used network isolation technology, emphatically analyzes the application and characteristics of business separation technology of smart substation communication network, and points out urgent demand of communication service flow for the safe isolation. The main characteristic index and the classification of the mainstream technology of all optical switching technology are studied, the power business safety isolation scheme based on all-optical wavelength and optical label mixed switching technology is explored, and the implementation of measures and the technical principle of the program are introduced in detail. Through the introduction of business segregation evaluation model, the feasibility of the scheme is proved by way of experiment.

This work is supported by Science and Technology Project of State Grid Corporation of China.

Key words: communication network; security; optical wavelength switch; optical label switch; service isolation

中图分类号: TM73 文献标识码: A 文章编号: 1674-3415(2015)17-0139-06

0 引言

智能变电站遵循 IEC 61850 标准, 采用网络通信技术承载站内的保护、控制等关键业务报文^[1-3]。通信网络成为全站数据交汇的枢纽, 是保护、控制等功能赖以实现的基础。国网公司新一代智能变电站的建设, 提出了构建站内一体化高速通信网络, 实现站内信息的高度共享。因此, 关注变电站通信网络的业务传输的安全性十分必要。

基金项目: 国家电网公司科技项目(全光交换关键技术及电网应用研究)

传统变电站的关键业务通过专用电缆直接传送, 随着智能变电站以及新一代智能变电站的建设, 原有业务传送模式已不能满足信息共享和互操作的需要, 特别是信息处理就地化、保护功能的“网采网跳”、“三层一网”和“共网共口”等的需求^[4-6], 使得站内信息交互更频繁, 对信息的安全传输的需求也更加急迫。关于智能变电站的信息安全传输问题有许多文献提及^[7-10], 但是, 这些文献主要从信息本身的加密算法、安全策略, 网络的安全性, 网络流量管理等方面来论述, 而从信息隔离的角度来论述变电站业务安全传输的未见有报道。

本文详细分析了智能变电站通信业务的特点,

针对业务的安全传输需求,提出了基于光波长和光标签混合交换技术的电力业务安全隔离方案。

1 智能变电站通信业务分析

智能变电站的通信业务主要有 SV、GOOSE、MMS 和时钟同步等几种报文。

SV 报文用在过程层的合并单元与间隔层的保护控制设备间传输智能一次设备的现场运行数据,是保护、控制装置正常运行的数据源。为保障 SV 报文实时、可靠传输,智能变电站的保护装置采用直接采样的方式。SV 报文的数据流量大(合并单元每个出口的流量大约在 5 Mbps 左右),但是报文长度固定。

GOOSE 报文主要用于承载间隔层之间的联闭锁报文、失灵启动信号等和过程层与间隔层之间的位置信息、控制信息以及状态信息等。GOOSE 报文的实时性要求高。国家电网公司要求跳闸类 GOOSE 应在 7 ms 内,保护互锁类 GOOSE 小于 20 ms,实际应用中这两类 GOOSE 都小于 3 ms。为保障跳闸 GOOSE 报文的实时性和可靠性,保护装置一般都采用独立光纤通道的直接跳闸方式。GOOSE 报文通常情况下数据流量比较小,在几百 Kbps 量级;在故障情况下,GOOSE 报文流量会突变增大,占用较多的网络资源。

MMS 报文主要分布在站控层设备间和站控层与间隔层设备间,用于监控站内通信网,并为实现不同制造商的设备互操作提供基础,为把站内信息上送调度中心提供通道。

时钟同步报文为全站提供统一的时钟基准,目前变电站提供 IEC 61588 或 B 码同步对时信号。时钟同步报文数据流量小,为几 Kbps 量级,占用网络资源也少。但是,对其同步精度要求很高,特别是 SV 报文,要求同步误差不大于 $\pm 1 \mu\text{s}$,在外部同步信号消失后,至少能在 10 min 内持续保持 $4 \mu\text{s}$ 同步精度要求。

可以看出,智能变电站通信网络中包含有保障变电站安全、可靠运行的关键报文,如采样值报文、跳/合闸报文、闭锁报文、时钟同步报文等,一旦被外界攻击,轻则使变电站工作异常,重则导致全站瘫痪甚至出现重大事故,造成不必要的经济损失和恶劣的社会影响。因此,智能变电站通信网络的安全隔离问题不容忽视。

2 现有业务隔离技术研究

2.1 网络隔离技术概述

网络隔离机制按照信息通信网络建设的原则

可分为:物理隔离和逻辑隔离(虚拟隔离)两类。

依据隔离的严格程度,物理隔离又可分为物理媒介隔离和物理信道隔离。

物理媒介隔离:对网络中物理传输媒介上以电、光或磁等形式存在的信号进行隔离。其是最严格的隔离方式。

物理信道隔离:是对不同信道之间传输的信息进行隔离,是基于物理层信道的隔离技术。

逻辑隔离:是指基于数据链路层及以上层次所采用的隔离技术,常见的有:虚拟局域网(Virtual Local Area Network, VLAN)和虚拟专用网络(Virtual Private Network, VPN)等技术。

VLAN 是二层隔离技术,其原理是将局域网中的设备逻辑地划分为多个网段(或子网、VLAN),每个 VLAN 内的设备可以互访,不同 VLAN 间的设备不能互访,从而实现了不同业务的隔离。

VPN 是三层隔离技术,是在三层通信设备上为每种数据建立专用的虚拟路由转发(Virtual Route Forwarding, VRF)表,并配有特殊的标记,采用专用的隧道进行传输。通过特殊的标记,VPN 数据在 VRF 和专用隧道中相互隔离。

2.2 智能变电站现有业务隔离技术分析

目前智能变电站在组网中采用以下业务隔离机制:

(1) 物理媒介隔离。智能变电站的保护装置采用的“直采直跳”方式,是基于光纤的物理媒介隔离。保护装置的采样数据、跳/合闸信息等分别单独通过光纤传输,能够严格保证数据的安全性、实时性以及可靠性。但是,这种方式需要敷设大量光缆,同时过程层和间隔层的设备也需要增加大量光接口,从而造成建网成本增加、网络运维繁琐以及设备可靠性下降等问题。

(2) VLAN 逻辑隔离。在智能变电站中 SV 和 GOOSE 共网传输时,利用 VLAN 技术使 SV 和 GOOSE 在不同功能子网传输,不仅保证了 SV 和 GOOSE 的安全隔离,而且可以启用交换机的 QoS 优先服务机制,保证业务报文的实时性。此外,在各网内部,如 GOOSE 网络,也需要采用 VLAN 将本间隔设备的业务信息与母线间隔设备和其他间隔设备的业务信息进行隔离。一方面保证安全性;另一方面将广播报文限制在 VLAN 内,避免不必要的端口占用和网络资源浪费。采用 VLAN 逻辑隔离,能够充分利用网络资源,简化网络结构,降低网络成本,但是,VLAN 属于逻辑隔离,易受网络攻击,达不到物理隔离的安全性要求。

如上分析,现有智能变电站的业务隔离技术存

在缺陷, 为保障全站安全可靠地运行, 亟需研究适合站内业务流安全需求的隔离技术。

3 全光交换技术

全光交换技术是不经过任何光/电转换, 在光域上直接将输入光信号交换到不同的输出端, 具有实时、可靠、安全等特点。全光交换技术可分为全光线路交换(OCS)和全光分组交换两种类型。全光线路交换技术根据技术原理, 可分为光空分交换技术、光时分交换技术、光波分/频谱交换技术和复合型交换技术。全光分组交换技术可分为: 光分组交换技术(Optical Packet Switch, OPS)、光突发交换技术(Optical Burst Switch, OBS)、光标记分组交换技术(Optical Label Switch, OLS)、光时隙交换技术(Optical Slot Switch, OSS)等。表1列举了几种全光交换技术的主要性能指标。

表1 光交换技术的主要性能指标

Table 1 Main performance of optical switch technology

序号	项目	OCS	OPS	OBS	OLS	OSS
1	交换粒度	波长/ 波带/ 光纤	光分组	突发包	光分组	光时隙
2	交换方式	直通	存储/ 转发	直通	存储/ 转发	直通
3	控制方式	带外	带内	带外	带内	带外
4	信息长度	可变	定长	可变	定长	定长
5	链接时延	高	低	低	低	低
6	链接信道	有	无	有	无	有
7	带宽利用率	低	高	较高	高	较高
8	灵活性	低	高	较高	高	较高
9	光缓存/ 光逻辑	无	有	无	无	无
10	开销	低	高	低	低	低

从表1可以看出: 全光线路交换虽然技术成熟, 但是采用端到端的刚性管道, 不具备带宽统计复用能力, 极大地增加了网络建设成本以及设备复杂度。全光分组交换技术适合承载各种类型业务, 但是, 目前全光缓存和全光逻辑技术并不成熟, 限制了其应用。全光突发交换采用数据通道和控制通道分离的方式, 使数据在发送端汇聚然后直接传输, 虽然不需要使用全光逻辑和全光缓存, 但资源冲突问题难以解决, 无法保障业务传输质量。全光时隙交换可以看成是全光突发交换的改进, 增加了时隙同步和集中式带宽资源调度, 有效解决了资源冲突问题,

但是需要全网同步, 依赖于外部时钟, 不利于业务的实时传输。全光标签交换技术对分组包头采用电处理方式, 不需要全光逻辑技术; 对于缓存, 可使用可调谐光纤延迟线与少量电缓存相结合的措施, 并采取适当的资源调度算法, 能够较好地解决存储问题。

综上所述, 每一种光交换技术都有各自的优势和应用场景, 单一的一种技术不太适合智能变电站多业务传输的需求, 结合智能变电站业务特征和组网需求, 本文提出采用全光波长和全光标签混合交换技术来进行智能变电站的通信网络建设。该方案既有全光波长交换技术的灵活波长/业务映射机制, 又具有光标签交换技术的高效资源利用, 突破了光缓存/逻辑技术的束缚, 而且属于物理隔离, 是理想的业务安全隔离措施。

4 基于混合光交换技术的业务隔离方案

基于光波长和光标签混合交换技术的智能变电站通信业务隔离方法, 根据智能变电站通信业务类别、实时性、可靠性以及安全性等需求, 对于不同类型的业务使用光波长交换进行波长级的调度控制, 对同一波长承载的业务进行分组交换调度策略, 解决了单一全光交换机制存在的不足, 提升了全光交换网络性能, 满足智能变电站应用环境需求。

基于光波长和光标签混合交换技术的业务隔离方案基本原理如图1所示。在智能变电站业务进入全光交换网络前, 根据数据业务的特性和具体的需求先在业务端口对相应的数据业务进行基于波长的业务映射, 也就是说将不同的业务承载到不同的光波长上, 如SV报文映射到波长 λ_1 、GOOSE报文映射到波长 λ_2 、MMS报文映射到波长 λ_3 、时间同步报文通过 λ_4 传输。然后将映射好的数据业务送入光标签分组交换网络进行业务的分组传送。

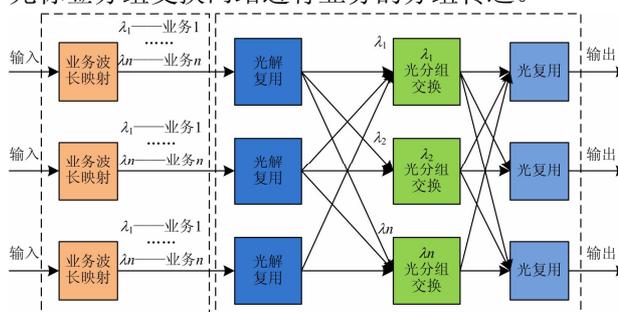


图1 新型业务隔离技术原理图

Fig. 1 Schematic diagram of new service isolation technology

基于光波长和光标签分组混合交换技术的业务隔离方法属于物理层隔离技术, 其光交换技术实

现方案如图 2 所示。该技术方案由输入部分、交换处理部分和输出部分三块组成，输入部分主要由解复用器构成，解复用器的主要作用是将波分复用 (Wavelength division multiplexing, WDM) 光纤上承载的业务按照不同的波长分解开来，并送入交换处理部分；交换处理部分主要由光交换矩阵构成，实现不同波长的交换；输出部分主要由复用器构成，复用器的主要作用与解复用器相反，对不同波长承

载的业务进行波分复用，并送入 WDM 光纤进行远程传送。本方案的具体实现过程为：进入全光交换功能模块的业务采用基于波长的分配策略，不同的波长承载不同类型的业务，进入全光交换功能模块后，首先由解复用器将波长分开，承载不同业务的波长分别进入相对应的交换单元，从交换单元出来后由复用器加载到光纤上。整个过程中，光路保持独立，做到对业务的物理隔离。

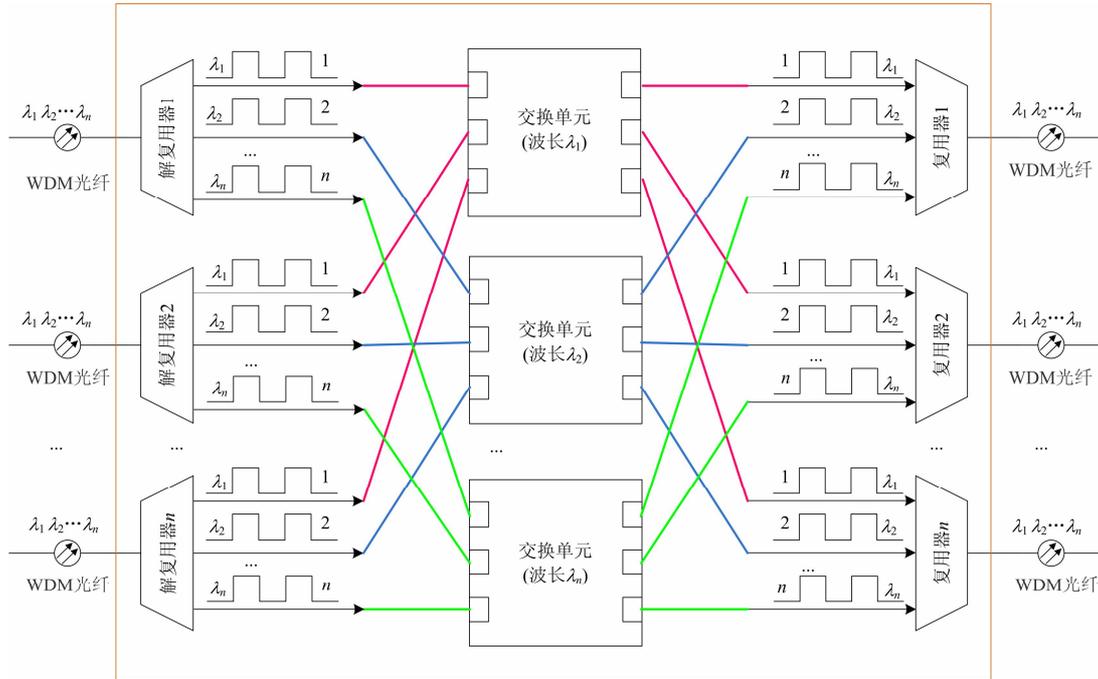


图 2 新型业务隔离技术实现方案

Fig. 2 Implementation scheme of new service isolation technology

5 实验验证

5.1 业务隔离评估方法

业务的隔离是保障业务传送的可靠性和安全性，其目的是防止来自业务传输通道外的恶意攻击和业务传输通道对外的信息泄露。为了评估业务的隔离效果，文章借鉴了文献[11-12]的研究成果，利用信息论中的互信息理论来描述。互信息 $I(X,Y)$ 是指通道 A 中的信息 X 对通道 B 中的信息 Y 的统计约束程度，也即在收到的信息 X 中获得了信息 Y 的信息量。

互信息 $I(X,Y)=H(X)+H(Y)-H(X,Y)$ ，其中 $H(X)$ 是 X 事件指标的变化频率熵， $H(Y)$ 是 Y 事件指标的信息熵， $H(X,Y)$ 是 X 和 Y 的联合信息熵。

$$H(X)=-\sum P(X)\log P(X)$$

$$H(X, Y)=-\sum P(X, Y)\log P(X, Y)$$

定义当 $I(X,Y)=0$ ，通道隔离度为 1；当 $I(X,Y)=1$ ，

通道隔离度为 0。针对通道 A、通道 B，如果二者是纯物理隔离，那么通道 A 中的信息 X 在任何传输速率的情况下都不会对通道 B 中的信息 Y 造成影响，也就是 $I(X,Y)=0$ ，即 X 与 Y 统计约束程度为 0，此时通道 A、B 中的业务隔离度为 1；如果通道 A、B 不完全隔离， $I(X,Y)$ 不等于 0，随着信息 X 与信息 Y 的相关性越大， $I(X,Y)$ 的值也越大，其通道业务隔离度越小。

5.2 实验部署与分析

运用数字仿真系统对典型的 110 kV 电压等级的智能变电站进行实验模拟。变电站配置 3 台 3 绕组变压器，110 kV 采用双母线接线方式，6 回出线，3 回主变进线，1 个母联；35 kV 侧 3 分段，9 回出线；10 kV 侧 3 分段，32 回出线，6 组电容。

二次系统网络采用星型单网架构，实现三层共网组网方式，即 MMS、GOOSE、SV 信息通过同一网络组网传输，间隔层保护、测控装置、MMS、

GOOSE、SV 信息采用共口处理方式, 全部设备采用 IEC 61588 同步对时方式。全站共设置 1 台主干

网交换机, 用于级联各间隔交换机, 同时接入对时、站域保护和故障录波装置, 具体网络结构如图 3 所示。

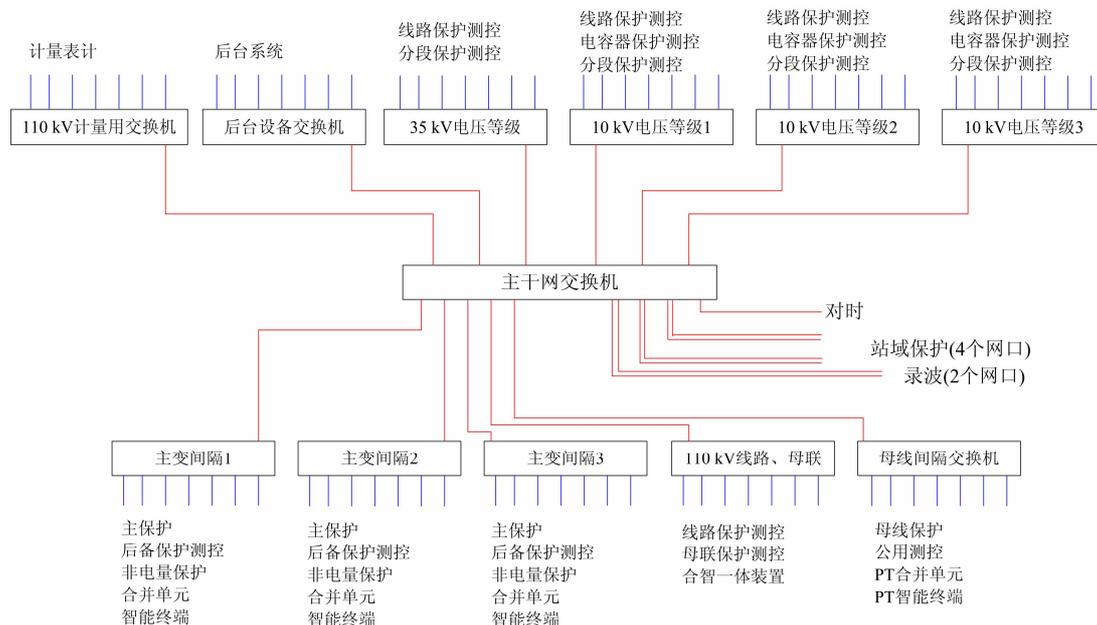


图 3 通信网络结构图

Fig. 3 Structure diagram of communication network

实验中采用智能变电站专用的工业以太网交换机和基于光波长和光标签混合技术的全光交换机进行对比测试, 验证两种交换机在业务隔离方面的效果。由于在没有故障和网络攻击的情况下, 网络性能中的误码率、抖动以及丢包率都可以忽略不计, 在计算业务隔离度的时候, 主要考虑业务传输的延时和吞吐量所造成的业务互信息值。对业务传输通道施加背景流量来模拟干扰信息源。通过模拟母线保护 GOOSE 报文网络跳闸情况, 来测试业务传输的隔离度。

通过对交换机施加 10 Mbps、30 Mbps、50 Mbps、70 Mbps 和 100 Mbps 的背景流量来测试验证。在施加 100 Mbps 的背景报文时, 工业以太网交换机出现了数据丢包现象, 如图 4 所示。全光交换机在任何情况下都能达到 100% 的吞吐量。工业以太网交换机的时延测试结果如图 5 所示, 全光交换机的时延测试结果如图 6 所示。

通过对实验结果的分析 and 计算, 可以得到如图 7 所示的隔离度测试结果。结果表明基于光波长和光标签混合交换技术的全光交换机的业务隔离度能够达到物理隔离的效果, 与前面的理论分析结果相符; 而工业以太网交换机的隔离度约为 0.8, 由于工业以太网交换机采用 VLAN 实现业务的隔离, 属于

逻辑隔离方式, 不能实现业务的精确区分。

[环网到远端]吞吐量测试结果 (BPS)				
帧大小	最大速率	实际速率	丢帧数	接收的利用率
68	99999680	99999976	0	99.99%
132	99999976	99999976	0	100.00%
260	99998080	99998080	0	100.00%
516	99996160	99996160	0	100.00%
1028	99995968	99995968	0	100.00%
1284	99990720	99990720	0	99.99%
1522	99995616	99995616	0	100.00%
[远端到本地]吞吐量测试结果 (BPS)				
帧大小	最大速率	实际速率	丢帧数	接收的利用率
68	99999680	99999976	0	99.99%
132	99999976	99999976	0	100.00%
260	99998080	99998080	0	100.00%
516	99996160	99996160	0	100.00%
1028	99995968	99995968	0	100.00%
1284	99990720	99990720	0	99.99%
1522	99995616	99995616	0	100.00%

图 4 工业以太网交换机吞吐量测试结果

Fig. 4 Test result of industrial ethernet switch throughput

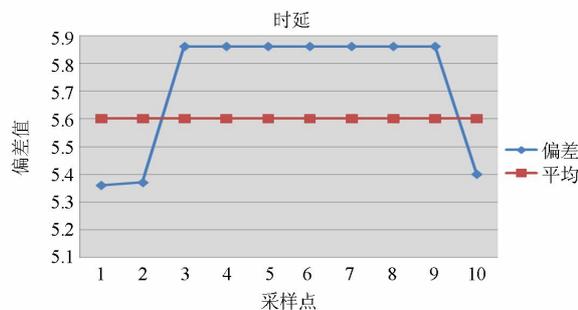


图 5 工业以太网交换机时延测试结果

Fig. 5 Test result of industrial ethernet switch delay

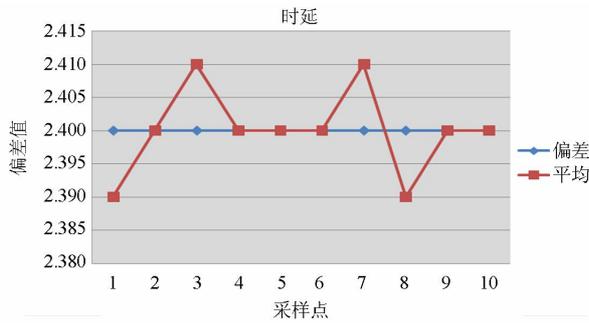


图 6 全光交换机时延测试结果

Fig. 6 Test result of all optical switch delay

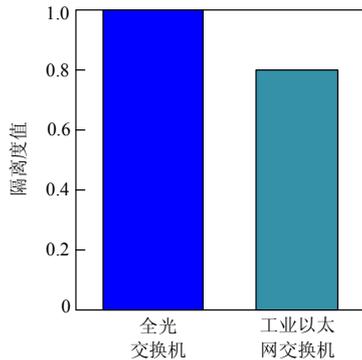


图 7 隔离度测试结果

Fig. 7 Test result of isolation degree

6 结语

本文尝试从业务隔离的角度，提出保障智能变电站业务安全、可靠传输的基于光波长/光标签混合的全光业务隔离方法。该方案能够对传输的业务实现物理隔离，同时兼具光波长灵活的业务映射功能和光标签分组传输的高效性以及快速性，是适合智能变电站和新一代智能变电站发展需求的理想安全隔离措施，能够保障全站业务可靠传输。并通过仿真实验测试，表明该方案切实可行，并能达到与理论研究一样的业务隔离效果。基于光波长和光标签混合的全光交换技术是一项全新的技术，为智能变电站信息通信以及业务的安全隔离探索了一种新思路。本文的研究工作对今后的智能变电站以及新一代智能变电站的建设具有重要参考价值。

参考文献

[1] Q/GDW 383-2009 智能变电站技术导则[S]. 2009.
 [2] IEC 61850 communication networks and systems in substations[S]. 2004.
 [3] 汪强, 徐小兰, 葛光胜. 智能变电站专用通信设备的关键技术[J]. 电力系统保护与控制, 2014, 42(7): 150-153.
 WANG Qiang, XU Xiaolan, GE Guangsheng. Key technologies of special communication device in smart substation[J]. Power System Protection and Control, 2014, 42(7): 150-153.
 [4] 宋漩坤, 李敬如, 肖智宏, 等. 新一代智能变电站整体

设计方案[J]. 电力建设, 2012, 33(11): 1-6.
 SONG Xuankun, LI Jingru, XIAO Zhihong, et al. Overall design scheme for new generation intelligent substation [J]. Electric Power Construction, 2012, 33(11): 1-6.
 [5] 李宝伟, 文明浩, 李宝潭, 等. 新一代智能变电站 SV 直采和 GOOSE 共口传输方案研究[J]. 电力系统保护与控制, 2014, 42(1): 96-101.
 LI Baowei, WEN Minghao, LI Baotan, et al. Research of the scheme for SV direct sampling and GOOSE transmit in the same port in new generation smart substation[J]. Power System Protection and Control, 2014, 42(1): 96-101.
 [6] 幸培哲, 闫培丽, 肖智宏. 新一代智能变电站通信网络技术应用研究[J]. 电力建设, 2013, 34(7): 17-23.
 [7] 曹进明, 房鑫炎, 吴蓉. 基于 IEC61850 标准的变电站高可靠性通信研究[J]. 电力自动化设备, 2008, 28(9): 89-93.
 CAO Jinming, FANG Xinyan, WU Rong. Reliable substation communication based on IEC61850[J]. Electric Power Automation Equipment, 2008, 28(9): 89-93.
 [8] 苗新, 张恺, 田世明, 等. 支撑智能电网的信息通信体系[J]. 电网技术, 2009, 33(17): 8-13.
 MIAO Xin, ZHANG Kai, TIAN Shiming, et al. Information communication system supporting smart grid[J]. Power System Technology, 2009, 33(17): 8-13.
 [9] 潘超. 电网监控系统与信息系統网络融合隔离的研究[J]. 现代电力, 2002, 19(3): 66-70.
 PAN Chao. Research on network isolation between electric network monitoring system and information system[J]. Modern Electric Power, 2002, 19(3): 66-70.
 [10] 刘明慧, 赵晓东. 智能变电站过程层网络流量管理方式研究与应用[J]. 电力系统保护与控制, 2012, 40(23): 87-92.
 LIU Minghui, ZHAO Xiaodong. Research and application of process level network flow management in smart substation[J]. Power System Protection and Control, 2012, 40(23): 87-92.
 [11] 傅祖芸. 信息理论基础理论与应用[M]. 北京: 电子工业出版社, 2009.
 [12] 薛金, 余江, 常俊. 基于 PTN 技术的配电通信网隔离度评估研究[J]. 电力系统保护与控制, 2013, 41(16): 60-64.
 XUE Jin, YU Jiang, CHANG Jun. Research on isolation degree for distribution communication network based on PTN technology[J]. Power System Protection and Control, 2013, 41(16): 60-64.

收稿日期: 2015-01-12; 修回日期: 2015-03-26

作者简介:

汪强(1978-), 男, 高级工程师, 主要从事电力通信技术研究; E-mail: scbzyanglong813@163.com

徐小兰(1984-), 女, 工程师, 主要从事电力中低压保护方面的技术支持工作;

张剑(1977-), 男, 高级工程师, 主要从事电力通信技术支持工作。

(编辑 魏小丽)