基于智能计量系统的会话密钥管理方案

简富俊[1,3]，曹敏[2]，张建伟[2]，毕志周[2]，孙中伟[3]，王洪亮[4]，王磊[2]
（1. 华北电力大学云南电网公司研究生工作站，昆明 650217；
2. 云南电网公司电力研究院，昆明 650217；
3. 华北电力大学电气与电子工程学院，北京 102206；
4. 云南电网公司博士后工作站，昆明 650217）

摘要：分析了AMI网络结构和该结构下的安全问题。针对通信供应商提供的安全机制和DL/T698安全机制所存在的问题，本文采用属性基加密的方案解决高级量测体系中的会话密钥管理问题，能够有效解决AMI广播中需要多次加密的问题，并能保障AMI系统信息的私密性，对AMI系统建设有参考意义。

关键词：AMI；基于属性加密；网络结构；会话密钥管理

A Research on Session Key Management in Advanced Metering Infrastructure

JIAN Fujun[1,3], CAO Min[2], ZHANG Jianwei[2], BI Zhizhou[2], SUN Zhongwei[3],
WANG Hongliang[4], WANG Lei[2]
Graduate Workstation of North China Electric Power University & Yunnan Power Grid Corporation, Kunming 650217;
2. Yunnan? Electric Power Research Institute, Kunming 650217;
3. North China Power And Electricity University, Beijing 102206;
4. Post Doctor Workstation of Yunnan Power Grid Corporation, Kunming 650217)

Abstract: Advanced metering infrastructure brings new challenges to power grid. This paper analyzes the AMI network structure and the security issues in this structure of. In order to achieve security under the security mechanisms of Communications providers and security mechanisms of DL/T698, this paper uses attribute-based encryption solutions to address session key management issues in advanced metering infrastructure, which can solve the efficiency problem of many times encryption when primary station broadcast. The issue also protects the confidentiality of AMI. This paper can achieve a reference value to the construction of AMI.

Key words: AMI, Attribute Based Encryption, Network structure, Session key management
中图分类号：TM76 **文献标识码**：B **文章编号**：1006-7345（2014）02-0053-04

1 前言

高级量测体系（Advanced Metering Infrastructure，AMI）利用智能电表、双向通信网络、计量数据管理系统和用户户内网来构建电网公司和用户及时信息交互的平台，能够为电力用户提供实时的电价信息，方便电力用户调整自己的用电策略，是智能电网建设的第一步。

目前，国内计量自动化主站到现场终端之间的安全性主要依托于DL/T698提供的关于用户使用16字节的密码，并使用询问相应机制提供身份认证功能。但是该协议并未提供群组加密的功能，在下发消息或指令时，需要针对每一个终端设备进行加密，造成计算开销大的问题。

为了解决AMI主站下发消息时计算开销大的问题，以下使用基于属性加密（Attribute Based Encryption，ABE）的方案来实现智能计量下会话密钥管理功能和访问控制功能。能有效降低群组信息发布时服务器的计算复杂度，并能抵抗合谋攻击。

2 AMI网络结构与安全性分析

AMI系统由计量数据管理系统（Meter Database Management system，MDMS）、双向通信网

络、智能电表和用户户内网四部分组成，网络结构如图 1 所示。图中主站系统通过网络接入技术接入到光纤专网、3G/GPRS/CDMA 无线公网、230MHZ 无线专网和中压电力线载波专网等网络。图中 M 表示智能电表。主站通过通信信道提供的网络和现场终端交互，在一些特殊环境下甚至可以支持直接和智能电表交互。交互终端提供信息交换和管理的功能。自助服务终端提供电力公司信息发布和用户信息查询的功能。智能电表除了提供传统电表的计量功能外，其作为用户侧网关还具备用户户内网的管理功能。

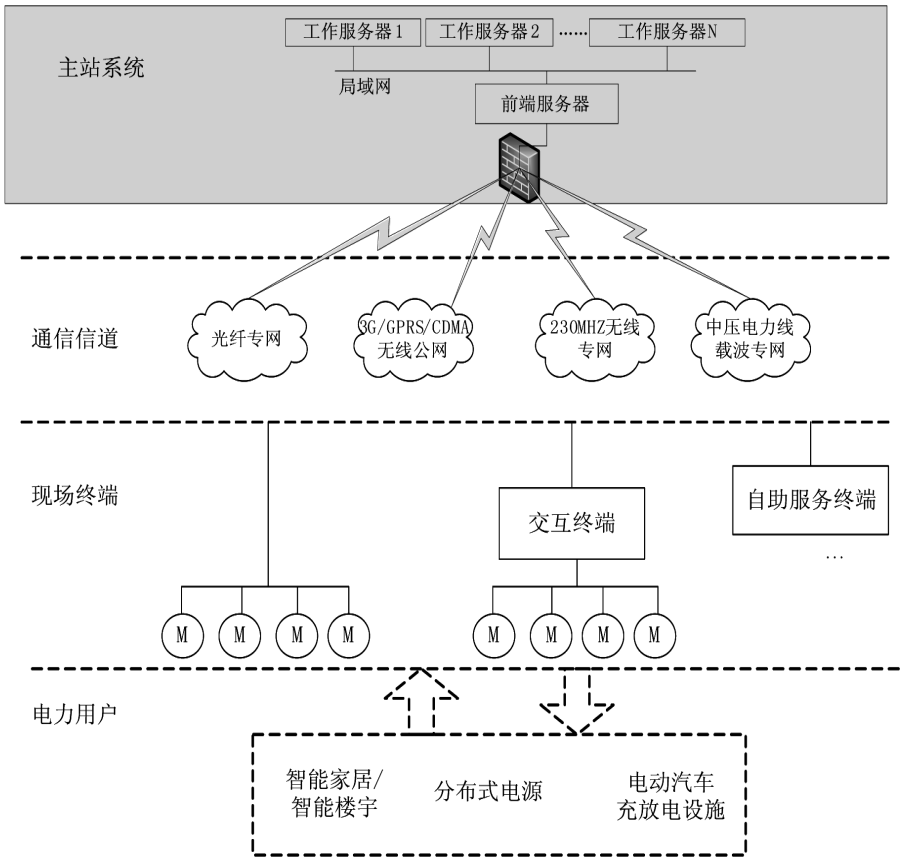

图 1　AMI 网络结构图

从图中可以看出主站到智能电表间的安全性主要依赖于通信信道提供方既有的安全机制和电力系统信息传输所采用的安全机制。以 GPRS 为例，其存在安全方面的一些缺陷，如认证是单向的，加密密钥太短[1]。并且移动台和 SGSN（Serving GPRS Support Node）之间使用对称加密方式通信，如果电力系统信息传输没有相应的安全机制，则会导致通过 GPRS 传送的电力信息对于通信服务提供方来说是透明的。目前主站到智能电表侧安全性主要依赖于 DL/T698 的安全性。DL/T698 使用 16 字节的密码，并使用询问相应机制提供身份认证功能。但是对于具有相同属性的用户操作仍然需要对每一个用户分别进行操作，这样在大量消息的群发、广播时，对服务器的要求较高。而电力系统的管理往往是针对群组的操作，例如：对某一个小区所有用户进行抄表、对某一地区的商业用户进行抄表、对特殊用户发送通知等。本文采用 ABE 的方案解决 AMI 系统群组超标时需要多次加密发送的问题，并保证了 AMI 系统的私密性。

3　ABE 理论基础

3.1　双线性映射

$G1$，$G2$ 和 T 是两个 p 阶的乘法循环群，一个双线性映射，e：$G_1 \times G_2 \rightarrow GT$ 有如下特性：

1）双线性：对于所有的 $g_1 \in G1$，$g_2 \in G2$ 和 a，$b \in z_p{}^*$ 有 $e(g_1{}^a, g_2{}^b) = e(g_1, g_2)^{ab}$。

2）非退化性：$e(g_1, g_2) \neq 1$。

3）可计算性：对于所有的 $g_1 \in G1$，$g_2 \in G2$ 有一个有效的算法计算 e（g_1，g_2）。

3.2　访问控制树

假设 τ 是一棵表示访问结构的树。每一个非叶子节点代表一个用子节点和门限值表示的门限（threshold gate）。用 num_x 表示节点 x 的子节点个数，k_x 表示门限值，则 $0<k_x \leqslant num_x$。当 $k_x=1$ 时，门限是一个门，当 $k_x=num_x$ 时，门限是一个 AND 门。访问控制树的每个叶子节点 x 用一个属性描述且门限值 $k_x=1$。

为了使得访问控制树更好地工作，定义几个函数。用 *parent*（x）表示 x 节点的父节点。在是叶子节点的时候 *att*（x）表示访问控制树中和 x 相关的属性。访问控制树在每个节点的子节点间定义了顺序，也就是，每个节点的子节点用 1 到 *num* 的数字编号。函数 *index*（x）返回一个和节点相关的数字。这个数字作为一个给定的密钥是一个以随机方式分发给访问控制树节点的唯一的值。

假设 τ 是一个以 r 为根节点的访问控制树。以 x 节点为根节点的树 τ 的子树用 τ_x 表示。因此 τ 和 τ_r 相同。如果属性集 γ 满足访问控制树 τ_x，我们把他表示为 $\tau_x(\gamma)=1$。我们按以下步骤计算 $\tau_x(\gamma)$。如果是一个非叶子节点，对于 x 节点的所有子节点 x' 计算 $\tau_{x'}(\gamma)$。当且只当至少 k_x 个子节点返回 1 时 $\tau_x(\gamma)$ 返回 1. 当 x 是叶子节点的时候，$\tau_x(\gamma)$ 只有当 $att(x) \in \gamma$ 时返回 1。

3.3　拉格朗日插值定理

设 q 是一个素数，$f(x)$ 是一个 k 阶多项式；设 j_0，K，j_k 是 z_p 上的不同元素。设 $f_0=f_{j0}$，K，$f_k=f_{jk}$ 利用拉格朗日插值定理，我们可以得多项式 $f(x)$ 表示成：$f(x)=\sum_{t=0}^{k}(f_t \cdot \lambda_t(x))$

其中 $\lambda_t(x)=\prod_{0\leqslant i\neq t\leqslant k}\frac{j_i-x}{i_i-i_t}$，$t=0$，$K$，$k$ 为拉格朗日系数。

4　密钥管理方案

采用 CP－ABE（ciphertext policy attribute based encryption）实现 AMI 主站到智能电表侧的密钥管理和访问控制，用户的密钥是一组属性，存放在智能电表中等职能设备中，主站系统使用一棵访问控制树来加密明文，智能电表使用自己获得的属性解密密文。算法如下：

初始化：选择一个 p 阶的生成元为 g 的双线性组 G_0，然后选择两个随机数 α，$\beta \in z_p$，公共参数 $PK=G_0$，g，$h=g^{\beta}$，$f=g^{1/\beta}$，$e(g,g)^{\alpha}$ 主密钥 $MK=(\beta, g^{\alpha})$。（注意：f 只用于授权。）

加密（PK，M，τ）：计算：

$$CT=(\tau, \widetilde{C}=Me(g,g)^{\alpha s}, C=h^s, \forall y \in Y: C_y=g^{q_y(0)}, C'_y=H(att(y))^{q_y(0)})$$

其中 Y 是 τ 中的叶子节点的集合。$H:\{0,1\}^{*}\rightarrow G_0$ 是一个随机预言函数。

密钥生成（MK，S），S 是一组属性集合。算法首先选择一个随机数 $r \in z_p$，然后对每一个属性 $j \in S$ 选择一个随机数 $r_j \in z_p$。计算：

$$SK=(D=g^{\frac{\alpha+\gamma}{\beta}}, \forall j \in S: D_j=g^r \cdot H(j)^{r_j}, D'_j=g^{r_j})$$

授权（SK，$\widetilde{S}$）在该算法中 $\widetilde{S} \subseteq S$。该算法首先选择随机数 $\tilde{r}$ 和 $\widetilde{rk}\ \forall k \in \widetilde{S}$，然后生成新密钥：

$$\widetilde{SK}=(\widetilde{D}=Df^{\tilde{r}}, \forall k \in \widetilde{S}: \widetilde{D_k}=D_k g^{\tilde{r}} H(k)^{\widetilde{rk}}, \widetilde{D_K'}=D'_k g^{\widetilde{rk}})$$

解密（CT,SK）：如果节点 x 是叶子节点，我们设 $i=att(x)$，计算：

$$DecryptNode(CT,SK,x)=\begin{cases}\dfrac{e(D_i,C_i)}{e(D'_i,C'_i)}=e(g,g)^{rq_x(0)} & \text{如果 } i \in S\\ \perp & \text{其他情况}\end{cases}$$

对于其他节点，我们由下到上递归得到：

$$F_x=\prod F_z^{\Delta iS_x'(0)}=e(g,g)^{r,qx(0)}$$

其中 $i=\mathrm{index}(z)$，$S'_x=\{\mathrm{index}(z): z \in S_x\}$。接下来对根节点使用该算法得到 $A=DecryptNode(CT;SK;r)=e(g,g)^{r\cdot s}$。最后计算：

$$\widetilde{C}/(e(C,D)/A)=\frac{\widetilde{C}}{e(h^s,g^{\frac{\alpha+\gamma}{\beta}})/e(g,g)^{r\cdot s}}=M$$

从而得到明文 M。

该方案属于非对称密码体制，一般明文 M 用于传输系统的会话密钥，而不直接用于传送数据。系统所需要交互的信息根据不同 AMI 系统设计使用对称密码算法加密，例如 DES、3DES、TDEA 等。

方案流程如下：

1）主站系统中使用初始化算法生成系统的公共参数和主密钥 $\{PK, MK\}$；

2）主站系统根据智能电表的属性 S 和 MK，生成智能电表的私钥 SK，并通过安全方法将 $\{PK, SK\}$ 下载到智能电表中；

3）如果智能电表需要在自己所具有的权限范围内给其它设备授权则使用自己的私钥 SK 和授权算法生成子密钥 SK；

4）当主站系统需要向用户发送信息时，使用对称密码算法和会话密钥 SessionKey 加密待传送的信息；然后使用 ABE 加密算法加密会话密钥。并把加密过的信息和会话密钥进行定向广播；

5）当智能电表接收到广播的消息后，只有属性密钥符合访问控制树的智能设备才能解密出会话密钥，从而解密出主站传送的明文消息。

6）同理，当某合法用户需要发送消息给主站时重复第 4 个步骤，合法用户收到消息后可以重复第 5 步获取消息。

5　结束语

综上所述在 AMI 系统中采用了 CP-ABE 的方案解决主站到智能电表的会话密钥管理问题，该方案能有效降低 AMI 主站系统在群组通信中加密的复杂度，实现一次加密多用户解密，支持智能设备授权，并且能有效防止合谋攻击。方案不依赖于特定的通信方式，能够在不同的通信环境下提供可靠的安全保障。希望本文对 AMI 建设的安全研究有一定借鉴意义。系统能解决 AMI 系统的私密性、访问控制问题，但是对于可验证性和完整性问题并未讨论，如何保证系统的完整性和可验证性将是将来的工作重点。

参考文献：

[1] 单广玉，范晓晖，杨义先，GPRS 系统的安全性分析［J］，电信科学，2002（12）：35-38.

[2] 余贻鑫．智能电网的技术组成和实现顺序［J］．南方电网技术，2009，3（2）：1-5.

[3] 曾梦岐，卿昱，谭平璋，杨宇等，基于身份的加密体制研究综述［J］．计算机应用研究，2010（27）：27-31.

[4] J. Bethencourt，A. Sahai，B. Waters. Chiphertext-policy attribute-based encryption［C］，IEEE Symposium on Security and privacy. 2007：321-334.

[5] 王文强．属性基加密及签名体制的研究［D］．郑州：解放军信息工程大学，2010.

[6] Shucheng Yu，Kui Ren，Wenjing Lou. FDAC：Toward fine-grained distributed data access control in wireless sensor networks［J］．IEEE Transactions on Parallel and Distributed Sysems. 2011，22（4）：673-686.

[7] 曾鸣．电力需求侧管理［M］．北京：中国电力出版社，2001：200-210.

[8] Doshi，Nishant，Jinwala. Constant ciphertext length in multi0-authority Ciphertext Policy Attribute Based Encryption［C］．Computer and Communication Technology（ICCCT）．2011：451-456.

收稿日期：2014-01-12

作者简介：

简富俊（1988），男，硕士研究生，华北电力大学云南电网公司研究生工作站，研究方向为电子与通信工程（e-mail）hdjianfujun@163.com。

1 月 9 日，山东一建丰汇设备公司承揽的“华能莱芜电厂 2X1 000 MW 1 号机组二次再热塔式锅炉钢结构”项目关键构件制作完成，达到发货条件。

此项目是国内首台百万千瓦二次再热塔式锅炉钢结构。其箱型柱截面尺寸大、单体重量近 130 t，内部结构异常复杂，质量标准要求严格，制作难度前所未有。在没有前期任何相关检验借鉴的情况下，丰汇设备公司凭借长期积累的丰富的生产经验，克服大型结构件焊接、翻身等诸多困难，从前期策划到过程控制，均高标、严要求，不断调整细化工艺，按照“特种设备制作”要求进行钢结构制作，产品质量水平不断提高。

目前，该项目顺利完成一层、二层钢构制作，第三层工作也已过半，争取春节前完成，为保证莱芜项目按计划安装打下坚实的基础。

（信息来源：北极星电力网新闻中心）