基于IEC60870-5-104的配电自动化通信安全协议

马 钧[1,2] 张一斌[2]
(电力系统安全运行与控制湖南省高校重点实验室(长沙理工大学) 长沙 410004)[1]
(长沙理工大学电气与信息工程学院 长沙 410015)[2]

摘 要 基于IEC60870-5-104规约的配电自动化通信过程存在信息安全隐患。为了实现配电主站前置机和配电终端之间的相互身份认证和共享密钥建立,提出了一种基于单向数字签名和单向哈希认证码算法的安全协议,分析了配电自动化通信EPON网络的结构特点以及与之相应的信息安全威胁和安全需求,给出了协议的实现过程。协议考虑了配电终端的有限计算能力,配合使用专用的安全设备,不改变原有配电终端的软硬件。对协议的安全分析证明该协议能抵御外部攻击、重放攻击和假冒攻击。与已有的协议相比,新协议具有更高的安全性和较高的效率,能够满足实际的应用需求。

关键词 配电自动化,网络安全,IEC60870-5-104规约,数字签名,HMAC算法
中图法分类号 TM76,TP393 **文献标识码** A

Security Protocol Based on IEC60870-5-104 for Communication in Distribution Automation

MA Jun[1,2] ZHANG Yi-bin[2]
(Hunan Province Higher Education Key Laboratory of Power System Safety Operation and Control (Changsha University of Science and Technology), Changsha 410004, China)[1]
(School of Electrical and Information Engineering, Changsha University of Science and Technology, Changsha 410015, China)[2]

Abstract It has been found that there are some cyber security risks in the communication process of distribution automation system(DAS) based on IEC60870-5-104 protocol. In order to realize mutual authentication and shared key establishment for DAS Front-End Processor(FEP) and any terminal, this article presented a scheme based on unidirectional digital signature and unidirectional Keyed-Hashing for Message Authentication(HMAC) algorithm. It analyzed the features of communication network architecture based on EPON in DAS, the corresponding cyber security risks and security requirements, showed the implementation procedure of the scheme. The scheme needs not change original software and hardware of legacy terminals and considers resource-constraint terminals by using dedicated security devices. Security analysis proves that the scheme can resist outsider attack, replay attack and impersonation attack. Compared with the related works, the proposed scheme is more secure and practical, which can satisfy the application requirement.

Keywords Distribution automation, Cyber security, IEC60870-5-104 protocol, Digital signature, HMAC algorithm

1 引言

配电自动化通信系统是配电安全供电不可或缺的重要组成部分。如果配电自动化通信系统受到网络攻击,则可能造成配电系统的停电事故或电力设备损坏,这是智能配电网安全风险的主要来源。国际组织非常重视电力系统网络安全问题,国际电工委员会(IEC)在信息安全方面的标准《IEC 62351电力系统管理及信息交换-数据和通信安全性》[1],是IEC TC57第15工作组为保障电力系统安全运行,针对IEC 60870-5、IEC 61850等常用电力系统通信规约的数据和通信安全制定的增强标准[2]。然而,IEC 62351标准仍需完善,在其得到广泛认可和执行之前仍需要先解决现有标准的问题和挑战。一直以来,电力SCADA系统网络安全研究受到普遍重视[3-5]。但对于网络攻击来说,配电自动化系统在许多方面相比SCADA系统更脆弱,因为SCADA一般在一个固定的区域,而配电自动化系统中的配电终端设备大多数情况下位于远程和无人的站点,并分布在广泛的区域。在我国,配电自动化系统通信规约主要是基于IEC60870-5的101和104等规约,而这些规约的数据包以明文形式传输。因此,控制命令等消息在通信传输过程中有可能受到恶意攻击。

近年来,配电自动化通信系统安全研究取得进展,文献[6]提出了在消息中增加哈希认证码来实现配电自动化通信中数据来源的真实性和数据完整性验证的安全协议,并提出了基于对称加密和认证码的密钥协商方法。文献[7]在前者提出的协议基础上增加了基于角色的操作权限限制和基于用户ID的安全审计等功能,解决了远程电力监控通信中非法用

到稿日期:2013-01-31 返修日期:2013-05-22 本文受湖南省科技厅科技计划一般项目(2012GK3053)资助。
马 钧(1974-),男,硕士,讲师,主要研究方向为电力通信网络安全,E-mail:majun333553@163.com;张一斌(1957-),男,教授,硕士生导师,主要研究方向为电力电子技术、电力通信技术。

户操作、用户越权操作等问题。文献[8]提出了一种多通道安全认证组播方法，实现了配电自动化智能电子设备之间的认证与密钥更新，但是该方法仅限于通信节点数目比较少的情况。文献[9,10]提出了一种基于身份的智能配电网访问控制方案，即采用双线性对构建子站和终端的共享密钥。但是该方案的共享密钥固定不变，影响了其安全性。针对智能电网电力线通信，文献[11]讨论了采用基于 IPv6 的 IPsec 技术的安全通信方案。对于配电网中的高级测量基础设施(Advanced Metering Infrastructure，AMI)通信，文献[12]介绍了一种采用逐跳传输并结合认证加密的安全规约方案。

本文通过分析现有配电自动化通信中存在的信息安全隐患，提出了一种配电自动化通信系统安全协议，协议在原有 IEC60870-5-104 规约的基础上结合了单向数字签名认证和单向哈希认证码 HMAC 算法等安全措施。然后讨论了该方案的安全性并与相关协议进行了比较，结果证明该通信协议具有更高的安全性和较高的效率。

2 配电自动化通信网络安全威胁

2.1 配电自动化通信系统结构特点

配电自动化系统包括配电主站、配电子站和配电终端等。目前配电自动化通信系统架构主流为以太网无源光网络(Ethernet Passive Optical Network，EPON)。EPON 基于以太网标准，它由局端的光线路终端(Optical Line Terminal，OLT)、光分配网络(Optical Distribution Network，ODN)和用户测的光网络单元(Optical Network Unit，ONU)组成，为单纤双向系统。如图 1 所示，配电系统中的通信前置机(Front-End Processor，FEP)联接到了 OLT 上，配电子站是一个汇聚中心，一般设置在变电站内，配电终端通过串口接到 ONU 上，多个 ONU 联接到 OLT 上。FEP 通过 IEC 60870-5-104 规约与配电终端进行通信并交换信息。

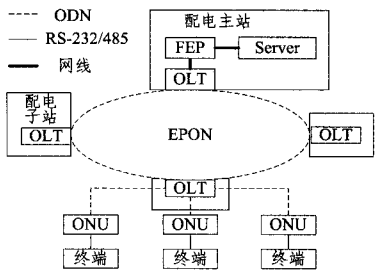

图 1 基于 EPON 的配电自动化结构

2.2 网络威胁

我国基于 EPON 的配电自动化系统主要采用基于以太网的 IEC60870-5-104 规约，而这种规约在制定时并没有考虑到网络安全问题，因此，采用这种规约的配电自动化系统存在网络安全风险，具体如下：

(1)旁路控制：攻击者假冒配电主站 FEP 对配电终端发送非法控制命令，如非法合闸或分闸命令，可能导致停电事故或人员伤亡等。

(2)假冒：攻击者发送假冒数据信息到通信系统中，干扰配电系统正常的数据分析。

(3)篡改：攻击者非法篡改主站下行或配电终端上传的各种数据信息，对系统运行产生不良影响。

(4)窃听：在 EPON 系统中，下行数据采用广播方式，攻击者可以通过探测工具探测所有下行数据。

(5)重放攻击：攻击者延迟或重复发送以前的有效消息，这可能造成事故。

(6)拒绝服务：攻击者通过窃听分析数据规约，伪造大量数据阻塞或拖延网络消息传送，影响配电系统正常通信。

综上所述，在配电终端与主站之间需要进一步加强网络安全防护才能保证配电系统安全稳定运行。

2.3 安全需求

表 1 对配电自动化系统网络威胁的重要性差异进行了分析。在这些因素中，最关键的安全类别是消息的身份认证、完整性和时效性验证。配电主站 FEP 需要发送基于 IEC60870-5-104 规约的远程控制命令和其他敏感数据给配电终端进行实时监测和控制。如果攻击者假冒 FEP 发送非法遥控命令或篡改命令遥控终端操作开关设备，则可能导致停电事故、设备损坏或人员伤亡。而如果攻击者假冒终端发送非法数据或篡改数据信息给主站 FEP，则可能影响 FEP 的数据处理，但一般不会造成重大事故。因此，对从主站到终端的消息进行身份认证和完整性验证比对从终端到主站的消息进行相同验证更重要。此外，消息应该是实时的，旧的消息需要避免被攻击者重发，因为重播一些远程控制命令可能会导致严重的意外。而机密性除了密钥分发和其他敏感数据的传输以外并不是特别重要。总之，配电自动化通信安全的关键是确保相互身份认证和完整性验证，防止重放攻击。其中重点验证从配电主站发送给终端的消息。

表 1 配电自动化系统网络威胁分析表

方向	网络威胁	可能影响	安全类别	重要性
主站-终端	旁路控制；篡改	停电事故，人员伤亡	身份认证和完整性	高
	重放攻击	造成事故	时效性	高
终端-主站	假冒；篡改	干扰主站处理	身份认证和完整性	中
	重放攻击	干扰主站处理	时效性	中
双向	窃听	影响机密性	机密性	低

文献[6,7]提出了用于配电自动化的基于哈希认证码的安全协议，本文在此基础上进一步研究基于 IEC60870-5-104 规约的配电自动化通信系统网络安全协议，其主要难点是：

(1)对于来自主站的消息需要重点进行身份认证和完整性验证。且配电终端对于来自主站的消息的不可否认性验证是不可或缺的，因为只有不可否认性验证才能确保分清某个控制命令究竟是由主站 FEP 发出的还是来自于其他发送者，如负责维护和调试终端的内部工作人员等。

(2)配电终端计算能力有限，特别是已经投入使用的遗留终端，这对身份认证和完整性验证的计算复杂性提出了要求。

3 安全协议方案

3.1 附加的安全设备

为了不影响配电系统遗留设备的原有规约和软硬件配置，可以使用专用安全设备透明接入通信网络来处理增加的安全验证计算量。建议的安全解决方案如图 2 所示。一个安全服务器 S 连接到配电 FEP，而现场的配电终端 D_A 连接到专用安全设备 A 上。密钥生成中心(Key Generation Center，KGC)用来完成系统初始化工作：

(1)利用椭圆曲线密钥体系选择系统公私钥对 K_Q 和 K_q。

(2)选择一个安全的单向 Hash 函数 H。

(3)KGC 为任一安全设备 A 指定唯一身份标识 ID_A，并

分配加密服务器 S 和安全设备 A 的临时共享密钥 K_{AS}，且每个安全设备与 S 共享的密钥各不相同。

(4)KGC 完成系统初始化后，通过离线方式发送{K_Q，$H(\cdot)$，K_{AS}}给 A 加以保护；同时，将其以及私钥 K_q 通过内网直接发送给 S 加以保护。

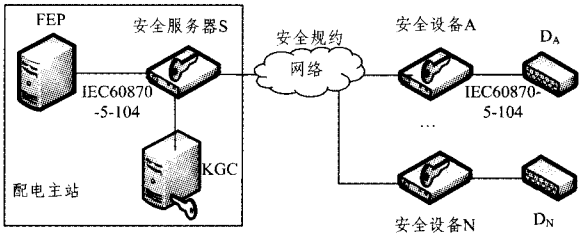

图 2　配电自动化系统安全设备接入

3.2　安全协议

根据 2.3 节分析，对来自配电主站 FEP 与配电终端发送的消息分别定义两种安全级别不同的协议。协议如下：

3.2.1　配电主站 FEP 发送消息 M_S 给配电终端 D_A

如果配电 FEP 需要发送消息给配电终端 D_A，其过程如图 3 所示，步骤如下：

(1)FEP 首先发送消息 M_S 给安全服务器 S，其中 M_S 采用 FEP 原有的 IEC60870-5-104 通信规约。

(2)S 组合消息 M_S 和代表当前时间的时间戳 T_S，然后用一个哈希函数 H 对其计算一个固定字长的消息摘要。接着，S 通过对这个消息摘要用私钥 K_q 计算一个数字签名 DS。而后，S 把 T_S 和 DS 组合在消息 M_S 上，并发送这个组合消息给安全设备 A。其过程如下：

$$DS=EK_q(H(M_S \parallel T_S))$$

$$S \rightarrow A:(M_S \parallel T_S \parallel DS)$$

注：$EK(\cdot)$表示用密钥 K 加密，$DK(\cdot)$表示用密钥 K 解密，$\parallel$ 表示消息的组合，$\rightarrow$表示发送。

(3)安全设备 A 收到消息($M_S \parallel T_S \parallel DS$)后，首先核对时间戳 T_S 的有效性，以确保消息没有被重播。如果 T_S 无效，则终止协议，否则 A 继续用公钥 K_Q 解密数字签名 DS，并对 M_S 和 T_S 的组合消息使用同样的哈希函数 H，接着 A 验证式(1)是否成立，如果等式成立，说明消息验证成功，否则 A 终止协议。

$$DK_Q(DS)=H(M_S \parallel T_S) \qquad (1)$$

(4)若消息验证成功，A 将消息 M_S 传送给 D_A。

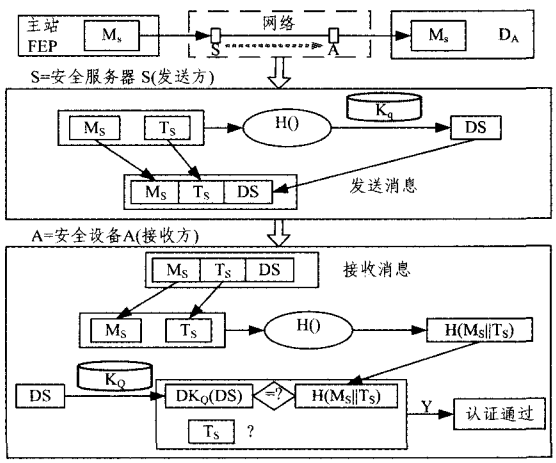

图 3　配电前置机发送消息给配电终端过程

3.2.2　配电终端 D_A 发送消息 M_A 给配电主站 FEP

如果 D_A 需要回应配电 FEP，或者 D_A 主动发送消息给配电 FEP，其过程如图 4 所示步骤如下：

(1)D_A 首先发送消息 M_A 给 A，其中 M_A 采用 D_A 原有的 IEC60870-5-104 通信规约。

(2)A 组合消息 M_A、时间戳 T_A、A 的节点号 ID_A 以及 A 与 S 的共享密钥 K_{AS}，然后 A 通过一个同样的单向哈希函数 H 计算消息认证码。接着 A 组合消息 M_A、时间戳 T_A、节点号 ID_A 和 H_{MAC}，其中 H_{MAC} 为 A 产生的 HMAC 认证码，最后 A 发送这个混合消息。过程如下：

$$H_{MAC}=H(M_A \parallel T_A \parallel ID_A \parallel K_{AS})$$

$$A \rightarrow S:(M_A \parallel T_A \parallel ID_A \parallel H_{MAC})$$

(3)S 在收到消息($M_A \parallel T_A \parallel ID_A \parallel H_{MAC}$)后，首先核对时间戳 T_A，如果 T_A 无效，则终止协议，否则 S 根据对应表中的 ID_A 得到与 D_A 的共享密钥 K_{AS}，然而对($M_A \parallel T_A \parallel ID_A \parallel K_{AS}$)应用同样的哈希函数，并验证式(2)是否成立。如果等式不成立，S 立即终止协议，否则 S 能确认终端身份以及消息的完整性没有被破坏。

$$H_{MAC}=H(M_A \parallel T_A \parallel ID_A \parallel K_{AS}) \qquad (2)$$

(4)如消息验证成功，则 S 传送消息 M_A 给配电 FEP。

本方案中，配电终端对来自配电 FEP 的单向数字签名进行认证，确保主站 FEP 的身份真实性、消息完整性和不可否认性。为了减少签名验证开销以及避免使用需要对称密钥加密的消息认证码算法，配电 FEP 对来自配电终端的消息采用基于密钥的散列函数 HMAC 算法用于身份认证和完整性验证。国家密码管理局公布的 SM3 密码杂凑算法，可在计算 HMAC 中使用。

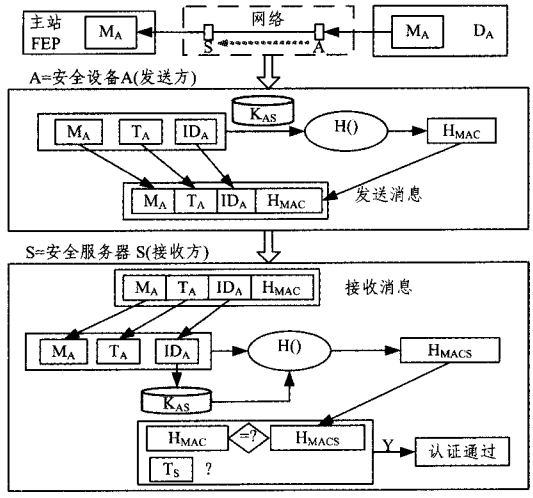

图 4　配电终端发送消息给配电前置机过程

3.3　共享密钥分配

配电 FEP 和配电终端之间的原始共享密钥由 KGC 离线发给每个终端。这些密钥需要定期更新，以保证安全。所以密钥管理机需要定期更新安全服务器 S 和每一个安全设备之间的会话密钥。当 KGC 准备更新 S 和任一安全设备 A 之间的共享密钥 K_{AS} 时，其步骤如下：

(1)KGC 将 A 的节点号 ID_A 以及新共享密钥 K_{AS1} 发送给 S。

(2)S 根据 ID_A 用原来的共享密钥 K_{AS} 加密新的会话密钥 K_{AS1}，得到密文 $EK_{AS}(K_{AS1})$。然后 S 组合一个请求消息 M_{SQ}、密文 $EK_{AS}(K_{AS1})$、时间戳 T_S 和数字签名 DS，其中，DS

由 M_{SQ}、K_{AS1} 和 T_S 组合的消息用单向哈希函数 H 计算并用私钥 K_q 加密得到。最后 S 发送这个混合消息给 A。过程如下：

$S \rightarrow A: (M_{SQ} \parallel EK_{AS}(K_{AS1}) \parallel T_S \parallel DS)$

其中，$DS = EK_q(H(M_{SQ} \parallel K_{AS1} \parallel T_S))$。

(3)当 A 收到消息 $(M_{SQ} \parallel EK_{AS}(K_{AS1}) \parallel T_S \parallel DS)$ 后，首先核对时间戳 T_S 的有效性，通过后用原来的共享密钥 K_{AS} 解密 $EK_{AS}(K_{AS1})$ 以得到新的共享密钥 K_{AS1}，然后 A 用公钥 K_Q 解密数字签名 DS，并运用同样的哈希函数 H 验证式(3)是否成立，如果不等式成立，A 终止协议，否则说明消息验证成功，A 更新共享密钥为 K_{AS1}。

$$DK_Q(DS) = H(M_{SQ} \parallel K_{AS1} \parallel T_S) \tag{3}$$

4 协议安全性分析和性能比较

4.1 安全分析

(1)假冒攻击。假设攻击者想冒充配电 FEP，他随机选择私钥 K_q'、哈希函数 H' 并用当前时间戳 T_S' 和消息 M_S' 计算数字签名 DS'，然后攻击者发送消息 $(M_S' \parallel T_S' \parallel DS')$ 给一个安全设备验证。由于 $DK_Q(DS') \neq H(M_S' \parallel T_S')$，因此消息被认为是非法的。类似地，攻击者也不可能冒充有效的配电终端，因为他没有共享密钥。因此，攻击者不可能执行旁路控制，以及假冒和篡改协议内容。

(2)外部攻击。假设攻击者窃听了安全服务器 S 和安全设备 A 之间的通信，他能够收集消息 $(M_S \parallel T_S \parallel DS)$ 和 $(M_A \parallel T_A \parallel ID_A \parallel H_{MAC})$。为了获得哈希函数 H，他需要从 $H_{MAC} = H(M_A \parallel T_A \parallel ID_A \parallel K_{AS})$ 中得到 H，然而这是不可能的，因为他不知道共享密钥 K_{AS}，并且必须面对单向哈希函数的不可逆性。为了获得 S 的私钥 K_q，他必须面对椭圆曲线密码体系的难题，而这些到现在为止还没有算法可以解决。

(3)重放攻击。假设攻击者收集了安全服务器 S 和安全设备 A 之间以前的通信消息。然后攻击者可以发送以前收集的消息 $(M_S \parallel T_S \parallel DS)$，以便假装他是 S。安全设备 A 能很容易辨明 T_S 是过去的时间并丢弃这个消息。当攻击者发送 $(M_S \parallel T_S' \parallel DS)$ 给 A 时，这里 T_S' 代表现在的时间。但是攻击者不能成功，因为数字签名 $DS = EK_q(H(M_S \parallel T_S))$ 是由过去的时间 T_S 而不是现在的时间 T_S' 计算出来的。所以验证等式 $DK_Q(DS) = H(M_S \parallel T_S')$ 不会成立，因为 $T_S' \neq T_S$。类似地，攻击者也不能用以前收集的消息 $(M_A \parallel T_A \parallel ID_A \parallel H_{MAC})$ 来假装他是安全设备 A，因此，重放攻击对本安全协议无效。

4.2 相关工作比较

表 2 显示建议的协议和相关的配电自动化通信协议的比较。文献[6]的配电自动化系统通信协议采用两方 HMAC 算法进行认证，其节点对主站的消息认证不具备不可否认性验证，存在安全隐患。文献[10]提出了基于身份的配电网通信系统访问控制方案，所有节点首先需要通过认证，然后通过共享密钥进行通信，该方案认证较复杂，且其由物理地址为 ID 构建的共享密钥固定不变，影响了其安全性。文献[12]介绍了一种在配电网中 AMI 节点与配电主站通信的安全规约方案，其智能仪表节点采用逐跳方式先汇集在馈线，然后传输到主站，规约采用加密方式和 HMAC 认证码算法，但该方法经过逐跳方式，其实时性受到影响。本文提出的基于 EPON 网络的协议根据消息重要性不同，分别采用数字签名和 HMAC 算法进行认证，数字签名的计算和验证由具有强大计算功能的专用安全设备执行，终端一方只需验证，不需要签名，且不影响配电终端原有软硬件。相比而言，其安全性更高，通信次数较少而效率较高。

表 2 相关工作比较

协议	不可否认性	对称加/解密	认证码	非对称加/解密	通信次数	安全性
文献[6]协议	无	0	2	0	1	中
文献[10]协议	无	8(4/4)	0	0	2	低
文献[12]协议	无	2(1/1)	2	0	2	中
本文协议	有	0	1	2(1/1)	1	高

注：对称加/解密下的 2(1/1)表示一共进行了 2 次该类型运算，包括 1 次加密运算和 1 次解密运算，其他类似。

结束语 本文针对采用 IEC60870-5-104 规约的配电自动化通信系统 EPON 网络安全现状，分析了配电系统通信的安全需求，根据消息的重要性不同，在原规约基础上加入不同的身份认证方法，提出了一种安全协议，以确保配电自动化系统的可靠性，防止假冒主站对终端的操作，并能够让主站分析真实的配电终端数据。与现有的电力系统安全协议解决方案相比，本文提出的协议具有更高的安全性和较高的效率。下一步将设计开发配电网安全协议仿真系统，进一步评估在配电网通信中使用新协议对抗网络攻击的能力，并开展安全协议的性能优化研究。

参 考 文 献

[1] IEC TS 62351-1, IEC Technical Committee 57, Data and Communications Security, Part1: Communication Network and System Security-Introduction to Security Issues[S]. 2007

[2] IEC TS 62351-5, IEC Technical Committee 57, Data and Communications Security, Part5: Security for IEC 60870-5 and derivatives[S]. 2009

[3] Ma Jun, She Jun. Research on Cyber Security Segre-gation for Industrial Control Systems[J]. International Journal of Digital Content Technology and its Applications, 2011, 5(8): 9-15

[4] Igure V M, Laughter S A, Williams R D. Security issues in SCADA networks [J]. Computers and Security, 2006, 25(7): 498-506

[5] III B C L, Buennemeyer T K , Thomas R W. Next generation SCADA security: best practices and client puzzles[C] // Proc. 6th Annual. IEEE System, Information Assurance Workshop. 2005: 426-427

[6] Lim I H, Hong S, Lee S J, et al. Security Protocols Against cyber attacks in the distribution automation system[J]. IEEE Transactions on Power Delivery, 2010, 25(1): 448-454

[7] 黄梦婕，胥布工. 基于 HMAC 算法的远程电力监控通信安全策略[J]. 电力系统保护与控制，2011, 39(19): 79-82

[8] Kim M, Metzner J J. A key exchange method for intelligent electronic devices in distribution automation[J]. IEEE Transactions on Power Delivery, 2010, 25(3): 1458-1463

[9] 孙中伟，张荣刚. 智能配电网通信系统访问控制研究[J]. 电力系统保护与控制，2010, 38(21): 118-121

[10] Sun Zhong-wei, Wu Ju-ying. Identity-based access con-trol for distribution automation using EPON[J]. Chinese Journal of Electronics, 2011, 20(3): 443-446

[11] Hirschler B, Treytl A. Internet Protocol Security and Power Line Communication[C] // 2012 IEEE International Symposium on Power Line Communication and its Applications. 2012: 102-107

[12] Yan Ye, Hu R Q, Das S K, et al. An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid [J]. IEEE Network, 2013, 27(4): 64-71