Received February 20, 2013, accepted April 11, 2013, published May 10, 2013.

Digital Object Identifier 10.1109/ACCESS.2013.2260815

A Distortion-Based Approach to Privacy-Preserving Metering in Smart Grids

Xingze He (Student Member, IEEE)[1], Xinwen Zhang (Member, IEEE)[2], and C.-C. Jay Kuo (Fellow, IEEE)[1]

[1]Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90007, USA
[2]Huawei Research Center, Santa Clara, CA 95050, USA

Corresponding author: X. He (xingzehe@usc.edu)

ABSTRACT In this paper, we propose an efficient distortion-based privacy-preserving metering scheme that protects an individual customer's privacy and provides the complete power consumption distribution curve of a multitude of customers without privacy invasion. In the proposed scheme, a random noise is purposely introduced to distort customers' power consumption data at the smart meter so that data recovery becomes infeasible. Using the power consumption data and prior knowledge about added random noise, we develop an efficient algorithm for power consumption distribution reconstruction needed for power demand analysis and prediction. As a complete solution, our scheme also supports a privacy-preserving billing service. Using experimental results from real world single household power consumption data set and synthesized data of a large number of households, we demonstrate that the proposed scheme is robust against known attacks. Since it does not demand new facilities on existing smart grids, the proposed scheme offers a practical solution.

INDEX TERMS Data privacy, power consumption, privacy protection, privacy-preserving, smart grids, smart meter.

I. INTRODUCTION

By combining physical electrical systems with digital information and communication technologies, smart grids aim to provide highly efficient, intelligent, and environmentally-friendly electricity services. This ambition makes smart grids rather different from legacy power systems in many aspects such as widely used renewable energy sources, two-way electricity flow, distributed power sources, and dynamic pricing and load control. To achieve these challenging goals, a smart grid system usually contains many different functional subsystems to form a highly complex system. As shown in Fig. 1, a smart grid system generally consists of seven major domains: bulk generation, transmission, distribution, customers, service providers, operations, and markets. Systems in bulk generation, transmission, and distribution domains focus on energy generation and delivery from power plants to customers. According to the power demand level, customers are usually classified to three categories: commercial, industrial, and residential customers. Unlike legacy power systems, customers in a smart grid are both electricity consumers and providers. They can freely sell their locally generated electricity to the system at a dynamic price determined by the market domain in real time. A service provider provides a variety of services (*e.g.*, billing and account management) to both customers and utility companies. All these domains are connected with the operation domain for central control and management.

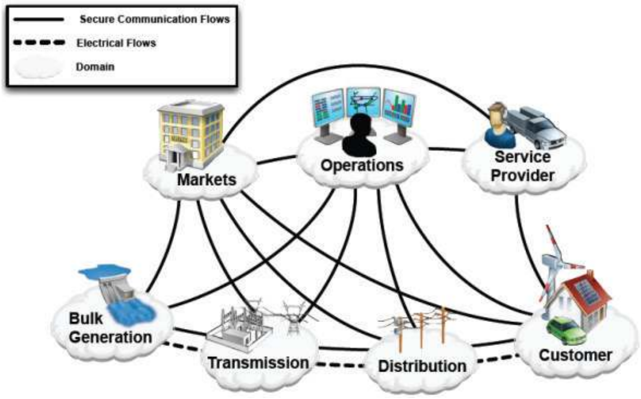


FIGURE 1. Illustration of a typical smart grid system [1].

To achieve high efficiency and intelligence for such a large complex system, real-time power consumption

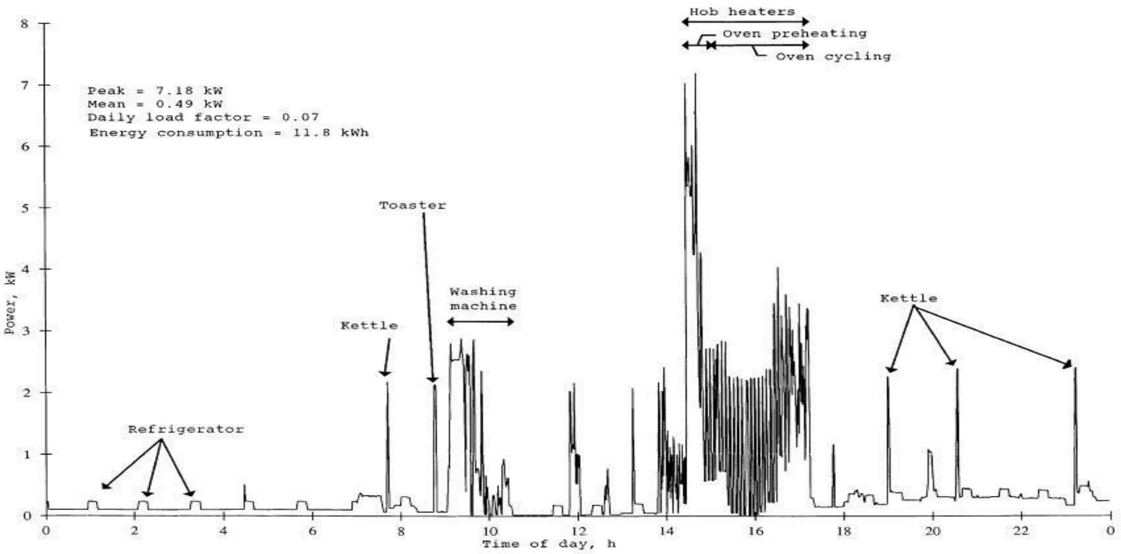


FIGURE 2. Mapping from the power usage to personal activities [2].

statistics of the entire system are essential to all domains in estimating the current system state and predicting future conditions. Decisions are cautiously made according to the analysis of customers' power consumption data. For example, the information of fine-grained customer's power consumption is required by the market domain to determine the electricity price in real time, and the bulk generation domain also needs the information for power demand prediction.

In a legacy power system, the total power consumption of a household is collected by a utility company every two weeks or monthly. There is no data privacy concern in this situation since power consumption details are hidden in the aggregated readings. In a smart grid system, however, the high efficiency and intelligence features demand more granular power consumption data for real-time system monitoring and management as discussed before. This transformation of information granularity leads to severe privacy issues. Fig. 2 shows a customer's daily power consumption trace (PCT) that was obtained by a utility company. With simple observation, an attacker can easily find out what time and how much electricity is used in a customer's home. With advanced power signature analysis tools such as the non-intrusive load monitoring (NILM), the attacker can easily find out what types of appliances are used at any time and learn more detailed information about customer's daily activities. Examples are shown in Table 1. This behavior mapping enables the derivation of a detailed profile of a customer's daily activities from his/her power consumption trace.

Various entities are interested in this type of sensitive information. First, thieves may exploit the information to study the behavior of a customer living in a target house. They can easily break into the house when they derive the information like "nobody is in the house tonight." Commercial companies are also interested in the power consumption behavior of customers. For example, advertising household appliances will become more effective when sales people figure out which appliances are widely used by customers in their daily lives. Besides, a smart grid system may allow many third party companies to access customers' power consumption data to help them manage energy usage. As a result, third party applications may become another potential source of privacy abuse. Without proper protection, customer privacy and even security will be severely threatened, especially when the public network (*e.g.*, the Internet) is adopted for data transmission in a smart grid system.

TABLE 1. Behavior mapping from the power usage to daily activities.

Power Usage	Activities
Energy cycle of TV Energy cycle of coffee pot Energy cycle of water heater ...	Anybody at home? When people wake up? How many people living there? ...

To solve this problem, previous work has focused on cryptography-based solutions, where customers' power consumption data are protected under certain cryptographic schemes. One of the common problems of this type of solutions is how to efficiently share real-time power consumption data with different functional domains. Key-sharing among different parties is a potential problem with security concern. In addition, frequent encryption and decryption operations harm system's efficiency. Another problem is related to key management. In a smart grid, there are typically millions of customers located in different regions for one utility company. The conventional public key infrastructure cannot meet the key management requirements of such a large scale network [3]. Privacy-protection schemes from other perspectives have been studied recently, yet they have issues towards practical deployment. That is, there is no efficient way to extract the statistical information of power consumption data for critical features needed for power consumption analysis, forecasting and dynamic pricing. More related work will be reviewed in Section II.

In face of the privacy issue in smart grids and drawbacks of existing solutions, we propose a distortion-based privacy-preserving metering scheme. To be more specific, we introduce random noise on purpose to distort customers' power consumption data at the smart meter in a way that data recovery becomes infeasible. Under the assumption that all other parties except smart meters are semi-trusted, the proposed scheme protects customers' data privacy to a high degree. With distorted power consumption data and prior knowledge about the added random noise, we develop an efficient algorithm for power consumption distribution reconstruction needed for power demand analysis and prediction. With this proposed algorithm, any party in a smart grid can derive complete power consumption statistics of certain geographical area without privacy invasion. To make our scheme more complete, the billing issue is also addressed. We evaluate the proposed scheme with both real world and synthesized power consumption data, and demonstrate that it is robust and efficient in practical implementations.

The rest of this paper is organized as follow. Section II discusses related work on privacy issues in smart grids. The proposed metering scheme is presented in Section III. Privacy protection and efficiency analysis of the proposed scheme is analyzed in Sections IV and V, respectively. Section VI presents experimental results and, finally, Section VII concludes this paper.

II. RELATED WORK

The NIST Cyber Security Working Group published three-volume guidelines [4]–[6] on security and privacy issues of smart grids in 2010. The guidelines focus on high level requirements and potential technologies in the design of secure smart grid systems. In the same year, the importance of data privacy in smart grids was once again emphasized in the context of smart grid interoperability [7]. In 2011, IEEE published a trial-use standard [8] on a cryptographic protocol for cyber security of substation serial links. The protocol provides integrity and optional confidentiality for communications between substations. However, there is no standard in protecting customer's data privacy in smart grids up to now.

Cryptography-based privacy-preserving data aggregation schemes have been proposed for smart grids, *e.g.* [9]–[12]. Garcia and Jacobs [9] introduced an advanced partially homomorphic encryption scheme to prevent the data aggregator from accessing individual readings. To address the privacy concern of billing service, Molina-Markham *et al.* [13] proposed a zero-knowledge-based protocol to privately derive and prove the correctness of bills. Along the similar technique, Rial and Danezis [11] proposed a cryptographic protocol for general calculations on meter readings. These studies mainly address privacy concerns from the data aggregation process or the billing service. However, none of them can solve both of them at once. Recently, Lin *et al.* [14] proposed a lightweight cryptographic scheme with the support of a trusted platform module for both privacy-preserving billing and load monitoring purposes. However, the load monitoring task is limited to collecting the sum of metering data over a certain period of time. Generally speaking, privacy-preserved data sharing and real-time power consumption analysis and forecasting are not well addressed in the above-mentioned work. Furthermore, cryptography-based schemes generally demand a complex key management process, including key revoking, distribution and updating, particularly for smart grids where scalability is a major issue [3].

In addition to cryptography-based schemes, several other ideas have been proposed recently to protect customer data privacy in a smart grid. Efthymiou and Kalogridis [15] introduced an anonymization scheme by assigning each smart meter two different identifiers, the real identity and the pseudonym. The real identity is used for readings associated with billing while the pseudonym for anonymous readings. The escrow, which is the only trusted third party, knows the relationship between the two identifiers. Although the scheme provides a way to hide customer's identity, the trust relies on the third party. Besides, Jawurek *et al.* [16] showed that basic data mining and pattern recognition techniques can break this anonymization scheme by building connections from customers' pseudonyms to their real identities. Another interesting idea is to mask fine-grained power consumption information with the help of re-chargeable batteries. Schemes proposed in [17] and [18] fall into this category. Both schemes use re-chargeable batteries to hide, smoothen or obscure the fine-grained power consumption trace by charging and discharging operations. However, battery's lifetime is short while its cost is high, which is approximately $1000 for a household [18]. Energy loss in battery storage results in higher energy consumption. Furthermore, real-time power consumption analysis and dynamic pricing are difficult due to the lack of the real original power consumption data.

III. PRIVACY-PRESERVING METERING SCHEME

In this section, we propose a lightweight privacy-preserving metering scheme. The main motivation is to enable effective interoperation of power consumption data by different parties while protecting customer's privacy. Without requiring extensive cryptographic operations on metering data and extra hardware support such as batteries, our scheme is more efficient and practical as compared to previous schemes. The fundamental idea is to distort customer's metering data with random noise in such a way that data recovery is impossible while the extraction of statistic information for regional power usage is easy. In this way, distorted readings can be shared among different parties for different purposes, *e.g.*,

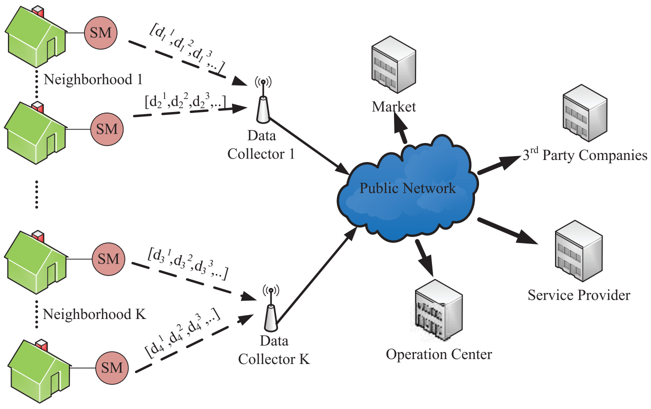


FIGURE 3. The system model of the proposed privacy-preserving metering scheme.

power consumption analysis, forecasting, dynamic pricing, and so on.

A. SYSTEM OVERVIEW AND TRUST ASSUMPTIONS

Fig. 3 shows the system model based on the widely accepted wireless-wired multi-layer architecture [3], [19]–[21]. A smart meter in each household aggregates the power consumption data from various appliances through the home area network (HAN). Before sending to a data collector of the neighborhood through a wireless mesh network, the smart meter first distorts the aggregated fine-grained power consumption data. After receiving the distorted data, the data collector located in the neighborhood transmits the data to different parties through the public network directly or to a central data center which can be accessed by those parties.

The following three assumptions are made in the proposed scheme.

1) The smart meter has a security mechanism to maintain the integrity of its computing code and prevent illegal reading and manipulating of energy readings and its secrets (*e.g.*, private keys). Furthermore, it has sufficient computing and storage capability to guarantee that the aggregation of original readings is accurate and reliable.
2) Both data collectors and other entities in the smart grid (*e.g.*, service providers, markets, and 3rd-party companies) are semi-trusted. They follow a protocol to provide services and meet users' service requirements. On the other hand, they also attempt to retrieve the information of customer's behavior as much as possible.
3) Authentication mechanisms are adopted for data transmission among smart meters, data collectors, and other entities in the system, *e.g.*, each smart meter is embedded with a public/private key pair. The private key is protected by the device while the public key can be trusted by the data collector or other entities.

The proposed scheme consists of three parts: (1) power consumption data distortion conducted by smart meters, (2) aggregated billing conducted by the utility company, and (3) power consumption distribution reconstruction by interested parties. They are detailed below.

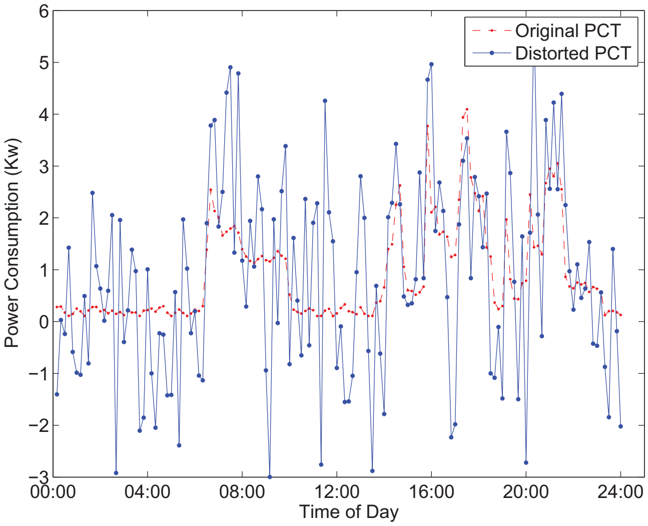


FIGURE 4. Example of a distorted power consumption trace.

B. POWER CONSUMPTION DATA DISTORTION

Power consumption data distortion is implemented at the smart meter, where random Gaussian noise is added to the aggregated power consumption data of various appliances. For simplicity, we assume each electricity consumer is bound to one smart meter. For an M-consumer power grid, we have a group of smart meters distributed in different places. Each smart meter reports its distorted power consumption data every T seconds, where T is known as the reporting period. The sequence, $r_i[0], r_i[1], r_i[2], \ldots r_i[j], \ldots$ represents the sample sequence of the aggregated power consumption of the i^{th} customer from time $t = 0$ to $t = nT$. The distorted data can be expressed in form of

$$d_i[j] = r_i[j] + n_i[j], \quad i = 1, 2, \ldots, M, \quad j = 0, 1, 2, \ldots, n, \tag{1}$$

where $n_i[j]$ is a sample of random Gaussian noise with zero mean and variance σ_N^2. The noise power significantly affects the performance of the proposed metering scheme, which will be discussed in detail in Section VI.

Fig. 4 gives an example of a distorted power consumption trace in a single day. The red curve is the original power consumption trace while the blue one is the distorted one. It is obvious that high frequency distortions have masked a large amount of valuable information about customer's power usage. Besides, many fake events are fabricated. Without knowing the exact noise samples used for distortion, the original power consumption trace is impossible to be recovered. Since we use relatively large noise as compared to the original data, conventional de-noising techniques and long-term averaging schemes are not able to retrieve privacy-sensitive power usage patterns. We will provide mathematical analysis and experimental results in Sections IV and VI, respectively.

C. AGGREGATED BILLING

In order to facilitate accurate and efficient billing without privacy invasion, an aggregated billing mechanism is adopted as part of the proposed metering scheme. Specifically, we use a storage unit in the smart meter device to accumulate the electricity bill. The initial value of the accumulator is set to 0. Given dynamic electricity price, $P[j]$, at time $t = j$, the aggregated bill AB of the i-th customer can be updated after each reporting time as

$$AB_i[j] = AB_i[j-1] + r_i[j] \times P[j], \tag{2}$$

where $r_i[j]$ denotes power consumption during the time period from $t = j-1$ to $t = j$. When the smart meter receives a billing query from the billing service provider, it sends back the updated AB and resets the storage unit. Since we assume the smart meter is securely protected against energy theft and it can authenticate itself to the billing service provider, any unauthorized party cannot access and manipulate the power consumption data in the smart side and during data transmission. Optionally, the service provider can exploit the zero-knowledge proof technique as detailed in [11], [13] to verify the correctness of the bill.

D. POWER CONSUMPTION DISTRIBUTION RECONSTRUCTION

Billing is not the only purpose of collecting customer's power consumption data in a smart grid. Another essential usage of the collected data is power consumption analysis and prediction for power generation and distribution. Many third party companies are interested in the statistical information of customers' power consumption for business planning and development.

Being distinct from previous schemes that provide limited statistical information (*e.g.*, only the total power consumption and the average power consumption of a neighborhood), our scheme can provide a complete distribution curve of the original power consumption for a multitude of customers. On the other hand, by only dealing with distorted power consumption data, the distribution reconstruction process does not leak any private information of a specific customer.

The reconstruction process is conducted on the distorted data as given in Eq. (1). Given the density function of noise N and a sample sequence of distorted power consumption data at time $t = jT$, we have

$$d_i = r_i + n_i, \quad i = 1, \ldots, M,$$

where $d_i = d_i[j]$, $r_i = r_i[j]$, $n_i = n_i[j]$ and M is the number of customers. We use D, R and N to denote random variables for $d_i[j]$, $r_i[j]$ and $n_i[j]$. By adopting the data mining approach as given in [22], the conditional probability density function $f_{R|D}(r|d_i)$ can be written as

$$f_{R|D}(r|d_i) = \frac{f_N(d_i - r) f_R(r)}{\int_{\infty}^{\infty} f_N(d_i - z) f_R(z) dz}, \tag{3}$$

where $f_X(x)$ is the probability density function of random variable X. Then, one can recover the power consumption distribution, $f_R(r)$, from $f_{R|D}(r|d_i)$ via an iterative algorithm as summarized in Algorithm 1.

Algorithm 1 Power Consumption Distribution Reconstruction

```
Inputs: samples $\{d_i\}$, $i = 1, 2, \ldots, M$ and probability density function of additive Gaussian noise $f_N(n)$
States: Initialize the original power consumption distribution, $R$, as a uniform distribution, i.e., $f_R^0 = \frac{1}{V}$,
        where $V$ is the value range of the power consumption data.
Procedure:
    for $k = 1, 2, \ldots, \infty$ do
        $f_{R|D}^k(r|d_i) = \frac{f_N(d_i - r) f_R^{k-1}(r)}{\int_{\infty}^{\infty} f_N(d_i - z) f_R^{k-1}(z) dz}$;
        $\tilde{f}_R^k(r) = \frac{1}{M} \sum_{i=1}^{M} f_{R|D}^{k-1}(r|d_i)$
        if the stopping criterion is satisfied ($\chi^2$ goodness-of-fit test with confidence level 95%) then
            $\tilde{f}_R(r) = \tilde{f}_R^k(r)$;
            break;
        end if
    end for
    Declare the recovered distribution of power consumption as $f_R(r)$.
```

As described in Algorithm 1, the averaged conditional probability density function, $f_{R|D}(r|d_i)$, in Eq. (3) is used to update $f_R(r)$ in the next round of iteration. In fact, the averaging step is equivalent to multiplying each $f_{R|D}(r|d_i)$ with weight $f_D(d_i)$. Thus, we have

$$\begin{aligned}
\tilde{f}_R(r) &= \frac{1}{M} \sum_{i=1}^{M} \frac{f_N(d_i - r) f_R(r)}{\int_{\infty}^{\infty} f_N(d_i - z) f_R(z) dz} \\
&= \sum_{i=1}^{M} f_{R|D}(r|d_i) f_D(d_i) \\
&= \sum_{i=1}^{M} f_{R,D}(r, d_i) \\
&= \sum_{i=1}^{M} f_{R,N}(r, d_i - r). \qquad (4)
\end{aligned}$$

Since the original power consumption data and additive noise are independent, we can rewrite $\tilde{f}_R(r)$ as

$$\tilde{f}_R(r) = \sum_{i=1}^{M} f_R(r) f_N(d_i - r). \tag{5}$$

If there is a sufficient number of customers, we have $\tilde{f}_R(r) \approx f_R(r)$. Thus, the averaging is actually the estimation of the probability density function $f_R(r)$ from the conditional probability density function, $f_{R|D}(r|d_i)$, and samples d_i, $i = 1, 2, \ldots, K$.

The above sample-by-sample distribution reconstruction algorithm demands the availability of power consumption

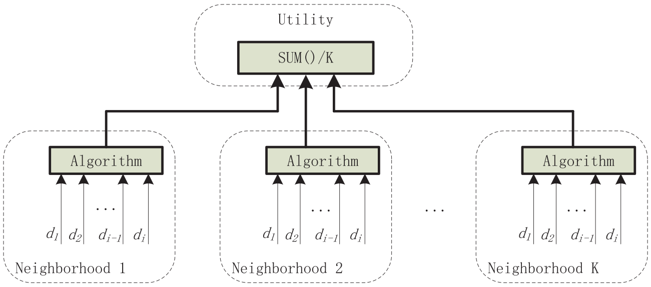

Utility
SUM()/K
Algorithm
Algorithm
Algorithm
d_1 d_2 ... d_{i-1} d_i
d_1 d_2 ... d_{i-1} d_i
d_1 d_2 ... d_{i-1} d_i
...
Neighborhood 1
Neighborhood 2
Neighborhood K

FIGURE 5. A hierarchical architecture to reconstruct the power consumption distribution.

data from all customers. In a smart grid, millions of customers' data are gathered and processed in real time, and a centralized processing approach not only entails the high data processing capability of the computational units, but also exerts much pressure on data communications because of a large amount of network traffic.

Towards a scalable implementation of the proposed system, it is advantageous to adopt a hierarchical processing architecture as depicted in Fig. 5, where a two-layer architecture is given as an example for distributed processing. The first layer is composed of customers and corresponding data collectors located in a single neighborhood. The second layer consists of data collectors and related parties (*e.g.*, utility company). In the first-layer, each data collector runs the iteration algorithm on power consumption data collected from the neighborhood. For the second layer, the data collector sends the reconstructed local power consumption distribution to related parties for integration. The overall power consumption distribution is then calculated by averaging all received local distribution results.

IV. PRIVACY PROTECTION ANALYSIS

In the proposed hierarchical processing architecture, the local power consumption distribution (*e.g.* the reconstructed PDF) is transmitted between a data collector and a service provider. Since the distribution of the neighborhood power consumption reveals nothing about the individual power usage pattern, the privacy threat is confined to a local neighborhood.

In this section, we investigate such a privacy threat. It is assumed that eavesdroppers can intercept all reported data from a smart meter to a data collector in their distorted form. De-noising schemes might be perceived as an effective method to recover the original signal from its distorted version. Here, we will analyze two popular de-noising schemes to demonstrate the effectiveness of the proposed privacy-preserving scheme.

A. LINEAR MEAN FILTER ATTACK

The linear mean (LM) filter is a widely-adopted technique to recover the original signal from its noisy version. The fundamental idea is to attenuate the noise influence by averaging cumulative values.

Given a sequence of samples from a customer's distorted power consumption trace $d[j], j = 1, 2, \ldots$, with the linear mean filter de-noising technique, an attacker can derive the de-noised signal $\{r'(j), j = 1, 2, \ldots\}$ of the following form

$$\begin{aligned} r'[j] &= \sum_{j-L\le i\le j+L} w[i]d[i] \\ &= \sum_{j-L\le i\le j+L} w[i](r[i]+n[i]). \end{aligned} \tag{6}$$

The expectation and the variance of $r'(j)$ can be derived, respectively, as

$$\begin{aligned} E[r'[j]] &= E\left[\sum_{j-L\le i\le j+L} w[i](r[i]+n[i])\right] \\ &= \sum_{j-L\le i\le j+L} w[i]E[r[i]] \end{aligned} \tag{7}$$

and

$$\begin{aligned} Var[r'[j]] &= Var\left[\sum_{j-L\le i\le j+L} w[i](r[i]+n[i])\right] \\ &= \sum_{j-L\le i\le j+L} w^2[i](Var[r[i]]+Var[n[i]]) \\ &= \sum_{j-L\le i\le j+L} w^2[i](Var[r[i]]+\sigma_N^2) \end{aligned} \tag{8}$$

where $2L + 1$ is the sliding window size of the linear mean filter.

By choosing σ_N^2 greater than $Var[r(i)]$, the noise term will dominate in the de-noised signal. The smaller the window size, the poorer the de-noising result. For a large window size, both noise and the variance of the signal are smoothed out and only a smoothed signal remains. In either case, no detailed privacy information is revealed.

B. NON-LOCAL MEAN FILTER ATTACK

The non-local mean (NLM) filtering method is a state-of-the-art de-noising technique widely used for image de-noising. For a given pixel, it adopts a weighted average of other pixels that have a similar local structure to remove its noise. The higher the similarity, the larger the weight. Here, we present the 1-D version of the non-local mean filter and use it as an attack (*i.e.* recovering the original power consumption data of an individual user).

With the application of NLM filtering to a sequence of samples from a customer's distorted power consumption trace $d[j], i = 1, 2, \ldots$, the recovered power consumption at time k can be written as

$$r'[k] = \sum_{j\in\Omega_d} w[k,j]d[j], \tag{9}$$

where Ω_d is a sliding window of size $2s + 1$ centered around the kth sample and $w[k, j]$ is a weight indicating the contribution from sample $d[j]$. The weight is in form of

$$w[k,j] = \frac{1}{C_k}\exp\left\{-\frac{||D(NH_k)-D(NH_j)||_{2,a}^2}{h}\right\}, \tag{10}$$

TABLE 2. Statistics derivation of an oven.

	Aggregated Values				Parameters	
	Day 1	Day 2	Day 3	...	Mean	Variance
01:00	3 W	2 W	10 W	...	3.62 W	600.44 W^2
02:00	10 W	0 W	0 W	...	0.38 W	1500.01 W^2
...	1500 W	2000 W	50 W	...	1200.36 W	14000213.33 W^2
...	...	...	...	...	...	...
24:00	150 W	200 W	50 W	...	63.88 W	133324.89 W^2

where C_k is a normalizing factor (*i.e.*, $\sum w[k,j] = 1$), $D(NH_k)$ denotes a group of distorted power consumption samples in the neighborhood of the kth sample, $||\cdot||^2_{2,a}$ is the Euclidean distance weighted by a Gaussian kernel of standard deviation a, and the decay of the weight is adjusted by h.

The mean of $||D(NH_k) - D(NH_j)||^2_{2,a}$ in Eq. (10) can be written as

$$\begin{aligned} E[D(k,j)] &= E||D(NH_k) - D(NH_j)||^2_{2,a} \\ &= ||R(NH_k) - R(NH_j)||^2_{2,a} + 2(2s+1)\sigma_N^2, \end{aligned}$$

where $R(NH_k)$ is the group of original power consumption samples in the neighborhood of the kth sample. Thus, the mean of weights is

$$\begin{aligned} E[w[k,j]] = \frac{1}{C_k} \exp\left\{-\frac{2(2s+1)\sigma_N^2}{h}\right\} \times \\ \exp\left\{-\frac{||R(NH_k) - R(NH_j)||^2_{2,a}}{h}\right\}. \quad (11) \end{aligned}$$

Clearly, if we choose σ_N^2 larger than $Var[r[j]]$, weight $w[k,j]$ is dominated by the variance of additive noise rather than the signal similarity measure. In other words, a more similar sample may not be assigned a larger weight due to the noise effect and, therefore, NLM is not able to recover the original signal from the distorted one.

V. EFFICIENCY ANALYSIS

As compared with cryptography-based solutions [9]–[12], the proposed scheme is more efficient since it does not demand frequent encryption and decryption operations for the transmission of each power consumption data. Instead, a smart meter requires one extra additive operation in every report period (every minute or second). In addition, there is no stringent timeliness requirement for billing request and response. Therefore, reading distortion and aggregated billing have no efficiency concern.

The complexity of power consumption distribution reconstruction can be analyzed as follows. Assume that we have M (the number of customers) power consumption data and the value range is split into Q bins for processing. According to Algorithm 1, $Q+2$ multiplications and $Q-1$ additions are needed to calculate $f^{k-1}_{R|D}(r|d_i)$, and M additions and 1 multiplication from $f^{k-1}_{R|D}(r|d_i)$ to $\tilde{f}^k_R(r)$. As a result, at each iteration, we need $M+Q-1$ additions and $Q+3$ multiplications. The adoption of the hierarchical architecture discussed in Section III further reduces the network traffic and operations of related parties (*e.g.*, utility company). The low-complexity of required operations and highly reduced network traffic make the proposed scheme a practical privacy-preserving solution in a smart grid.

VI. EXPERIMENTAL EVALUATION

We evaluate the proposed scheme in the following two aspects.

- Privacy protection
  We adopt a widely used energy signature analysis technology known as non-intrusive load monitoring to examine the privacy-preserving effect of the proposed scheme. Two de-noising attacks (*i.e.*, linear mean and NLM filters) are investigated in both the short-term and the long-term cases. A real world single household power consumption dataset is used in this evaluation.
- Power consumption distribution reconstruction
  As to power consumption distribution reconstruction, both the accuracy of the proposed algorithm and its relationship with other factors (*e.g.*, the distortion level, the number of households, and the number of iterations) are studied. Synthesized datasets from a smart grid data generator for a large amount of households are used in this evaluation.

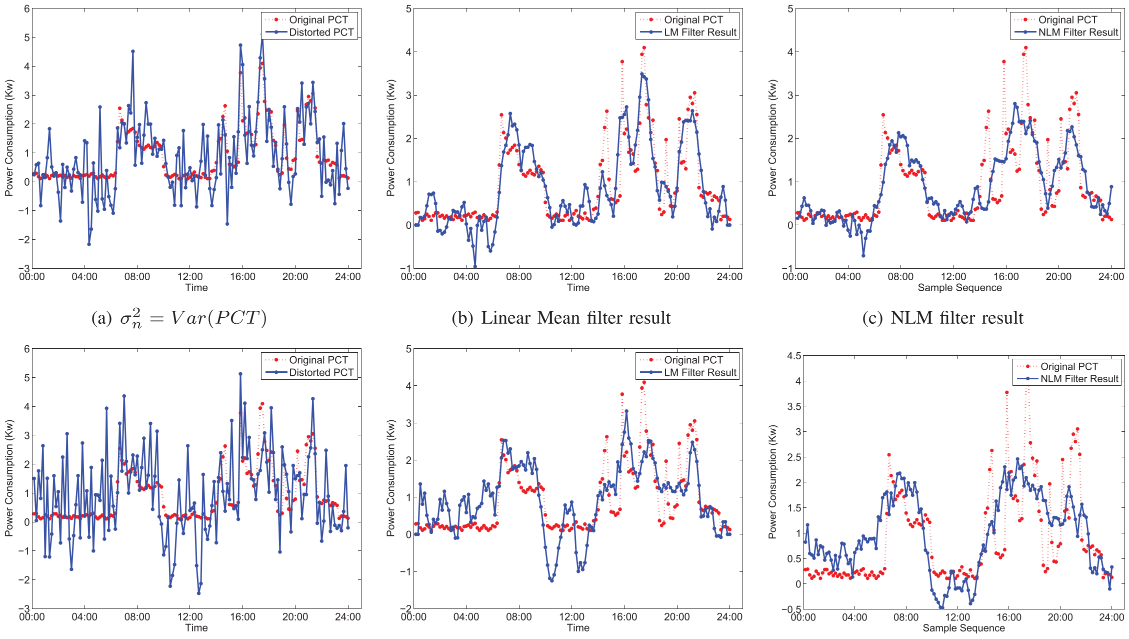
A. DATA SETS

1) Power Curve Dataset

We use a power curve dataset for privacy-preserving evaluation, which was collected by the Business Intelligence Lab of Telecom ParisTech [23]. It contains 349 days of electric power consumption data recorded every 10 minutes in a household in 2007. It has 144 readings starting from 00:00 to 23:50 for each day.

2) Smart Grid Simulator

For the distribution reconstruction, we simulate a large number of households with a smart grid Simulator, which is a software tool developed by AIFB and Wechselfunchs [24]. The simulator generates data from electronic appliance statistics (mean and variance) learned from three weeks of real world power consumption data. Table 2 shows the parameters for an oven. The generated data are in N3 format and they include detailed hourly power consumption of each electronic device in each household.



(a) $\sigma_n^2 = Var(PCT)$ (b) Linear Mean filter result (c) NLM filter result

(d) $\sigma_n^2 = 1.5Var(PCT)$ (e) Linear Mean filter result (f) NLM filter result

FIGURE 6. Reading distortions and de-noising results.

B. NON-INTRUSIVE LOAD MONITORING

Non-intrusive load monitoring (NILM) is frequently used by utility companies to understand the load status of a power system. With this technology, customer's power consumption trace is decomposed into profiles of different appliances in different time periods. The method used in NILM is to measure changes in voltages and currents. The measured changes are then mapped to events of "ON/OFF" to indicate when appliances start to work and stop. For example, a 3-second load profile $\{(t_0, 0W), (t_1, 100W), (t_2, 200W), (t_3, 100W)\}$ could generate features as: $\{(t_1, +100W), (t_2, +100W), (t_3, -100W)\}$.

According to extracted features and properties of various appliances, types and working hours of different appliances can be accurately detected. In general, both the reactive power and the real power are measured to distinguish appliances with the same total power draw. As power consumption data traces become more fine-grained, NILM has brought up a severe privacy concern. That is, customers' behavioral patterns can be easily derived from their power consumption traces with NILM. A rechargeable battery was introduced in [18] to smoothen the load profile to reduce the potential privacy leakage of a household, which can reduce up to 95% of potential features. Although this is effective, we demonstrate by experimental results that our proposed scheme can achieve better results with less cost.

C. PRIVACY PROTECTION

Two levels of distortion are added to the original power consumption trace that was the recorded data for a single household on 2007 Jan. 1^{st} in the power curve dataset, and they are shown in red curves in Figs. 6(a) and (d). The blue curves in Figs. 6(a), (b), and (c) are, respectively, the distorted trace with noise variance $\sigma_n^2 = Var(PCT)$, the de-noised trace after LM filtering, and the de-noised trace after NLM filtering. Fig. 6(d), (e), and (f) show the corresponding results under noise variance $\sigma_n^2 = 1.5Var(PCT)$, respectively. We see that additive noise severely distorts the original trace, and it is difficult to derive the detailed power usage information from the distorted sequence. As a result of the large noise, both linear mean filtering and NLM filtering fail to recover the accurate power consumption traces of customers. The loss of accuracy makes the mapping to customer's daily activities infeasible.

We adopt NILM to further verify this conclusion. We extract the ON/OFF feature from the distorted traces under three different distortion levels with a pre-defined threshold set to 0.3 KW and plot the result in Fig. 7. We see that many detected ON/OFF features from the distorted trace are fabricated and real ON/OFF features are severely distorted. Figs. 8 and 9 show the extracted features from the de-noised trace with different filters. Again, the features extracted from the de-noised trace are still noise-like, which could not provide any valuable information about customer's profile of daily activities.

As shown in Table 3, after distortion, the number of features extracted with NILM increases and it deviates from the original substantially. With additive noise of a larger variance, more features can be extracted. After the linear mean filtering and the NLM filtering, the numbers of features decrease, but they are still higher than the original

TABLE 3. Features extracted with NILM.

Distortion	Original			Distorted			After LM			After NLM		
	TF	EF	EF/TF	TF	EF	EF/TF	TF	EF	EF/TF	TF	EF	EF/TF
$\sigma_n^2 = Var(PCT)$	32	32	100%	112	1	0.83%	44	2	3.17%	15	0	0%
$\sigma_n^2 = 1.5Var(PCT)$	32	32	100%	120	3	2.42%	67	2	2.47%	31	0	0%
$\sigma_n^2 = 2Var(PCT)$	32	32	100%	129	1	0.76%	70	2	2.5%	39	0	0%

TF : total number of features EF : number of effective features EF/TF : ratio of effective features to total features

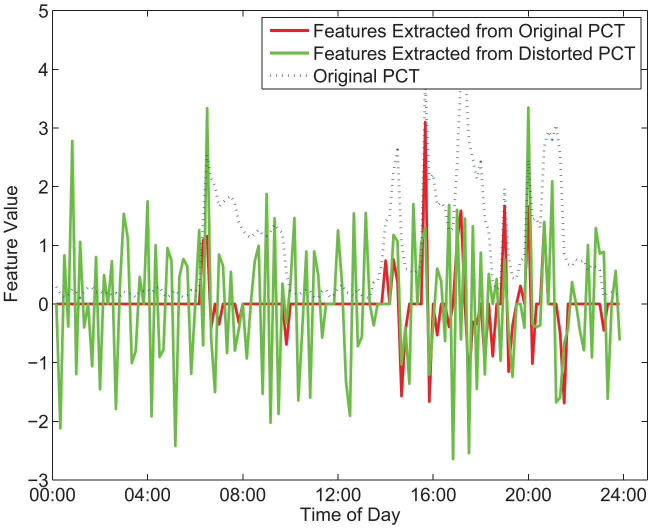


FIGURE 7. Features extracted from the distorted power consumption trace.

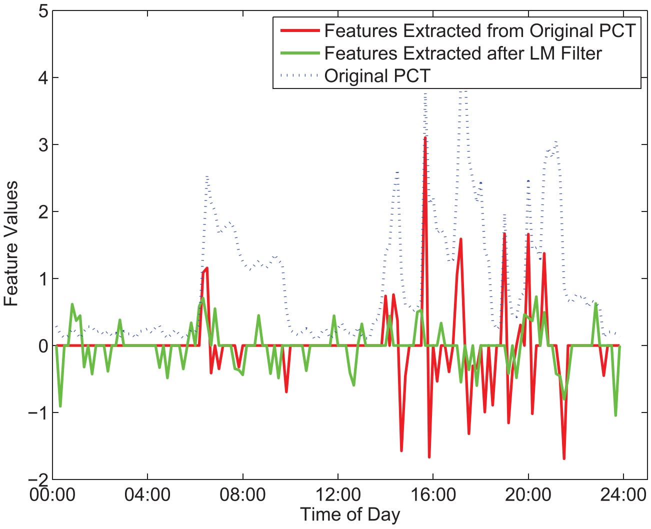


FIGURE 8. Features extracted from the de-noised trace using the linear mean filter.

one except for NILM processed results under noise variance $\sigma_n^2 = Var(PCT)$. Although the number of features is closer to the original one, the minimal ratio of effective features to the total features (*e.g.*, EF/TF) makes the feature recovery almost useless.

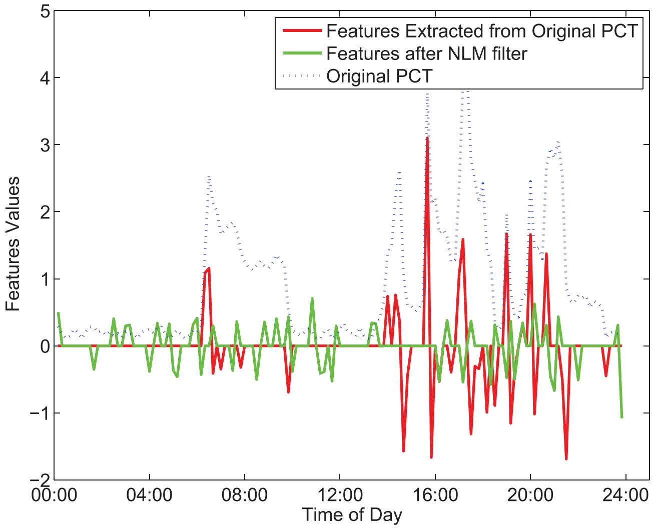


FIGURE 9. Features extracted from the de-noised trace using the non-local mean (NLM) filter.

Another possible attack is long-term averaging, where the power consumption traces from different periods are averaged to obtain the daily power usage pattern of the customer. Under this scenario, the random distortion is gradually diminished as more power consumption traces contribute to the long-term averaging. However, the long-term averaging also largely reduces the variance of the original power consumption trace. This is particularly true in the proposed scheme where a relatively large distortion is adopted.

Fig. 10 shows the result of an averaging attack with a long-term period of 349 days. Although the averaged distorted trace (green curve) converges to the averaged original trace, the averaged original trace loses almost all high-frequency variations in daily power consumption traces (dashed curves). Hence, with long-term averaging, the unauthorized party may derive the yearly average peak and pit period of daily power consumptions, but cannot obtain detailed privacy-related information on a daily basis. Moreover, it is convenient in the proposed scheme to change the disturbance level from time to time which hides the original information furthermore.

D. POWER CONSUMPTION DISTRIBUTION RECONSTRUCTION

It is shown in Fig. 6 that the larger the additive noise, the worse the recovery results of the original power consump-

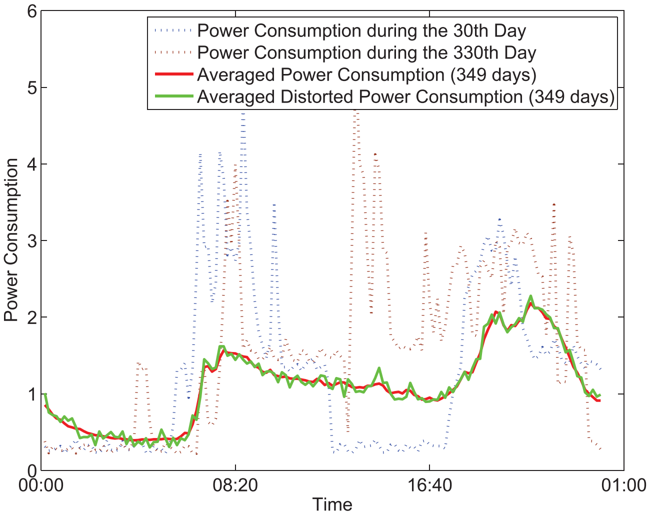


FIGURE 10. Long-term averaging results.

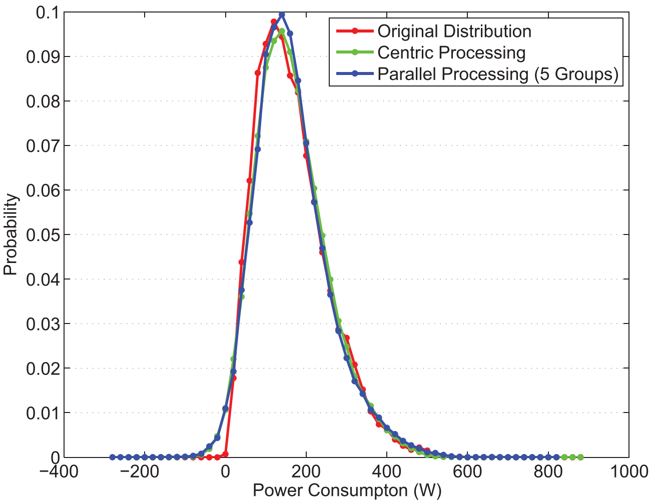


FIGURE 12. Comparison of centralized and distributed processing of power consumption distribution reconstruction.

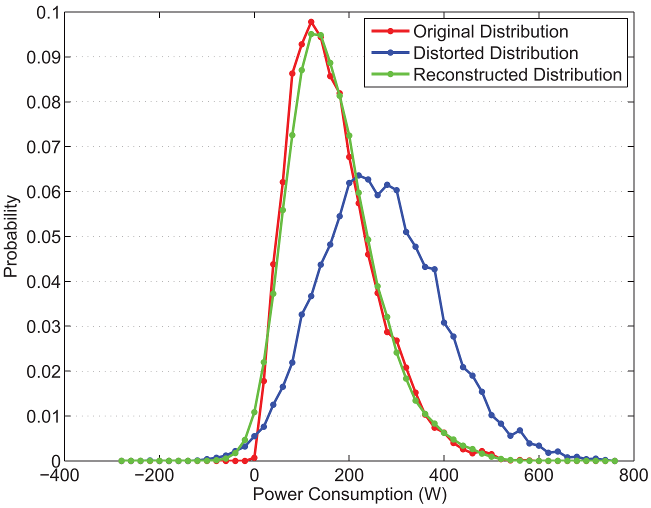


FIGURE 11. Power consumption distribution reconstruction.

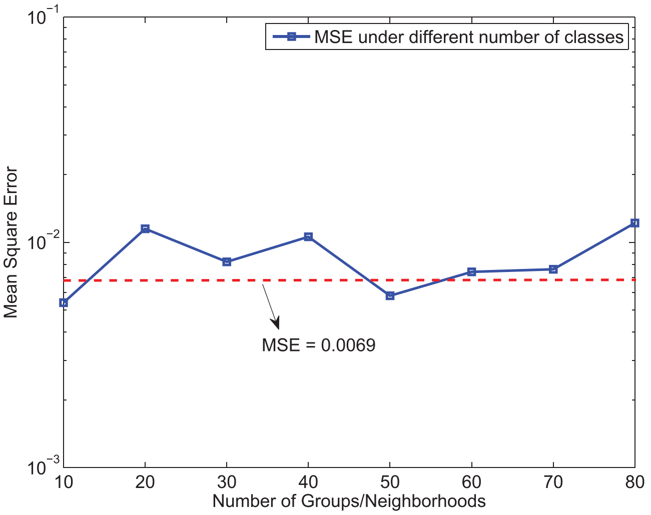


FIGURE 13. MSE under a different number of groups.

tion trace. However, this does not mean that we can choose arbitrarily large noise since we have to make sure that the power consumption distribution can be accurately reconstructed. For a fixed number of users, the larger the random noise, more samples are required to get the accurate estimate of the power consumption distribution. This will be discussed in this section.

Fig. 11 shows the distribution reconstruction result of the proposed scheme without distributed processing. The dataset is generated by the smart grid Simulator. It consists of the power consumption data of 10,000 households in the same time period. The variance of the original power consumption data is 7892.2W. The disturbance added to the original trace is additive Gaussian noise with mean 100W and its variance being the same as the original power consumption data. The number of bins for data splitting is 53. The red and blue curves show the aggregate original and distorted power consumption data of 10,000 households, respectively. The green curve is the reconstructed power consumption distribution using the proposed scheme presented in Section III-D. The averaged mean square error (MSE) of the distorted power consumption distribution is 0.1608, while that of the recovered distribution is enhanced to 0.0232.

Fig. 12 shows the distributed processing results under the same setting. The blue curve shows the reconstructed distribution with 10-group distributed processing. The MSE of a distributed processing system is 0.0251, which is almost the same as the centralized one.

To further compare the accuracy of the centralized and the distributed processing schemes, we test the performance of distributed processing with a different grouping number, denoted by K in Fig. 5, and show the averaged performance as a function of K in Fig. 13. We see that the distributed processing scheme achieves about the same level of accuracy for a wide range of K values.

Fig. 14 shows the distribution reconstruction accuracy with a different number of households in the local aggregation process. We see that the averaged MSE decreases as the

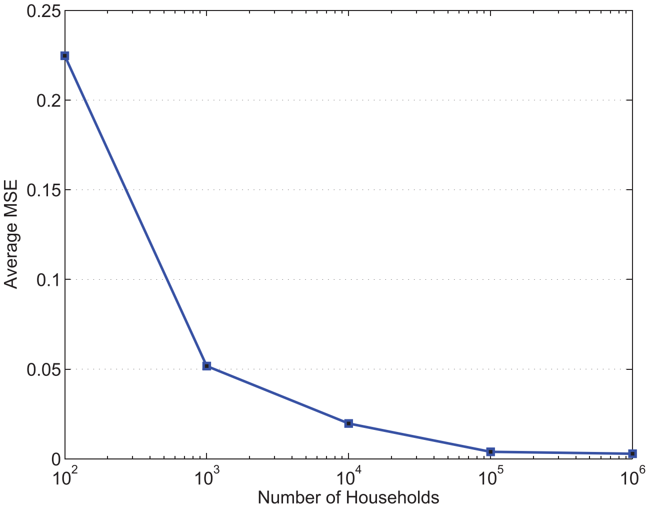


FIGURE 14. The MSE of the reconstructed power consumption distribution as a function of the number of households.

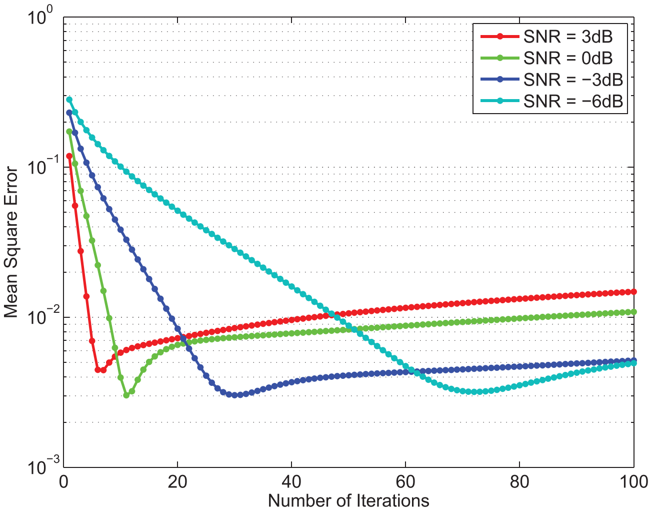


FIGURE 15. The MSE of the reconstructed power consumption distribution as a function of the iteration number parameterized by different SNR values.

household number grows. For a power utility company with millions of customers, the averaged MSE could reach 0.001. Fig. 15 shows the MSE curve as a function of the iteration number of the power consumption distribution recovery algorithm parameterized by different distortion levels. We see that the distortion level does not affect the accuracy of distribution recovery. With a fixed number of households, the maximum reconstruction accuracy keeps the same. However, different distortion levels demand a different number of iterations to achieve the optimal reconstructed distribution. For the real world system design, a proper trade-off between privacy protection and accuracy of power consumption distribution reconstruction should be considered.

VII. CONCLUSION

A lightweight, efficient and robust privacy-preserving metering scheme for smart grids was proposed in this work. In the proposed scheme, a customer's power consumption data are first distorted by additive noise before being sent to other entities in a smart grid system. Any party receiving the distorted data cannot restore the original fine-grained power consumption trace so that customer privacy is protected. At the same time, related parties can still derive the complete distribution of the original power consumption data from a multitude of customers in a certain geographic area, which enables several important functions of smart grids such as production prediction, dynamic pricing, and billing service. It was shown analytically that several well known denoising attacks fail to recover the original power consumption trace. Experimental evaluations with real world and simulated power consumption datasets confirm the feasibility and practicality of the proposed scheme.

REFERENCES

[1] G. Locke and P. D. Gallagher, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2010.

[2] E. Quinn, "Smart metering and privacy: Existing laws and competing policies," Univ. Colorado Law School—CEES, Boulder, CO, USA, SSRN Rep. 1462285, 2009.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May–Jun. 2009.

[4] *Guidelines for Smart Grid Cyber Security: Vol.1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2010.

[5] *Guidelines for Smart Grid Cyber Security: Vol.2, Privacy and the Smart Grid*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2010.

[6] *Guidelines for Smart Grid Cyber Security: Vol.3, Supportive Analyses and References*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2010.

[7] *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*, IEEE Standard 2030-2011, 2011.

[8] *IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links*, IEEE Standard 1711-2010, 2011.

[9] F. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in *Proc. 6th Int. Conf. Security Trust Manage.*, 2011, pp. 226–238.

[10] K. Kursawe, G. Danezis, and M. Kohlweiss, "Privacy-friendly aggregation for the smart-grid," in *Proc. 11th Int. Conf. Privacy Enhancing Technol.*, 2011, pp. 175–191.

[11] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proc. 10th Annu. ACM Workshop Privacy Electron. Soc.*, 2011, pp. 49–60.

[12] X. He, M.-O. Pun, and C.-C. Kuo, "Secure and efficient cryptosystem for smart grid using homomorphic encryption," in *Proc. IEEE PES Innovative Smart Grid Technol.*, Jan. 2012, pp. 1–8.

[13] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. 2nd ACM Workshop Embedded Sens. Syst. Energy-Efficiency Building*, 2010, pp. 61–66.

[14] H.-Y. Lin, W.-G. Tzeng, S.-T. Shen, and B.-S. P. Lin, "A practical smart metering system supporting privacy preserving billing and load monitoring," in *Proc. Appl. Cryptogr. Netw. Security*, 2012, pp. 544–560.

[15] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.

[16] M. Jawurek, M. Johns, and K. Rieck, "Smart metering de-pseudonymization," in *Proc. 27th Annu. Comput. Security Appl. Conf.*, 2011, pp. 227–236.

[17] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Toward undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 232–237.

[18] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proc. 18th ACM Conf. Comput. Commun. Security*, 2011, pp. 87–98.

[19] W. H. Sanders, "Progress toward a resilient power grid infrastructure," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2010, pp. 1–3.

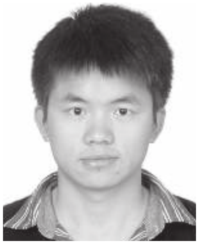
[20] A. G. van Engelen and J. S. Collins, "Choices for smart grid implementation," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Jan. 2010, pp. 1–8.

[21] A. Bose, "Smart transmission grid applications and their supporting infrastructure," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 11–19, Jun. 2010.

[22] R. Agrawal and R. Srikant, "Privacy-preserving data mining," *ACM SIGMOD Rec.*, vol. 29, no. 2. pp. 439–450, 2000.

[23] G. Hébrail, B. Hugueney, Y. Lechevallier, and F. Rossi, "Exploratory analysis of functional data via clustering and optimal segmentation," *Neurocomputing*, vol. 73, no. 7, pp. 1125–1141, 2010.

[24] S. R. Andreas Harth and A. Wagner. (2011). *Smart Grid Emulator* [Online]. Available:http://code.google.com/p/smart-grid-emulator/



XINGZE HE received the B.S. and M.S. degrees from the Department of Communication and Information System, Xi'an Jiaotong University, Xi'an, China, in 2007 and 2009, respectively. He is currently pursuing the Ph.D. degree with the Ming Hsieh Department of Electrical Engineering, University of Southern California, Los Angeles, CA, USA. His current research interests include sequential analysis, security, and data privacy.

XINWEN ZHANG received the B.Eng. degree from the Huazhong University of Science and Technology, Wuhan, China, in 1995, and the M.Eng. degree from Nanyang Technology University, Singapore, in 2000, and the Ph.D. degree from George Mason University, Fairfax, GA, USA, in 2006. He is a Senior Staff Researcher with the Huawei Research Center, Santa Clara, CA, USA. His current research interests include security policies, models, architectures, mechanism in general computing and networking systems, secure and trusted network architecture, cloud computing, mobile platforms, and storage systems.

C.-C. JAY KUO received the B.S. degree from National Taiwan University, Taipei, Taiwan, in 1980, and the M.S. and Ph.D. degrees from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1985 and 1987, respectively, all in electrical engineering. He is currently the Director of the Media Communications Laboratory and a Professor of electrical engineering, computer science, and mathematics with the University of Southern California, Los Angeles, CA, USA, and the President of the Asia-Pacific Signal and Information Processing Association. His current research interests include digital image/video analysis and multimedia data compression. He is a fellow of the American Association for the Advancement of Science and the International Society for Optical Engineers.