Joint Encryption and Compressed Sensing in Smart Grid Data Transmission

Juntao Gao1,2, Xiuming Zhang1,2, Hao Liang1, and Xuemin (Sherman) Shen3
1State Key Laboratory of Integrated Services Networks, Xidian University, Xi’an, China
2Department of Electrical and Computer Engineering, National University of Singapore, Singapore
3Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, Canada
E-mails: jtgao@mail.xidian.edu.cn, zhangxiuming@u.nus.edu, hao2@ualberta.ca, xshen@bbcr.uwaterloo.ca

Abstract—In smart grid, a huge amount of privacy data need to be transmitted securely and efficiently. Compressed sensing can be used to improve the transmission efficiency by exploiting the data sparsity, while this sparsity is usually destroyed by the encryption process, making compressed sensing inapplicable. A possible workaround is to perform compressed sensing first and then encrypt the compressed data. However, this two-step workaround lowers the efficiency. In this paper, we propose a novel data transmission scheme EncryCS. Compressed sensing in EncryCS provides security and simultaneously enhances the transmission efficiency in one step. The prerequisite of compressed sensing is to construct a measurement matrix satisfying the restricted isometry property that ensures the perfect recovery of the signal. To make the matrix secret and feasible, we generate it with a pseudorandom sequence generator. By using this matrix, EncryCS transforms a large amount of plaintext data into a small amount of ciphertext data. EncryCS is proven to possess a high security. Extensive simulations are performed based on the real-world data obtained from the PowerNet project at Stanford University. The results demonstrate that EncryCS can compress data by order of magnitude, and the transmitted data can be almost perfectly recovered.

I. INTRODUCTION

Telefónica reports that 800 million smart meters will be installed globally by 2020 [1]. Smart meters help the users monitor, manage, and reduce their power consumptions; they also help the utilities set the electricity price [2], reduce meter reading labor costs, and manage power better [3]. Despite these benefits, the popularization of the smart meters causes privacy concerns among the users, because one can infer a user’s life pattern, or a utility may spy on its competitor’s trade secrets with the smart meter readings [4][5]

As the number of smart meters soars, huge amounts of reading data need to be sent to the control center via access points (AP). This huge amount of data imposes a severe challenge on the processing capability of the APs. Inefficient data transmission not only burdens the APs but also retards the power controls from the utilities. In addition, the user privacy and the utility benefits can be harmed during the reading transmission, if the data confidentiality is not handled properly [6].

There are several works that address the efficiency problem with compressed sensing (CS) [7][8]. Some others handle the security issue in smart grid with the encryption techniques [7][9]. However, in smart grid, how to perform encryption and CS in one step remains as an open issue.

In [10], Orsdemir et al. presented a general idea of encryption via CS. Based on this, we propose EncryCS, a detailed data transmission scheme in smart grid that encrypts and compresses the data to transmit in one step. Investigating into the real smart meter readings from Stanford PowerNet [11], we discover that the difference sequence of the power readings between two adjacent time intervals is sparse, i.e., with many entries close to zero. This sparsity enlightens us to apply CS. The foundation of CS is the measurement matrix that reduces the signal amount. In order to ensure the data security, we generate the measurement matrix from a pseudorandom sequence generator (PRSG) with secret parameters.

Our three contributions can be summarized as follows.

• Unlike the previous CS works in smart grid, we integrate the encryption step directly into the CS process, meaning that our measurement matrix is secret by itself. This one-step approach, while ensuring the data security, improves the transmission efficiency of the readings.

• We provide a concrete construction method of the measurement matrix based on a structurally simple and implementation-wise feasible PRSG. Such a matrix satisfies the restricted isometry property (RIP), an indispensable condition for the perfect restoration of the signals in CS. Furthermore, the matrix can be resized freely, making EncryCS universal with various numbers of smart meters.

• Different from many other smart grid works, we perform extensive simulations with the real-world smart meter data. The simulation results not only support our claims but also provide several insights into the real data, which may be beneficial for the future researchers.

The remainder of the paper is organized as follows. Section II summarizes the related works. Section III provides a basic model for EncryCS and the preliminaries of CS and PRSG. Section IV presents EncryCS and analyzes its security. The simulation results are shown in Section V. Finally, Section VI concludes the paper and points out future work.

II. RELATED WORK

CS has been employed in smart grid [7][8]. Li et al. investigated the data correlations among the smart grid readings
and applied CS to the correlated data [8]. To achieve different security objectives, the homomorphic encryption and searchable encryption have been applied to smart grid [3][5][9]. Combining CS and the homomorphic encryption, Cai et al. in [7] proposed a reading transmission scheme in smart grid, which contains two steps. The first step is to encrypt the data with the Pallier cryptosystem and then sign them with the standard digital signature. The second step is to compress the encrypted data with CS.

In [10], Orsdemir et al. showed that the pseudorandom measurement matrix in CS could act as the secret key and gave a security analysis on the brute and structured attacks. However, a concrete construction method of such a pseudorandom measurement matrix was not presented. In [12], Rachlin and Baron pointed out that schemes similar to [10] achieve the computational security instead of the perfect security. In fact, the perfect security is the ultimate limit of cryptography and is infeasible in practice. Thus, most of the cryptographic schemes possess only the computational security.

III. SYSTEM MODEL

In this section, we present the general setting of our system model and provide some basic knowledge on the CS technique and PRSG. As shown in Figure 1, our smart grid model consists of three parties: smart meters, APs, and a control center. The smart meters collect the power readings labeled with the meter IDs and send them to the APs. These readings are stacked up and then sent together to the control center by APs. In this model, the APs play an intermediary role and need to deal with huge amounts of data, when numerous smart meters are installed. CS can be used to improve the transmission efficiency.

An N-dimensional real-value vector \( \mathbf{x} \) is said to be \( K \)-sparse, if there exists an orthonormal matrix \( \Theta = (\theta_1^T, \theta_2^T, ..., \theta_K^T) \) such that there are at most \( K \) nonzero coefficients \( v_i \) in

\[
\mathbf{x} = \sum_{i=0}^{N-1} v_i \theta_i^T.
\]

CS is able to compress the sparse signal by using an \( M \times N \) matrix \( \Psi \), called the measurement matrix. \( \Psi \) needs to satisfy the following restricted isometry property (RIP).

**Definition 1** ([13][14]). An \( M \times N \) matrix \( \Psi \) is said to satisfy the RIP of sparsity \( K \), if there exists a restricted isometry constant (RIC) \( \delta_K \in (0, 1) \) such that

\[
(1 - \delta_K) \| \mathbf{x} \|_2^2 \leq \| \Psi \mathbf{x} \|_2^2 \leq (1 + \delta_K) \| \mathbf{x} \|_2^2
\]

holds for any \( K \)-sparse \( N \)-dimensional vector \( \mathbf{x} \), where \( \| \cdot \|_2 \) denotes the \( \ell_2 \) norm.

We transform the \( N \)-dimensional vector \( \mathbf{x} \) into a new \( M \)-dimensional vector \( \mathbf{y} \), i.e., \( \mathbf{y} = \Psi \mathbf{x} = \Psi \Theta \mathbf{v} \), where the sparse representation \( \mathbf{v} = (v_0, v_1, ..., v_{N-1}) \). Although \( \mathbf{y} = \Psi \mathbf{x} \) is an underdetermined system with infinitely many solutions, \( \mathbf{x} \) can still be accurately found by solving a tractable \( \ell_1 \) convex optimization problem. The following lemma presents two types of measurement matrices that satisfy RIP with an overwhelming probability.

**Lemma 1** ([15]). The probability that an \( M \times N \) matrix \( \Psi \) satisfies the RIP of sparsity \( K \) with a RIC \( \delta_K \in (0, 1) \) is at least \( 1 - \exp(c_1M) \) for any \( c_1 < \delta_K^2(3 - \delta_K)/48 \), if \( M \geq c_2K \log N \), where

\[
c_2 = \frac{192 \log(12/\delta_K)}{3\delta_K^2 - \delta_K - 48\delta_K}.
\]

and the entries \( \psi_{ij} \)'s in \( \Psi \) are independent and identically distributed (i.i.d.) in either of the following zero-mean distributions with a variance of \( 1/M \),

\[
\psi_{ij} \sim \mathcal{N}(0, 1/M)
\]

and

\[
\psi_{ij} \sim \begin{cases} 1/\sqrt{M} & \text{with a probability of } 1/2 \\ -1/\sqrt{M} & \text{with a probability of } 1/2 \end{cases}
\]

The vector sparsity and RIP of the measurement matrix together determine whether a signal can be recovered perfectly. Thus, the sparse expression of the vector and the construction of the RIP-satisfying matrix become very essential for CS.

We adopt a class of PRSG called generalized self-shrinking (GSS) generator for the measurement matrix construction. Established over the finite field \( \mathbb{F}_2 \), the GSS sequence is defined as follows.

**Definition 2** ([16]). Let \( a = a_0a_1a_2 \ldots \) be a binary maximal length shift register sequence (m-sequence) with the least period \( 2^n - 1 \). Let \( g = (g_0, g_1, \ldots, g_{n-1}) \in \mathbb{F}_2^n \). For \( k = 0, 1, 2, \ldots \) if \( a_k = 1 \), store \( g_0a_k + g_1a_{k-1} + \ldots + g_{n-1}a_{k-n+1} \) into a sequence \( b(g) \), where both the addition and multiplication are binary. Otherwise, discard the result. We then call the result sequence \( b(g) = b_0b_1b_2 \ldots \) a binary GSS sequence. \( B(a) = \{ b(g) \mid \exists \mathbf{g} \in \mathbb{F}_2^n \} \) is called the GSS family based on the m-sequence \( a \).

There are two reasons for choosing the GSS sequence to construct the measurement matrix. First, a GSS generator can be easily implemented by only one linear feedback shift register and one shrinking structure. Second, the GSS sequences possess good pseudorandom properties, such as large period, large linear complexity, and so on.

IV. PROPOSED ENCRYCS SCHEME

We elaborate EncryCS step by step, and then perform the security analysis of EncryCS. Let both the control center and APs hold the GSS generator with three parameters, i.e., the primitive polynomial \( f(x) \in \mathbb{F}_2^2[x] \), initial state
A. Procedure

At time $t$, an AP receives $N$ readings from $N$ smart meters, denoted by a reading vector $p(t) = (p_0(t), p_1(t), \ldots, p_{N-1}(t))$. We apply the measurement matrix $\Psi$ to transform the $N$-dimensional vectors into the $M$-dimensional vectors and encrypt the vectors simultaneously in one step.

Step 1: The AP obtains the initial reading vector $p(0)$ and then directly sends an unprocessed copy to the control center.

Step 2: At time $t \geq 1$, the AP computes the difference vector $p(t) - p(t-1) = (p_0(t) - p_0(t-1), \ldots, p_{N-1}(t) - p_{N-1}(t-1))$.

Step 3: With a secret $m$-sequence and a secret vector $g$, we can generate an $M \times N$ measurement matrix $\Psi$, which will remain unchanged until the security margin gets broken. The secret measurement matrix is held by both the AP and the control center.

Step 4: The AP computes $y = \Psi(g(t) - p(t-1))$ and then transmits the resulting $M$-dimensional vector $y$ to the control center.

Step 5: Relying on CS, the control center recovers the difference vector $p(t) - p(t-1)$ given $y$ and $\Psi$.

Step 6: With the initial vector $p(0)$, the control center is able to compute the vector $p(t)$ at time $t$.

For Step 3, we generate the $m$-sequence with a primitive polynomial $f(x)$ and an initial state $(a_0, a_1, \ldots, a_{n-1})$. With this $m$-sequence and a vector $g$, we are able to produce a GSS sequence $b(g) = b_0b_1 \ldots$ according to Definition 2. Following from Equation (3) in Lemma 1, the $M \times N$ measurement matrix $\Psi$ can be constructed from $b(g)$ as follows:

$$
\Psi = \begin{pmatrix}
(-1)^{b_0} / M & \ldots & (-1)^{b_{N-1}} / M \\ (-1)^{b_1} / M & \ldots & (-1)^{b_{N-1}} / M \\ \vdots & \ddots & \vdots \\ (-1)^{b_{M-1}} / M & \ldots & (-1)^{b_{M-1}} / M 
\end{pmatrix},
$$

where $MN \leq 2^{n-1}$. Section V will show that $\Psi$ satisfies the RIP and $p(t) - p(t-1)$ can be almost perfectly recovered.

Appropriately, it may be more efficient for the AP to transform an $M$-dimensional vector instead of an $N$-dimensional one, because $M$ is much smaller than $N$. As for the security, an attacker can decode the encrypted data by obtaining the secret $\Psi$. However, it is rather difficult for the attacker to directly obtain $\Psi$, because there are $MN$ unknown binary bits in $\Psi$. In [10], Orsdemir et al. analyzed two types of attacks on the secret measurement matrix based on its symmetry and sparsity structure. The result shows that the unknown measurement matrix cannot be broken with a low complexity. Another possibility for the attacker to capture $\Psi$ is by analyzing the weakness of the GSS generator, since the measurement matrix is constructed from a binary GSS generator. Hence, we will next provide the security analysis of the binary GSS generator.

B. Security Analysis

We summarize the relevant pseudorandom properties of the GSS generator as follows [16].

- $b(g)$ is a balanced sequence in one period except for $g = (0, 0, \ldots, 0)$ and $g = (1, 0, \ldots, 0)$.
- In $B(a)$, more than 75% of the sequences have the linear complexity greater than $2^{n-2}$, which guarantees that the sequences can resist the well-known Berlekamp-Massey attack, when $n$ is an appropriately large number.
- $B(a)$ constitutes a linear space with an element-wise sequence addition operation $\oplus$. That is, for any two vectors $g^{(1)}$ and $g^{(2)}$ in $\mathbb{F}_2^n$, we have $b(g^{(1)}) \oplus b(g^{(2)}) = b(g^{(1)} + g^{(2)}) \in B(a)$.

In [17], Zhang et al. discussed the security of a GSS sequence from the following two aspects.

- If both $g$ and $f(x)$ are known, the computational complexity of an improved clock-guessing attack is $O(2^{0.694n})$, where $n$ is the degree of $f(x)$.
- Given $f(x)$, for a GSS generator with $n = 61$, the computational complexity of a fast correlation attack to obtain the initial state and the vector $g$ is $O(2^{26})$.

In [18], Gao et al. provided a security analysis based on the correlations among different GSS sequences. The result demonstrates that the attack complexity can be reduced by using several sequences produced with an identical initial state but different $g$s. Furthermore, it is shown that the unknown initial state can be found with a time complexity

$$O(t^2 \times (r - 1)! \times 2^{1+71} \times n^3),$$

where $r$ is the number of the correlated GSS sequences, and specifically, $r = 5$ for $60 < n < 130$. Although the time complexity is not large, the required GSS sequences are still difficult to find, because those $g$s have to be chosen delicately.

Remark 1. The difference between the attack complexities of [17] and [18] results from different attack assumptions on $g$ and $f(x)$. More details can be found in [17] and [18].

The analysis above demonstrates that breaking a GSS generator with the existing attack methods is infeasible due to either a large computational complexity or strong attack assumptions that are difficult to achieve.

As for the exhaustive attack, note that there are $\phi(2^n - 1)$ primitive polynomials with degree $n$, $2^n - 1$ possible initial states, and $2^n - 2$ possible $g$s, where $\phi(\cdot)$ denotes the Euler function. Therefore, the exhaustive attack on a GSS generator has a complexity of

$$O((2^n - 1)(2^n - 2) \phi(2^n - 1)/n).$$

Definition 3 ([16]). Let $\alpha = a_0a_1a_2 \ldots$ be an $m$-sequence with the period $2^n - 1$. Let $T = \{u(t) \mid t = 0, 1, 2, \ldots\}$ be a subset of $\mathbb{Z}$ such that $0 \leq u(0) < u(1) < \ldots, a_{u(t)} = 1$ for
each \( u(t) \in T \), and \( a_n = 0 \) for each \( u \notin T \). We then call \( u(t) \) the \( t \)-th output moment of family \( B(a) \).

**Lemma 2.** Let \((a_0, a_1, \ldots, a_{n−1})\) be the initial state of the \( m \)-sequence in a GSS generator. Then, there exists an equivalent state \( (a_{u(0)}, a_{u(0)+1}, \ldots, a_{u(0)+n−1}) \) that produces the same GSS sequence with the identical \( g \) and \( f(z) \).

**Proof:** As defined in Definition 2, a GSS generator outputs nothing, if \( a_0 = 0 \) at the very beginning. That is, only if \( a_0 = 1 \) does the generator start to output the sequence. Hence, there always exists an equivalent state with the first bit being 1 for any initial state.

**Lemma 3.** The vector \( g \) can be solved with a time complexity of \( O(n^3) \), if an attacker obtains the primitive polynomial, the \( m \)-sequence initial state, and a \( 2n \)-bit-long segment of \( b(g) \).

**Proof:** Knowing the primitive polynomial and the initial state of the \( m \)-sequence, the attacker is able to obtain the whole \( m \)-sequence \( a \). For the \( j \)-th bit \( a_j \) in \( b(g) \), the attacker formulates an equation of the unknown vector \( g \) as follows

\[ 90a_{u(j)} + 9a_{u(j)+1} + \ldots + 9n−1a_{u(j)+n−1} = b_j. \]

If the attacker learns a \( 2n \)-bit-long segment in \( b(g) \), according to the \( m \)-sequence theory, it is easy to find \( n \) linearly independent equations to form an equation group, which can be solved with a computational complexity of \( O(n^3) \).

**Theorem 1.** For a GSS generator with the key (the primitive polynomial, \( m \)-sequence initial state, and vector \( g \)), the attack complexity can be reduced to \( O(2^{n−1} \times n^3) \), if the attacker obtains a \( 2n \)-bit-long segment of \( b(g) \).

**Proof:** By Lemma 2, the attacker knows the first bit of the equivalent state to be 1. Thus, the complexity of the exhaustive search among the remaining bits of the initial state is \( O(2^{n−1}) \). Combining the \( 2n \)-bit-long segment of \( b(g) \) and the initial state of \( m \)-sequence, the attacker can obtain a bit segment of \( m \)-sequence that is longer than \( 2n \) bits. The primitive polynomial can be obtained with a complexity of \( O(n^3) \). By solving the equation of \( g \), the key can be obtained with a complexity of \( O(2^{n−1} \times n^3) \).

Therefore, the security of a GSS generator depends heavily on the confidentiality of the \( m \)-sequence initial state because of the exponential complexity increase as shown by Theorem 1. However, \( g \) is also vital, because it is possible to calculate the primitive polynomial and the initial state from the property \( b(g^{(1)}) \oplus b(g^{(2)}) = b(g^{(1)} \oplus g^{(2)}) \in B(a) \). To avoid this linear correlation, we only choose the \( g \)'s whose first entry is 1 to generate the measurement matrix. Following this rule, we guarantee that one cannot infer the next \( g \) to be used from any two used \( g \). Note that it is possible to launch an attack by exploiting the correlations among different \( m \)-sequences. However, such correlations have been thoroughly destroyed by the shrinking algorithm of the GSS generator.

EncryCS is flexible in the sense that one can control its security strength by adjusting \( M, N, f(z), (a_0, a_1, \ldots, a_{n−1}), g \), and in turn \( \Psi \). Given the values of these parameters, the control center is able to compute the attack complexity that explicitly manifests the security margin of the current implementation. According to the security margin, the control center knows exactly when to change the parameters.

V. SIMULATION RESULTS

The smart meter data used are from Stanford PowerNet [11] consisting of 266 smart meters. We use the data collected on November 5, 2010 in our following simulations and analysis.

A. Sparsity and Recovering

We study how the time interval (TI) duration affects the sparsity of the difference signal and evaluate how accurately EncryCS recovers the original signal. We characterize a pair of adjacent TIs with two parameters: the starting time \( t \) and the interval duration \( \Delta t \). Figures 2a to 2d show the average powers in the former TI and latter TI of each smart meter. The blue squares represent the average powers of the smart meters in the former TI, and the red asterisks are the average powers of the same smart meters in the latter TI. We evaluate EncryCS under four scenarios, i.e. \( t = 9:00 \) with \( \Delta t = 1 \) min, \( t = 9:00 \) with \( \Delta t = 15 \) min, \( t = 14:00 \) with \( \Delta t = 1 \) min, and \( t = 14:00 \) with \( \Delta t = 15 \) min. The reasons why 1 min and 15 min are chosen as the \( \Delta t \) values are that the current smart meters usually report the data once every 15 minutes [6], and we believe that the reporting interval will soon dwindle to 1 minute with the rapidly developing technology.

As shown in Figure 2, for each smart meter, the red asterisk usually falls very close to the blue square, which corresponds to the fact that the powers of one device in two adjacent TIs usually differ by little. Note that there are indeed some cases where the red asterisk and the blue square sit far apart (such as meter 16 in Figure 2c), leading to a power spike in the difference signal (Figure 3c). The device that meter 16 measures is looked up to be a printer whose average power rises from 19.92 W (during 14:00 - 14:01) to 333.20 W (during 14:01 - 14:02). This power spike may be caused by a printing command that brings the printer from its idle state to its working state. Based on the observations above, we take the difference between the blue and red curves in Figure 2 and manage to obtain very sparse signals (blue square signals in Figure 3) with most of the entries close to zero. Note that the difference signal in Figure 3a (Figure 3c) is sparser, i.e., with more close-to-zero entries, than that in Figure 3b (Figure 3d). This phenomenon is due to the fact that the average power of one device tends to fluctuate more violently over two long-duration TIs than over two short-duration TIs.

As shown in Figure 3, EncryCS is able to recover the signals nearly perfectly in small-\( \Delta t \) cases (Figures 3a and 3c). Even in the large-\( \Delta t \) cases (Figures 3b and 3d), the less sparse signals can still be recovered to an acceptable extent under the context of smart grid. To quantize the recovering errors, we tabulate the mean absolute errors (MAE) between the original signal and the recovered signal in all four scenarios in Table I.
MAE is computed as $\frac{1}{C} \sum_{i=1}^{C} |y_i - x_i|$, where $C$ is the total count of the smart meters, and $x_i$ and $y_i$ are the $i$th values of the original and recovered signals, respectively.

B. Encryption and Compression

In Figures 4a and 4b, the blue asterisk curves represent the raw 64-dimensional difference signals, and the red dot curves denote the encrypted and compressed 32-dimensional signals.

As shown in both figures, the originally sparse blue signals become no longer sparse and fluctuate violently after EncryCS. This serves as an easy and intuitive visualization of the encryption effect. As for the compression effect, the signal dimension reduces from 64 (the raw difference signals) to 32 (the processed signals) after EncryCS.

C. Restricted Isometry Constant

We compare the RIC $\delta_K$ value distributions of 1000 matrices generated with EncryCS and 1000 Gaussian random matrices (GRM). By definition, the entries of a GRM satisfy Equation (2). All these 2000 matrices are of size $32 \times 64$, and the sparsity $K$ is set as 10 based on the estimation that usually fewer than 10 out of 64 smart meters experience large power fluctuations between the two adjacent TIs.

Based on Definition 1, we test each matrix with 1000 random $K$-sparse signals and try to find a $\delta_K$ for each of the 1000 signals. In terms of the computer implementation, the value of $\delta_K$ increments from 0 to 1 with a step size of 0.001. Only when at least one qualified $\delta_K$ value is found for every signal can one matrix be said to satisfy the RIP of sparsity $K$. The distributions of all the first, or equivalently the smallest, $\delta_K$ values for EncryCS matrices and GRMs are presented in the form of cumulative distribution function (CDF) in Figure 5. It is evident that the $\delta_K$ values of EncryCS matrices are unanimously smaller than those of the GRMs.

D. Flexible Measurement Matrix Size

Figure 6 shows the probabilities that the variable-size EncryCS matrices satisfy the RIP of sparsity 10. The matrix row number $M$ ranges from 16 to 32, the order of the $m$-sequence $n$ ranges from 11 to 16, and the vertical axis is the RIP-satisfying probability given a $(M, n)$ pair. Recall that given $M$ and $n$, the column number $N$ of the measurement

| Time Interval | $t = 9:00$ | $t = 9:00$ | $t = 14:00$ | $t = 14:00$
|---------------|------------|------------|-------------|-------------
| MAE (W)       | 0.2162     | 1.0183     | 0.0340      | 0.7134      |

Fig. 2. Raw average powers of smart meters in the former TI and the latter TI.

Fig. 3. Sparse difference signals and recovered signals.

Fig. 4. Raw 64-D signals vs. encrypted and compressed 32-D signals.
Furthermore, we have provided a novel PRSG-based solution between APs and the control center. Our future work will focus on developing an end-to-end secure system for data transmission from the smart meter to the control center.

ACKNOWLEDGMENT

We would like to express our gratitude to the research group of the Stanford PowerNet project for providing the smart meter readings. This work was supported by the research grants from the Natural Sciences and Engineering Research Council of Canada (NSERC), the Natural Science Foundation of China (No. 61303217, 61373174), the 111 project (No. B08038), the Fundamental Research Funds for the Central Universities (No. K5051301044, K5051270003), the Natural Science Foundation of Shanxi province (No. 2013JQ002, 2014JQ0313), and Open Project of State Key Laboratory of Information Security.

REFERENCES