Secure Edge Electricity Data Aggregation Scheme for Low Voltage Transformer Areas

Zixiang Wang1*, Zhoubin Liu1, Ziqiang Zhou1 and Jiajia Han1

1State Grid Zhejiang Electric Power Research Institute, Hangzhou, Zhejiang, China
*Corresponding author’s e-mail: wangzixiang@zj.sgcc.com.cn

Abstract. The smart grid system is the physical power infrastructure integrated with many intelligent electronic devices. It supports the two-way flow of energy as well as information. The smart meters are important intelligent devices, which account for the largest portion among all terminals in the smart grid. In many application scenarios, the master station need high frequency total electricity consumption information of each low voltage transformer area. It requires frequent data interchange between smart meters and master station. However, the electric communication network cannot provide enough bandwidth resource to support such high frequency data interchange. Edge Computing Nodes (ECNs), which can be deployed at different low voltage transformer areas, can achieve the electricity data aggregation at the edge side. The communication resource can be saved since only aggregated electricity data will be uploaded to the master station. Traditional data aggregation scheme requires the plaintext from smart meters. From the viewpoint of security and privacy-preserving, it is not safe to implement the data decryption operation at edge side. Therefore, the data aggregation scheme with ciphertext is required at the edge side. In this paper, we propose a secure edge electricity data aggregation scheme based on homomorphic public key encryption techniques. The ECNs will implement the electricity data aggregation with the ciphertext from different smart meters, and the aggregated data will be transmitted to the master station through communication network. The master station can use its public key to obtain the total electricity consumption of each low voltage transformer area.

1. Introduction

A smart grid is an electrical grid integrated with a variety of operational and energy measures including smart meters, smart appliances, renewable energy resources, and energy efficient resources [1,2]. It is not only a power grid, but also an information network. A large quantity of terminals are connected to the smart grid to implement different measurement and control tasks, and the data from these terminals is transmitted to the corresponding master station through modern communication technologies. The data can be used to support many advanced applications and improve reliability, security, and efficiency of the electrical grid. Different terminals are linked together to provide interoperability between them. The smart meters, which are responsible for the users’ electricity power measurement, account for the largest portion among all terminals in the smart grid. Many applications, such as demand-side response, line loss calculation, 3-phase unbalance analysis, require the total electricity consumption information of low voltage transformer areas. Although an enormous amount of data has been generated by the smart meters every day, the utilization of the data is weak. The existing smart grid telecommunication access network still cannot support the electric power measurement data transmission and exchange on a very short timescale (minute scale). A lack of real-time data impairs the automated analysis and response ability of smart grid.
A possible method to deal with the smart grid communication network bandwidth insufficiency is using the edge computing techniques. Edge computing is a distributed computing paradigm compute resources placed closer to information-generation sources [3], which is seen as important in the realization of smart grid and Internet of Things. It is a method of optimizing applications or cloud computing systems by taking some portion of applications, data, or services away from central nodes to the edge side of the network [4]. Edge computing is able to reduce network latency and bandwidth usage generally associated with cloud computing. A large amount data is generated by the smart meters every day in a low voltage transformer area. From the perspective of edge computing, the original data do not need to transmit to the master station on a very short timescale. The Edge Computing Node (ECN) can be deployed at the edge side to perform the electricity data storage and aggregation [5-7]. In work [5], a solution that automates the switching between different data handling algorithms at the network edge is proposed. In work [6], a data aggregation approach is proposed to relieve the bandwidth capacity burden of power line communication. In work [7], an implantable data storage-and-processing solution for improving the existing smart meter infrastructure is proposed. However, the existing researches consider little about information security during edge data aggregation. The proposed methods call for plaintext operation at the edge side. ECNs, which interacts with smart meters and the master station, maintain two-way communications with the smart grid information system. These ECNs are usually located in physically insecure environments, which is possible for malicious attackers to exploit the potential vulnerabilities of these devices to either steal users’ data or gain access to the more critical parts of smart grid [8]. A secure electricity data aggregation strategy is required for the low voltage transformer areas. Authors in work [9] proposed a secure power-usage data aggregation scheme for smart grid, but verification operation is quite resource-consuming. Current edge computing devices cannot support such framework. In work [10], a lightweight message authentication scheme is proposed for secure electricity information exchange, but the data aggregation is not considered. In works [11,12], privacy-preserving data aggregation schemes are proposed, but the authentication among different terminals is not addressed.

In this paper, we propose the Secure Edge Electricity Data Aggregation (SEEDA) scheme to deal with the electricity consumption data aggregation problem at edge side. Based on homomorphic public key encryption approach, ECNs can implement the electricity data aggregation with the ciphertext instead of the plaintext, and the aggregated data will be transmitted to the master station through communication network. Bidirectional identity authentication is employed among ECNs, master station and smart meters. The mater station can use its public key to obtain the total electricity consumption of each low voltage transformer area. SEEDA can resist the possible internal and external attacks, and the users’ privacy can be preserved.

The article is organized as follows: in Section 2, we introduce the system model and formulate the secure electricity data aggregation problem; in Section 3, the SEEDA scheme is described; in Section 4, we analyze on the security and communication overhead performance of SEEDA; in Section 5, we conclude the paper.

2. Problem Formulation

In this section, we formulate our system model and the secure edge electricity data aggregation problem.

2.1. System Model

As shown in Fig. 1, the typical power user electric energy data acquire system in smart grid consists of smart meters, concentrators and master station.
The electric energy measurements of residential users and industry users are implemented by the smart meters. For each low voltage transformer area, there are many smart meters and one concentrator. These smart meters transmit the electricity consumption to the concentrators through wireless network or power line communication. The concentrator collects electricity consumption information of its corresponding low voltage transformer area, and uploads data to the master station. Due to the bandwidth limitation, the smart meters can only upload their data every 15 minutes at most.

Figure 2. Electricity data aggregation system architecture
In edge electricity data aggregation model, some ECNs are deployed in the low voltage transformer area. As shown in Fig. 2, our system consists of four groups of entities: smart meters, ECNs, trusted authority (TA), and master station. High frequency electricity consumption data will be transmitted to the ECNs at first. The ECNs implement the data aggregation, and report the aggregated results to the base station every Ts seconds. Since the data aggregation can reduce the amount of data effectively, Ts can be quite small. TA is a third party trusted entity, whose duty is system public parameter generation, key generation, system public parameter assignment and key assignment. TA will not participate in data exchange among smart meters, ECNs and master station, and it will be offline after the system parameter initialization and key assignment. We consider a hybrid power user electric energy data acquire system, which includes heterogenous smart meters. Multiple ECNs are deployed at the network edge. Assume there are M ECNs and N smart meters, and each ECN will connect to some smart meters through power line communication or RS485. The ECNs are denoted by $E_1, E_2, \ldots, E_M$, and the $j$-th smart meters connected to ECN $E_i$ are denoted by $D_{ij}$. To avoid data redundancy, a smart meter will connect to only one ECN. The number of smart meters connected to ECN $E_i$ is denoted by $N_i$, and $\sum_{i=1}^{M} N_i = N$.

### 2.2. Secure Electricity Data Aggregation

We denote the electricity consumption measured by $D_{ij}$ at $k$-th time slot as $x_{ij}(k), x_{ij}(k) < P_{\text{max}}$. $x_{ij}$ should be encrypted to the ciphertext $c_{ij}(k)$ at the smart meter side, and the ciphertext will be transmitted to the corresponding ECN $E_i$. From the viewpoint of security and privacy-preserving, the ECN should not obtain the plaintext. The ECN can only implement the electricity consumption data aggregation with the ciphertext. The privacy-preserving data aggregation at ECN side can be described as

$$ C_i(k) = f(c_{i_1}(k), c_{i_2}(k), \ldots, c_{i_{N_i}}(k)) $$

where $C_i(k)$ is the aggregated data, $f$ is a aggregation transform operator. $C_i(k)$ will be transmitted to the master station through wireless or power line communication, and the master station should recover the total electricity consumption of each low voltage transformer area based on the ECNs’ data, i.e.,

$$ \sum_{i=1}^{M} \sum_{j=1}^{N_i} x_{ij}(k) = g(C_1(k), C_2(k), \ldots, C_M(k)) $$

where $\sum_{i=1}^{M} \sum_{j=1}^{N_i} x_{ij}(k)$ is the total electricity consumption, $g$ is a decryption transform operator.

### 3. Secure Edge Electricity Data Aggregation

In this section, we present the Secure Edge Electricity Data Aggregation (SEEDA) strategy for the low voltage transformer areas. The SEEDA strategy consists of four phases: system data initialization, data encryption and digital signature, data aggregation, and data decryption. Each phase requires different entities to participate.

#### 3.1. System Data Initialization

In the system data initialization phase, TA will generate the system public parameters, public keys and private keys.

At first, TA chooses two cryptographic hash functions

$$ h: \{0,1\}^* \rightarrow Z_n^* $$

$$ H : \{0,1\}^* \rightarrow Z_n^* $$

The system public parameters are formulated as $\{H, h, T_s\}$.

Then the TA will generate two kinds of keys:
Homomorphic keys: The homomorphic keys are used to secure data aggregation. The smart meters will be assigned the homomorphic private keys for data encryption. The ECNs will be assigned homomorphic public keys for data aggregation. The master station will be assigned homomorphic public keys for data decryption.

Symmetric keys: The symmetric keys are used for secure communication. Bidirectional identity authentication among smart meters, ECNs and master station will be achieved based on symmetric keys.

Let $p=2p'+1$, $q=2q'+1$ be two safe primes which satisfy
(1) $p'$ and $q'$ are also primes.
(2) $n=pq$, and $n>N_{max}$.

We denote the least common multiple of $p-1$ and $q-1$ by
\[ \lambda = \text{lcm}(p-1, q-1) = 2p'q' \]  
(5)

TA chooses $N+M+1$ random positive integers $r_{00}$, $r_{01}$, $r_{11}$, $r_{12}$, ..., $r_{M0}$, $r_{M1}$, $r_{M2}$, ..., $r_{MN}$ that satisfy
\[ \sum_{i=1}^{N} \sum_{j=0}^{M} r_{ij} + r_{0} \equiv 0 \pmod{\lambda} \]  
(6)

The homomorphic private key, ECN's homomorphic public key and master station's homomorphic public key are formulated as $\{H, T_s\}$, $\{n, r_0\}$, $\{n, r_{0\cdot \lambda}\}$, respectively. TA will also generate $N+M$ pairs of symmetric keys. We denote the keys of $\{E_i, D_{ij}\}$ and $\{\alpha_{ij}, \beta_i\}$.

The system public parameters, private keys $\{n, r_0\}$, $\alpha_{ij}$ are assigned to the smart meter $D_{ij}$. The system public parameters, public keys $\{n, r_0\}, \alpha_{ij}$, $\beta_i$ are assigned to the ECN $E_i$. The system public parameters, public keys $\{n, r_0\}$, $\beta_i$ are assigned to the master station.

In addition, TA will also generate a white list based on the communication topology. The electricity consumption data aggregation obeys a hierarchy structure. Smart meters are only allowed to communicate with a fixed ECN, and only registered ECNs can access the master station. We denote the white lists of master station, ECN $E_i$ (i=1,2,..., M), smart meter $D_{ij}$ (i=1,2,...,M, j=1,2,...,$N_i$) by $W_m$, $W_e_i$, $W_d_{ij}$, respectively. Each white list contains the legitimate users that can communicate with the current terminal. The white lists will be assigned to corresponding entities.

After the assignment of system public parameters, public keys and private keys, TA turns to offline. Only when the system parameters or keys need to be updated, will the TA start to work again.

3.2. Data Encryption and Digital Signature

The smart meter $D_{ij}$ records the electricity consumption every $T_s$ seconds, and original electricity consumption measured is usually described by BCD code. The electricity consumption $x_{ij}(k)$ within $[kT_s, (k+1)T_s]$ can be calculated according to the BCD code.

With the private key $\{n, r_0\}$, the electricity consumption $x_{ij}(k)$ can be encrypted as
\[ c_{ij}(k) = (1 + nx_{ij}(k))H(kT_s)^{r_0} \pmod{n^2} \]  
(7)

where $c_{ij}(k)$ is the ciphertext.

The calculation $H(kT_s)^{r_0}$ is quite time-consuming. Since the private key $\{n, r_0\}$ is a steady value, $H(kT_s)^{r_0}$ can be pre-computed, which can accelerate the ciphertext generation.

![Figure 3. Bidirectional identity authentication between ECN and smart meter](image)
The smart meter $D_{ij}$ will report the electricity consumption after receiving the ECN’s request. The bidirectional identity authentication between $E_i$ and $D_{ij}$ will be implemented in our scheme. The authentication process is shown in Fig. 3.

The ECN $E_i$ generates a random number $\gamma$ at first. Then, $E_i$ uses the key $\alpha_{ij}$ to encrypt its MAC address and $\gamma$ as $e(\text{MAC}_{E_i} || \gamma, \alpha_{ij})$. $D_{ij}$ uses the key $\alpha_{ij}$ to decrypt $e(\text{MAC}_{E_i} || \gamma, \alpha_{ij})$ to acquire random number $\gamma$ and ECN’s MAC address. According to the white list, $D_{ij}$ can verify the validity of $\text{MAC}_{E_i}$. If $\text{MAC}_{E_i}$ exists in the white list $W_{Dij}$, the smart meter $D_{ij}$ will generate the message digest $h(c_{ij}(k) || \text{MAC}_{Dij} || \gamma, \alpha_{ij})$ based on the cryptographic hash function $h$.

The digital signature $s_{ij}(k)$ can be formulated as

$$s_{ij}(k) = e(h(c_{ij}(k) || \text{MAC}_{Dij} || \gamma), \alpha_{ij})$$  \(8\)

The ciphertext $c_{ij}(k)$ and signature $s_{ij}(k)$ will be transmitted to the ECN $E_i$ ($i=1,2,...,M$) through power line communication or RS485 every $T_s$ seconds.

### 3.3. Authentication and Data Aggregation

Within $[kT_s, (k+1)T_s]$, the ECN needs to collect $N_i$ connected smart meters’ electricity consumption ciphertext $c_{i1}(k), c_{i2}(k), ..., c_{IN_i}(k)$.

Due to the malfunctioning of smart meters or the abnormalities of communication, the ECN $E_i$ may receive multiple copies of data from $D_{ij}$. To guarantee $E_i$ only stores single piece of effective data, $E_i$ will discard the redundant data.

When $E_i$ receives the report from $D_{ij}$, it should authenticate the signature $s_{ij}(k)$ at first. The message digest can be obtained with the key $\alpha_{ij}$. $E_i$ uses the private key $\alpha_{ij}$ to get the message digest $h'(c_{ij}(k) || \text{MAC}_{Dij} || \gamma)$ (The decrypted data may not be the original message digest, so we use $h'(c_{ij}(k) || \text{MAC}_{Dij} || \gamma)$ to represent the received message digest). To verify the validity of digital signature, $E_i$ will check whether $h'(c_{ij}(k) || \text{MAC}_{Dij} || \gamma) = h(c_{ij}(k) || \text{MAC}_{Dij} || \gamma)$. If $h'(c_{ij}(k) || \text{MAC}_{Dij} || \gamma) = h(c_{ij}(k) || \text{MAC}_{Dij} || \gamma)$ is hold, $c_{ij}(k)$ is accepted. Otherwise, the message will be discarded.

Once authentication is completed, the following aggregation transform is implemented at the ECN side

$$C_i(k) = \prod_{j=1}^{N_i} c_{ij}(k)H(kT_s)^{n_i} \mod n^2$$  \(9\)

The calculation $H(kT_s)^{n_i}$ is quite time-consuming. Since the private key $\{n, r_0\}$ is a steady value, $H(kT_s)^{n_i}$ can also be pre-computed.

![Figure 4. Bidirectional identity authentication between ECN and master station](image)

Similar to Section 3.2, the bidirectional identity authentication between $E_i$ and master station is required. As shown in Fig. 4, the ECN $E_i$ will send the authentication request $e(\text{MAC}_{E_i} || \gamma, \beta_i)$ to the master station. The master station checks whether MAC address $\text{MAC}_{E_i}$ exists in the white list $W_m$. The legitimate ECN will be allowed to access, and the acknowledge command $e(\text{MAC}_{\text{master}} || \gamma, \beta_i)$ will be sent to $E_i$. $E_i$ will verify the acknowledge message by checking the message digest $h'(\text{MAC}_{\text{master}} || \gamma)$. $\text{MAC}_{\text{master}}$ can be acquired from the white list $W_m$, and $\gamma$ is the random number sent to the master station.
If $h'(\text{MAC}_{\text{master}}||\gamma) = h(\text{MAC}_{\text{master}}||\gamma)$, $E_i$ generates the message digest $h(C_i(k)||\gamma)$ based on the cryptographic hash function $h$. The digital signature of $E_i$ can be formulated as

$$S_i(k) = e(h(C_i(k)||\gamma), \beta_i)$$

(10)

$E_i$ will report the aggregated electricity consumption data $C_i(k)$ and digital signature $S_i(k)$ to the master station.

### 3.4. Authentication and Data Decryption

When the master station receives the report from $E_i$, it should authenticate the signature $S_i(k)$ first. The message digest $h'(C_i(k)||\gamma)$ can be obtained with the key $\beta_i$. $E_i$ will check whether $h'(C_i(k)||\gamma) = h(C_i(k)||\gamma)$ to authenticate the signature. If $h'(C_i(k)||\gamma) = h(C_i(k)||\gamma)$ is held, $C_i(k)$ is accepted. Otherwise, the message will be discarded.

After the authentication, the master station needs to calculate the total electricity consumption of each low voltage transformer area based on the aggregated data from ECNs. For the aggregated data $C_i(k)$ from the ECN $E_i$, the following transform should be made at first

$$C_i'(k) = C_i H(kT_s)^{nr_i} \mod n^2$$

(11)

$$= \prod_{j=1}^{N_i} (1 + nx_j(k))H(kT_s)^{m(j_0 + r_0 + \sum_{j=1}^{N_i} r_j)} \mod n^2$$

(12)

$$= \prod_{j=1}^{N_i} (1 + nx_j(k)) \mod n^2 \cdot H(kT_s)^{n(j_0 + r_0 + \sum_{j=1}^{N_i} r_j)} \mod n^2 \cdot \mod n^2$$

(13)

**Theorem 1** For any $x \in Z_{n^2}$, we have

$$x^{nL} \equiv 1 \mod n^2$$

(14)

The proof of Theorem 1 may refer to [12].

**Theorem 2** For any $x \in Z_n$, we have

$$\prod_{i=1}^{m} (1 + nx_i) \equiv (1 + n \sum_{j=1}^{m} x_i) \mod n^2$$

(15)

Theorem 2 can be easily proved with mathematical induction, and the detailed proof of Theorem 2 may refer to [13].

Because $\sum_{i=1}^{M} \sum_{j=0}^{N} r_j + r_0 \equiv 0 \mod \lambda$, we have

$$H(kT_s)^{n(j_0 + r_0 + \sum_{j=1}^{N} r_j)} \mod n^2 \equiv H(kT_s)^{nL_\lambda} \mod n^2$$

(16)

where $L$ is a positive integer. Insert Eq. (16) to Eq. (13), and we have

$$C_i'(k) = \prod_{j=1}^{N_i} (1 + nx_j(k)) \mod n^2 \cdot H(kT_s)^{nL_\lambda} \mod n^2 \mod n^2$$

(17)

According to Theorem 1, we have

$$H(kT_s)^{nL_\lambda} \equiv 1 \mod n^2$$

(18)

Therefore, Eq. (17) can be further described as

$$C_i'(k) = \prod_{j=1}^{N_i} (1 + nx_j(k)) \mod n^2$$

(19)
According to Theorem 2, Eq. (19) can be further described as

\[ C_i'(k) = 1 + n \sum_{j} x_{ij} \] (20)

Then, the summation of electricity consumption among the smart meters connected to \( E_i \) can be explained as

\[ \sum_{j} x_{ij} = \frac{C_i'(k) - 1}{n} \] (21)

Within \([kT_s,(k+1)T_s]\), the total electricity consumption of a low voltage transformer area is

\[ \sum_{i=1}^{M} \sum_{j} x_{ij} = \frac{\sum_{i=1}^{M} C_i'(k) - 1}{n} \] (22)

4. Performance Analysis

In this section, we evaluate of the performance of the proposed SEEDA scheme.

4.1. Security Analysis

In the electricity data aggregation scenario, the major security risks are user privacy-preserving and false data injection.

The user privacy-preserving consists of two parts:

1. External users should not obtain the plaintext of each smart meter.
2. The authority of each internal user is limited. Each smart meter cannot obtain the data of other smart meters, and each ECN cannot obtain the plaintext of electricity.

As shown in Eq. (7), the original data \( x_{ij}(k) \) of \( D_{ij} \) at time \( kT_s \) is encrypted to \((1 + nx_{ij}(k))H(kT_s)^{\nu s} \mod n^2\). We can regard significant message as \((1+nx_{ij}(k))\), and \( H(kT_s)^{\nu s} \) is a large random integer. \((1+nx_{ij}(k))H(kT_s)^{\nu s} \mod n^2\) is a Paillier ciphertext. Because Pailler encryption is IND-CPA (indistinguishable under the chosen plaintext attack) secure [14,15], external users cannot read the plaintext \( x_{ij}(k) \) without the public key. For the internal users, both smart meters and ECNs have their own authority. Our scheme constructs a hierarchy structure. The smart meters can only communicate with the corresponding ECN, and ECNs cannot communicate with each other. In addition, each smart meter only has its own private key, and it cannot read the plaintext of other devices even though it eavesdrops their communication. The ECNs are responsible for data aggregation, and it can just handle the ciphertext \( c_{ij}(k) \) instead of the electricity consumption plaintext \( x_{ij}(k) \). The master station obtains the total electricity consumption through the decrypt the aggregated ciphertext \( C_1(k), C_2(k), \ldots, C_M(k) \).

In order to reject the false data injection, bidirectional authentication is employed among smart meters, ECNs and master station. For each smart meter, the message digest \( h(c_{ij}(k)||MAC_{Dij}||\gamma) \) contains a random number, Because\( s_i \) generated every handshake, adversaries cannot forge the signature through capture-replay attack. In addition, the ECN \( E_i \) collects the messages from smart meters every \( T_s \) seconds. Within time window \([kT_s,(k+1)T_s]\), \( E_i \) only store one piece of message from each smart meter, and the redundancy \( c_{ij}(k) \) will be discarded.

The authentication between ECN and the master station is similar to the authentication process between ECN and smart meter. Only the registered ECNs may access the master station.
4.2. Communication Overhead

![Figure 5. Communication overhead between ECNs and smart meters](image1)

![Figure 6. Communication overhead between ECNs and master station](image2)

The SEEDA scheme proposed in this paper focuses on the electricity data aggregation at edge side. Since the data from different smart meters are transferred to one data block, the communication overhead can be reduced. In order to evaluate the communication overhead of our scheme, we compare SEEDA with the traditional data transmission scheme of power user electric energy data acquire system. In the simulation, we assume 5000 smart meters are deployed in a low voltage transformer area. In the traditional data transmission scheme, smart meters transmit their data to the concentrator, and the concentrator will relay the data to the master station without any aggregation transform. In SEEDA, M ECNs will aggregate multiple smart meters' electricity consumption data into one. We assume each ECN is connected with m (0<m<1000) smart meters. Both ECNs and smart meters have 6-byte MAC address. SEEDA need symmetric and asymmetric cryptography to perform digital signing and encryption. In the simulations, AES128 is used as the symmetric cryptography, and SHA256 is used as cryptographic hash function to generate the asymmetric keys. Fig. 5 shows the communication overhead among ECNs and smart meters. As a comparison, the communication overhead among concentrator and smart meters in traditional data transmission scheme is also shown in Fig. 5. It can be found more communication overhead cost by SEEDA. The reason is that the bidirectional identity authentication is implemented before data exchange in SEEDA. Digital signature transmission will increase the communication overhead. Because ECNs are close to the edge side, such communication overhead will not bring burns to the communication networks.

For the user electric energy data acquirement, the major bandwidth bottleneck lies in the telecommunication access network. The communication overhead between ECNs and master station is the crucial point. Fig. 6 shows the communication overhead between ECNs and master station. Compared to the traditional data transmission scheme of power user electric energy data acquire system, the communication overhead decreases by more than 86.1%. Because the ECNs complete the electricity data aggregation, the amount of data is reduced. As a result, the network traffic burden of telecommunication access network can be relieved.

5. Conclusion

Because the electric communication network cannot provide enough bandwidth resource to support high frequency electricity data exchange, data aggregation at edge side is expected. The ECNs need to aggregate electricity data from multiple smart meters into one block, so the amount of uploaded data can be reduced. However, ECNs usually cannot be treated as trustable entities in smart grid. Privacy-preserving strategy is expected in the electricity data aggregation. In this paper, we proposed a novel data aggregation scheme SEEDA for low voltage transformer areas. Homomorphic encryption techniques were employed, and the ECNs just implemented the electricity data aggregation based on
ciphertext. SEEDA can resist the possible external attack, and privacy of user’s electricity consumption information is preserved.

Acknowledgments
This work was supported by State Grid Technology Project “Edge Computing Research in Smart Grid Application and Security” (Grant: 52110118001H, Contract No:52110418001B).

References
[1] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G. P. (2011) Smart Grid Technologies: Communication Technologies and Standards. IEEE Transactions on Industrial Informatics, 7: 529–539
[2] Fang, X., Misra, S., Xue, G., Yang, D. (2012) Smart Grid - The New and Improved Power Grid: A Survey. IEEE Communications Surveys Tutorials, 14: 944–980.
[3] Satyanarayanan, M., Bahl, P., Caceres, R., Davies N. (2009) The Case for VM-Based Cloudlets in Mobile Computing. IEEE Pervasive Computing, 8: 14–23.
[4] Lopez, P., Montresor, A., Epema, D., Datta, A., Riviere, E. (2015) Edge-centric Computing: Vision and Challenges. Acm Sigcomm Computer Communication Review, 45: 37–42.
[5] Papageorgiou, A., Cheng, B., Kovacs, E. (2015) Real-time data reduction at the network edge of Internet-of-Things systems. In: 2015 11th International Conference on Network and Service Management. Barcelona, Spain. pp 284–291.
[6] Nazmudeen, M. S. H., Wan, A. T., Buhari, S. M. (2016) Improved throughput for Power Line Communication (PLC) for smart meters using fog computing based data aggregation approach. In: 2016 IEEE International Smart Cities Conference. Trento, Italy. pp 1–4.
[7] Yan Y., Su, W. (2016) A fog computing solution for advanced metering infrastructure. In: 2016 IEEE/PES Transmission and Distribution Conference and Exposition. Dallas, USA. pp 1–4.
[8] Le, C., Lu, R., Cao, Z., Alharbi, K., Lin X. (2015) MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications. Peer-to-Peer Networking and Applications, 8: 777–792.
[9] Fan, C., Huang, S., Lai, Y. (2014) Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid. IEEE Transactions on Industrial Informatics, 10: 666–675.
[10] Fouda, M. M., Fadlullah, Z. M., Kato, N., Lu, R., Shen, X. (2011) A Lightweight Message Authentication Scheme for Smart Grid Communications. IEEE Transactions on Smart Grid, 2: 675–685.
[11] Bao H., Chen L. (2016) A lightweight privacy-preserving scheme with data integrity for smart grid communications. Concurrency and Computation: Practice and Experience, 28:1094-1110.
[12] Zhuo G., Jia Q., Guo L., Li M., Li P. (2016) Privacy-preserving verifiable data aggregation and analysis for cloud-assisted mobile crowdsourcing. In 35th Annual IEEE International Conference on Computer Communications. San Francisco, USA. pp. 1-9.
[13] P. Paillier (1999) Public-key cryptosystems based on composite degree residuosity classes. In: International Conference on the Theory and Application of Cryptographic Techniques. Prague, Czech Republic. pp 223–238.
[14] Lu, R., Heung, K., Lashkari, A. H., Ghorbani, A. A. (2017) A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT. IEEE Access, 5: 3302–3312.
[15] Lu, R. (2016) Privacy-Enhancing Aggregation Techniques for Smart Grid Communications. In: Wireless Networks. Springer.