智能配电网通信系统访问控制研究

孙中伟，张荣刚

（华北电力大学电气与电子工程学院，北京 102206）

摘要：智能配电网信息安全是智能电网发展需要解决的关键问题。为了阻止恶意使用的智能电子设备（Intelligent Electric Device，IED）接入到智能配电网通信系统，在智能配电网通信系统层次化结构设计的基础上，提出一种基于身份的密码体制（Identity-based Cryptosystem，IBC）的智能配电网访问控制方案。实例分析表明，该方案减轻了终端 IED 设备的计算和通信开销，同时实现了设备的合法性认证问题，非常适合智能配电网的应用环境。

关键词：智能配电网；访问控制；基于身份的密码体制

Access control for communication network of smart distribution grid

SUN Zhong-wei，ZHANG Rong-gang

（School of Electric and Electronic Engineering，North China Electric Power University，Beijing 102206，China）

Abstract：Cyber security for smart distribution grid is one of the key problems to be solved. To prevent malicious intelligent electric device （IED）from joining the communication network of smart distribution grid，access control is required when a new IED is deployed in the system. Based on the hierarchical network model of communication system and identity-based cryptosystem（IBC），this paper proposes an access control scheme，which accomplishes both authentication and key establishment for new IEDs. The case study shows that the proposed scheme is well suited for smart distribution grid environment in terms of the computation and communication cost required by the IEDs.

Key words：smart distribution grid；access control；identity-based cryptosystem（IBC）

中图分类号： TM76 文献标识码：A 文章编号： 1674-3415(2010)21-0118-04

0 引言

电力是国家的支柱能源和经济命脉，电网是经济社会发展的重要基础设施。电力系统的安全、可靠运行对保障社会经济发展以及社会稳定至关重要。现代电网的发展已经迎来机遇与挑战并存的关键期。一方面，电网需要应对日益严峻的资源和环境压力，实现大范围的资源优化配置，提高全天候运行能力，满足能源结构调整的需要，适应电力体制改革；另一方面，输配电、发电以及信息通信等技术的进步也为解决这一系列问题提供了坚实的技术支持。因此，智能电网将成为现代电力工业发展的必由之路[1-4]。

智能电网，又称为知识型电网或者现代电网，是将现代先进的传感与测量技术、信息通信技术、控制技术和原有的输配电基础设施高度集成而形成的新型电网。以信息通信技术为支撑的智能电网，通过电力流、信息流、业务流的高度一体化融合，可实现多元化电源和不同特征电力用户的灵活接入和方便使用，极大提高电网的资源优化配置能力，大幅提升电网的服务能力。

智能电网是传统电力基础架构与信息通信基础架构共同建设与管理的过程，其安全运行将建立在设备的安全运行和信息的安全维护基础上，而且信息的安全性在很大程度上意味着电网控制系统的安全性。因此，如何有效保障智能电网的信息安全已成为一项非常紧迫的任务[5-6]。

电力系统信息安全问题受到人们的关注和重视，国外相关研究机构对此已展开了广泛的研究，其中以IEC TC57 WG15制定的IEC62351安全国际标准最为典型。然而，IEC62351只提出了使用哪些措施从哪些层面上保证整个通信体系的安全，并没有给出一套具体且完整的实现方案[6]。另外，相对于智能电网，传统的电力系统没有建立在开放的系统和共享的信息基础之上，因此，针对传统电网的一些安全方面研究成果并不完全适用于智能电网应

用环境。电力系统由发电、输电、配电、用电等环节组成，智能配电网是智能电网体系结构中的关键组成部分。配电网信息数据的重要性在建设智能电网中日渐显露，并且在未来将日益突出。然而有关智能配电网信息安全方面的研究到目前为止并不多[7-10]。

智能电网信息安全问题是信息通信技术在电力系统中广泛应用的产物，而密码技术是保障电力系统信息安全的核心技术。本文针对智能配电网通信系统访问控制开展研究，在现代密码理论的基础上，以IEEE34节点系统作为应用实例，提出一种基于身份密码体制（Identity-based Cryptosystem，IBC）的智能配电网访问控制方案。

1　密码技术基础

密码学能够为网络信息安全提供关键理论和核心技术。利用密码算法能完整地解决信息安全中的机密性、数据完整性、认证、身份识别、可控性和不可抵赖性等问题中的一个或几个问题[11]。

早期的加密系统是基于对称密码理论，其特点是通信双方需要共享一个密钥，发送者和接收者在安全通信之前需要商定或分配一个密钥。随着对称密码理论的发展，出现了许多对称密码算法如DES、AES 等。对称加密算法虽然解决了数据的保密传输问题，但是存在密钥的分发和管理困难问题。

1976 年，Diffie 和 Hellman 提出了公开密钥理论。而在公开密钥体系中，加密和解密使用两个不同的密钥。公开密钥理论提出后，出现了一些著名算法，例如 RSA、DSA 等。公钥密码理论解决了对称密码系统的密钥交换问题。公钥基础设施（Public Key Infrastructure，PKI）是目前被广泛采用的公钥密码体系结构。PKI 基于证书机制，而证书的管理是 PKI 的瓶颈。

为了解决证书的管理问题，Shamir于1984年提出了IBC的概念[12]。然而Shamir并未给出IBC系统的实现。直到2001年D.Boneh和M.Franklin利用双线性配对设计出了实用的基于身份的加密方案[13]。之后，许多学者也利用双线性配对性质，提出了各种基于身份的密码学方案[14]。IBC简化了传统基于证书的公钥体制的密钥管理，为1976年以来的公钥密码学增添了新的内容，也是目前密码学界的一个研究热点。基于此，本文将采用基于身份的密码体制实现智能配电网的访问控制。

2　智能配电网通信系统模型

从智能化的程度来讲，集中控制模式是智能配电网最为理想的控制模式，而通信系统是建设智能配电网的一个关键环节。智能配电网需依靠有效的通信手段，将控制中心的命令准确地传送到众多的终端智能电子设备（Intelligent Electric Device，IED），并且将终端IED采集的各类实时信息传送到控制中心。智能配电网通信系统可采取如下的两种通信方案：第一种是主站、子站、终端三层结构；第二种是主站、终端两层结构。由于配电网终端设备数量大、种类多、分布广，主站、终端两层通信结构形式并不适合智能配电网通信结构。因此，本文将针对智能配电网主站、子站、终端三层结构的通信系统加以研究。相应地，智能配电网通信系统可分为主站-子站以及子站-终端IED两个层次。每个层次的通信网络架构可采用总线型、星型和环型形式或它们的混合形式。图1所示为一种主站和子站之间采用星型架构、子站1和子站2和终端设备间采用总线型架构、而子站*n*则采用了总线和星型混合架构的通信模式。

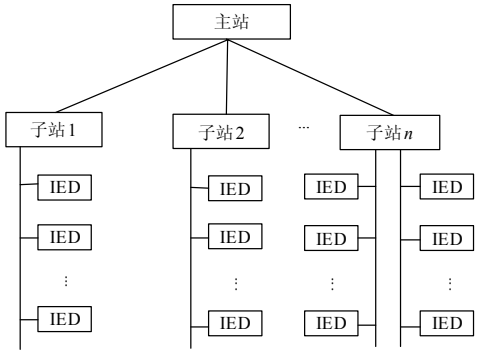

图1 智能配电网通信系统结构举例

Fig.1 Example communication system for smart distribution grid

3　访问控制方案

本方案采用基于身份的密码体制。在基于身份的密码系统中，用户或设备的公钥可由其唯一的身份信息确定，这样就避免了公钥目录的使用，而对应的私钥由一个可信任的密钥生成中心（Key Generation Center，KGC）来取得。在密码学的研究领域里，通常会有许多计算难题的假设，例如广泛使用的公钥密码算法RAS和DSA就分别基于因子分解的难题和离散对数的难题。基于身份的加密系统的困难问题则是双线性Diffie-Hellmen问题，更详细的描述见文献[11]。

3.1 系统初始化

设 q 为大素数，G_1 和 G_2 分别为 q 阶加法循环群

和乘法循环群，W 为 G_1 的生成元，映射 $\hat{e}: G_1 \times G_1 \to G_2$ 为双线性映射，系统主密钥 $s \in Z_q^*$ 是密钥生成中心KGC的私钥，$H_1: \{0,1\}^* \to G_1$ 是一个将任意长度的字符串映射到群 G_1 上的点的Hash函数。$H_2: \{0,1\}^* \to Z_\beta^*$ 是一个将任意长度的字符串映射到固定长度为 l 位的字符串Hash函数。公开 $<G_1, G_2, \hat{e}, W, H_1, H_2>$，同时规定一个供协议使用的对称加密算法（可使用传统的分组密码如DES或AES），其加密和解密操作分别表示为 $E_K(\cdot)$ 和 $D_K(\cdot)$。

3.2 节点密钥提取

节点密钥提取包括子站密钥提取和终端IED密钥提取两个部分。每个节点离线向密钥产生中心申请一个私钥/公钥对，密钥分配中心为子站节点和终端IED节点产生的私钥为 $IK = sH_1(ID)$，其中 $H_1(ID) \in G_1$ 为节点的公钥，ID 为节点的身份标示，例如设备的MAC地址或IP地址。为了简化表示，以后本文以 ID_i 来表示节点 i 的身份标示。考虑到配电网络子站与各终端IED之间的拓扑关系相对固定，在终端IED获取节点密钥的同时，密钥分配中心将其 ID 信息传输给所隶属的子站。

由于终端IED的计算能力相对有限，在为终端IED生成私钥/公钥对后，KGC并不直接将其私钥/公钥对注入终端IED节点，而是根据该终端IED所隶属的子站信息，首先利用双线性性质计算配电网络子站与该终端IED的共享密钥 $K = \hat{e}(sH_1(ID_{\text{Sub}}), H_1(ID_{\text{IED}}))$，然后将共享密钥并注入到终端IED中。

3.3 访问控制

协议总的目标是通信双方进行相互认证，从而达到访问控制的目的。协议由新配置到配电网的终端IED发起会话，具体执行步骤描述如下：

1）终端IED产生一随机数 n_j，向所属子站发出连接请求，其内容包含自己的 ID 信息。

2）子站收到终端IED的信息后，将执行如下操作：

（1）查询自己的 ID 信息数据库，若该终端IED的 ID 存在，则表明其是一有效的IED设备；否则协议终止；

（2）计算与终端IED的共享密钥 $K = \hat{e}(H_1(ID_{\text{Sub}}), sH_1(ID_{\text{IED}}))$；

（3）选择一个随机数 n_i，用 K 加密 n_i 和 n_j 并发送 $E_K(n_i, n_j)$ 给终端IED。

3）终端IED收到消息后，将执行如下操作：

（1）用 K 解密 $E_K(n_i, n_j)$ 求出 n_i 和 n_j；

（2）如果 n_j 与自己发送给子站的随机数一致，则确认对方为掌握 K 的实体，并将 n_i 发送给子站。

4）子站收到 n_i 后，比较 n_i 与原先自己产生的随机数是否相同。如果相同，则终端IED的合法性得到验证；否则，子站拒绝终端IED的连接请求。

4 实例应用分析

为了论述方便，应用实例采用物理电网结构相对简单的IEEE34节点系统。IEEE34节点系统见图2，详细参数见文献[15]。智能配电网的发展目标之一是解决大量分散的分布式电源在配电网中的运行问题，为了体现这一思想，假定在节点848、840以及890位置连接有不同容量和类型分布式电源DG。

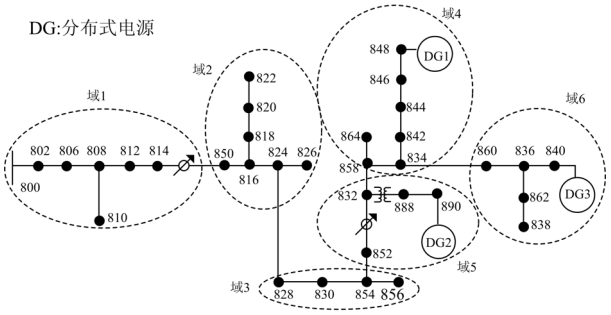

图2 IEEE34 节点馈线系统

Fig.2 IEEE34-node feeder power system

DG接入传统配电网，由于电网的双潮流特性，将对配电网的保护产生根本性的影响。如果以通信系统为支撑并利用多点信息，将极大地提高系统的可靠性。为了有效地监控三个分布式电源以及两个电压调压器，这里将系统被分割成六个监控域，并根据智能配电网通信系统三层网络模型建立如图3所示的通信网络。

信息通信技术给系统带来保护与控制便利的同时，也带来了安全隐患。在安全通信领域，访问控制具有重要的基础性作用。基于上述通信系统模型，利用本文提出的访问控制方案，能够保证非法使用的终端IED无法接入到系统中，从而阻止非法入侵者对系统的恶意攻击。分析如下：

首先，由于电力自动化系统严格的集中化管理等特点，子站和终端IED被配置到系统之前需要到KGC离线注册，并获得KGC颁发的私密钥，因此，

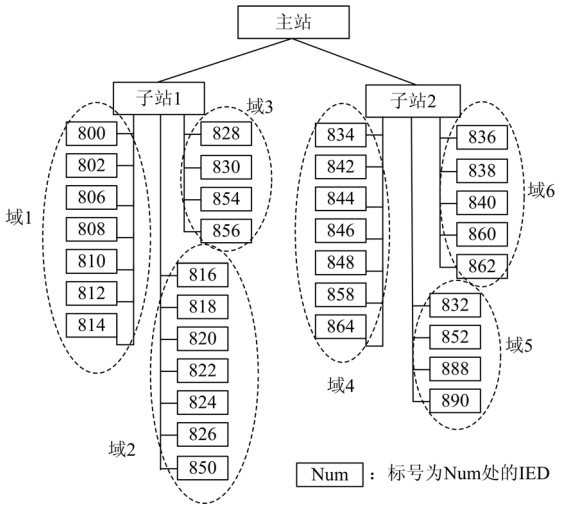

图3 IEEE34节点馈线系统通信系统结构

Fig.3 Communication system for IEEE34-node feeder power system

子站和终端IED的隶属关系通过KGC被建立起来。由于方案使用了基于身份的密码体制，因此，根据双线性性质，子站利用终端IED设备的身份信息即可计算出与终端IED设备的共享密钥K，即

$$K=\hat{e}(H_1(ID_{\text{Sub}}),sH_1(ID_{\text{IED}}))=\hat{e}(sH_1(ID_{\text{Sub}}),H_1(ID_{\text{IED}}))$$

对于终端IED设备来说，由于在会话期间双方始终没有传递密钥K，因此该机制也阻止密钥K的泄露问题，简化了系统实现的复杂度。

其次，协议使用了询问-应答机制。随机数n_i为子站向IED发出的询问，n_j为IED向子站发出的询问，使用对称密码算法，如果子站和IED能分别正确解密n_i和n_j，则子站和终端IED能验证它们是共享密钥的实体，并成功地完成双方实体认证。运行了密钥建立协议。由于询问-应答机制属于强实体认证机制，非授权的设备则无法获得正确的密钥，从而无法完成询问-应答过程，该机制阻止了非授权使用的IED接入智能配电系统。

最后，由于终端IED设备在访问控制的协议执行过程中只需要执行对称密码算法，减轻了终端IED设备的计算和通信开销，从而简化了系统实现的复杂度和实施的难度。

5　结语

本文在智能配电网通信系统结构设计的基础上，针对智能配电网存在的信息安全问题，采用基于身份的密码体制，提出了一种适合智能配电网通信系统的访问控制方案。该方案减轻了终端IED设备的计算和通信开销，同时实现了设备的合法性认证问题。尽管只是针对智能配电网而提出，该方案所基于的理论体系可很容易推广应用到智能电网信息安全的其他层次，从而为解决智能电网信息安全问题提供了一种新思路。

参考文献

[1] Wang J，Huang A Q，Sung W，et al. Smart grid technologies[J]. IEEE Industrial Electroncs Magazine，2009，3（2）：17-23.

[2] Farhangi H. The path of the grid[J]. IEEE Power and Energy Magazine，2010，8（1）：18-28.

[3] 余贻鑫，栾文鹏. 智能电网述评[J]. 中国电机工程学报，2009，29（34）：1-8.
YU Yi-xin，LUAN Wen-peng. Smart grid and its implementations[J]. Proceedings of the CSEE，2009，29（34）：1-8

[4] Metke A R，Ekl R L. Security technology for smart grid networks[J]. IEEE Trans on Smart Grid，2010，1（1）：56-64.

[5] Ericsson G. Cyber security and power system communication-essential parts of a smart grid infrastructure[J]. IEEE Trans on Power Delivery，2010，25（3）：1501-1507.

[6] IEC （International Electrotechnical Commission），Power system control & associated communications-data &communication security[S]. IEC62351 part 1 to 7，Technical Specification，2007.

[7] 孙中伟，马亚宁，王一蓉，等. 基于EPON的配电网自动化通信系统及其安全机制研究[J]. 电力系统自动化，2010，34（8）：72-75.
SUN Zhong-wei，MA Ya-ning，WANG Yi-rong，et al. Communication system for distribution automation using EPON and its security[J]. Automation of Electric Power Systems，2010，34（8）：72-75.

[8] SUN Zhong-wei，HUO Si-tian，MA Ya-ning. Security mechanism for smart distribution grid[C]. //The 2nd IEEE International Conference on Advanced Computer Control. 2010：967-971.

[9] Lim I H，Hong S，Choi M S，et al. Security protocols against cyber attacks in the distribution automation system[J]. IEEE Trans on Power Delivery，2010，25（1）：448-455.

[10] Hamlyn A，Cheung H，Mander T，et al. Computer network security management and authentication of smart grids operations[C]. //IEEE Canada Electrical Power Conference. 2008：31-36.

（下转第 125 页　continued on page 125）

的计算时间比仅依赖常规遗传算法随机操作的计算时间明显减少。

4　结论

运行配电网络具有图论中树的性质，网络重构优化的实质是在初步连接图的基础上寻找最优的生成树或某组树。根据该特点，本文设计了基于图论的改进遗传算法，采用基于环路和破圈法产生初始种群和进行交叉、变异操作，在产生初始解和变异操作时避免了不可行解的产生，在交叉操作时避免或大大减少了不可行解的产生，从而提高了算法的计算效率。

参考文献

[1] 黄彦浩，李晓明. 配电网重构遗传算法的不可行解问题研究[J]. 电力建设，2004，25（3）：23-27.
HUANG Yan-hao，LI Xiao-ming. Study on infeasible solution of distribution network reconfiguration genetic algorithm[J]. Electric Power Construction，2004，25（3）：23-27.

[2] 周辉，王击，罗安，等. 克隆遗传算法与模拟退火算法相结合的配电网络重构[J]. 继电器，2007，35（7）：41-45.
ZHOU Hui，WANG Ji，LUO An，et al. Distribution network reconstruction based on the combination of CGA and SA[J]. Relay，2007，35（7）：41-45.

[3] 麻秀范，张粒子. 基于十进制编码的配网重构遗传算法[J]. 电工技术学报，2004，19（10）：65-69.
MA Xiu-fan，ZHANG Li-zi. Distribution network reconfiguration based on genetic algorithm using decimal encoding[J]. Transactions of China Electrotechnical Society，2004，19（10）：65-69.

[4] 黄健，张尧，李绮雯. 蚁群算法在配电网重构的应用[J]. 电力系统及其自动化学报，2007，19（4）：59-64.
HUANG Jian，ZHANG Yao，LI Qi-wen. Application of ant colony system in distribution reconfiguration[J]. Proceedings of the CSU-EPSA，2007，19（4）：59-64.

[5] 杨建军，战红，陈宪国. 基于遗传算法并避免不可行解的配电网络重构优化[J]. 电力系统保护与控制，2008，36（17）：43-46.
YANG Jian-jun，ZHAN Hong，CHEN Xian-guo. Optimization of distribution network reconfiguration of avoiding infeasible solutions based on genetic algorithm[J]. Power System Protection and Control，2008，36（17）：43-46.

[6] 刘健，毕鹏翔，董海鹏. 复杂配电网简化分析与优化[M]. 北京：中国电力出版社，2002：39-40.
LIU Jian，BI Peng-xiang，DONG Hai-peng. Simplified analysis and optimization of complicated distribution networks[M]. Beijing： China Electric Power Press，2002：39-40.

[7] 刘缵武. 应用图论[M]. 长沙：国防科技大学出版社，2006：15-17.
LIU Zuan-wu. Applied graph theory[M]. Changsha：National University of Defense Technology Press，2006：15-17.

[8] 刘莉，陈学允. 基于模糊遗传算法的配电网络重构[J]. 中国电机工程学报，2000，20（2）：66-69.
LIU Li，CHEN Xue-yun. Reconfiguration of distribution networks based on fuzzy genetic algorithms[J]. Proceedings of the CSEE，2000，20（2）：66-69.

收稿日期：2010-04-30

作者简介：

杨建军（1977-），男，博士，副教授，研究方向为系统工程优化、优化算法；E-mail：yjjdem@163.com

战　红（1978-），女，硕士，讲师，研究方向为电力系统优化与控制。

（上接第 121 页　continued from page 121）

[11] Mao W. Modern cryptography：theory and practice[M]. NJ：Prentice-Hall，2004.

[12] Shamir A. Identity based cryptosystems and signature schemes. Lecture Notes in Computer Science[M]. New York：Springer-Verlag，1984：47-53.

[13] Boneh D，Franklin M. Identify-based encryption from the weil pairing[J]. SIAM Journal of Computing，2003，32（3）：586-615.

[14] Chen L，Cheng Z，Smart N P. Identity-based key agreement protocols from pairings[J]. International Journal of Informtion Security，2007，6（4）：213–241.

[15] Kersting W H. Radial distribution test feeders[C]. //Proceedings of IEEE PES Winter Meeting. Columbus（USA）：2001：908-912.

收稿日期：2010-04-06；　修回日期：2010-09-06

作者简介：

孙中伟（1970-），男，博士，副教授，从事电力系统信息安全的理论与应用研究；E-mail：zwsun@ncepu.edu.cn

张荣刚（1985-），男，硕士研究生，研究方向为网络与信息安全等。