When Privacy Meets Economics: Enabling Differentially-Private Battery-Supported Meter Reporting in Smart Grid

Zijian Zhang*†, Wenqiang Cao*, Zhan Qin†, Liehuang Zhu*, Zhengtao Yu‡ and Kui Ren†
*School of Computer Science and Technology
Beijing Institute of Technology, Beijing, China
†Department of Computer Science and Engineering
State University of New York at Buffalo, New York, United States of America
‡School of Information Engineering and Automation
Kunming University of Science and Technology, Kunming, China

***Abstract*—Millions of the smart meters, as essential components, are being deployed ubiquitously in the next generation power system. However, the public privacy concerns over the users' power consumption leakage raise, since the smart meters' unintermittent readings contain customers' behavior patterns. To alleviate this problem, the state-of-the-art techniques are common to use a rechargeable battery to hide the actual power consumption. Unfortunately, none of the existing works completely provide a rigorous privacy protection with reasonable cost under real-world battery settings, i.e., achieving the well-known differential privacy guarantee economically using batteries with limited charge/discharge rate and capacity.**

To attain this goal, this paper proposes a differentially private meter reading report mechanism. The main idea is to first narrow down the domain of the noise distribution parameter, in order to decrease the possibility of violating the battery limits. It also combines a multi-armed bandit algorithm to further reduce the cost as much as possible. In addition, a novel switch mechanism is proposed to prevent the meter from reporting its reading when the battery limitations might be violated. The theoretical analysis provides a formal proof of the privacy guarantee of the proposed scheme. Besides, experimental results show that the privacy protection of the proposed scheme is at least nine times stronger than that of the existing solutions with acceptable extra cost.

I. Introduction

Smart grid is considered to be the future of the current electricity grid system. Technically, it is a complex application which utilizes sophisticated equipment, advanced perceiving and gaging technologies. Further, it employs progressive management methods and decisions to achieve security, reliability, efficiency, affordability and adaptability of the power grid. Over the years, different countries throughout the world have tried to build their own smart grid infrastructures, and grand designs for the future are presented in [1].

While the use of smart grids is still only prospective, problems remain to be addressed, with one of the most important issues being privacy concerns. For instance, electricity consumption readings of appliances in a house can be revealed by eavesdropping the smart meter, from which the adversary can mine the customers' behavior patterns by employing different data mining algorithms. Among all the attack methods, load monitor is a common technique to unveil customers' privacy by disaggregating total load power into appliance level components. It can be classified into intrusive load monitor (ILM) and non-intrusive load monitor (NILM) [2]. The former requires extra sensors and auxiliary approaches combined with the meter readings to identify appliances, while, the latter needs only aggregated power consumption to discern usage of different appliances. Instead of just obtaining readings from extra sensors, machine learning algorithms can also be utilized to recognize operational sequences of each appliance. Furthermore, the accuracy in identifying appliances can be improved by using prior appliance information [3]–[5].

To address privacy concerns, some battery-supported solutions have been recently proposed [6], [7]. Instead of reporting the actual appliances' consumption readings, the basic idea of battery-based solutions is to inject noises generated by battery charging or discharging into the meter readings. Then these perturbed meter readings are reported to the electricity supplier [8]. Battery-based schemes could not only provide a useful approach to protect customers' privacy, but also save electricity costs due to the fluctuations in daily electricity prices [9]. Recently, differential privacy, a formal privacy-preserving approach, has caught researchers' attention [10], [11], and has been broadly studied in several areas such as smart grids, mechanism design and geometry privacy. A differentially private scheme guarantees privacy protection and could also be formally proven to ensure the goal is attained. Therefore, in this paper, we explore the utilization of differential privacy for protecting privacy.

We investigate research literature on applications of battery-based solutions in smart grids, and analyze their common defects for either lacking of formal privacy guarantee or becoming vulnerable when violating battery's inherent charging/discharging limitation. Concretely, Kalogridis proposes a power mixing algorithm [8] to keep the meter readings at a fixed value. Similarly, McLaughlin's Non Intrusive Load Leveling scheme [6] attempts to protect privacy by enabling

978-1-5386-2704-4/17/$31.00

the battery to charge or discharge automatically according to its capacity. Further, an approach from Yang [7] solves the privacy issue by flexibly altering meter readings. However, none of these approaches satisfies the requirement of differential privacy. Others, such as Koo's cost-saving work under static policy [9], Yang's optimal privacy preserving energy management using minimizing variance of meter readings [12], ormultitasking-BLH-exp3 [10] cannot provide integrate proof for differential privacy [11], [13]. Zhang et al. [13] also propose two cost-friendly schemes, CDP1 and CDP2, to ensure (ϵ, δ) differential privacy and save costs at the same time. However, experimental results indicate that the privacy protection in CDP1 achieves only slightly better outcomes than other works, because δ in CDP1 is large.

In order to ensure better privacy protection as well as offer strict security analysis, we design a differentially private smart meter reading report scheme (PrivMeter). Our contributions are summarized below:

1) A novel switch mechanism that prevents smart meter privacy leakage is proposed for the first time. It effectively solves the energy disaggregation threats induced by the battery limitations of the current solutions.
2) Thorough privacy analyses of the proposed scheme are presented. The theoretical analysis of the proposed scheme shows that differential privacy is satisfactorily achieved, and the experimental results indicate that the privacy loss of the proposed scheme is at least nine times smaller than that of all existing works.
3) The simulation results show that the extra cost of the proposed scheme can reach 5.9% of the original cost.

The rest of this paper is organized as follows: In Section II, we provide some prior research knowledge used in the proposed scheme. While in Section III, the proposed scheme models are explained and followed by mathematical notations. Section IV describes the proposed scheme in detail. In addition, security analysis and experimental evaluations are given in Section V, combined with a review of related work in Section VI. Finally, the conclusion and potential for future work are presented in Section VII.

II. Preliminaries

A. Differential Privacy

Differential privacy aims to minimize distinguishability between two datasets which vary from the same algorithm by only one record [14]. It is formally defined as follows: For two datasets D_1 and D_2 that differ only in one item, a randomized algorithm A achieves ϵ-differential private if and only if [15]:

$$\Pr[\mathrm{A}(\mathrm{D}_1) \in \mathrm{S}] \leq \mathrm{e}^{\epsilon} \times \Pr[\mathrm{A}(\mathrm{D}_2) \in \mathrm{S}] + \delta \tag{1}$$

where $A(D_1)$ and $A(D_1)$ denote the output of algorithm A on datasets D_1 and D_2 respectively, S is the subset of the output domain of A. Also ϵ, δ are two coefficients used to quantify privacy [15]. For algorithm A, its sensitivity is defined as follows: given a function $A : D \to R^d$, its sensitivity [15] ΔA is $\max_{D_1, D_2} \{\|A(D_1) - A(D_2)\|\}$.

B. Laplace Distribution

Laplace distribution is a continuous probability distribution, and its probability density function (pdf) is [14]:

$$pdf(x) = \frac{1}{2\sigma} e^{-\frac{|x-\mu|}{\sigma}},\ x \in (-\infty, +\infty) \tag{2}$$

where the mean value of this distribution is μ and the variance is $2\sigma^2$ [14]. Differential privacy could be achieved by drawing noises from Laplace distribution. Concretely, when D_1 and $D_2(D_1, D_2 \in D)$ differs in, at most, one element, then differential privacy can be achieved if $\Delta A/\epsilon \leq \sigma$ [15].

C. Multi-Armed Bandit Problem

The multi-armed bandit problem is a classic mathematical model originating from multiple bandit scenarios in casinos. Its prototype is stateless reinforcement learning which has been widely used in the field of robot technology, website optimization and advertising [16]. In some versions of the multi-armed bandit problem, the gambler does not have prior knowledge about the arms, only the ones he has already played [16]. Therefore, the key tradeoff faced by the gambler at each trial is between "exploitation" and "exploration". The former focuses on historical optimal choice while the latter tries to obtain information about the new arms [16], [17]. A regret mechanism is thereby applied to deal with the "exploitation" and "exploration" tradeoff by evaluating the distance between the chosen arm and the historical optimal choice [18]. A regret mechanism based solution is formally presented in the following: Assume that K arms and n round games are considered. In addition, the gambler can only choose one arm each time [18]. In the first round game, the gambler randomly chooses one arm. We denote $P_{j,i}$ as the payoff of choosing arm j at time i. and the gambler earns $P_{S_{j,i}}$ profit if he selects arm j at time i according to his experience. Therefore, in round k, the value of regret could be viewed as the difference between the theoretically highest payoff and the gambler's actual payoff for k rounds [18]. The specific value can be computed as follows:

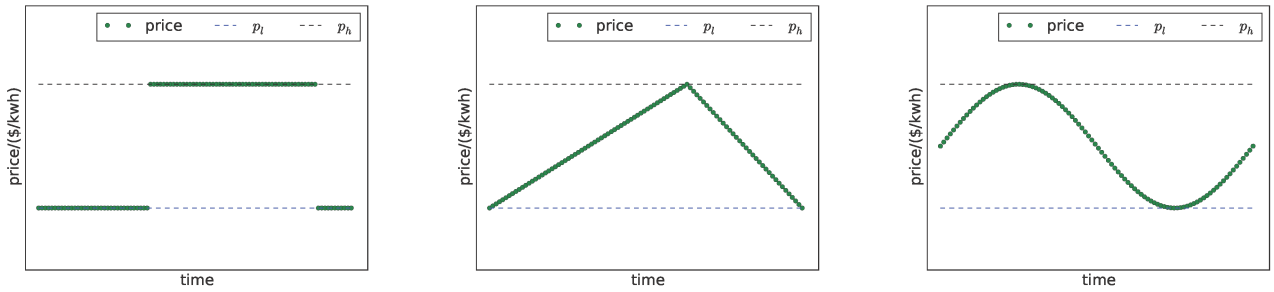
$$R_n = \sum_{i=1}^{k} \max_{j \in \{1,2,\ldots m\}} \{P_{j,i}\} - \sum_{i=1}^{k} P_{S_{j,i}} \tag{3}$$

based on updated regret values, the probability of choosing one arm in next round could be calculated.

III. System Architecture and Models

A. System Architecture

Five components are included in the proposed scheme as illustrated in Fig. 1. They are: household electrical appliances; a smart meter for collecting consumption data; a rechargeable battery; a battery controller for modifying meter readings by controlling a battery's charge or discharge rate; and a switch capable of denying reporting of the meter readings when necessary. Assume that the total number of household electrical appliances is M. Notation t denotes the time when the t^{th} meter reading is reported, $r(t)$ represents the meter reading at time t. We use $n(t)$ to demonstrate the charge



(a) Square Price (b) Triangle Price (c) Sinusoidal Price

Fig. 2: Three Different Price Models [13]

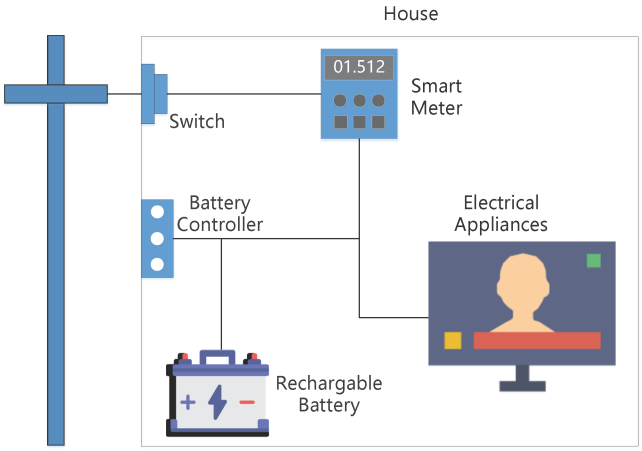


Fig. 1: System Model

or discharge rate of the battery at time t. For simplicity, we assume that time slot in this paper is unit time, which indicates that $n(t)$ also equals to the charged or discharged power of the battery at time t. While $c(t)$ is the quantity of electricity left in the battery and the total capacity of the battery is C. We also use α and β to denote the maximum discharge and the maximum charge rate separately, and s demonstrates the scale parameter for narrowing down the domain of μ, where μ is the mean value of our Laplace distribution. Moreover, d_i^t is the energy consumption of the i^{th} appliance at time t, and the total consumption at time t is denoted by $D(t)$. As the result, we have $r(t) = D(t) + n(t)$.

The execution of the whole system is concluded in the following: Firstly, customers use electrical appliances which consume electricity. Consumption data is then collected by the smart meter. Almost at the same time, the battery controller modifies the charge or discharge rate of the battery to obscure the actual consumption data. Lastly, the smart meter reports the blurred reading to the electricity supplier.

B. Price Model

In this paper, we adopt time of use (TOU) pricing policy in the proposed scheme. It is necessary to mention that, under static policy, the real-time electricity price is accessible in advance. Taking the diversity of the actual electricity price into consideration, square model, triangle model and sinusoidal model are utilized as shown in Fig. 2 [13]. We also assume that only the real-time electricity price for one day could be obtained. TOU price at time t is represented by $p(t)$.

C. Adversarial Model

The adversary in this paper is defined as honest-but-curious. It is merely passive in monitoring the meter reports [10]. On one hand, the meter readings would not be modified viciously. On the other hand, techniques like NILM would are likely to be used to mine customer's privacy out of curiosity. In other words, if the real meter readings are revealed to the adversary, then the customers' privacy is at risk. Therefore, our design goal is to devise a formally provable privacy-preserving scheme in smart grid under a static policy.

IV. Differentially Private Meter Reading Report Scheme

In this section, we introduce the differentially private meter reading report scheme. Specifically, the parameter notations of the proposed scheme are first presented in Table I. As discussed in Section I, sensitive information could be revealed by analyzing the real meter readings, and one intuitive method to avoid privacy leakage is adding random noises.

No privacy would be disclosed if the modified readings are completely independent with original readings, so keeping the final meter reading at a fixed value is one intuitive solution. However, boundary limitations brought about by the battery have not been solved. Recall that our goal is designing a differential private scheme to preserve privacy in a smart grid. Since differential privacy could be achieved by drawing noises from Laplace distribution, we use noises drawn from a Laplace distribution to blur the meter readings. The probability density function of a Laplace distribution with mean value μ and variance $2\sigma^2$ is: $pdf(x) = \frac{1}{2\sigma} e^{-\frac{|x-\mu|}{\sigma}}$, $x \in (-\infty, +\infty)$. Also,

TABLE I: Parameter Notations of the Proposed Scheme

t	Time Point	$c(t)$	Energy left in the battery at time t
M	Number of appliances	d_i^t	Energy consumption for the i^{th} appliance at time t
$r(t)$	Meter reading at time t	$D(t)$	Real consumption at time t
$n(t)$	Charge or discharge rate of the battery at time t	$p(t)$	Electricity price at time t
α	Maximum discharge rate of the battery	ϵ	Coefficient of differential privacy t
β	Maximum charge rate of the battery	δ	Coefficient of differential privacy
C	Capacity of the battery	σ	Standard deviation of Laplace distribution
p_l	Minimum electricity price	p_h	Maximum electricity price
d_1	Minimum consumption of all appliances	d_2	Maximum consumption of all appliances
s	Scale parameter	m	Number of arms

we know that the battery has a limited capacity and charge or discharge rate. Therefore, the noises generated by Laplace distribution become trivial because the battery limitations may be violated (these noises are defined as invalid noises). Since the charge rate and discharge rate are α and β, the mean value μ of Laplace distribution should fall in $[\alpha, \beta]$. However, invalid noises still emerge easily when μ approaches α or β. To resolve this problem, we narrow the domain of μ to $[\alpha^{'}, \beta^{'}]$ with a scale parameter s to decrease the probability of obtaining invalid noises, where interval $[\alpha, \beta]$ and interval $[\alpha^{'}, \beta^{'}]$ overlapped at a central point. These two intervals satisfy $s(\beta - \alpha) = (\beta^{'} - \alpha^{'})$. Hence, $\alpha^{'}, \beta^{'}$ can be computed as:

$$\begin{cases} \alpha^{'} = [\alpha(1+s) + \beta(1-s)]/2 \\ \beta^{'} = [\alpha(1-s) + \beta(1+s)]/2 \end{cases} \tag{4}$$

Recall that the proposed scheme works under a static electricity price policy, therefore, we can decrease bills by maneuvering the mean value of our Laplace distribution. To be more specific, we could set μ to a smaller value to discharge the battery with a high probability when the electricity price is high, and set μ to a larger value to charge the battery with a high probability when the electricity price is low. To update μ according to electricity price, the relationship between μ and $p(t)$ is often assumed as linearity [13]. So, a u_0 is computed given $p(t)$ as follows:

$$\mu_0 = (p(t) - p_l) \times \frac{\beta^{'} - \alpha^{'}}{p_h - p_l} + \alpha^{'} \tag{5}$$

where p_l, p_h are the minimum and maximum electricity prices in a single day respectively. μ_0 computed in equation (5) decides whether the battery charges or discharges with a high probability. For instance, if μ_0 is close to $\alpha^{'}$, then there is a high probability that the battery would discharge. If μ_0 is close to $\beta^{'}$, there is a high probability that the battery would charge.

Although the restricted domain of μ can lower the probability of producing invalid noises, noises violating the battery limitations still emerge, breaking the Laplace distribution and revealing customers' privacy in consequence. In the proposed scheme, we decline to report the meter readings utilizing a switch to prevent privacy leakage when the battery limitations are violated. Unfortunately, denying reporting the meter readings may instigate punitive actions from the electricity supplier, which would create an extra expense to customers. Since invalid noises would incur extra costs, diminishing extra costs by lowering the probability of sampling invalid noises should be considered. Recall that decreasing the domain of μ to $[\alpha^{'}, \beta^{'}]$ can lower the probability of getting invalid noises resulting from violating the battery charge and discharge rate limitations. However, the battery capacity has limitations too, which can be represented as $0 \leq c(t) \leq C$ at time t. At this point, if $c(t) > C/2$, μ_0 is appropriate, otherwise, μ_0 might violate the battery capacity limitation with a higher probability. Actually, if the battery tends to charge when $c(t) < C/2$ or the battery tends to discharge when $c(t) > C/2$, the battery capacity limits would not be violated easily, hence, setting $\mu = \mu_0$ is acceptable. However, other conditions could be troubling. For instance, if μ_0 is close to $\alpha^{'}$ and $c(t)$ is close to 0, then the battery does not have enough electricity to discharge. To address the dilemma resulting from violating the battery capacity limitation, we make use of the regret mechanism in the multi-armed bandit problem as described in Section II to adapt the value of μ. Details about the regret mechanism for the multi-armed bandit problem in the proposed scheme are presented in the following.

Intuitively, the smaller $|\mu - \mu_0|$ is, the less extra costs will be incurred. On the other hand, the smaller $\left|c(t) - \frac{C}{2}\right|$ is, the greater the opportunity of getting a valid noise. So, at each time t, an appropriate regret value of the chosen arm j can be defined as:

$$R[j] = \omega|\mu - \mu_0| + (1-\omega)f(t)\left|c(t) - \frac{C}{2}\right| \tag{6}$$

where ω is a predefined parameter. Afterwards, $Pr[j] = 1 - R[j]/\sum_{k=1}^{m} R[k]$ is calculated as the probability of choosing the j^{th} arm the next time. At each iteration, with a predefined coefficient λ used to balance the tradeoff between μ_0 and the chosen arm, we compute the mean value of our Laplace distribution μ as a linear combination of μ_0 and the selected arm as [13]

$$\mu = \lambda\mu_0 + (1-\lambda)Arm(j) \tag{7}$$

All in all, the proposed scheme requires a preprocess stage at which $\alpha^{'}$ and $\beta^{'}$ is calculated according to α, β and s. Then, we sample m discrete values from $[\alpha^{'}, \beta^{'}]$ evenly as m arms. Then, we initialize $Pr(k) = \frac{1}{m}$ and $R(k) = 0$ for all k in $\{1, 2, \ldots, m\}$, where $Pr(k)$ denotes the probability of choosing $Arm(k)$ and $R(k)$ is the regret value for $Arm(k)$. In addition, p_l and p_h are required, and we present the preprocess part in Algorithm 1.

Algorithm 1 Preprocess

Input: $\{\alpha, \beta, s\}$
Output: $\{\alpha^{'}, \beta^{'}, \{Pr(k), R(k), Arm(k)|k \in \{1, 2, \ldots, m\}\}\}$
1. $\alpha^{'} = [\alpha(1+s) + \beta(1-s)]/2$
2. $\beta^{'} = [\alpha(1-s) + \beta(1+s)]/2$
3. **For** k *in* $\{1, \ldots, m\}$
4. $\quad Pr(k) = 1/m$
5. $\quad R(k) = 0$
6. $\quad Arm[k] = \alpha^{'} + \frac{k(\beta^{'} - \alpha^{'})}{m}$
7. **Return** $\{Pr(k), R(k), Arm(k)|k \text{ in } \{1, 2, \ldots, m\}, \alpha^{'}, \beta^{'}\}$

After the preprocess stage, day-wise price data can be processed. In each day, we first compute the minimum electricity price p_l and the maximum electricity price p_h. Then, in each iteration, μ_0 and the chosen arm $Arm(j)$ are calculated according to $p(t)$ and $Pr(k)$ respectively, where $k \in \{1, 2, \ldots, m\}$. After drawing noises from Laplace distribution in each iteration, $R(j)$ is calculated as equation (6), while $Pr(k)$ should be updated as $Pr(k) = 1 - \frac{R(k)}{R}$, $k \in \{1, 2, \ldots, m\}$. From the view of $r(t)$, as discussed in [13], any $r(t)$ larger than $d_1 + \beta$ or smaller than $d_2 + \alpha$ violates differential privacy. In the proposed scheme, these $r(t)$ are prevented from reporting, so, the domain of the reported meter reading is $[d_2 + \alpha, d_1 + \beta]$. Accordingly, it is reasonable for customers to take penalty from electrical supplier. In the proposed scheme, The punishment at each time is defined as the multiplication of the electricity unit price and the customers historically highest energy consumption.

In a word, we use $\{\alpha^{'}, \beta^{'}, \alpha, \beta, m, \epsilon, C, c(t-1), p(t)\}$ combined with $\{\{d_i^t | i \in [1, M]\}, \{Pr(k), R(k), Arm(k)|k \in \{1, 2, \ldots, m\}\}\}$ as input and the final meter reading as the output. Details of the proposed scheme are presented in Algorithm 2 and, as shown, p_l and p_h are calculated in the first place. Then, data in each time slot is processed iteratively. Concretely, in each iteration, we first compute μ according to current electricity price and multi-armed bandit mechanism, then noise is drawn from Laplace distribution with mean μ. Next, regret value of each arm is updated accordingly. At last, the algorithm generate output and check its validity. If the algorithm output is $null$, then the final meter reading would not be reported to the electricity supplier.

Algorithm 2 Differentially Private Meter Reading Report Scheme

Input: $\{\alpha^{'}, \beta^{'}, \alpha, \beta, m, \epsilon, C, c(t-1), \{d_i^t | i \in [1, M]\}, \{Pr(k), R(k), Arm(k)|k \in \{1, 2, \ldots, m\}\}, \{p[t]\}\}$
Output: $\{r(t)\}$
1. $p_l = p_h = p(0)$
2. **For** k in $\{1, \ldots, m\}$
3. $\quad$ **If** $p(k) > p_h$
4. $\quad\quad p_h = p(k)$
5. $\quad$ **If** $p(k) < p_l$
6. $\quad\quad p_l = p(k)$
7. **For** all t
8. $\quad D(t) = \sum_{k=1}^{M} d_k^t$
9. $\quad$ **For** all k, l in $\{1, \ldots, M\}$
10. $\quad\quad \Delta f = max|d_k^t - d_l^t|$
11. $\quad \sigma = \frac{\Delta f}{\epsilon}$
12. $\quad \mu_0 = (p(t) - p_l) \times \frac{\beta^{'} - \alpha^{'}}{p_h - p_l} + \alpha^{'}$
13. $\quad Arm(j) \leftarrow \{Pr(k)|k \text{ in } \{1, \ldots, m\}\}$
14. $\quad$ **If** $\mu_0 \left(c(t) - \frac{C}{2}\right) < 0$
15. $\quad\quad \mu = \mu_0$
16. $\quad$ **Else**
17. $\quad\quad \mu = \lambda\mu_0 + (1-\lambda)Arm(j)$
18. $\quad pdf(x) = \frac{1}{2\sigma} e^{-\frac{|x-\mu|}{\sigma}}$
19. $\quad n(t) \leftarrow pdf(x)$
20. $\quad tmp = c(t-1) + n(t)$
21. $\quad R(j) = \omega|\mu - \mu_0| + (1-\omega)p(t)\left|tmp - \frac{C}{2}\right|$
22. $\quad R = \sum_{k=1}^{m} R(k)$
23. $\quad$ **For** k in $\{1, \ldots, m\}$
24. $\quad\quad Pr(k) = 1 - \frac{R(k)}{R}$
25. $\quad r(t) = D(t) + n(t)$
26. $\quad$ **If** $tmp < 0$ *or* $tmp > C$ *or* $n(t) < \alpha$ *or* $n(t) > \beta$
27. $\quad\quad$ **Return** $null$
28. $\quad$ **If** $r(t) \geq d_1 + \beta \;||\; r(t) \leq d_2 + \alpha$
29. $\quad\quad$ **Return** $null$
30. $\quad$ **Else**
31. $\quad\quad c(t) = tmp$
32. $\quad\quad$ **Return** $r(t)$

V. Evaluation

A. Theoretical Analysis

We first prove that the proposed scheme achieves (ϵ, δ) differential privacy in two parts. In the first part, we present our proof when $n(t) < \alpha$ or $n(t) > \beta$ or $c(t) < 0$ or $c(t) > C$ or the final meter reading $r(t)$ falls in $(-\infty, d_2 + \alpha]$ or $[d_1 + \beta, \infty)$. Under this circumstance, the meter readings will not be reported in the proposed scheme. In the second part, we finalize the proof by verifying that differential privacy is achieved when $d_2 + \alpha < r(t) < d_1 + \beta$.

Part 1: As described in Section IV, we do not report the meter readings if $n(t) < \alpha$ or $n(t) > \beta$ or $c(t) < 0$ or $c(t) > C$. Also, when the final meter reading $r(t)$ falls in $(-\infty, d_2 + \alpha]$ or $[d_1 + \beta, \infty)$, the meter readings will not be reported. Thus, no readings are reported and no privacy is compromised. Therefore, $(0, 0)$ differential privacy is achieved.

Part 2: Note that the core idea of this proof is similar to that in [13]; however, it is still presented here for completeness. In this part, $d_2 + \alpha < r(t) < d_1 + \beta$ is satisfied. Assume there are two datasets $D(t)$ and $D^{'}(t)$ including all the appliances, and they differ in only one appliance. Since $r(t) = D(t) + n(t)$, we have $r(t) = D^{'}(t) + n^{'}(t)$. In addition, we set the mean value of Laplace distribution for $D(t)$ and $D^{'}(t)$ to be μ and $\mu^{'}$ respectively. The specific derivation is as follows:

$$P(t) = \frac{Pr[r(t) = D(t) + n(t)]}{Pr[r(t) = D^{'}(t) + n^{'}(t)]} = \frac{Pr[n(t) = r(t) - D(t)]}{Pr[n^{'}(t) = r(t) - D^{'}(t)]}$$

According to the formulation (1), $P(t)$ is computed in the following:

$$P(t) = \frac{\int_{r(t)-D(t)}^{r(t)-D(t)+\Delta x} \frac{e^{-\frac{|x-\mu|}{\sigma}}}{2\sigma} dx}{\int_{r(t)-D'(t)}^{r(t)-D'(t)+\Delta x} \frac{e^{-\frac{|x-\mu'|}{\sigma}}}{2\sigma} dx}$$
$$= \frac{\frac{1}{2\sigma} \times e^{-\frac{|r(t)-D(t)-\mu|}{\sigma}}}{\frac{1}{2\sigma} \times e^{-\frac{|r(t)-D'(t)-\mu'|}{\sigma}}}$$
$$\leq e^{\frac{|D'(t)-D(t)|}{\sigma}} \times e^{\frac{|\mu'-\mu|}{\sigma}}$$

We set μ_l and μ_h to be the minimum and maximum value of μ, therefore, we have $|\mu' - \mu| \leq |\mu_h - \mu_l| = \Delta\mu$. Also, we have $\Delta f = max|d_i^t - d_l^t|$ for all combinations of i, t, l. Furthermore, we have $\sigma = \Delta f/\epsilon$, hence, further derivation could be:

$$\frac{\Pr[\mathrm{r(t)} = \mathrm{D(t)} + \mathrm{n(t)}]}{\Pr[\mathrm{r(t)} = \mathrm{D'(t)} + \mathrm{n'(t)}]} \leq e^{\epsilon} \times e^{\frac{\Delta\mu}{\sigma}}$$

As the result, we have

$$\Pr[\mathrm{r(t)} = D(t) + n(t)] = e^{\epsilon} \times \Pr[\mathrm{r(t)} = \mathrm{D}'(\mathrm{t}) + \mathrm{n}'(\mathrm{t})] + e^{\epsilon} \times (e^{\frac{\Delta\mu}{\sigma}} - 1) Pr[r(t) = D'(t) + n'(t)] \quad (8)$$

where $e^{\epsilon} \times (e^{\frac{\Delta\mu}{\sigma}} - 1) Pr[r(t) = D'(t) + n'(t)]$ is δ in the proposed scheme. So, (ϵ, δ) differential privacy is achieved when $\alpha \leq n(t) \leq \beta$, $0 \leq c(t) \leq C$ and $d_2 + \alpha < r(t) < d_1 + \beta$.

B. Experimental Analysis

In this paper, we consider privacy leakage and extra costs as two measurements for quantifying the proposed scheme. Our experiment utilizes the dataset sampled from MIT's dataset REDD [19]. Consumption data in REDD is extracted every 15 minutes, or, in other words, 96 data items are collected each day. The data is collected from 3 houses for 36, 35, 44 days respectively. For the real time electricity price, given the minimum price p_l and maximum price p_h, we sample price values at different times according to predefined models, including square model, triangle model and sinusoidal model as shown in Fig. 2. Some predefined parameters used in our experiment are listed in Table II.

Mutual information is a useful metric for quantifying data relevance in statistics. In this paper, we use mutual information [20] between real consumption data and the reported readings to quantify privacy loss. Instead of computing mutual information of two entire datasets, we focus on the maximum single-point privacy leakage. Mutual information utilized in the proposed scheme denoted as M is defined as follows [21]:

$$M = \max_{t, D(t), r(t)} \left\{ Pr[D(t), r(t)] log \frac{Pr[D(t), r(t)]}{Pr[D(t)] Pr[r(t)]} \right\} \quad (9)$$

where Pr[D(t),r(t)] denotes the joint probability of D(t) and r(t) [20], [21]. Intuitively, the smaller M is, the smaller the correlation between D(t) and r(t) will be, or, in other words, the better the privacy protection will be. Extra costs can be computed directly given electricity prices and noises.[1] In order to decrease influences brought about by randomness, every experiment is executed 50 times and the mean of the results is considered the final result.

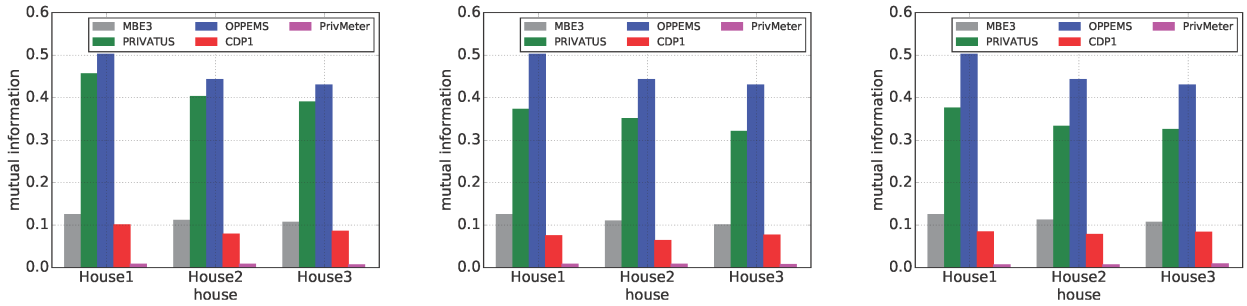
TABLE II: system parameter setting

m	100	ω	0.3
α	$-12.0\ kW$	λ	0.3
β	$12.0\ kW$	ϵ	0.2
C	$70\ kWh$	s	0.10
d_1	$0\ kWh$	d_2	$6.081\ kWh$
p_h	$0.02109\ \$/kWh$	p_l	$0.00704\ \$/kWh$

Based on the experimental results of our differentially private smart meter reading report scheme (PrivMeter), we make comparisons with the optimal privacy-preserving energy management scheme [12] (OPPEMS), Zhao's multitasking-BLH-exp3 scheme [10] (MBE3), the wallet friendly privacy-preserving scheme by Koo [9] (PRIVATUS), and CDP1 in [13] in terms of extra costs and mutual information. Their schemes are all implemented and executed based on our experimental settings. Mutual information of these schemes for three houses and three price models is shown in Fig. 3. Specifically, the proposed scheme achieves mutual information as little as 0.007 which is around 70 times less than OPPEMS's mutual information (about 0.5), and the mutual information of MBE3 is around 0.11 which is about 15 times as much as ours. In addition, compared with the proposed scheme, mutual information of MBE3 and OPPEMS have larger fluctuations of different price models and houses, which leads to a greater variance. Hence, the proposed scheme is more stable in terms of privacy protection. For Figure 4, MBE3 could not guarantee a cost saving, and OPPEMS barely saves money according to our experimental results. PRIVATUS could save money in any combination of price models and houses and it could even save as much as 25 dollars. However, its mutual information (around 0.35) could be about 50 times larger than that of the proposed scheme. While CDP1 could save less than 5 dollars, its mutual information is at least 0.07 which is 9 times larger than that of the proposed scheme. The main reason that the proposed scheme achieves better privacy protection is that the switch mechanism essentially eliminates all the reports generated by the invalid noises. However, the proposed scheme could not save money because the invalid noises would incur punitive actions such as fines from the electricity supplier. The extra costs of the proposed scheme are at most 8 dollars, as shown in Fig. 3.

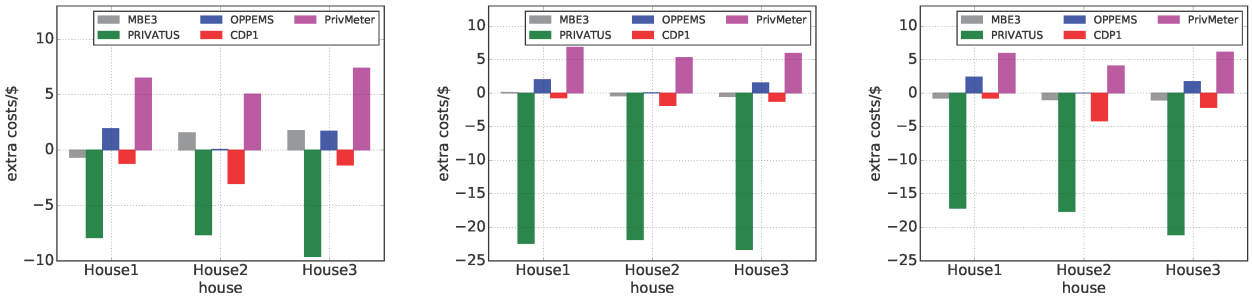
In the proposed scheme, invalid noises create significant effects both on extra costs and mutual information. So, we also investigate the correlation between the number of invalid noises, extra costs and mutual information, as presented in Fig. 5. Fig. 5(a) demonstrates the relationship between the number of invalid noises and extra costs with three different price models considered. As shown in Fig. 5(a), extra costs grow as the number of invalid noises increase because penalty

[1]The punishment at each time is defined as the multiplication of the electricity unit price and the customer's historically highest energy consumption.



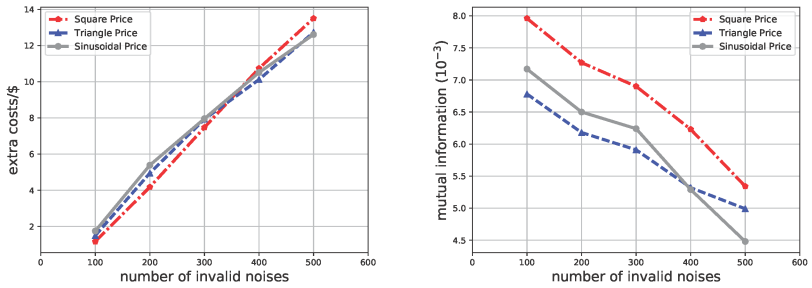
(a) Square Price (b) Triangle Price (c) Sinusoidal Price

Fig. 3: Mutual Information of Different Schemes



(a) Square Price (b) Triangle Price (c) Sinusoidal Price

Fig. 4: Extra Costs of Different Schemes



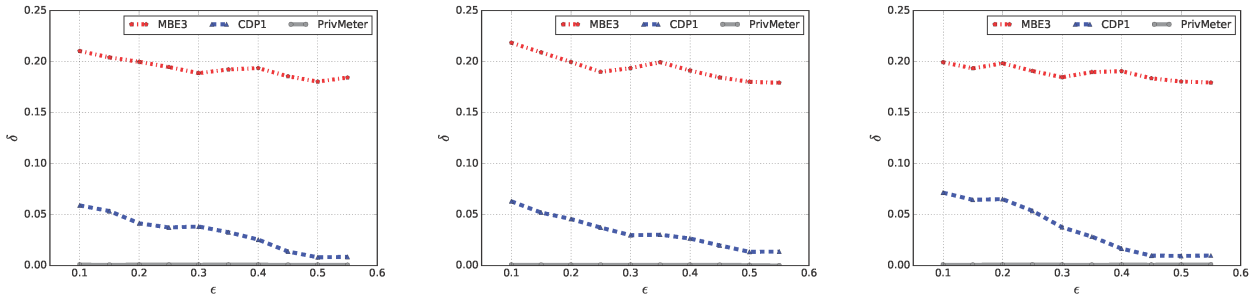
(a) Extra Costs (b) Mutual Information

Fig. 5: Extra Costs and Mutual Information with Different Number of Invalid Noise

costs are higher. The growth trend could be approximated as linearity, or specifically as nearly 3 dollars every 100 invalid noises. Also, results for the different price models are close to each other, which, to some degree, demonstrates the robustness of the proposed scheme in terms of data diversity. Quantitatively, extra costs are around 1.18 dollars when 100 invalid noises emerge, while more than 11.8 dollars would be charged if 500 invalid noises are generated. Fortunately, the number of invalid noises could be no more than 100 with proper parameter settings. In house 1, the original cost is about \$20 for the three price policies, therefore, the extra cost is just 5.9% of that.

Regarding mutual information, more invalid noises result in smaller amounts of mutual information because those meter readings associated with invalid noises would not be reported. As shown in Fig. 5(b), the result is in line with our expectations. When the number of invalid noises is less than 300, the proposed scheme still achieves mutual information less than 0.01 for 3 different price models.

We also explore the relationship between δ and ϵ, and comparisons with MBE3 [10] and CDP1 [13] are made for 3 different price models. The results are presented in Fig. 6. In this paper, due to the fact that meter readings that violate differential privacy are prevented from being reported, δ in



(a) Square Price (b) Triangle Price (c) Sinusoidal Price

Fig. 6: Relationship Between δ and ϵ of Different Schemes

the proposed scheme should be less than MBE3 and CDP1. As shown in Fig. 6, with the increase of ϵ, δ fluctuates around 0.2 which is more than 20 times greater than that of the proposed scheme. CDP1 achieves better δ in contrast to MBE3, specifically, $\delta < 0.1$ is satisfied for different ϵ and different price models, while the proposed scheme achieves smaller δ than CDP1. Quantitatively, the proposed scheme could achieve $\delta < 0.006$ for different ϵ and different price models. Lastly, it is necessary to mention that the proposed scheme has stable performance in terms of the relationship between δ and ϵ. In a word, for the relationship between δ and ϵ, the proposed scheme outperforms CDP1 and MBE3.

VI. Related Work

In order to address privacy concerns in a smart grid, a series of Battery-based Load Hiding (BLH) schemes have been proposed to achieve privacy protection based on a rechargeable battery. For example, the power management model based on a rechargeable battery was introduced by Kalogridis [8] where the power mixing algorithm tried to keep the meter readings as a fixed value. To the best of our knowledge, this was the first scheme utilizing a rechargeable battery to fuzz real household energy consumption. However, the limited battery capacity and charge or discharge rates were not considered, which would reveal customers' privacy. McLaughlin presented a non-intrusive load leveling scheme [6] to address this problem by enabling the battery to charge or discharge automatically according to the energy left in the battery, trying to compensate for the battery limitations [6]. The battery should be charged when the remaining energy is low, otherwise, the battery discharges. The schemes above could protect privacy to a certain degree, but neither achieves differential privacy [7] due to the battery's inherent charging/discharging limitation.

Based on Kalogridis's work, a stepping approach was proposed by Yang [7] to maximize the deviation between the actual household consumption and the meter readings [7] from an adversary point of view. What's more, a wallet friendly privacy-preserving scheme [9] was designed by Koo to protect privacy through diminishing the relevance of the meter readings and actual electricity usages. Also, stochastic dynamic programming was employed to save money as much as possible [9]. Yang and Chen presented an optimal privacy preserving energy management scheme, trying to minimize the variance of the meter readings to achieve privacy protection [12]. In their work, the problem was initially reduced by the Lyapunov optimization technique [12]. Then, the problem was divided and conquered separately [12]. Unfortunately, both Koo's and Yang's schemes fail to satisfy differential privacy for violating the battery's inherent charging/discharging limitations [11]. Moreover, Zhao proposed a randomized BLH approach and a multitasking-BLH-exp3 scheme [10] with differential privacy achieved by adaptively updating the BLH algorithm according to constraints and instantaneous status. However, its proof is incomplete due to the fact that it ignores certain scenarios when the limitations of the battery are considered [13]. Two cost-friendly and differentially private algorithms were proposed in [13] for static price models and dynamic price models respectively. Specifically, in CDP1, Laplace distribution was modified according to electricity prices to save costs. While in CDP2, the multi-bandit mechanism was employed when prices could not be accessed in advance. CDP1 could save money, but its privacy protection level is slightly better than previous works and could be improved.

VII. Conclusion and Future Work

In this paper, we investigated existing literature for battery-supported solutions to solve privacy issues in smart grid. The common defects were analyzed for either lacking of formal privacy guarantee or becoming vulnerable when used with real-world batteries with the inherent charging/discharging and capacity limitation. In order to solve these problems, we proposed a differentially private smart meter reading report scheme by adding a switch-and-penalty mechanism. The proposed scheme was formally proven to satisfy the definition of differential privacy. In addition, simulation experiments were performed on the REDD. We not only made comparisons with existing works, but also quantitatively analyzed the influences induced by electricity price diversity and system parameters like ϵ. Based on real experimental results, the proposed scheme achieved better privacy protection compared with previous works at the expense of tolerable extra costs.

For future work, on one hand, we focus on diminishing extra costs brought about by invalid noises through changing the method of calculating μ, modifying the multi-armed bandit mechanism or employing other gaming theories. On the other hand, it is possible that altering the Laplace distribution in the proposed scheme may also help reduce extra costs. Also, we would explore the possibilities of employing differential privacy in other data-sensitive areas and try to combine differential privacy with other theories to bring a greater practical value.

ACKNOWLEDGMENT

Corresponding Author: Liehuang Zhu. This work is supported by National Science Foundation grants CNS1262275, CNS-1318948, China National Key Research and Development Program No. 2016YFB0800301, and National Natural Science Foundation of China NSFC No. 61300177.

REFERENCES

[1] H. Farhangi, "The path of the smart grid," *Power and energy magazine, IEEE*, vol. 8, no. 1, pp. 18–28, 2010.

[2] A. Zoha, A. Gluhak, M. A. Imran, and S. Rajasegarar, "Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey," *Sensors*, vol. 12, no. 12, pp. 16 838–16 866, 2012.

[3] Z. Guo, Z. J. Wang, and A. Kashani, "Home appliance load modeling from aggregated smart meter data," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 254–262, 2015.

[4] M. J. Johnson and A. S. Willsky, "Bayesian nonparametric hidden semi-markov models," *The Journal of Machine Learning Research*, vol. 14, no. 1, pp. 673–701, 2013.

[5] E. Elhamifar and S. Sastry, "Energy disaggregation via learning powerlets and sparse coding." in *AAAI*, 2015, pp. 629–635.

[6] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 87–98.

[7] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 415–427.

[8] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010*. IEEE, 2010, pp. 232–237.

[9] J. Koo, X. Lin, and S. Bagchi, "Privatus: Wallet-friendly privacy protection for smart meters," in *Computer Security–ESORICS 2012*. Springer, 2012, pp. 343–360.

[10] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proceedings of the 2014 IEEE INFOCOM*. IEEE, 2014, pp. 504–512.

[11] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," in *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2014, pp. 194–212.

[12] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Optimal privacy-preserving energy management for smart meters," in *Proceedings of the 2014 IEEE INFOCOM*. IEEE, 2014, pp. 513–521.

[13] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Transactions on Smart Grid*, vol. 8, pp. 619–626, 2017.

[14] C. Dwork and J. Lei, "Differential privacy and robust statistics," in *Proceedings of the forty-first annual ACM symposium on Theory of computing*. ACM, 2009, pp. 371–380.

[15] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proceedings of the forty-second ACM symposium on Theory of computing*. ACM, 2010, pp. 705–714.

[16] S. Bagheri and A. Scaglione, "The restless multi-armed bandit formulation of the cognitive compressive sensing problem," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1183–1198, 2015.

[17] W. Cowan and M. N. Katehakis, "Multi-armed bandits under general depreciation and commitment," *Probability in the Engineering and Informational Sciences*, vol. 29, no. 01, pp. 51–76, 2015.

[18] S. Bubeck, N. Cesa-Bianchi *et al.*, "Regret analysis of stochastic and nonstochastic multi-armed bandit problems," *Foundations and Trends® in Machine Learning*, vol. 5, no. 1, pp. 1–122, 2012.

[19] J. Z. Kolter and M. J. Johnson, "Redd: A public data set for energy disaggregation research," in *Workshop on Data Mining Applications in Sustainability (SIGKDD), San Diego, CA*, vol. 25. Citeseer, 2011, pp. 59–62.

[20] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2011*. IEEE, 2011, pp. 1932–1935.

[21] L. Sankar, S. Kar, R. Tandon, and H. V. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *IEEE International Conference on Smart Grid Communications (SmartGridComm) 2011*. IEEE, 2011, pp. 220–225.