



面向智能化变电站的光网络信令安全优化

赵宇皓¹, 郝晓光¹, 耿少博², 罗蓬¹, 周坤³, 甄家林³, 毛玉荣³

(1. 国网河北省电力有限公司电力科学研究院, 河北 石家庄 050021;

2. 国网河北省电力有限公司, 河北 石家庄 050021;

3. 武汉凯默电气有限公司, 湖北 武汉 430023)

摘要: 智能化变电站建设的稳步推进对变电站内光通信网络的安全性要求日益提高。为了解决该问题, 首先对智能变电站环境下光网络所面临的通信安全挑战进行了分析, 提出了一种面向智能化变电站业务的光网络的信令安全优化技术。该技术充分利用电力光网络现有的信令协议进行扩展加强, 设计了一种轻量级的安全信令机制以建立面向电力业务的端到端可信连接。以智能化变电站通信业务作为典型应用场景, 对站内光网络的安全信令交互进行仿真验证。仿真结果表明, 本文所提出的机制有效提高了变电站通信业务与电力光网络交互的安全性, 并有力保证了电力通信业务的连接成功率。

关键词: 智能电网; 电力光网络; 安全信令; 可信连接

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019026

Security signaling optimization in optical network for smart substation

ZHAO Yuhao¹, HAO Xiaoguang¹, GENG Shaobo², LUO Peng¹, ZHOU Kun³, ZHEN Jialin³, MAO Yurong³

1. Electric Power Research Institute of State Grid Hebei Electric Power Co., Ltd., Shijiazhuang 050021, China

2. State Grid Hebei Province Electric Power Co., Ltd., Shijiazhuang 050021, China

3. Wuhan Kemov Electric Co., Ltd., Wuhan 430023, China

Abstract: The communication security issue brought by smart substation is of great importance and should not be ignored in backbone optical networks. To solve this problem, firstly, the communication security challenges faced by optical networks in smart substation environment were analyzed, a signaling security optimization technique for optical networks for smart substation services was proposed. A so-called light-weighted security signaling scheme was designed to establish the end-to-end trusted connection. Under the environment of multi-domain communication services in smart substation, evaluation simulation for the signaling interaction was conducted. Simulation results show that the proposed approach can greatly enhance the security ability of multi-domain optical network with better performance in term of connection success rate.

Key words: smart power grid, power optical network, security signaling, trusted connection

收稿日期: 2018-06-09; 修回日期: 2019-01-21

通信作者: 毛玉荣, maoyurong@kemov.com

基金项目: 国网河北省电力有限公司科技项目 (No.kj2017-016)

Foundation Item: State Grid Hebei Electric Power Co., Ltd. Science and Technology Project (No.kj2017-016)

1 引言

能源互联网的发展、能源与信息通信的深度融合,将引领以智能化变电站为核心的能源传输、能源转换和能源控制产生巨大的革新^[1-2]。面向智能变电站的电力光网络既要满足能源互联新业务对高带宽、高可靠性、长距离数据的传输要求,还要具备相应的网络安全能力。

随着能源互联网建设稳步推进,先进的信息通信技术发挥了重大作用。众多研究者提出了多种能源互联网信息通信新型架构。面向能源互联网的电力光网络架构主要分为数据转发平面、控制平面和应用平面^[3-7]。其中,控制平面和数据转发平面互相分离。控制信道与数据平面的数据传输信道相互独立,通过控制平面的信令协议交互,实现对数据传输业务连接的高效控制。

因此,光网络控制平面可信连接技术的重要性日益显现。可信连接是指在光传送网技术体制的基础上,建立具备节点可信度、带宽和优先级保障的端到端业务连接,提供高安全可信的网络服务,有效防范各类安全攻击。针对可信连接网络架构存在的安全缺陷,参考文献[8]提出了一种可信网络连接协议模型,并证明其具有一定的安全性。参考文献[9]提出了一种基于动态信任熵的路由算法,但是该路由安全算法仅考虑了路由的安全性,未充分考虑信令过程的安全性,难以满足电力业务对光网络的安全需求。此外,参考文献[9-10]中进一步提出了多种可信度量模型,参考文献[11]中对 master QUEST 信令网络监视系统进行了介绍,但对电力光网络可信连接的建立方法有待进一步的深入研究。

为此,本文提出了一种光网络的轻量级安全信令优化机制,充分利用光网络现有的信令协议进行扩展加强,设计了轻量级的安全信令交互流程,以实现面向智能变电站通信业务的光网络端

到端可信连接。

2 电力光网络的信令安全分析

电力光网络的信令协议用于智能化变电站通信业务连接的创建、拆除和修改等操作,通过信令机制实现电力光网络的业务连接控制与资源分配。在能源互联网多业务的复杂背景下,智能变电站中光网络信息安全问题具有一定的敏感性,信令消息的开放性使其更容易在涉及电力光网络的所有层面受到安全攻击^[12-13]。电力光网络与电信光网络最主要的特殊之处在于其对信令的安全性有着较高的要求。由于电力光网络中信令的传送要经过多个中间节点,信令协议的开放性在一定程度上增加了其受到网络攻击的安全风险,这些典型的安全威胁介绍如下。

(1) 窃听攻击

光网络的信令消息在控制平面中进行交互时,攻击者可能通过相关设施截获这些信号,分析消息的内容,作为发动安全攻击的第一步。

(2) 阻塞攻击

光网络中的非法节点发起大量的非法业务连接请求,加剧路由计算与信令交互的负担,导致业务连接的阻塞率居高不下。

(3) 消息篡改

将信令消息进行修改后再传给原定的接收者,从而破坏业务连接的正常建立,造成光连接的建立、拆除出现混乱。

(4) 重放攻击

将截获到的数据分组或协议消息反复传给消息的下游节点,破坏光连接的正常建立和维持。

(5) 业务量分析

通过通信量进行反演仍然有可能窃取信令消息的模式以及光网络节点的位置和标识,进一步导致正常的信令过程遭到攻击。

综上所述,电力光网络在信令消息的安全方面仍然存在隐患。随着光网络信令技术研究的不



断深入,光网络安全技术取得了长足的发展,对电力光网络信令安全技术的研究将为面向智能变电站的光网络提供重要的安全保证。

3 电力光网络的轻量级安全信令机制

为了解决上述的安全威胁问题,本文引入了改进的数字签名和消息反馈方法,同时运用 PKI (public key infrastructure, 公钥基础设施) 密钥策略,提出并设计了一种基于增强 RSVP-TE 的光网络信令安全的优化技术。

3.1 密钥策略

本文所提出的信令安全优化技术主要引入了 PKI 进行安全信令所需的密钥交互。该密钥策略主要分为 3 个部分: 密钥生成、密钥分发和密钥更新。

(1) 密钥生成

光网络中所有节点运用数字签名算法产生自己的公钥和私钥。

(2) 密钥分发

在信令协议运行前把各节点的公钥证书分发至各节点。

(3) 密钥更新

将周期更新和事件触发更新结合起来以达到密钥安全更新的目的。

3.2 增强 RSVP-TE 的安全信令流程

目前 ITU-T、IETF 等国际组织提出了多种光网络信令协议。其中,基于流量工程扩展的资源预留协议(RSVP-TE)因其特有的技术优势,在光网络中已经得到了普遍应用。鉴于目前已有众多厂商在其光网络技术方案中广泛采用 RSVP-TE 信令协议,其稳定性和成熟度也日益提高。通常,RSVP-TE 消息中的参数主要分为两类,即固定值对象参数与可变值对象参数。本文基于增强的 RSVP-TE 信令协议,引入了可信连接的思想,在信令交互过程中,结合攻击预防和入侵检测的原理,对 RSVP-TE 消息中的固定参数进行数字签名保护,使用消息反馈等安全机制对可变参数进行恶意行为检测。

安全信令的交互过程如图 1 所示。安全信令的交互过程由 6 个步骤组成,具体描述如下。

步骤 1 源节点收到来自业务端的连接请求后,首先计算出光路由,并将路由的相关信息封装

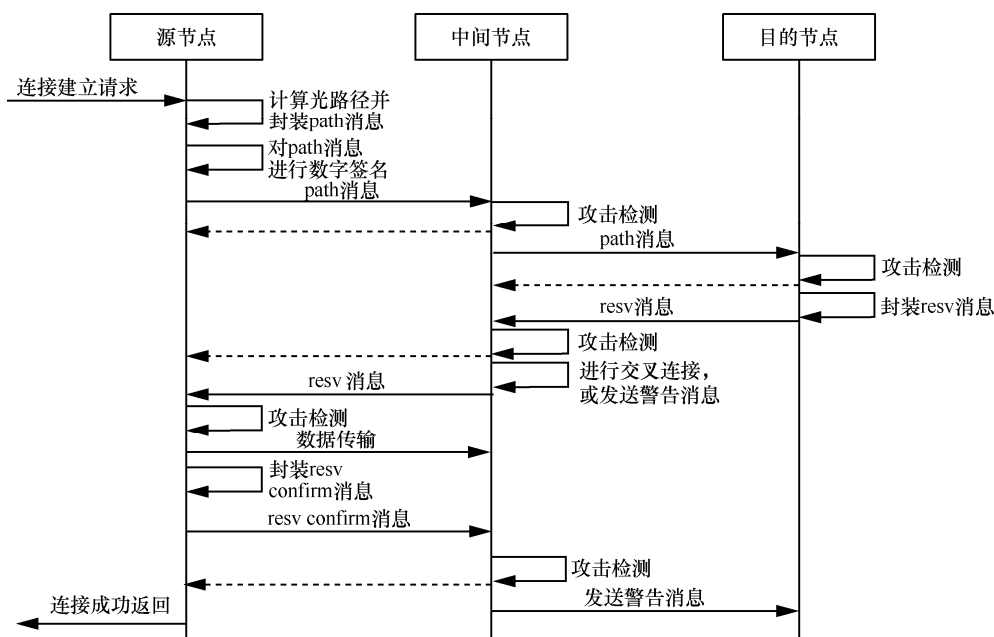


图 1 安全信令的交互过程

在 path 消息的 Sub-LSP 列表中。并将业务质量参数、路由参数、可用波长参数等可变值对象封装在 path 消息中；再将相关标记位设置为 0，即光路径建立；之后使用本节点的私钥对 path 消息中的 ID、业务流特征参数等用数字签名进行加密。

步骤 2 中间节点收到 path 消息后，若检测到 INTEGRITY 的相应标识为 0，则触发攻击检测并修改 path 消息中的 ERO 和 Adspec 等可变对象的值，然后向下一个节点发送此 path 消息。

步骤 3 目的节点收到来自源节点的 path 消息后，若检测到 INTEGRITY 中相关标识的值为 0，则触发攻击检测；若检测通过，该目的节点使用自身的私钥进行解密，生成 resv 消息；对波长标签 Label 等固定值对象进行数字签名，封装在 resv 消息中，之后向源节点反向发送该 resv 消息。

步骤 4 中间节点收到 resv 消息，首先执行攻击检测，并检测可变对象的值是否异常；若检测未通过，节点直接触发并上报安全告警；若检测通过，中间节点控制其光交换矩阵，执行光波长的交叉连接操作。

步骤 5 源节点收到 resv 消息后，同样先进行攻击检测。若攻击检测通过，源节点首先通过已经建立的光路径传输业务数据，接着使用本节点私钥对收到的固定值对象利用数字签名进行加密，并为其设置较高的转发优先级封装入 resv confirm 消息中，向目的节点发送此消息。

步骤 6 中间节点收到来自上游节点发送的 resv confirm 消息，同样进行攻击检测，并比较该 resv confirm 消息中的 Rspec 对象值是否异常。若检测通过，该节点则继续转发 resv confirm 消息，否则丢弃 resv confirm 消息或发起连接拆除的信令消息，同时触发安全告警。

3.3 安全性与复杂度分析

安全度为安全信令机制的首要关键性能指标。本文所提出的安全信令机制主要针对以下 4 个

方面进行安全防护：完整性攻击、内部攻击、重放攻击和伪造消息。

(1) 完整性保护

通过对消息中不变对象的消息摘要进行数字签名及验证，检测来自外部和内部的消息篡改攻击，实现对信令消息的完整性保护。

(2) 内部攻击防护

对重要可变对象采用反馈比较的方法，防止重要 QoS 参数被非法节点恶意篡改，保证实际光连接与业务请求的一致性。

(3) 重放攻击防护

通过在信令消息中引入序列号，防范节点对信令消息的重放攻击。

(4) 伪造消息防护

通过引入基于数字签名的消息认证方法，以确保信令消息本身的准确性。

假设整个网络有 n 个节点，其集合为 $\{N_1, N_2, \dots, N_n\}$ ， N_s 为源节点， N_d 为目的节点；若光网络中的各节点均符合信令交互所需的保密性、完整性和可用性等要求，并提供端到端可管可控的安全服务，则 $SC(N_s, N_d) = \{N_s, \dots, N_d\}$ 为节点 N_s 与 N_d 之间的安全连接 (security connection, SC)。DSC 表示在节点 N_s 和 N_d 间满足安全度、阻塞率和时延要求的安全连接的度量。

$$DSC(N_s, N_d, V_{SC}, V_B, V_D) = w_1 \cdot \sum_s \frac{1}{V_{SC,i}} + w_2 \cdot \sum_s \frac{1}{V_{B,i}} + w_3 \cdot \sum_s \frac{1}{V_{D,i}} \quad (1)$$

其中， $V_{SC,i}$ 为节点 i 的综合安全度， $V_{B,i} = (1 - P_{block})$ 为阻塞率满足度 (阻塞率为 P_{block})， $V_{D,i}$ 为时延满足程度； w_1 、 w_2 、 w_3 分别为各自对应的权重，且满足 $w_1 + w_2 + w_3 = 1$ 的限制条件。

复杂度是考量光网络信令机制的另一个关键指标。在协议复杂度方面，由于本文机制与原有 RSVP-TE 信令协议在信令消息以及交互过程中保持整体一致性，并且无需额外的信令消息，只对信令消息进行轻量级的安全性扩展。



在时间复杂度方面,由于引入了攻击检测与加解密处理,安全交互的时间复杂度为 $O(N)$,其中, N 为光通路所经过的平均节点数。虽然信令的安全处理时延会略有增加,但对于安全等级要求较高的光网络来说,该时间复杂度在可接受范围内。

4 仿真结果与分析

为了验证本文所提出的光网络信令安全交互技术,本文以支撑智能变电站业务的光网络作为典型应用场景,从阻塞率、业务连接建立时延两个方面,对具有安全信令机制的光网络和不具有安全信令的光网络进行仿真评估。仿真环境采用 NS2 网络仿真软件构建,网络结构参照典型的 NSFnet 的拓扑,网络规模为包含 32 个节点和 41 条光链路的电力光网络。设置网络中每个节点都具备完全分光 and 完全波长转换能力,以离线方式为每个节点配置签名的公钥。在仿真过程中,网络分别设置 3 个攻击节点随机执行重放信令消息、伪造信令消息的攻击行为。

仿真环境中的连接请求服从泊松分布,而业务量则服从均匀分布,即时间 t 内的连接请求服从泊松分布,并将业务负载换算成归一化强度表示,则业务平均到达速率可表示为式 (2)。

$$P_n(t) = \frac{\lambda(t)^n}{n!} e^{-t} \quad (2)$$

在智能变电站的光网络系统中分别采用本文机制(安全信令)与传统机制(非安全信令)进行仿真比较,得到图 2~图 4 的对比结果。其中, Case_1 和 Case_2 分别对应 8 个波长条件下的传统机制和本文机制, Case_3 和 Case_4 则为 16 个波长配置下的传统机制和本文机制。

图 2 分别给出了两种机制下业务请求数量对平均连接阻塞率的影响。由图 2 可见,当光纤链路中波长数 W 分别为 8 个和 16 个时,随着业务连接请求数目的增加,两种机制的业务连接请求阻塞

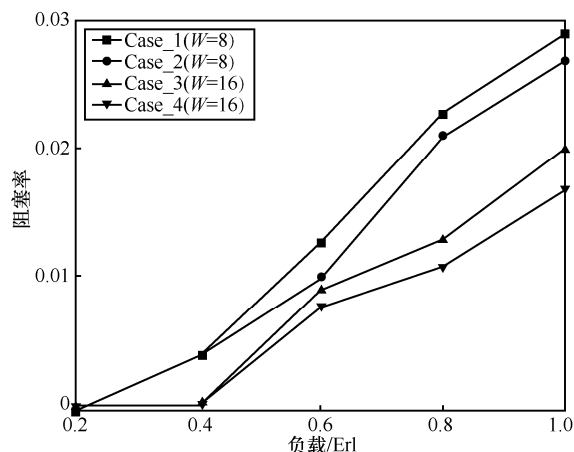


图 2 业务负载对阻塞率的影响

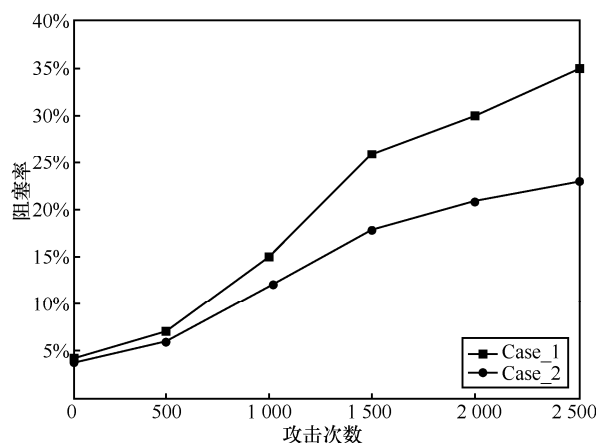


图 3 安全攻击强度对阻塞率的影响

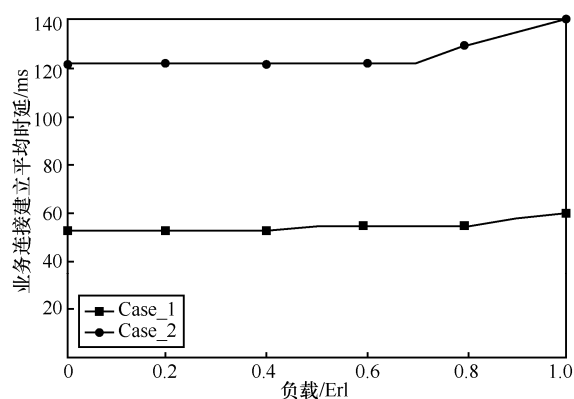


图 4 业务连接建立平均时延比较

率都呈显著上升趋势;但是随着波长数目的增加,平均连接阻塞率有了明显的改善。在相同波长与业务请求数量的情况下,本文所提出的信令安全优化方法在相同网络攻击下的连接阻塞率有所优化。

图3显示了安全攻击强度对阻塞率的影响。随着安全攻击次数的增加,传统机制的阻塞率明显高于本文机制。在传统的信令机制下,对信令过程的安全攻击会导致信令处理的混乱和波长资源被非法占用,造成业务连接建立失败。而本文所提出的信令安全机制能较好地防范安全攻击所引发的业务连接阻塞。

业务负载规模对连接建立时延的影响对比如图4所示。本文机制的平均时延大于传统机制,这是因为业务连接请求的数量和光网络的规模增大,密钥更新涉及的节点数增多,从而需要的处理时延也随之增加。这也是本文机制为了提高信令的安全性所付出的代价。

两种信令的综合安全度对比见表1。在不同攻击节点数和业务负载的条件下,统计其节点平均安全度、建路成功率以及时延满足率,根据式(1)得出信令综合安全度DSC的值。当负载较低且攻击强度较小时,传统机制的综合表现略高于本文机制;但是在负载较高的情况下,本文机制的综合安全度明显高于传统机制。

表1 信令综合安全度比较

	攻击节点数	业务负载/Erl	综合安全度
传统机制	1	0.4	0.97
	3	0.8	0.73
本文机制	1	0.4	0.92
	3	0.8	0.83

综上所述,本文所提出的电力光网络安全信令优化方法与传统机制相比,能够使业务连接的信令交互过程获得更好的安全保障,同时也优化了阻塞率方面的性能。因此,与传统信令机制相比,本文所提的机制能够有效增强电力光网络对智能变电站通信业务安全交互的支持能力,实现了电力光网络端到端的可信连接,优化了其面向能源互联业务承载能力。

5 结束语

本文为了提高光传送网对智能变电站业务的支持能力,提出了一种面向智能变电站的光网络安全信令优化技术。该技术对光网络现有的RSVP-TE信令协议进行安全性扩展加强,在业务连接建立的过程中,针对信令交互引入攻击检测、安全加密等手段。仿真结果表明,本文所提出的机制能有效提高智能变电站业务与光网络交互的安全性。

但是,当前光网络信令安全的研究主要集中于单域光网络,而采用分布式结构的多域光网络必须考虑域内与域间的信令安全问题。此外,随着基于软件定义网络(SDN)思想的新型智能光网络的兴起,软件定义光网络与传统光网络的差异很大,因此将软件定义光网络的安全信令技术作为未来重点方向之一,有待进一步深入研究。

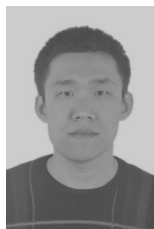
参考文献:

- [1] TIAN S, LUAN W, ZHANG D, et al. Technical forms and key technologies on energy internet[J]. Proceedings of the CSEE, 2015, 35(14): 3482-3494.
- [2] TSOUKALAS L H, GAO R. From smart grids to an energy internet: assumptions, architectures and requirements[J]. Smart Grid & Renewable Energy, 2008(1): 94-98.
- [3] TALEBI S, ALAM F, KATIB I, et al. Spectrum management techniques for elastic optical networks: a survey[J]. Optical Switching & Networking, 2014, 13(9): 34-48.
- [4] YIN Y, WEN K, GEISLER D J, et al. Dynamic on-demand defragmentation in flexible bandwidth elastic optical networks[J]. Optics Express, 2012, 20(2): 1798-804.
- [5] GONG L, ZHU Z. Virtual optical network embedding (VONE) over elastic optical networks[J]. Journal of Light Wave Technology, 2013, 32(3): 450-460.
- [6] DAHAN D, MAHLAB U. Security threats and protection procedures for optical networks[J]. IET Optoelectronics, 2017, 11(5): 186-200.
- [7] WU H, ZHOU F, ZHU Z, et al. Interference-and-security-aware distance spectrum assignment in elastic optical networks[C]// European Conference on Networks and Optical Communications, June 1-3, 2016, Lisbon, Portugal. Piscataway: IEEE Press, 2016.



- [8] BAI H F, LI M W, WANG D S. Bayesian classifier based service-aware mechanism in 10G-EPON for smart power grid[J]. Acta Photonica Sinica, 2013, 42(6): 668-673.
- [9] SKORIN-KAPOV N, FURDEK M, ZSIGMOND S, et al. Physical-layer security in evolving optical networks[J]. IEEE Communications Magazine, 2016, 54(8): 110-117.
- [10] LIU Y, LI H, HOU Y, et al. Protocol independent transmission method in software defined optical network[C]//International Symposium on Optoelectronic Technology and Application, May 9, 2016, Beijing, China. [S.l.:s.n.]. 2016.
- [11] 赵英. 浅谈信令网络监测系统[J]. 电信科学, 2001, 17(7): 44-49.
ZHAO Y. On the detection system of signaling network[J]. Telecommunications Science, 2001, 17(7): 44-49.
- [12] LI Y, HUAN N, YU Y, et al. Light source and trail recognition via optical spectrum feature analysis for optical network security[J]. IEEE Communications Letters, 2018, PP(99): 1.
- [13] PEDERZOLLI F, FURDEK M, SIRACUSA D, et al. Towards secure optical networks: a framework to aid localization of harmful connections[C]//Optical Fiber Communications Conference and Exposition, March 11-15, 2018, San Diego, CA, USA. Piscataway: IEEE Press, 2018: Th2A.42.

[作者简介]



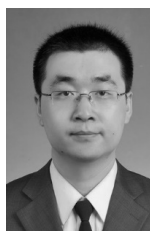
赵宇皓（1983- ），男，国网河北省电力有限公司电力科学研究院高级工程师，主要研究方向为智能变电站继电保护。



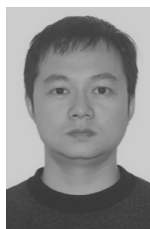
郝晓光（1980- ），男，国网河北省电力有限公司电力科学研究院高级工程师，主要研究方向为智能变电站二次设备检测技术。



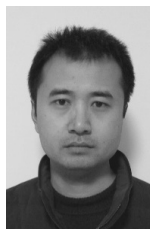
耿少博（1986- ），男，国网河北省电力有限公司工程师，主要研究方向为智能变电站继电保护技术。



罗蓬（1984- ），男，博士，国网河北省电力有限公司电力科学研究院高级工程师，主要研究方向为智能变电站二次设备检测技术。



周坤（1981- ），男，武汉凯默电气有限公司工程师，主要研究方向为智能变电站测试技术。



甄家林（1980- ），男，武汉凯默电气有限公司工程师，主要研究方向为智能变电站测试技术。



毛玉荣（1989- ），女，武汉凯默电气有限公司工程师，主要研究方向为电力系统及其自动化。