

智能电网中面向安全计量的数据聚合方案

朱 丹, 温 蜜

(上海电力学院计算机科学与技术学院, 上海 200090)

摘要: 针对现有的大部分学者主要关注用电数据的安全性而忽略了数据的可用性, 而在实际电力系统的应用中大部分只关注数据的可用性而忽视了数据安全性的问题, 基于门限ElGamal同态加密和动态加密提出了一种面向安全计量的数据聚合方案。本方案既能保护智能电能表数据的安全性, 同时由于扩展数据聚合的层次, 提高了数据可用性, 又便于电网运营人员对社区用电情况进行分析。通过与其他电能安全计量方案对比分析, 该方案能够在保护用户隐私的前提下保证电网运营人员能够对用户用电需求进行了解, 这将有助于电力负荷预测。

关键词: 智能电网; 同态加密; 隐私保护; 电能数据使用; 数据聚合

Data aggregation Scheme for Secure Metering in Smart Grid

ZHU Dan, WEN Mi

(College of Computer Science and Technology, Shanghai University of Electric Power,
Shanghai 200090, China)

Abstract: Most of the existing scholars mainly focus on the security of power consumption data and ignore the availability of data. In the application of actual power system, most of them only pay attention to the availability of data and ignore the problem of data security. Based on the threshold ElGamal homomorphic encryption and dynamic encryption, a data aggregation scheme for security metering is proposed. This solution not only protect the security of smart meter data, but also improve the data availability by expanding the level of data aggregation, and it is convenient for grid operators to analyze the community power consumption. By comparing and analyzing with other electric energy safety measurement schemes, the scheme can ensure that the grid operators can understand the user's electricity demand while protecting the user's privacy, which will help the power load forecasting.

Key words: smart Grid; homomorphic encryption; privacy protection; energy data usage; data aggregation

0 引言

随着我国特高压电网的建设和电力体制改革的不断深化, 智能电网已经成为我国电网发展的新方向。智能电网是将信息技术、通信技术、计算机技术、先进的电力电子技术、可再生能源发电技术和原有的输配电基础设施高度集成的新型

电网, 实施智能电网发展战略不仅能使用户获得高安全性、高可靠性、高质量、高效率 and 价格合理的电力供应, 还能提高国家的能源安全, 改善环境, 推动可持续发展, 被世界各国视为推动经济发展和产业革命, 实现可持续发展的新基础和新动力^[1-3]。

智能电能表^[4]则是智能电网的客户终端, 但是其已经不是传统意义上的电能表, 除了具备传统电能表基本用电量的计量功能以外, 还具有多种

国家自然科学基金 (61572311); 国家自然科学基金 (61602295);
上海市曙光计划 (16SG47)

数据传输模式的通信等智能化功能,由于用电情况被十分详细地记录,智能电表也将产生大量数据,这将有助于电网运营人员详细掌握用户的用电状况,对未来供电进行更好的规划,减少电能浪费并提高电网的稳定性^[5]。

但是,通过智能电网传输的消息可能包含用户的隐私信息^[6]。例如,通过图1用户每日用电曲线可以很容易地分析出用户所使用的电器,进而分析出用户家里的人员数目和行为。如果这些信息被非法利用,将给用户带来很多害处。

在学术领域,对用户隐私数据保护,防止外部和内部攻击者获取用户隐私已有大量研究,这些研究主要集中在如何更加安全地对用户数据传输进行保护,或是对隐私数据进行聚合保护。单纯进行数据传输的保护无法防止内部攻击者获取隐私数据^[7],数据聚合保证了用户隐私不被外部和内部攻击者获取,但是这将给电网运营带来极大困扰。在实际的电网运营中,运营人员并不希望看到完全聚合加密的数据,如图2所示,无法知道一些具体社区的细粒度用电数据将无法使运营人员了解区域的用电情况,从而无法精确地指导未来配电网的智能发供电和电网的升级改造。然而若是只考虑数据可用性,用户隐私很有可能被内部攻击者泄露^[8],单方面考虑信息安全或者可用性都不适应现实需求。

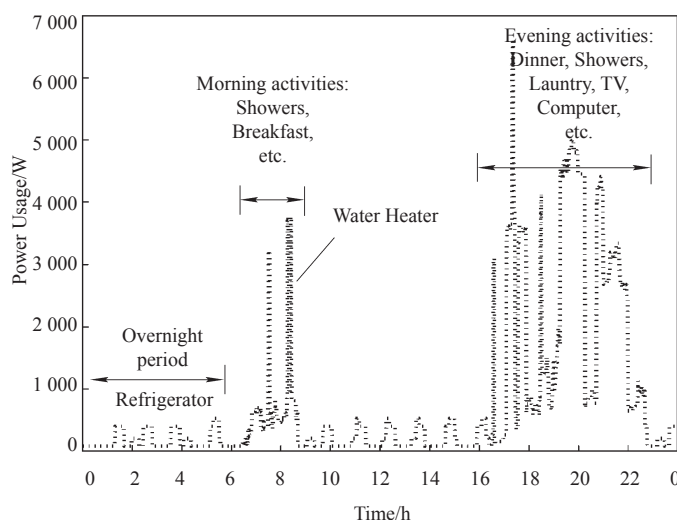


图1 用户用电信息泄露了隐私

Fig.1 User power information leaked privacy

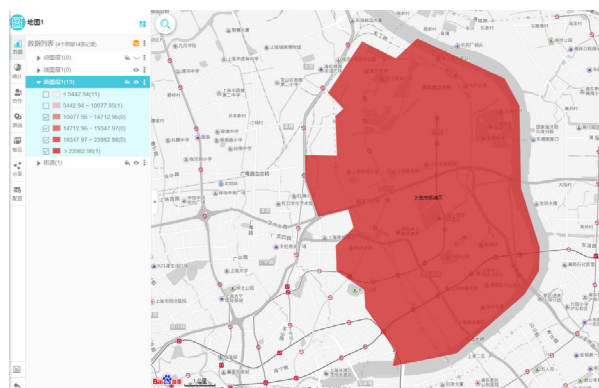


图2 其他聚合方案在大屏中显示

Fig.2 Aggregated data is displayed in a large screen

为了在保护用电数据应对内外攻击的基础上,便于用电情况分析等实际应用的需要,本方案在文献[9]的基础上,进行了层次化的扩展,在同样用户数目下将聚合层次扩展为三层,将密钥聚合任务由中心转移给网关,利用ElGamal加密技术^[10],待电表数据生成之后,在电表表中进行同态加密,然后再利用互联网将加密的数据传到网关,利用ElGamal加密的特性,可以在网关对加密数据进行多个用户总用电量的聚合计算,从而在单个电表电量未知的情况下得到聚合的数据。网关到信息中心的数据通过动态加密技术^[11]进行数据传输,保证数据安全和数据传输效率。本方案的主要优势在于:将用户用电数据进行加密聚合,保护用户用电数据的隐私,而且相比其他聚合方案,在同样用户数目下可以获得某区域细粒度数据,如图3所示(注:现有数据加密传输方案可以在获取所有用户用电信息情况下做到图3的

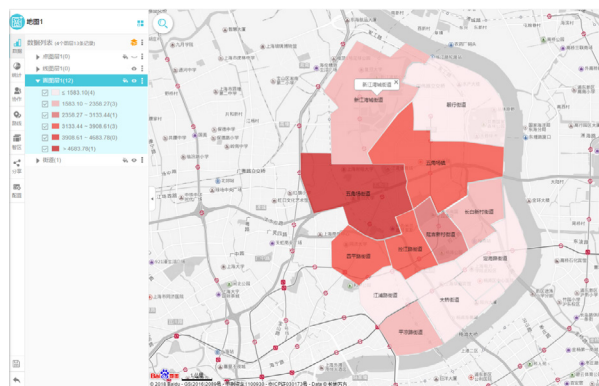


图3 本方案数据在大屏中显示

Fig.3 The scheme data is displayed in a large screen

分区计量，但是无法防止电力运营商内部攻击者泄露用户隐私，本方案利用加密聚合实现图3，可以防止内部攻击），能在未知用户具体用电数据的情况下，对用户用电情况进行了解，为电网升级改造提供参考。

本文首先简述智能电网计量系统国内外研究现状，阐述门限ElGamal密码系统和动态密钥加密以及智能电网安全计量方案，然后对系统性能和安全性进行分析，最后对全文进行总结。

1 国内外研究现状

文献[12]介绍了一种三层网络拓扑结构，网关利用同态加密，对电能表数据先加密，然后向控制中心上传。为了保证数据前向安全，网关和控制中心通过旧密钥计算出新密钥，无须每次进行交互。这种方案控制中心拥有所有用户的详细数据，对内部攻击者无法保障用户数据隐私安全，而且控制中心拥有所有经过同态加密的数据，数据处理和存储压力太大。

文献[13]提出了一个匿名的多维数据聚合方案。在该方案中，每个用户的计算成本与收集的数据类型数量是独立的。此外，通过使用批量验证技术，信息中心的计算成本可以降低。但是，此方案只实现了签名的聚合，并没有实现对加密数据的聚合操作，且交互很多，各用户被动提交数据，增加了通信负荷。

文献[14]为智能电网设计了分散式安全框架，并具备数据聚合和访问控制的能力。用户的隐私安全是通过数据加密传输来实现的，且使用同态加密对加密数据执行聚合任务。其中访问控制的细节描述得很清晰，尤其是用户如何通过远程终端访问数据，但是该工作尚未对基于云的数据存储和计算部分以及云如何对加密数据实施聚合进行描述，而且KDC负责网关和电能表密钥管理，一旦被攻破，所有用户隐私数据将会被泄露。

文献[15]利用两次不同形式的数据扰动实现了数据对基站以及网内其他节点的隐私保护，基站只能得到聚合的实际数据，节点也只能得到子节点的聚合数据，防止了基站入侵对数据隐私的

泄露，同时二次扰动防止了对邻居节点的隐私保护。此方案中基于随机密钥的分配方法中密钥池如果被攻击者获取，将威胁整个系统，且每个节点负责数据收集、数据加密、数据聚合和数据加密传输，实际中节点不一定能胜任如此多的工作。

文献[9]中提出一种电能表定期上传经过同态加密的用电数据给运营商，运营商可以获得所有电能表的聚合明文数据，但是无法获得单个用户的用电数据，这样保护了用户的用电隐私，即便是电网运营人员也无法获得用户的用电数据。但是此方案拓扑结构只有两层，这使网关（或中心）的数据存储和处理压力很大，无法处理区一级以上的用户范围。本方案在文献[9]的基础上进行层次化扩展，将电能表划分到较小邻域内，电能表的加密数据定期上传到负责邻域的网关内，网关负责数据的聚合，网关到信息中心的数据通过动态加密技术进行数据安全传输，最终经过动态加密的历史数据存储在云中，减少信息中心存储压力。

2 本方案使用的密码系统

2.1 门限ElGamal加密方案

在一个有 n 个成员的公钥密码系统中，密钥 x 被分成 n 份： $x_1, x_2, \dots, x_n$ ，每个密钥 x_i 被不同的 n 个成员所拥有。只有当这 n 个成员合作时，才能解密密文^[10]。在门限ElGamal密码系统中，私钥被分成 n 份，生成公钥和私钥不需要可信方。

该密码系统的工作流程如下。

1) 初始化。选择两个大素数 p 和 q ，使 $q|p-1$ 。然后选择生成元为 g 的 q 阶乘法群 $G \in Z_p^*$ ，然后公布 g, p 和 q 。

2) 密钥生成阶段。每个成员 P_i 取一个随机数 $x_i \in Z_q^*$ ，并相应地计算自己的公钥 $y_i = g^{x_i} \bmod p$ ，并将 y_i 公布，然后每个成员计算公钥 y ，即

$$y = \prod_{i=1}^n y_i \bmod p \quad (1)$$

3) 加密阶段。每 m 个成员（例如 P_i ）选择随机数 $r_i \in Z_q^*$ ，计算

$$c_i = g^{r_i} \bmod p \quad (2)$$

$$d_i = g^{m_i} y_i^{r_i} \bmod p \quad (3)$$

将自己的明文 m_i 加密为 $E_y(m_i) = (c_i, d_i)$ ，并将其发送给聚合方。聚合方计算

$$c = \prod_{i=1}^n c_i \bmod p \quad (4)$$

将 c 发送给每个成员。每个成员计算

$$T_i = c^{x_i} \bmod p \quad (5)$$

将 T_i 发送给聚合方。

4) 解密阶段。聚合方计算

$$d = \prod_{i=1}^n d_i \bmod p \quad (6)$$

$$T = \prod_{i=1}^n T_i \bmod p \quad (7)$$

最终通过 d 和 T 计算聚合解密的结果，即

$$\begin{aligned} & dT^{-1} \\ &= g^{\sum m_i} y^{\sum r_i} c^{-\sum x_i} \bmod p \\ &= g^{\sum m_i} g^{\sum x_i \sum r_i} g^{\sum r_i (-\sum x_i)} \bmod p \\ &= g^{\sum m_i} \bmod p \\ & \sum m_i = \log_g (dT/T) \end{aligned} \quad (8)$$

2.2 动态密钥加密

动态密钥加密是Master和Slave的对称密钥加密通信，一般是在固定间隔内定时通信^[11]。

Master和Slave使用Diffie-Hellman^[16]密钥交换法生成初始密钥str，共享密钥由Master和Slave通过str以相同计算方法计算出。之后Slave通过共享密钥加密数据并传输给Master，并在传输后更新密钥，Master接收数据进行解密，并用同样的方法更新自身的密钥。

在动态密钥加密中使用哈希函数、XOR等方法降低计算量。在本方案中，信息中心代表Master，网关代表Slave。

3 智能电网安全计量方案

3.1 系统架构

本方案系统结构由智能电能表、邻域管理网关、信息中心和云组成，如图4所示。系统数据传输主要分成两部分，电能表到网关间数据聚合是第一部分，使用门限ElGamal加密，网关到信息中心和云的数据传递是第二部分，使用动态密钥加密。

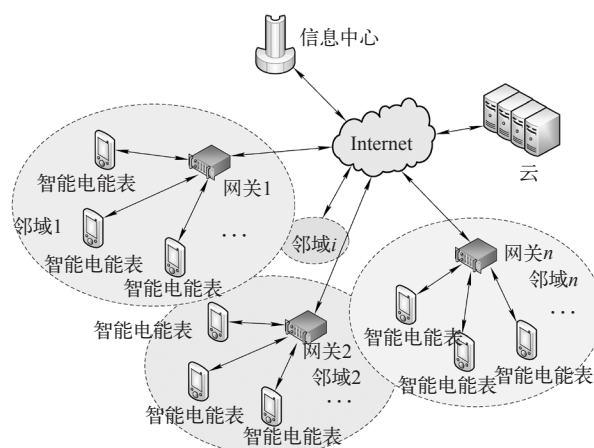


图4 系统架构

Fig.4 System model

每个用户的智能电能表定期向自己所属的网关发送加密的用电数据，网关将自己所得加密的用电数据进行聚合解密操作。获得聚合结果后，利用动态加密，将各网关聚合数据上传到信息中心，信息中心负责对数据进行分析。信息中心定期将网关发来的经过动态加密的历史数据放入云中进行存储。云是不可信第三方，提供信息存储功能。信息中心是可信方，负责电能表认证和用电信息的读取。

3.2 电能表到网关的数据聚合

本方案变量声明如表1所示。

表1 变量声明1

Table 1 Variable declaration 1

变量名	含义
n	网关(邻域)个数
i	网关(邻域)编号，取值1, 2, 3..., n
w_i	邻域 i 内电能表个数
j	电能表编号，取值1, 2, 3..., w^i
p	大素数
q	大素数 $q p-1$
g	群生成元
G	生成元为 g 的 q 阶乘法群
x_{ij}	邻域 i 内电能表 j 的私钥， $x_{ij} \in Z_q^*$
y_{ij}	邻域 i 内电能表 j 的公钥， $y_{ij} = g^{x_{ij}}$
y_i	邻域 i 的公钥
m_{ij}	邻域 i 内电能表 j 的明文
m_i	邻域 i 内明文聚合 $m_i = \sum_{j=1}^{w_i} m_{ij}$

(1) 系统初始化

当系统搭建完成后,系统执行以下操作:在系统完成智能电能表、网关、云和信息中心间的网络连接等搭建后,智能电能表、网关、云和信息中心建立网络连接,信息中心将会执行以下操作。

选择两个大素数 p 和 q ,使 $q|p-1$,然后选择生成元为 g 的 q 阶乘法群 $G \in Z_p^*$,信息中心公布 g 、 p 和 q 。

(2) 密钥生成

1) 每个电能表选择一个随机数 $x_{ij} \in Z_q^*$ 作为私钥,计算相应的公钥为 $y_{ij} = g^{x_{ij}}$,并将公钥 y_{ij} 和电能表ID发送到信息中心进行认证。信息中心向电能表对应的用户邮箱返回电子邮件,确认电能表合法身份。

2) 信息中心对电能表的公钥加上数字签名,发给电能表对应的网关。

3) 网关使用信息中心的公钥对收到的电能表公钥加数字签名的证书进行验证。

4) 网关 i 将自己邻域内 w_i 个公钥进行聚合,生成此邻域的公钥,即

$$y_i = \prod_{j=1}^{w_i} y_{ij} \mod p \quad (9)$$

并将本邻域公钥 y_i 公布给邻域内的所有电能表。

(3) 用电信息加密传输

邻域 i 内的所有电能表每15 min加密自己的用电数据并上传到网关,假设邻域 i 中的电能表 j 要传输的信息为 m_{ij} ,邻域 i 内有智能电能表 w_i 个,具体步骤为如下。

1) 电能表选择随机数 $r_{ij} \in Z_q^*$ 和随机噪声 $z_{ij} \in Z_q^*$ (用来保护私钥),电能表计算 c_{ij} 、 d_{ij}

$$c_{ij} = g^{r_{ij}} \mod p \quad (10)$$

$$d_{ij} = g^{m_{ij} + z_{ij}} y_i^{r_{ij}} \mod p \quad (11)$$

最终将自己的加密数据 $E_{y_i} = (c_{ij}, d_{ij})$ 发送到网关。

2) 网关计算

$$c_i = \prod_{j=1}^{w_i} c_{ij} \mod p \quad (12)$$

并将 c_i 发送到邻域内每个电能表。

3) 电能表计算

$$T_{ij} = c_i^{x_{ij}} g^{z_{ij}} \mod p \quad (13)$$

并将 T_{ij} 上传到网关。

(4) 用电信息聚合解密

设邻域 i 内所有电能表数据明文聚合值为 m_i ,

$$\text{其中, } m_i = \sum_{j=1}^{w_i} m_{ij}, x_i = \sum_{j=1}^{w_i} x_{ij}, r_i = \sum_{j=1}^{w_i} r_{ij}, z_i = \sum_{j=1}^{w_i} z_{ij},$$

$$d_i = \prod_{j=1}^{w_i} d_{ij}, T_i = \prod_{j=1}^{w_i} T_{ij}。$$

1) 网关收集邻域内所有电能表的加密用电信息,进行聚合解密

$$m_i = \log_g(d_i/T_i) \quad (14)$$

2) 每个网关计算出邻域内聚合的数据后上传到云中,信息中心可以随时进行数据访问,给未来发电和电能调度提供参考。

(5) 数据聚合和数据解密的正确性验证

1) 网关对电能表上传的数据进行聚合解密的步骤为

$$\begin{aligned} & g^{m_i} \\ &= d_i T_i^{-1} \\ &= d_i \left(\prod_{j=1}^{w_i} T_{ij} \right)^{-1} \\ &= g^{m_i + z_i} g^{x_i r_i} (g^{r_i x_i} g^{z_i})^{-1} \\ &= g^{m_i} \end{aligned} \quad (15)$$

$$m_i = \log_g(d_i/T_i) \quad (16)$$

3.3 网关到中心的信息传输

变量声明如表2所示。

(1) 动态秘密更新

在此,信息中心即Master,网关即Slave,信息中心和网关使用Diffie-Hellman^[16]密钥交换法生成初始密钥str,然后网关向信息中心发送随机数,为之后生成动态密钥作准备。

动态密钥在网关和信息中心的生成在算法1和算法2中详细阐述。

1) 算法1: 网关更新动态秘密

count=0

for 每个要发送的数据包 pkt_i **do**

 计算网关 id 的哈希 $H=(id_g || str)$;

表2 变量声明2

Table 2 Variable declaration2

变量名	含义
str	网关和中心的初始密钥
id_g	网关编号
i	数据包传输成功迭代次数
j	数据包传输失败迭代次数
pkt_i	第 i 次传输的数据包
t_{g_i}	网关的时间戳
t_{c_i}	信息中心的时间戳
τ_c	网关的合理传输时间
τ_c	中心的合理传输时间
ack_i	中心第 i 次的回应
count	初始秘密
g_count	网关每次更新的动态秘密
c_count	中心每次更新的动态秘密
$[msg_i]$	加密后的数据
k	生成动态密钥的迭代次数
SK_{g_i}	网关动态密钥
SK_{c_i}	中心动态密钥

生成时间戳 t_{g_i}

计算 $hash_i = H(H(id_g \parallel str) \parallel [msg_i] \parallel t_{g_i})$

$pkt_i = H(id_g \parallel str) \parallel [msg_i] \parallel hash_i \parallel t_{g_i}$

发送 pkt_i 到中心

while! 在每个会话发送包结束后 **do**{

if 网关收到acki的时间 $t_{g_i} \leq t_{c_i} + t_g$

 proceed

else

$pkt_flag=1$

for 每个正确的包回应 ack_i **do**

 count++

for 每个错误的包回应 ack_j **do**

 再次发送 pkt_j

}

$g_count=count$

2) 算法2: 中心更新动态秘密

count=0

for 每个收到的的数据包 pkt_i **do**

if (时间戳 $t_{c_i} \leq t_{g_i} + \tau_c$)&&(当前时间 $t \leq t$)

 存储 $H(id_g \parallel str)$

else

 终止与网关连接

if 在收到的包 pkt_i 中 $hash_i = hash_i'$

then 执行下一步

else

 终止会话

while ! 在每个会话收到包结束后 **do**{

 发送 ack_i 给网关

for 每个正确的 pkt_i

 count++

for 每个错误的 pkt_i

$pkt_flag=1$

}

$c_count=count$

(2) 生成密钥

生成密钥环节是利用已经生成的动态秘密 g_count 和 c_count 生成密钥。

网关动态密钥 SK_{g_i} 生成

$$DS_{g_i} = H(g_count)$$

$$SK_{g_i} = (DS_{g_i} \oplus str) \quad (17)$$

在生成密钥环节, i 表示生成动态密钥的迭代次数, 与前面的 i 不同。之后的网关动态密钥为

$$SK_{g_{i+1}} = (DS_{g_{i+1}} \oplus SK_{g_i}) \quad (18)$$

中心动态密钥 SK_{c_i} 生成

$$DS_{c_i} = H(c_count)$$

$$SK_{c_i} = (DS_{c_i} \oplus str) \quad (19)$$

在这里 i 表示生成动态密钥的迭代次数, 与前面的 i 不同。之后的中心密钥为

$$SK_{c_{i+1}} = (DS_{c_{i+1}} \oplus SK_{c_i}) \quad (20)$$

(3) 加解密

在网关侧, 加密如下

$$CT_i = f(PT_i, counter_i, SK_{g_i}) \quad (21)$$

在中心侧, 解密如下

$$PT_i = f(CT_i, counter_i, SK_{c_i}) \quad (22)$$

在加解密中, 每个明文是 $PT_i (i=1, 2, \dots, d, d$ 为每个数据包中数据值的个数)。

加解密函数 f 的定义如下

$$\begin{aligned} &f(PT_i, counter_i, SK_{g_i})\{ \\ &CT_i = (PT_i + counter_i) \oplus SK_{g_i}; \\ &counter_i++; \\ &return CT_i;\} \end{aligned} \quad (23)$$

$counter_i = H(lseq_no \oplus lask_no)$ 用于改变原始明

文，并在每次解密数据值的时候增加，lseq_no和lask_no分别为最近一次成功传输数据包的序列号和确认号。网关到中心信息传输如图5所示。

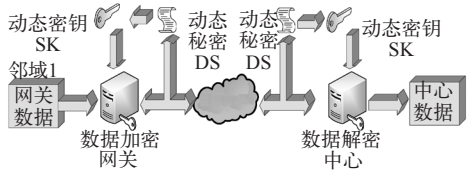


图5 网关到中心的信息传输

Fig.5 Gateway to central information transmission

(4) 数据存储

信息中心将所有成功收到的历史数据包转存到云中，将所有动态密钥和对应时间戳存到本地。当信息中心想要查询历史数据时，可以利用本地对应时间戳的密钥将云传回的密文进行解密查询。

4 性能评价

4.1 本系统通信开销分析

假设有 n 个电能表系统家庭入户线为 10 mm^2 ，承受功率为 $0\sim 13.8\text{ kW}$ ，电能表每 15 min 上传一次数据，上传一次的电能数据范围为 $0\sim 3.45\text{ kW}\cdot\text{h}$ ，假设邻域有 50 只电能表，最大功率为 $172.50\text{ kW}\cdot\text{h}$ ，需要至少 15 bit 的存储空间，根据国家标准^[17-18]，电能表使用 88 bit 的数据包来发送功率数据，格式如下。

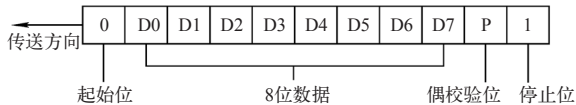


图5 字节传输序列

Fig.5 Byte transfer sequence

根据相关文献^[10]可知，使用 $1\ 024\text{ bit}$ 密钥的ElGamal既可以保证信息的安全性，又可以满足对电能数据进行加密的要求。

密钥生成阶段：信息中心向所有电能表公布 g, p, q 的通信开销为 $1\ 024\text{ bit} \times 3 = 3\ 072\text{ bit}$ ；每个电能表将自己的公钥 y_{ij} 发送到信息中心开销为 $1\ 024\text{ bit}$ ，总开销为 $1\ 024n$ (n 为电能表总数)；信息中心将每个电能表公钥发给其对应网关开销为 $1\ 024n$ 。

用电信息加密传输阶段：电能表上传加密信息 $E_{y_i} = (c_{ij}, d_{ij})$ ，通信开销为 $1\ 024\text{ bit} \times 2 = 2\ 048\text{ bit}$ ，电能表上传 T_{ij} 至通信开销为 $1\ 024\text{ bit}$ 。

相比文献[9]的方案，在密钥生成阶段，文献[9]的方案将公钥聚合交给电能表来完成，所以中心的通信开销为 $1\ 024n^2$ ，本方案将聚合的任务交给网关来做，将信息中心的通信开销降为 $1\ 024n$ ，两种方案通信开销比较如表3所示。

表3 通信开销比较(bit)

Table 3 Comparison of communication overhead

密钥生成阶段	本文方案	Busom N ^[9] 方案
电能表发出	$1\ 024$	$1\ 024$
电能表接收	$1\ 024$	$1\ 024n$
中心发出	$1\ 024n$	$1\ 024n^2$
中心接收	$1\ 024n$	$1\ 024n$

本方案虽然比不加密的原始方案有一定的信息扩张，即为了保证安全性使用门限ElGamal方案，传输每个电能数据由 88 bit 扩张为 $1\ 024\text{ bit}$ ，但是相较于文献[9]来说，总体开销是减少的，如图6所示。

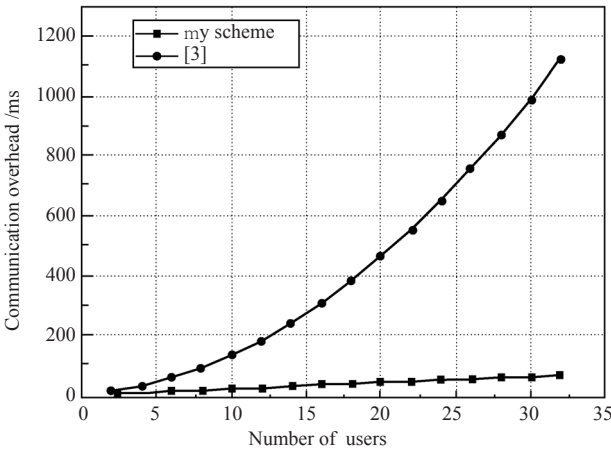


图6 通信时间复杂度比较

Fig.6 Comparison of communication time complexity

4.2 功能性比较

表3给出了本方案和文献[9]、文献[12-14]和文献[15]中方案的功能性比较。首先文献[9]和本方案都采用了门限ElGamal加密，信息中心和网关都无法获得用户详细信息，可以防止内部攻击，但是文献[9]数据聚合只有两层，数据可用性较低。文献[12-13]信息中心可以获得所有用户的详细数据，信息中心内部人员可能泄露用户隐私数据。文献[14]使用同态加密实现加密数据的聚合，信息中心和网关都无法获得用户详细信息，但是每个网关和其负责的电能表的密钥都由一个KDC负责管理，虽然方便管理，但是一旦KDC被攻击，所

有用用户隐私数据将泄露。文献[15]节点负责数据收集、数据加密、数据聚合和数据加密传输，节点负担太重，且数据在各节点之间传输，网络拓扑结构的设计对性能影响较大。综上所述，该方案在功能性方面更胜于其他四个方案，更适合于智能电网中数据的传输和隐私的保护。

表4 功能比较

Table 4 Functional comparison

方案	能否应对内部攻击	模型层次	数据可用性	信息中心解密结果	中心存储压力
文献[9]	√	2层	低	网关聚合数据	大
文献[12]	×	2层	高	所有用户数据	大
文献[13]	×	2层	高	所有用户数据	大
文献[14]	×	3层	高	网关聚合数据	大
文献[15]	√	多层	低	网关聚合数据	大
本文方案	√	3层	高	网关聚合数据	小

5 安全性分析

此方案的目的是保护用户私人用电信息的隐私，防止攻击者通过用户的用电信息推测用户的隐私。该方案面对外部攻击是安全的，因为对外本方案的安全性和ElGamal密码系统相同。接下来对内部安全进行分析。

针对外部网络流量监听和内部人员窥探用户隐私的攻击，本文作出以下设定。

1) 电能表内部存放私钥 x_{ij} 和公钥 y_{ij} ，电能表被完全攻陷时会泄露其公钥 y_i 和私钥 x_i 。

2) 第三方的云是不可信第三方，其中存放的信息可能被攻击者获取。

3) 电能表到网关之间的通信是不可信通道，可能被窃听。

4) 网关数据可以被电网内部人员查看。

5.1 安全性分析

1) 攻击者攻陷一个智能电能表，其他电能表安全不受影响。在此场景下，攻击者将获得电能表的私钥 x_{ij} 、公钥 y_{ij} 和邻域公钥 y_i ，此电能表的数据将被攻击者获取，但是由于每个电能表的私钥是不一样的，攻击者只能获取此电能表的数据，邻域内其他电能表由于其私钥没有被攻击者获取，电能表的相关数据是安全的。

2) 攻击者窃听电能表和网关之间的通信，电能表隐私不会泄露。由于电能表的数据是加密之后上传到网关中的，所以攻击者只能得到加密数据 d_{ij} 和 T_{ij} ，无法得到每个电能表真实明文数据 m_{ij} ，即使攻击者获取邻域内电能表加密数据，也只能将这些数据进行聚合解密得到邻域用电数据的聚合值，无法得到每一个具体用户的用电信息，用户隐私从而得到保护。

3) 攻击者是内部人员，用户隐私还可以得到保护。攻击者攻陷网关后，因为网关只有邻域内电能表的加密信息和聚合的解密信息，所以攻击者仍然无法获得每个电能表的具体数据。

4) 攻击者攻陷云，用户隐私还可以得到保护。攻击者攻陷云后，只能获取云端的聚合数据，无法获得每个电能表的具体数据，每个用户的隐私得以保护。

5) 攻击者使用假冒电能表。每个电能表安装完成之后，会同信息中心进行认证，网关用信息中心的公钥解密证书里面的签名，将会识别出哪些是有正规证书的邻域电能表，那些是冒充的电能表。

6 结束语

提出了一种电能计量方案，主要利用ElGamal加密技术和动态加密技术进行实现。对用户来说数据加密保护了用户的用电隐私，同时邻域将聚合用电信息的上传，相比其他方案，兼顾了保护用户隐私并充分利用电能数据；对电网运营人员来说，能在不知道用户具体用电数据的情况下，对用户用电情况进行了解，为以后发供配电和电网升级改造提供参考。

本方案将电能表分到不同邻域当中，减少了信息中心的通信计算开销，并利用现有云服务将海量用电数据存放在云中，减少了网关和信息中心的存储和运算成本。

参考文献

- [1] 丰叶. 中国智能电网技术发展实践综述[J]. 工程技术, 2016(10): 164.
FENG Ye. Summary of china's smart grid

- technology development practice[J]. Engineering and Technology, 2016(10): 164.
- [2] XU Yixin, LIU Yanli. Challenging issues of smart grid[J]. Automation of Electric Power Systems, 2015, 39(2): 1-5
- [3] KABALCI Y. A survey on smart metering and smart grid communication[J]. Renewable and Sustainable Energy Reviews, 2016, 57(5): 302-318.
- [4] WANG Yi, CHEN Qixin, HONG Tao, et al. Review of smart meter data analytics: applications, methodologies, and challenges[J]. IEEE Transactions on Smart Grid, 2018, PP(99): 1.
- [5] SIANO P. Demand response and smart grids—a survey[J]. Renewable and Sustainable Energy Reviews, 2014, 30(2): 461-478.
- [6] FINSTER S, BAUMGART I. Privacy-aware smart metering: a survey[J]. IEEE Communications Surveys and Tutorials, 2014, 16(3): 1732-1745.
- [7] WANG F, LEI Z, YIN X, et al. Information security in the smart grid: survey and challenges[J]. Computer Networks, 2017, 57(5): 1344-1371.
- [8] YANG L, CHEN X, ZHANG J, et al. Optimal privacy-preserving energy management for smart meters[M]. International Conference on Computer Communications, 2014.
- [9] BUSOM N, PETRLIC R, SEBE F, et al. Efficient smart metering based on homomorphic encryption[J]. Computer Communications, 2016, 82(5): 95-101.
- [10] DESMEDT Y. Threshold Cryptography[M]. Encyclopedia of Cryptography and Security, 2015: 606-611.
- [11] SAXENA N, GRIJALVA S. Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication[J]. IEEE Transactions on Industrial Informatics, 2017, 13(3): 1482-1491.
- [12] 陈亮, 林永峰. 基于同态加密的智能电网安全数据融合技术[J]. 现代电子技术, 2016, 39(9): 82-86.
- CHEN Liang, LIN Yongfeng. Homomorphic encryption based security data fusion technology of smart grid[J]. Modern Electronics Technique, 2016, 39(9): 82-86.
- [13] LIU X, ZHANG Y, WANG B, et al. An anonymous data aggregation scheme for smart grid systems[J]. Security and Communication Networks, 2014, 7(3): 602-610.
- [14] RUJ S, NAYAK A. A decentralized security framework for data aggregation and access control in smart grids[J]. IEEE Transactions on Smart Grid, 2013, 4(1): 196-205.
- [15] 付帅, 姜奇, 马建峰. 一种无线传感器网络隐私保护数据聚合方案[J]. 计算机研究与发展, 2016, 53(9): 2030-2038.
- FU Shuai, JIANG Qi, MA Jianfeng. Wireless sensor network privacy protection data aggregation scheme[J]. Journal of Computer Research and Development, 2016, 53(9): 2030-2038.
- [16] Diffie-Hellman key exchange (exponential key exchange)[EB/OL]. <https://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange>.
- [17] MENG J, ZHU N, BAI X, et al. Research and development of embedded communication software for smart meters based on DL/T 645—2007 protocol[J]. Power System Technology, 2010, 34(9): 7-12.
- [18] Ma Licui, Li Meihong, WU Qianqian, et al. Research of dynamic key encryption algorithm in smart grid communication[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(4): 74-79.

作者简介



朱丹

朱丹(1994—),男,硕士研究生,主要研究方向为智能电网安全、密码学等。

(收稿日期:2018-06-23) **EA**