Cost and Pricing of Differential Privacy in Demand Reporting for Smart Grids

Xin Lou, David K.Y. Yau, Rui Tan, Peng Cheng

***Abstract*—In smart grid, the highly dynamics of electrical loads introduce uncertainty to the system, which also brings new challenges for the power grid control and optimization. Reporting demand information by customers in solving the economic dispatch control (EDC) problem in power grids is a promising approach, but it raises important privacy concerns. One solution is to add random noise to aggregate queries of demand reports can provide differential privacy (DP) for the individual customers. However, the noisy query information can adversely degrade the EDC's optimality. In this paper, we first analyze the cost in demand reporting in terms of how DP-induced noise will increase the total generation cost. We show that the noise amounts for different customers are intricately coupled with one another in determining the total cost. To deal with the coupling, we apply the principle of Shapley value to attribute fair shares of the total cost to the power grid buses and study the properties of this cost sharing approach. For efficient sharing of the privacy cost, in a manner scalable to large power systems with many buses, we propose heuristic algorithms to approximate the Shapley value. Moreover, we study important network effects of the per-customer DP cost within a privacy group attached to the same bus, in that this cost depends on how many other customers choose the same privacy group. Accordingly, we design a pricing scheme for the customers that we prove to be truthful, i.e., customers have no incentives to deviate from the group that represents their true privacy needs. We also discuss the impact of the high-demand customer on other customers' cost and propose an approach in the pricing scheme to charge higher cost on the high-demand customer. Trace-driven simulations based on a 5-bus power system model validate our analysis and illustrate the performance of the proposed cost sharing algorithms.**

***Index Terms*—smart grid, differential privacy, demand reporting, cost sharing**

I. Introduction

In the era of smart grids, highly dynamics at the electrical loads are introduced due to, for example, the proliferation of demand-side renewables (e.g., solar panels), batteries for energy storage, and smart appliances that can react to their environments, as well as real-time energy pricing increasingly required by law for customers [1], which makes the load demand even harder to predict. The unpredictability of load brings new challenges for grid operators to optimize the efficiency of their power networks. The classic economic dispatch control (EDC) [2], which plans the active power outputs of generators to meet future demand at the lowest total generation cost, is an important example problem. In current power grids, a forecast-demand vector of the buses is used in EDC to calculate the optimal power flow and the output is scheduled at generators. The forecast accuracy of demand will be necessarily reduced by higher load dynamics and hence the EDC's optimality will be undermined [3]. To combat the uncertainty, one promising solution is the demand reporting from end customers, in which smart meters installed at the consumption points report their future demand for the purpose of the EDC. Demand reporting has also been used in other demand response applications such as bid-based market clearing [4].

Demand reporting, although useful, it can lead to natural privacy concerns, i.e., the knowledge of power consumption may generally reveal sensitive information such as users' daily activities. For example, non-intrusive load monitoring (NILM) may infer a household's detailed tasks from a trace of its power consumption [5]. To mitigate the privacy concern, we can apply the differential privacy (DP) [6] technique, which is a rigorous information-theoretic approach to prevent leakage of individual records by statistical (e.g., aggregate) queries on a database of these records. DP is relevant to the privacy of demand reporting for EDC, because EDC requires only *aggregate* demand forecast per-bus for its decisions. Hence, following the principle of DP, we may add random noise to the aggregate (future) demand reported by the customers and reveal only this noisy version of the aggregate [5], [7], [8], [9], [10]. The amount of noise added is commensurate with the required level of privacy protection. However, due to the noisy per-bus aggregates, the suboptimal control will be led in EDC. The resulting increased generation cost represents the cost of privacy. Understanding this privacy cost is important to the design of demand reporting.

Based on the above key observations, we study two fundamental problems in this paper. First, how to quantify the system-wide total DP cost of demand reporting for EDC, in which different groups of customers may require different levels of privacy? Second, how to attribute fair shares of the total DP cost to the heterogeneous groups of customers so that, for example, customers having more stringent privacy requirements will have to bear a higher privacy cost because they impose higher inaccuracy of the input to the EDC? Our analysis and cost sharing algorithms will provide an important basis for practical implementation of demand reporting for EDC and other smart grid control applications, by allowing customers to acquire sufficient privacy protection on a fair cost basis. The attribution of privacy cost in this study is meant to

X. Lou is with Advanced Digital Sciences Center, Illinois at Singapore, Singapore (e-mail: lou.xin@adsc-create.edu.sg).

D. K.Y. Yau is with Singapore University of Technology and Design, Singapore (e-mail: david_yau@sutd.edu.sg).

R. Tan is with Nanyang Technological University, Singapore (e-mail: tanrui@ntu.edu.sg).

P. Cheng is with Zhejiang University, P. R. China, China (e-mail: pcheng@iipc.zju.edu.cn).

apply in the context of an incentive program that motivates customers to take part in the demand reporting by passing on generation cost savings to the customers, although detailed design of this incentive program is beyond the scope of this paper. Hence, we do not expect that customers will make net payments for buying privacy for their demand reports. Rather, it is expected that they will receive compensation as reward for their participation in the demand reporting. The privacy cost may then serve as a negative adjustment to this compensation, so that the net incentive compensation for a more privacy-stringent customer will be lower but still positive.

In answering our research questions, we address the following three key challenges. **First**, existing studies on DP for smart meter data aggregation have considered only a single homogeneous level of required DP [5], [7], [8], [9], [10]. We believe that, whereas heterogeneous customers in the real world will desire different levels of privacy protection, a demand reporting scheme that admits a range of the provided DP will be more responsive to their needs. Moreover, existing studies do not address key features of the physical system, e.g., the grid's topology, required by the EDC. In this paper, we analyze heterogeneous DP protection and its impact based on realistic power grid topology. **Second**, inaccuracy of demand reports will mislead the EDC into a generation dispatch that does not balance the supply and demand, thereby causing under-/over-frequency. Load-frequency control (LFC), a closed-loop control system that regulates the grid frequency, will kick in to fix the mismatch in practice. Thus, we define the DP cost as discrepancy between the post-LFC generation cost and the generation cost without DP protection. However, because of complex dynamics of the LFC, it is non-trivial to derive the relationship between the post-LFC generation cost and the noise amounts in demand reports. **Third**, as our analysis shows, the noise amounts for different privacy groups are deeply coupled with one another in determining the total DP cost. This property precludes independent attribution of the DP cost for each group in isolation. We must account for any network effects of the DP between interdependent groups.

In addressing the above challenges, we make the following contributions:

- We propose a demand reporting scheme in which each customer chooses a privacy level characterized by an ϵ value from a predefined offered set according to the ϵ-DP definition, and all the customers choosing the same ϵ constitute each privacy group. We extend the approach in [6] to achieve ϵ-DP for each group.
- Based on a power engineering model of the LFC, we derive an analytic expression for the total privacy cost. We prove that it is always non-negative. This expression is a prerequisite for computing the fair DP cost shares for the different buses.
- We apply the principle of Shapley value to attribute fair shares of the total privacy cost to the buses. However, although the Shapley value is an effective and well accepted conceptual device, its implementation does not scale well to a large power system with many buses. Thus, we propose heuristic algorithms of low complexity for the DP cost attribution problem among the buses, and similar baseline algorithms for sharing the per-bus cost among the privacy groups. We compare their performance with the Shapley value-based approach.
- We study important network effects of the per-customer DP cost within a privacy group associated with a bus, in that this cost depends on each group's "popularity" or how many other customers on the bus choose the same group. We present game-theoretic arguments that the baseline pricing schemes for the per-bus privacy groups are not *truthful*, in that customers may have motivation to deviate from the group that truly represents their privacy needs. Accordingly, we ameliorate the pricing scheme of the groups to ensure its truthfulness.
- We also study the network effects of the high-demand customer on the per-customer privacy cost, where the high-demand customer can greatly increase the group cost due to its high upper bound. To ensure the fairness for low-demand customers, one alleviation approach is proposed to impose higher cost to the high-demand customers in corresponding groups.
- We conduct extensive simulations based on a 5-bus power system model and real load traces to validate our analysis and illustrate the performance of cost sharing algorithms.

Our prior work [11] presented the analysis of the grid's total DP cost and the design of various cost sharing schemes. Based on [11], we make the following new contributions in this paper: 1) For the completeness of the discussion on the pricing scheme, we analyze several properties of Shapley cost sharing scheme. Specifically, in Section VI-B1, we add the introduction of the basics of Shapley value. Then, in Section VI-B3, we present two key properties on the Shapley cost sharing scheme, which show how the noise introduced at each bus can affect the per-bus and overall privacy cost in the whole system. 2) We add Section VII to study the important network effects of the per-customer DP cost within a privacy group. The work [11] only studied the baseline cost sharing scheme at the customer-level and did not investigate the customer-level properties. In Section VII of this paper, we show that the per-customer DP cost within a privacy group depends on each privacy group's "popularity" or the number of customers on the bus choosing the same group. We present game-theoretic arguments that the baseline pricing schemes for the per-bus privacy groups are not truthful, where customers may have motivation to deviate from the group that truly represents their privacy needs. Therefore, we propose a novel pricing scheme to ensure the truthfulness and analyze the properties of this new pricing scheme. Moreover, we also discuss the impact of the high-demand customer to the privacy cost in the same group and propose the alleviation scheme to impose the higher cost to the high-demand customer who introduces additional privacy cost to other low-demand customers.

The balance of the paper is organized as follows. Section II reviews related work. Section III presents preliminaries and states our problem. Section IV presents the proposed demand-reporting scheme to support a range of DP requirements. Section V analyzes the total privacy cost. Section VI presents

algorithms for attribution of fair shares of this privacy cost among the buses, as well as among privacy groups of customers attached to each bus. Section VII analyses the network effects of the per-customer DP cost within each per-bus privacy group, and presents the design of a truthful pricing scheme for these different groups. Section VIII presents simulation results. Section IX discusses the impact on customer's cost due to the high-demand customer and proposes an approach to alleviate this impact. Section X concludes.

II. Related work

DP has been applied in smart metering to protect customers' privacy [5], [7], [8], [9], [10]. Its implementation is mainly based on distributing additive random noises [7], [8] among the smart meter readings to achieve DP of aggregate queries, such that demand-response aggregators cannot identify the data of individual customers. Since smart meters may fail, fault tolerance in modular addition-based encryption of aggregate meter readings is an important problem [7]. Won *et al.* [9] propose a proactive fault-tolerant aggregation protocol based on future ciphertexts, to ensure DP at higher communication efficiency and lower errors than previous fault tolerance approaches. Gulisano *et al.* [10] argue that DP-induced noises to metering data may adversely affect certain data analytics applications, and propose approaches to limiting the noise amounts. In battery-based load hiding, Zhao *et al.* [5] show that by enforcing household battery charging/discharging amounts to follow a binomial distribution, it is possible for the aggregation of power consumption over time to satisfy (ϵ, δ)-DP.

Although the research discussed above analyzes privacy in a power grid context, none of the results address how DP for customers' demand reports may impact the optimality of EDC as an important power grid control problem. We provide a novel analysis of the system's privacy cost that considers key characteristics of the physical control (e.g., power system topology and interaction between EDC and LFC), and present original insights of attributing fair shares of the overall cost among heterogeneous privacy groups of the customers.

EDC and LFC in power grids face new challenges due to increased supply/demand uncertainty arising from renewable generation and dynamic load. To mitigate the loss of efficiency stemming from this uncertainty, recent work [3], [12] has proposed to synchronize the EDC and LFC, whereas traditionally the two control mechanisms operate at different time scales. In [3], for example, the EDC is incorporated into generation-side LFC such that they both run at the same pace. In [12], load-side LFC is additionally integrated. Although synchronization of the EDC with LFC can improve the control in the face of uncertainty, such integrated EDC-LFC faces significant deployment barriers in that it will require major redesign of existing power grid control systems and electricity markets. In contrast, in this paper we leverage the increasing availability of advanced metering infrastructure (AMI) to allow accurate control without major changes to the EDC and LFC.

III. Preliminaries

In this section, we first present preliminaries of DP and EDC. Then, we introduce the problem of EDC based on demand reporting. The notation convention of this paper is as follows. Take a symbol x as an example. $\mathbf{X}$ denotes a matrix, $\mathbf{x}$ a column vector, $x[t]$ the tth sample of a time series x (we omit the time index $[t]$ when it is clear), $\widetilde{x}$ the Laplace transform of x, $\dot{x}$ the derivative of x with respect to time. $\mathbb{R}^p$ and $\mathbb{R}^{p\times q}$ denote the sets of p-dimensional real column vectors and real $p \times q$ matrices, respectively. $\mathbb{D}$ denotes the domain of data sets. $\|\cdot\|$ denotes cardinality.

A. Differential Privacy (DP)

In this paper, we use ϵ-DP [6] as our privacy definition. It is formally defined as

Definition 1 ([6]). *A randomized algorithm $\mathcal{A} : \mathbb{D} \to \mathbb{R}^t$ gives ϵ-DP if for all data sets $D_1 \in \mathbb{D}$ and $D_2 \in \mathbb{D}$ differing on at most one element, and all $S \subseteq Range(\mathcal{A})$, $Pr(\mathcal{A}(D_1) \in S) \leq e^\epsilon \cdot Pr(\mathcal{A}(D_2) \in S)$.*

In other words, a differentially private algorithm $\mathcal{A}$ produces indistinguishable output for any two datasets which differ on a single element. Thus, an adversary cannot infer the value of a single user's data in the dataset. The parameter ϵ characterizes the level of privacy. A smaller ϵ implies better privacy. Prior research [13] shows that, by adding independent and identically distributed (i.i.d.) Laplacian noise to the output of a function $\mathcal{F}$, we may achieve ϵ-DP. Let $\mathrm{Lap}(\lambda)$ denote a zero-mean Laplace distribution of probability density function (PDF) $f(x|\lambda) = \frac{1}{2\lambda} e^{\frac{|x|}{\lambda}}$. We have the following lemma.

Lemma 1 ([13]). *For all function $\mathcal{F} : \mathbb{D} \to \mathbb{R}^t$, the following algorithm $\mathcal{A}$ gives ϵ-DP: $\mathcal{A}(D) = \mathcal{F}(D) + [x_1, x_2, \ldots, x_r]^\intercal$, where the x_i are drawn i.i.d. from $\mathrm{Lap}(S(\mathcal{F})/\epsilon)$ and $S(\mathcal{F})$ denotes the global sensitivity of $\mathcal{F}$.*

We also introduce an *infinite divisibility property* [14] of the Laplace distribution. Denote by $\mathrm{Gamma}(n, \lambda)$ a Gamma distribution whose PDF is $f(x|n, \lambda) = \frac{(1/\lambda)^{1/n}}{\Gamma(1/n)} x^{\frac{1}{n}-1} \mathrm{e}^{-x/\lambda}$, where $\Gamma(1/n)$ is the Gamma function evaluated at $1/n$. Let $\gamma_{1,i}$ and $\gamma_{2,i}$ denote two random variables that are drawn in an i.i.d. way from $\mathrm{Gamma}(n, \lambda)$. Then, for any natural number n, $x = \sum_{i=1}^{n} \gamma_{1,i} - \gamma_{2,i}$ follows $\mathrm{Lap}(\lambda)$.

B. Economic Dispatch Control (EDC)

EDC is the determination of active power outputs of generators to meet the system load at the lowest generation cost, subject to various transmission and operational constraints. It is a form of tertiary generation control that updates the setpoints of LFC periodically (e.g., every five minutes or longer [15], [16]). A formal formulation of EDC is as follows.

Consider a power grid with N buses and L transmission lines. Denote by $\mathcal{G}$ and $\mathcal{L}$ the sets of generator buses and load buses, respectively. For a generator or load bus, say i, denote by p_i^g and p_i^l the active power generation and consumption, respectively, where $p_i^g \geq 0$ and $p_i^l \leq 0$ following the convention that power injection/draw is positive/negative. To simplify the discussion, we assume that a load bus is not connected with any generator (i.e., $p_i^g = 0$ if $i \in \mathcal{L}$) and a generator bus is not connected with any load (i.e.,

$p_i^l = 0$ if $i \in \mathcal{G}$). Denote by $\mathbf{p}^g$ and $\mathbf{p}^l$ the vectors composed of p_i^g and p_i^l for all buses, respectively. EDC is subject to the following three constraints. First, the following linearized nodal power flow constraint is widely adopted in power system analysis [17]:

$$\mathbf{p}^g + \mathbf{p}^l = \mathbf{A}^\intercal \mathbf{B} \mathbf{A} \boldsymbol{\theta}, \tag{1}$$

where $\mathbf{A} \in \mathbb{R}^{L \times N}$ is the incidence matrix characterizing the power grid topology, $\mathbf{B} \in \mathbb{R}^{L \times L}$ is a diagonal matrix whose diagonal elements represent the susceptance of the corresponding line, and $\boldsymbol{\theta} \in \mathbb{R}^N$ is a vector of the voltage phase angles at the buses. Second, the difference between the phase angles of any two connected buses should be within $[-\pi/2, \pi/2]$ to ensure the grid's stability [18]. This constraint can be represented compactly as

$$-\boldsymbol{\pi}/2 \leq \mathbf{A}\boldsymbol{\theta} \leq \boldsymbol{\pi}/2, \tag{2}$$

where $\boldsymbol{\pi} = [\pi, \ldots, \pi]^\intercal$. Lastly, each generator's output is within its capacity, i.e.,

$$0 \leq p_i^g \leq \overline{p}_i^g, \quad \forall i \in \mathcal{G}, \tag{3}$$

where $\overline{p}_i^g$ represents the capacity of the generator at bus i. Let $C_i(p_i^g)$ denote the generation cost of this generator. EDC solves the following constrained optimization problem:

$$\underset{\mathbf{p}^g, \boldsymbol{\theta}}{\text{minimize}} \sum_{i \in \mathcal{G}} C_i(p_i^g), \text{ subject to (1), (2), (3).} \tag{4}$$

Note that the input to Eq. (4) is $\mathbf{p}^l$. In this paper, we use $\text{EDC}(\mathbf{p}^l)$ to denote the solution to Eq. (4).

C. Demand Reporting based EDC (DR-EDC)

In today's deregulated electricity markets, EDC is deeply integrated with real-time pricing systems [2]. Specifically, a profit-neutral independent system operator (ISO) takes as input offers of supply from generators and demand bids from utilities to compute real-time locational prices to clear the market. Meanwhile, it uses demand forecast from the bids as $\mathbf{p}^l$ to solve the EDC problem in Eq. (4). Thus, improving the quality and accuracy of the demand forecast will improve the cost optimality and reliability of the EDC [19]. This is especially important in the era of smart grids, where there are increased demand dynamics and uncertainty.

In this paper, we consider a new scheme of EDC that we call demand-reporting based EDC (or DR-EDC). At the beginning of each DR-EDC cycle, the smart meters of customers report their demand in one or more future cycles to their respective utilities. The aggregated future demand is then used as input to the EDC. Note that an EDC cycle is typically five minutes or longer [15], [16], and existing AMIs can already sustain five-minute reporting intervals [20]. Compared with conventional EDC driven by utilities' per-bus demand forecasts, the DR-EDC driven by direct demand reports from the customers can better manage load uncertainty. It is because the customers' own smart meters have much better knowledge of the future consumption than the utilities, e.g., they have direct access to control and scheduling decisions of home automation systems, smart appliances, battery systems, etc. The more accurate control will reduce generation costs (as illustrated in Section VIII-A), which will translate generally into monetary rewards for the customers as incentives or rebates. However, there is the concomitant need to understand how the privacy requirements of customers will impact the performance limits of the DR-EDC and hence their net contributions, which is a main concern of this paper.

IV. Differentially Private Demand Reporting

This section proposes a demand-reporting scheme that provides ϵ-DP under different ϵ values for different groups of users. In the following, Section IV-A describes our system and threat models. Section IV-B describes the proposed scheme.

A. System and Threat Models

1) System model: For simplicity, we assume that the demand (or load) of each customer does not change during an DR-EDC cycle. Denote by $\mathcal{N}_i$ the set of customers attached to load bus i, $p_{i,j}^l[t]$ the demand report sent by the jth customer in $\mathcal{N}_i$ at the beginning of the tth DR-EDC cycle. We assume that each bus i is served by an *aggregator*, denoted by A_i. A_i receives the demand reports from the customers in $\mathcal{N}_i$ and reports the aggregated demand to the ISO for the EDC. The demand aggregation among $\mathcal{N}_i$ can be implemented based on homomorphic encryption [21] to prevent the aggregator and any intermediate nodes in the aggregation tree from knowing the individual $p_{i,j}^l$. In this paper, we assume that all the customers participate in the demand reporting. But our analysis can be readily extended to address non-participating customers.

2) Threat model: The adversary can be any "curious" entity having access to the per-bus aggregated demand reports, but not the actual per-bus power consumption that is available to the ISO only. For example, the adversary can be an DR-EDC aggregator or a subscriber to the per-bus aggregated demand reports (e.g., the DR-EDC operator). The adversary aims to infer the demand reports of individual customers from the aggregates. Our scheme provides a guaranteed level of DP to the customers against such an adversary. Our threat model is similar to those used in representative DP research for smart metering (e.g., [7], [8]).

B. DP-Assured Demand Reporting Scheme

This section presents a demand reporting scheme that guarantees DP. It is based on the basic principle discussed in [8], although our scheme is more general in that it supports multiple levels of privacy requirement. Moreover, our scheme differentiates customers according to the load buses they are on, which is needed for analyzing the impact of DP on the EDC in Section V. The proposed scheme works as follows.

1) Formation and maintenance of privacy groups: Our scheme offers K different predefined ϵ values denoted by $\epsilon_1, \epsilon_2, \ldots, \epsilon_K$, where $0 < \epsilon_1 < \epsilon_2 < \ldots < \epsilon_{K-1}$ and $\epsilon_K = \infty$. As discussed in Section III-A, a smaller ϵ implies better privacy. In particular, from Lemma 1, with an infinitely large ϵ (i.e., ϵ_K), the variance of the zero-mean Laplace

distribution $\mathrm{Lap}(S(\mathcal{F})/\epsilon)$ is zero, which suggests there is zero noise and hence no DP protection. Each customer chooses an ϵ from the K values offered, according to her needs. In practice, smart meters owned by the customer can be configured and programmed to suitable settings automatically. At bus i, the set of customers choosing ϵ_k is denoted by $\Phi_{i,k}$, where $1 \leq k \leq K$. Thus, $\sum_{k=1}^{K} \|\Phi_{i,k}\| = \|\mathcal{N}_i\|$. In this paper, $\Phi_{i,k}$ is also called the kth *privacy group* of the bus i and k represents the *privacy level*. The customers in $\mathcal{N}_i$ send their selected privacy levels to the aggregator A_i. Then, for each $k \in [1, K]$, the aggregator sends the size of the kth privacy group, i.e., $\|\Phi_{i,k}\|$, to the customers in $\Phi_{i,k}$. When a new customer joins the bus i or an existing customer leaves it or changes her privacy level, A_i will inform relevant customers in $\mathcal{N}_i$ of the change, to ensure that each customer knows the current size of the privacy group that she belongs to.

2) Noising demand reports: At the tth DR-EDC cycle, for the kth privacy group at the bus i, we define the function $\mathcal{F}$ in Lemma 1 as $\mathcal{F}_{i,k}(p^l_{i,j}[t']|j \in \Phi_{i,k}, t' \in [1,t]) = [\sum_{j\in\Phi_{i,k}} p^l_{i,j}[1], \ldots, \sum_{j\in\Phi_{i,k}} p^l_{i,j}[t]]^\intercal \in \mathbb{R}^t$. At the beginning of the tth DR-EDC cycle, each customer j in $\Phi_{i,k}$ draws two i.i.d. samples, $\gamma_{j,1}[t]$ and $\gamma_{j,2}[t]$, from the Gamma distribution $\mathrm{Gamma}(\|\Phi_{i,k}\|, S(\mathcal{F}_{i,k})/\epsilon_k)$. Recall that the customer obtains the parameter $\|\Phi_{i,k}\|$ of the Gamma distribution during the formation or maintenance of the privacy groups. By extending the approach in [8] to address privacy groups, $S(\mathcal{F}_{i,k})$ can be set to an upper bound of the per-customer demand among all the customers in $\Phi_{i,k}$.[1] Then, the customer generates a noisy version of the demand report, i.e., $p^l_{i,j}[t] + \gamma_{j,1}[t] - \gamma_{j,2}[t]$. Through an aggregation protocol based on homomorphic encryption, A_i obtains an aggregated demand for the kth privacy group denoted by $P_{i,k}[t]$:

$$P_{i,k}[t] = \sum\nolimits_{j\in\Phi_{i,k}} p^l_{i,j}[t] + \sum\nolimits_{j\in\Phi_{i,k}} \gamma_{j,1}[t] - \gamma_{j,2}[t]. \quad (5)$$

From Lemma 1 and the infinite divisibility property of the Laplace distribution (see Section III-A), the scheme above gives ϵ_k-DP for the kth privacy group at each bus.

3) DP in demand reporting: As we discussed in Section I, NILM techniques can infer the appliances' energy usage profiles based on the aggregated smart meter readings. Thus, to prevent the adversary from distinguishing two smart meter readings, we apply the DP on the smart meter demand reporting values. Suppose the aggregated set of demand reporting $\mathcal{P}_{i,j}[t] = \{p^l_{i,j}[t']|j \in \Phi_{i,k}, t' \in [1,t]\}$ is the target dataset, the reported demand is the query $\mathcal{F}(\cdot)$, and the noise added is $n_{i,j}[t] = \gamma_{j,1}[t] - \gamma_{j,2}[t]$, we can formulate the DP in demand reporting as:

Definition 2 (DP in demand reporting)**.** *$\forall i \in \mathcal{L}$, given the dataset $\mathcal{P}_{i,j}[t]$ and the query function $\mathcal{F}(\cdot)$, we have a randomized algorithm $\mathcal{A}$ which adds noise $n_{i,j}[t]$ to the query result to hide $p^l_{i,j}[t]$ from the adversaries so that $\epsilon-$differential privacy is guaranteed.*

[1]To guarantee ϵ-DP, the historical peak load of the bus can be used as a conservative and loose upper bound. The privacy cost analysis in this paper does not rely on accurate setting of this upper bound. We refer the reader to [10] for managing large noises resulting from conservative settings.

By building the DR-EDC with DP protection as defined in Definition 2, the demand reporting privacy can be achieved by $\epsilon-$DP. In the following, we will analyze the additional generation cost due to the DP protection.

V. Total Cost of Differential Privacy

In this section, we first define the total cost of DP in the DR-EDC. Then, we derive its analytic expression and show that it is always non-negative.

A. Definition of Total Privacy Cost

At the beginning of an EDC cycle, if given the true demand vector $\mathbf{p}^l$, the optimal economic dispatch (denoted by $\mathring{\mathbf{p}}^g$) is given by Eq. (4), i.e., $\mathring{\mathbf{p}}^g = \mathrm{EDC}(\mathbf{p}^l)$. However, under the demand reporting scheme in Section IV to ensure DP, the ISO obtains a noisy demand vector $\widehat{\mathbf{p}}^l = \mathbf{p}^l + \mathbf{n}$, where the ith element of $\mathbf{n}$ (denoted by n_i) that corresponds to the load bus i is given by $n_i = \sum_{k=1}^{K} \sum_{j\in\Phi_{i,k}} \gamma_{j,1} - \gamma_{j,2}$. Based on the inaccurate demand vector $\widehat{\mathbf{p}}^l$, the EDC solution $\widehat{\mathbf{p}}^g_0 = \mathrm{EDC}(\widehat{\mathbf{p}}^l)$ will be a generation dispatch that generally cannot balance the total generation and the total demand. As discussed in Section III-B, the EDC solution is used to update the setpoints of the LFC. Starting from the initial setting $\widehat{\mathbf{p}}^g_0$, the LFC will adjust the power outputs of the generators, via a closed-loop control based on real-time measurements of $\mathbf{p}^l$, to exactly meet the demand and regulate the system frequency at the required nominal value. Thus, under the LFC, the actual generator outputs will converge to a new state, which we denote as $\widehat{\mathbf{p}}^g$. We note that the control cycle of the LFC is often two to four seconds and the convergence from $\widehat{\mathbf{p}}^g_0$ to $\widehat{\mathbf{p}}^g$ often takes a few LFC cycles. Denote by $\mathring{p}^g_i$ and $\widehat{p}^g_i$ the ith element of $\mathring{\mathbf{p}}^g$ and $\widehat{\mathbf{p}}^g$, respectively. For the tth DR-EDC cycle, the total privacy cost, denoted by $c[t]$, is defined as

$$c[t] = \sum\nolimits_{i\in\mathcal{G}} C_i(\widehat{p}^g_i[t]) - C_i(\mathring{p}^g_i[t]). \quad (6)$$

Thus, the accumulated total privacy cost up to the tth DR-EDC cycle is given by $\sum_{t'=1}^{t} c[t']$.

We now use Fig. 1 to illustrate the total privacy cost for a certain DR-EDC cycle. The two subfigures of Fig. 1 show the trajectories of the total generation cost during the DR-EDC cycle. To simplify the illustration, each customer adds a positive noise in the demand reporting in Fig. 1(a) and a negative noise in Fig. 1(b), respectively. In both the subfigures, the horizontal straight dotted lines represent $\sum_{i\in\mathcal{G}} C_i(\mathring{p}^g_i)$, i.e., the minimized total generation cost when the ISO is given the true demand vector $\mathbf{p}^l$. In Fig. 1(a), as the customers report demand values that are larger than their actual loads during the DR-EDC cycle, by following the generation dispatch $\widehat{\mathbf{p}}^g_0$, the generators will generate more power than actually demanded. As a result, the total generation cost will be high (as illustrated by the starting point of the blue curve) and over-frequency will be observed. After a transient LFC process, at the end of the DR-EDC cycle, the system frequency is restored back to the nominal value and the generators' outputs converge to $\widehat{\mathbf{p}}^g$. The associated total generation cost is $\sum_{i\in\mathcal{G}} C_i(\widehat{p}^g_i)$, as illustrated by the end point of the blue curve. The height of the vertical

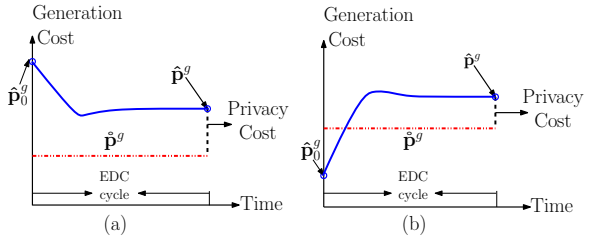


Fig. 1. Illustration of the total privacy cost in DR-EDC. Each customer adds a positive noise in (a) and a negative noise in (b), respectively.

dashed line represents the total privacy cost. In Fig. 1(b), as the customers report demand values that are smaller than their actual loads, the generators will generate less power than actually demanded, resulting in low total generation cost and under-frequency. After a transient LFC process, the total generation cost will be higher than $\sum_{i\in\mathcal{G}} C_i(\mathring{p}_i^g)$.

B. Analytic Expression of Total Privacy Cost

An analytic expression of the total privacy cost is a prerequisite for fairly attributing shares of this cost to the customers. The ISO can compute $\mathring{p}_i^g$ in Eq. (6) right after it measured the actual bus loads $\mathbf{p}^l$. We note that the total power draw at each load bus is often directly measured in real time (e.g., every second) by power flow meters. However, the ISO has to wait until the convergence of the LFC to measure the $\widehat{p}_i^g$ in Eq. (6). In this section, through analysis based on a dynamic model of LFC that is widely adopted in power engineering, we obtain analytic expressions of $\widehat{p}_i^g$ and the total privacy cost defined in Eq. (6). The analytic expressions will be needed to compute the privacy cost shares of buses using the Shapley value approach in Section VI-B. Moreover, the ISO can use them to compute the total privacy cost once the $\mathbf{p}^l$ is measured. This improves the timeliness of the ISO's knowledge of the privacy cost.

Denote by $\widehat{p}_{0,i}^g$ the ith element of the DR-EDC solution $\widehat{\mathbf{p}}_0^g$ that corresponds to a generator bus i, and n_i the ith element of $\mathbf{n}$ that corresponds to a load bus i (i.e., the total noise in the aggregated demand report for load bus i). We note that $\mathbf{n}$ and n_i can be measured by the ISO once $\mathbf{p}^l$ is measured, since $\mathbf{n} = \widehat{\mathbf{p}}^l - \mathbf{p}^l$. We have the following lemma. The proof can be found in the appendix.

Lemma 2. *For a certain DR-EDC cycle,*

$$c = \sum_{i\in\mathcal{G}} C_i\left(\widehat{p}_{0,i}^g + \frac{G_i}{\sum_{i\in\mathcal{G}} G_i}\cdot\sum_{i\in\mathcal{L}} n_i\right) - C_i(\mathring{p}_i^g), \quad (7)$$

where G_i is the LFC gain for the generator at the bus i.

Note that the LFC gain G_i is a constraint known to the ISO. We refer to the proof in the appendix for details of this constant gain. Note that Eq. (7) is not a closed-form formula for c, because both $\widehat{p}_{0,i}^g$ and $\mathring{p}_i^g$ are obtained through solving the constrained optimization problem in Eq. (4). The following lemma gives an important property of the total privacy cost c.

Lemma 3. *For any DR-EDC cycle, $c \geq 0$.*

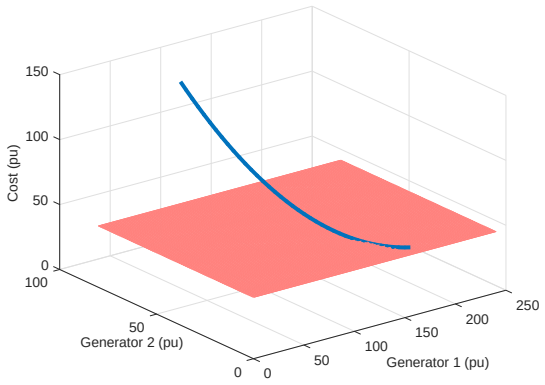


Fig. 2. All possible values of $\sum_{i\in\mathcal{G}} C_i(\widehat{p}_i^g[t])$ after LFC converges (represented by the blue curve) and the minimized generation cost $\sum_{i\in\mathcal{G}} C_i(\mathring{p}_i^g[t])$ (represented by the red flat plane) for the IEEE 14-bus test system.

Proof. After the LFC converges, the generators' outputs $\widehat{\mathbf{p}}^g$ must satisfy the steady-state constraints in Eqs. (1), (2), and (3) with $\mathbf{p}^g$ replaced by $\widehat{\mathbf{p}}^g$ and p_i^g replaced by $\widehat{p}_i^g$. Since $\mathring{\mathbf{p}}^g$ is the optimal solution that minimizes the total generation cost subject to the same steady-state constraints that $\widehat{\mathbf{p}}^g$ satisfies, we must have $\sum_{i\in\mathcal{G}} C_i(\widehat{p}_i^g[t]) \geq \sum_{i\in\mathcal{G}} C_i(\mathring{p}_i^g[t])$ and $c \geq 0$. □

We now use a numeric example to illustrate the above non-negative property. The example is based on an IEEE 14-bus test system [22] that has two generators at bus 1 and bus 2, respectively. (There are three synchronous condensers that output reactive power only.) The following results are for a certain DR-EDC cycle, where the loads are fixed to their initial values specified in the system model. In Fig. 2, the blue curve illustrates all the possible values of $\sum_{i\in\mathcal{G}} C_i(\widehat{p}_i^g[t])$ when the $\widehat{\mathbf{p}}^g$ satisfies the steady-state constraints in Eqs. (1), (2), and (3). To help illustration, we use a flat plane in Fig. 2 to represent $\sum_{i\in\mathcal{G}} C_i(\mathring{p}_i^g[t])$. We can see that $\sum_{i\in\mathcal{G}} C_i(\widehat{p}_i^g[t])$ is lower-bounded by $\sum_{i\in\mathcal{G}} C_i(\mathring{p}_i^g[t])$.

VI. Differential Privacy Cost Sharing

A. Hierarchical Cost Sharing Scheme

Given the total cost of DP, a fundamental question is how to fairly attribute fair shares of the cost among customers requesting different privacy levels. We need to address the challenge in designing the DP cost sharing approaches. The ISO has different levels of information regarding the buses and the customers, respectively. Specifically, as discussed in Section V-B, the aggregated noise in the demand report of each bus, i.e., n_i, can be measured, but the customer-level noises are not available to the ISO to protect the customers' DP. Thus, the cost sharing design at the bus level and that at the customer level should be different.

To address the challenge, we propose a hierarchical cost sharing scheme. We apply the principle of Shapley value [23] for attributing privacy costs with several desirable properties among the buses. However, the computation of Shapley value has poor scalability to a large number of buses. Thus, we additionally propose two heuristic but efficient cost sharing approaches and compare their performance with that of the

Shapley value approach. After obtaining the per-bus privacy cost, we further share it between the customers attached to the same bus using heuristic methods that obey the limited per-customer information. The rest of this section presents the details of the bus- and customer-level privacy cost sharing.

B. Bus-Level Privacy Cost Sharing

We now discuss the Shapley value-based privacy cost sharing scheme at the bus level. Before presenting the details, we first introduce the basics of Shapley value.

1) Shapley value: The Shapley value is a solution concept for fairly distributing a total value generated by a coalition of players in cooperative games [23]. It is defined as follows.

Definition 3 ([23], [24])**.** *Consider a set $\mathcal{N}$ of N players. For each subset (coalition) $\mathcal{S} \subseteq \mathcal{N}$, denote $v(\mathcal{S})$ be the cost of coalition $\mathcal{S}$, i.e., if $\mathcal{S}$ is a coalition of players which agree to cooperate, then $v(\mathcal{S})$ determines the total cost from this cooperation. For a given cost function v, the Shapley value of player i is*

$$\phi_i(v) = \frac{1}{N!} \sum_{\pi \in \mathcal{S}_\mathcal{N}} \left(v(\mathcal{S}(\pi, i)) - v(\mathcal{S}(\pi, i) \backslash i) \right), \qquad (8)$$

where π is a permutation in set $\mathcal{N}$ and $\mathcal{S}(\pi, i)$ is the set of players precede i in the order.

The Shapley value has the following properties [23]:

Property 1. *Shapley value's properties:*

1) *Efficiency:* $\sum_{i \in N} \phi_i(v) = v(N)$*;*
2) *Symmetry: If players i and j are symmetric with respect to game v, $\phi_i(v) = \phi_j(v)$;*
3) *Dummy player: $i \in N$ is a "dummy player" if $v(S \cup \{i\}) = v(S)$ for all coalitions S that do not contain i.*
4) *Linearity/Additivity: For any two games v and w, $\phi(v + w) = \phi(v) + \phi(w)$.*

The Shapley value characterizes a player's marginal contribution to all possible coalitions. The solution concept can be similarly applied for attributing cost, which is a dual concept of value. To facilitate presentation, in this paper, we use the term "Shapley cost" to refer to the cost share of a "player" (i.e., a bus in the current context) as determined by the Shapley value principle. Specifically, the Shapley cost of a bus is the marginal increase in generation cost due to the bus in the coalition. In the following, we introduce the details of the Shapley cost-based approach for bus-level cost sharing.

2) Shapley cost-based approach: We now describe how to compute the Shapley costs of buses. For bus i, if it is in the coalition, it reports its *noisy* aggregated demand (i.e., $p_i^l + n_i$) to the aggregator; otherwise, it reports its *actual* aggregated demand (i.e., p_i^l). Denote by $\mathcal{S}$ the coalition of buses. From Lemma 2, the total privacy cost given a coalition of buses $\mathcal{S}$ is $c(\mathcal{S}) = \sum_{i \in \mathcal{G}} C_i \left(\widehat{p}^g_{0,i}(\mathcal{S}) + \frac{G_i}{\sum_{i \in \mathcal{G}} G_i} \cdot \sum_{i \in \mathcal{S}} n_i \right) - C_i(\mathring{p}^g_i)$, where $\widehat{p}^g_{0,i}(\mathcal{S})$ is the initial power output of the generator at bus i as solved by the EDC based on noisy demand reports from the buses in $\mathcal{S}$ and actual demand values from the remaining buses. By the Shapley's principle, the Shapley cost of a load bus i, denoted by c_i^s, is

$$c_i^s = \frac{1}{\|\mathcal{L}\|!} \sum_{\pi \in \text{perm}(\mathcal{L})} c(\mathcal{S}(\pi, i)) - c(\mathcal{S}(\pi, i) \backslash i), \qquad (9)$$

where π is a permutation of the load buses in $\mathcal{L}$, $\mathcal{S}(\pi, i)$ is a subset of π that includes the buses in π no later than i in order. From the efficiency property of Shapley value, the total privacy cost is shared among all the load buses, i.e., $c = \sum_{i \in \mathcal{L}} c_i^s$. We note that the Shapley cost of a load bus can be negative (see the numeric results in Section VIII-C). For example, when the demand report of the bus has negative noise and all the other buses use positive noise, the negative noise may offset in part the positive noise and hence reduce the total generation cost. In this case, the bus in point should be rewarded with a negative Shapley cost. For the load bus i, the accumulated Shapley cost up to the tth DR-EDC cycle is $\sum_{t'=1}^{t} c_i^s[t']$.

3) Properties of the Shapley cost: From Eq. (9), the privacy cost at each bus is affected by the noise at the bus. Our following analysis shows the monotonicity properties of the Shapley cost, i.e., for a given demand profile of the system, the change of the noise at a bus affects not only the privacy cost of the bus itself, but also those of other buses in the system.

Property 2. *The Shapley cost $c_i^s(n_i)$ at bus i increases with n_i, where $i \in \mathcal{L}$.*

Proof. From Eq. (9), the Shapley cost can be expressed as:

$$\begin{aligned} c_i^s(n_i) &= \frac{1}{\|\mathcal{L}\|!} \sum_{\pi \in \text{perm}(\mathcal{L})} c(\mathcal{S}(\pi, i)) - c(\mathcal{S}(\pi, i) \backslash i), \\ &= \frac{1}{\|\mathcal{L}\|!} \sum_{\pi \in \text{perm}(\mathcal{L})} c(n_\pi, n_i) - c(n_\pi), \qquad (10) \end{aligned}$$

As the generation cost increases with the power output, it also increases with n_i. Thus, from Eq. (9), $c(n_\pi, n_i)$ also increases with n_i. Hence, the Shapley value $c_i^s(n_i)$ at bus i increases with n_i. □

Moreover, we have the following inter-bus monotone property.

Property 3. *The Shapley cost c_i at bus i increases with n_j, where $i, j \in \mathcal{L}$ and $j \neq i$.*

Proof. Assume i and j are two different load buses in $\mathcal{L}$. We rewrite Eq. (9) as:

$$\begin{aligned} c_i^s &= \frac{1}{\|\mathcal{L}\|!} \Big(\sum_{\pi_1 \in \text{perm}(\mathcal{L}), j \notin \pi_1} c(n_{\pi_1}, n_i) - c(n_{\pi_1}) \\ &\quad + \sum_{\pi_2 \in \text{perm}(\mathcal{L}), j \in \pi_2} c(n_{\pi_2}, n_i) - c(n_{\pi_2}) \Big). \qquad (11) \end{aligned}$$

In Eq. (11), the summation in the bracket contains two parts: the first part calculates the permutation excluding bus j, while the second part includes bus j. If n_j increases, the first part remains the same. For the second part, as the generation cost function is increasing and convex, the gap between $c(n_{\pi_2}, n_i) - c(n_{\pi_2})$ also increases with n_j. Therefore, c_i^s increases with n_j. □

4) Heuristic cost sharing: Despite several desirable properties of the Shapley cost [23], Eq. (9) has exponential complexity in the number of load buses due to the permutation. This renders the Shapley cost infeasible to compute for large power grids. To manage the computational cost, a Monte Carlo method can be applied to approximate Eq. (9) [25]. However, the method does not guarantee exact answers and often it still requires high compute overhead for good results [25]. Therefore, we now present two heuristic cost sharing approaches based on assigning privacy cost as a function of the corresponding prescribed noise. Specifically, in the two approaches we use respectively the magnitude and variance of n_i as weight for proportional sharing of the privacy cost. Formally, the cost shares of load bus i, denoted respectively by c_i^n and c_i^σ for the two approaches, are given by $c_i^n = \frac{|n_i|}{\sum_{i\in\mathcal{L}}|n_i|}\cdot c$ and $c_i^\sigma = \frac{\sigma_i^2}{\sum_{i\in\mathcal{L}}\sigma_i^2}\cdot c$, where σ_i^2 is the variance of n_i. In the definition of c_i^n, the rationale of using the magnitude of n_i as weight is that either a positive or negative n_i should incur a positive privacy cost (see Fig. 1). The σ_i^2 in c_i^σ can be estimated based on historical trace of n_i.

In Section VIII-C, we will evaluate the effectiveness of the above two heuristic approaches by comparing their results with the corresponding Shapley costs. In terms of the computation complexity, the Shapley cost sharing scheme has the complexity of $O(2^{|\mathcal{L}|})$, where $\mathcal{L}$ is the set of load buses. Differently, as the heuristic cost sharing scheme calculates the cost based on the magnitude or the variance of the noise, it has constant computational complexity $O(1)$ in terms of the power system scale.

C. Customer-Level Sharing of Privacy Cost

This section discusses how to further distribute the cost share of bus i, i.e., c_i, to customers attached on the bus. We assume that the customers do not report their actual power consumption due to privacy protection. Thus, the noise introduced by an individual customer j, i.e., $\gamma_{j,1} - \gamma_{j,2}$, cannot be measured. As a result, the Shapley cost described in Section VI-B2 cannot be applied to customer-level cost sharing. Instead, our proposed baseline approach first divides c_i among the privacy groups, and then further divides a group's share to the group's customers. We adopt a heuristic approach similar to those proposed in Section VI-B4 that uses the variances as the weights to distribute c_i to the privacy groups on the bus. The variance of the kth privacy group's Laplacian noise that follows $\mathrm{Lap}(S(\mathcal{F}_{i,k})/\epsilon_k)$ is $2\cdot(S(\mathcal{F}_{i,k})/\epsilon_k)^2$. A privacy group's cost share is further divided equally among all the customers in the group. In the above approach, the customers who do not require DP (i.e., $\epsilon = \infty$) share no privacy cost.

Note that the customer-level cost depends on both the bus cost and the number of customers choosing that privacy level. Since we know that the generation cost is a convex function in terms of the demand and the Shapley cost corresponds to the marginal price as defined in Eq. (9), the per-bus cost introduced by the high-demand bus will be higher than that of the low-demand bus. Moreover, since the number of customers choosing the same privacy levels at different buses can be different, the cost for customers attached to different buses can be different even if they choose the same privacy level.

The power distribution network attached to a bus often adopts a tree topology, in which the customers are the leaf nodes of the tree. Some intermediate nodes of the tree may have power meters installed. Therefore, the noise amounts for demand reports of subtrees rooted at these intermediate nodes can be measured. Our future work will investigate how to apply Shapley costs to these subtrees in order to refine the fairness of the customer-level cost sharing.

D. Implementation Issues

The bus-level privacy cost sharing approaches can be readily integrated with various ex-post real-time pricing schemes that are popular in wholesale markets such as New England ISO, PJM, and Midwest ISO. Ex-post electricity prices are determined based on load measurements of the buses, which are often obtained at the end of each EDC cycle. The load measurements can also be used to compute the privacy cost shares of the buses using the methods in Section VI-B.

Relaying upstream real-time prices to end customers is generally considered a desirable feature of smart grids. It has been implemented by utilities such as ComEd [26] and Ameren [27]. The customer-level privacy cost sharing can be readily integrated with such real-time pricing for end customers.

VII. Network Effects of Cost Sharing & Truthful Pricing

Section VI-C establishes a baseline scheme for pricing the set of privacy groups offered to customers attached to a certain bus. The baseline scheme uses heuristics to approximate the Shapley costs of the different groups (attached to the same bus) at high computational efficiency. This section studies further *network effects* of the per-customer DP cost within a group. As in Section VI-C, we assume that the DP cost of the group is shared equally by all the customers in the same group, which is needed because the privacy impact of individual customers is unavailable due to the privacy protection. Hence, the per-customer cost depends on each privacy's group popularity, i.e., the number of customers (attached to the bus in question) who pick the group.

We now define the notion of *truthful* pricing. Our goal is to show that the baseline pricing scheme in Section VI-C is not truthful, and henceforth design a truthful pricing scheme for privacy groups attached to the same bus.

Definition 4 (Truthful pricing)**.** *A pricing scheme is* truthful *if none of its customers have incentives to deviate unilaterally from the privacy groups that represent their respective true privacy requirements.*

We assume that it is not acceptable to any customers to join a privacy group that is below their true privacy requirements. Moreover, the geographical location of a customer (e.g., a household) determines the bus that the customer is attached to; the customer does not have the freedom to change to another bus. Now, consider a game-theoretic formulation in

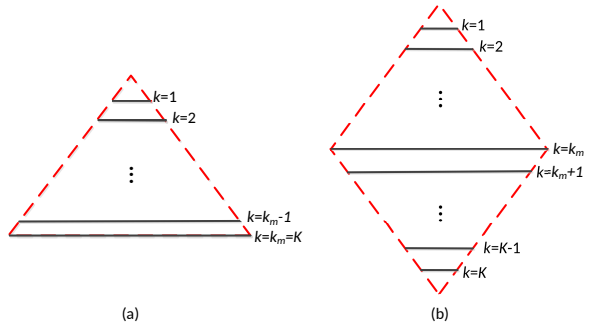


Fig. 3. Different distributions of privacy groups' sizes. Each line represents the size of a privacy group indexed by k, where a higher k represents a less stringent privacy level. k_m indicates the privacy level chosen by the most customers. (a) The number of customers increases with k. (b) Most customers choose an intermediate privacy level, and progressively fewer customers at either increasingly more or less stringent privacy levels from that intermediate level.

which each customer is a player whose strategy is to select the privacy group among the set of choices on offer. The utility function of each player, say i, is the satisfaction of i's (true) privacy requirement, minus the privacy cost. By the assumption that the player will join the EDC reporting only if his privacy requirement is met, the player would derive a utility of minus infinity by joining any group below this requirement. Moreover, to ensure that each player's strategy is non-trivial, we assume that there exists some privacy level at which the player's utility is positive and every player's utility is positive at their true privacy level. Consider the game solution in which every player has chosen its truthful privacy level. Clearly, no players will deviate to a lower privacy level or non-participation. Our task is to ensure also that no customers will be motivated to deviate to a more stringent privacy level, so that the game solution is a Nash equilibrium and the pricing scheme in question is truthful.

To assess the truthfulness of the baseline pricing scheme in Section VI-C, Fig. 3 illustrates two plausible distributions of the sizes of customers' truthful privacy groups. In Fig. 3(a), the group size decreases as the privacy level increases, i.e., towards smaller k values; we have a triangle shaped distribution. In Fig. 3 (b), we have a diamond distribution, in which most customers prefer some "typical" intermediate privacy group. As the privacy level becomes more (or less) stringent relative to this typical group's, progressively fewer customers require the corresponding privacy group.

According to the baseline pricing scheme in Section VI-C, given a certain load bus, the privacy cost of a group of customers attached to the bus depends on (i) the group's privacy level, and hence its required DP noise amount, and (ii) the global sensitivity of the group's customers. The privacy cost of the group is independent of the group size. Moreover, under the assumption that the global sensitivity does not differ by specific groups, this cost is strictly increasing with the privacy level, because of larger DP noises required at the higher levels. This ensures the truthfulness of the baseline pricing under the triangle distribution. More generally, however, a higher cost for the group does not necessarily imply a higher per-customer cost, because the group cost is shared by all the members of the group. Indeed, because the baseline pricing in Section VI-C sets the price of each group *independently* of the others, under the diamond distribution of Fig. 3, it is possible for customers to move up from an "usually relaxed" privacy requirement towards the more mainstream requirements.

A. Incremental Cost-Sharing Pricing

To address the untruthfulness of the baseline per-group pricing within a load bus, in this section we design an improved truthful pricing scheme based on *incremental cost sharing*. Denote by $c_{i,j}^k$ is the privacy cost charged to customer j in privacy group k $(1 \le k \le K)$ attached to bus $i \in \mathcal{L}$. For each demand bus, say i, for all non-zero group costs $c_i^k > c_i^{k'}$, where $k < k'$ and $1 < k \le K-1$, we set the per-customer cost as follows.

$$c_{i,j}^k = c_{i,x}^{k+1} + \frac{k(c_i^k - c_i^{k+1})}{\sum_{\ell=1}^k N_i^\ell},\ \forall k \in [1, K-1], x \in \Phi_i^{k+1}, j \in \Phi_i^k, \tag{12}$$

where N_i^ℓ is the number of customers at bus i with privacy level ℓ. From Eq. (12) note that the per-customer cost in each privacy group is based on the incremental cost this privacy group brings relative to the lower privacy groups.

We use Fig. 4 to explain the idea of Eq. (12). There are three privacy groups for bus i, whose privacy costs satisfy $c_i^1 > c_i^2 > c_i^3$. Note that a smaller group number has a higher privacy level, so that progressively higher noise requirements introduce higher costs. We denote the number of customers in the three groups by N_i^1, N_i^2 and N_i^3, respectively. Now for the group with the lowest privacy cost (i.e., Group 3), as the cost c_i^3 can be considered also part of the costs of the other two groups, all the customers (irrespective of their groups) attached to this bus share this cost. Thus, all the customers need to pay the cost $\hat{c}_i^3 = \frac{3c_i^3}{N_i^1+N_i^2+N_i^3}$.

Next, for the customers in Group 2, beyond the cost c_i^3 already accounted for above, they introduce an additional cost of $c_i^2 - c_i^3$, and this additional cost can likewise be considered part of the cost introduced by the customers in Group 1. Therefore, the customers in both Groups 1 and 2 share this cost of $\hat{c}_i^2 = \frac{2(c_i^2-c_i^3)}{N_i^1+N_i^2}$. Lastly, for the customers in Group 1, they introduce yet another additional cost of $c_i^1 - c_i^2$. Thus, the customers in Group 1 also need to bear this cost, which is calculated as $\hat{c}_i^1 = \frac{c_i^1-c_i^2}{N_i^1}$. In summary, the per-customer costs for the customers in Groups 1, 2, and 3 are $\hat{c}_i^1 + \hat{c}_i^2 + \hat{c}_i^3$, $\hat{c}_i^2 + \hat{c}_i^3$, and $\hat{c}_i^3$, respectively.

Property 4. *The incremental cost-sharing pricing scheme has the following properties:*

1) *Efficiency, i.e.,* $\sum_{k=1}^K \sum_{j=1}^{|\Phi_i^k|} c_{i,j}^k = c_i$, *where* $i \in \mathcal{L}$ *and* c_i *is the bus cost of demand bus* i.
2) *Truthfulness, according to Definition 4.*

Proof. **Efficiency.** Similar to Property 1 for the Shapley cost, we have the efficiency property here, i.e., the sum of all the customers' costs attached to a bus equals the privacy cost of the bus itself. We consider the sum of cost increments according to Eq. (12). For each k, ranging from $K-1$ down until 1, the corresponding cost increment is $\Delta c_i^k = \frac{k(c_i^k - c_i^{k+1})}{\sum_{\ell=1}^k N_i^\ell}$, where

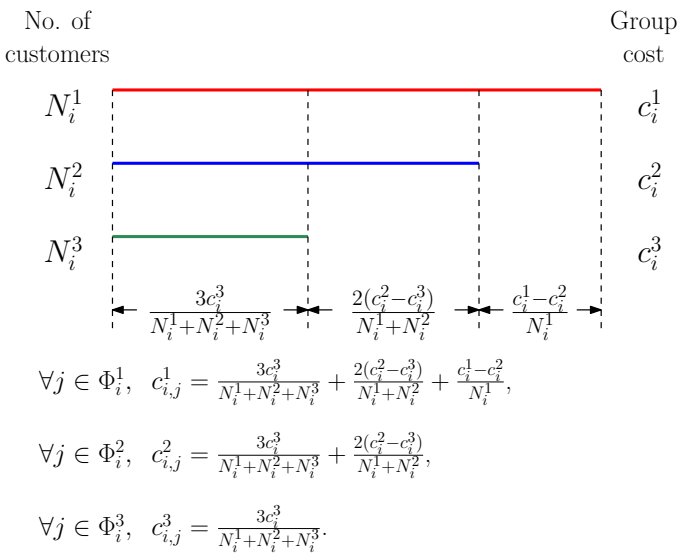


Fig. 4. Illustration of the pricing scheme based on incremental cost sharing.

$x \in \Phi_i^{k+1}, j \in \Phi_i^k$. Each Δc_i^k involves all the customers from Group 1 to Group k, i.e., totally $\sum_{\ell=1}^{k} N_i^\ell$ customers. Therefore, the overall sum is $\Delta C_i^k = \sum_{\ell=1}^{k} \Delta c_i^\ell = k(c_i^k - c_i^{k+1})$, where $1 \le k < K$. Summing up all the incremental costs for Bus i, we have $C_i = \sum_{k=1}^{K-1} \Delta C_i^k = \sum_{k=1}^{K-1} k(c_i^k - c_i^{k+1}) = c_i^1 - c_i^2 + 2c_i^2 - 2c_i^3 + \cdots + (K-2)c_i^{K-2} - (K-2)c_i^{K-1} + (K-1)c_i^{K-1} = c_i^1 + c_i^2 + \cdots + c_i^{K-1} = \sum_{i=1}^{K-1} c_i^k = c_i$.

Truthfulness. In the incremental cost-sharing pricing, for any two customers in two different privacy groups k and k' ($k < k'$) attached to bus i, by Eq. (12), we know that $c_{i,x}^k > c_{i,z}^{k+1} \ge c_{i,y}^{k'}$, where $x \in \Phi_i^k$, $z \in \Phi_i^{k+1}$ and $y \in \Phi_i^{k'}$. Therefore, $c_{i,x}^k > c_{i,y}^{k'}$ and a player's payoff cannot be increased by choosing either a higher or a lower group. This shows that truthful strategies by the players result in Nash equilibrium, and no players are motivated to unilaterally deviate from their strategies. □

Remark 1. *The incremental privacy cost-sharing pricing and Property 4 are derived for positive bus costs. However, as discussed in Section VI-B2, negative Shapley costs are possible. In such cases, our results still hold if we substitute corresponding absolute values of the costs for the negative costs.*

VIII. Simulations

Our numeric illustrations are based on the 5-bus power system model shown in Fig. 5 ([18], Chapter 6, pp.327). In this system, the two generators' cost functions are quadratic functions with different parameters. We simulate a total of 200 customers in the system. For DP, each customer chooses an ϵ value from $\{0.5, 1, 1.5, 2.5, \infty\}$. The EDC cycle is five minutes. Hourly load data traces of U.S. domestic customers in January 2015 [28] are interpolated and used to set the loading of buses in our simulations. Unless otherwise specified, all the power values associated with this 5-bus system are normalized to per unit (pu) values..

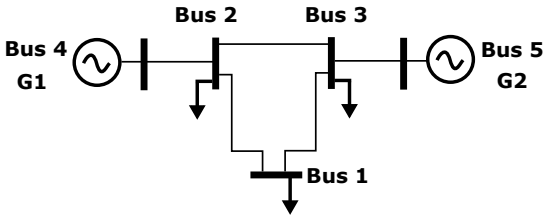


Fig. 5. 5-bus system ([18], Chapter 6, pp.327).

TABLE I
Demand Reporting vs. Demand Forecasting

Scheme	Additional cost (%)
DR-EDC with 5% customers choosing $\epsilon = 0.5$	3.28
DR-EDC with no customers choosing $\epsilon = 0.5$	2.83
EDC based on demand forecasting	5.02

A. Demand Forecasting vs. Demand Reporting

This set of simulations compares the privacy cost of DR-EDC with the additional generation cost caused by inaccuracy of traditional demand forecasting. The demand forecasting is based on the widely adopted persistence model [29], in which the immediate past load is used as the current demand forecast for each bus. To evaluate the DR-EDC, we simulate the system for 100 rounds, where each round corresponds to the load traces on one day. At the beginning of each round, the customers randomly choose their ϵ values. The average aggregated total privacy cost over the 100 rounds is presented.

Table I shows the results for DR-EDC under two settings, as well as traditional EDC based on demand forecast. The additional generation costs due to either DP-induced noise or inaccurate forecast are in percentages of the total generation cost. In the first DR-EDC setting, ten out of 200 (i.e., 5%) customers choose the highest privacy level, i.e., $\epsilon = 0.5$, resulting in a 3.28% privacy cost; in the second setting, no customers choose this highest privacy level, resulting in a 2.83% privacy cost. This result is consistent with intuition that the privacy cost decreases with the customers' required privacy. By comparison, the results based on demand forecast show an additional cost of around 5%, which is higher than the privacy cost of DR-EDC in either setting.

Note that this 5% additional cost is significant and comparable to line loss (e.g., 7% in U.S. [30]). Furthermore, it would increase with higher demand uncertainty. In contrast, as our results show, DR-EDC with DP protection can reduce the additional cost by up to 43%, which is substantial.

B. Total Privacy Cost over a Day

This set of results shows how the total privacy cost changes with load and customers' DP-induced noise over time. At the beginning of the simulation, each customer randomly chooses a privacy level. The distribution of customers choosing the five ϵ values from 0.5 to ∞ is 18.5%, 17%, 21%, 24%, and 19.5%. Fig. 6(a) shows the actual total load (red curve) and aggregate of the demand reports (blue curve) over a day. Fig. 6(b) shows the total generation costs of the EDC without DP (red curve) and the DR-EDC with DP (blue curve). We can see that the

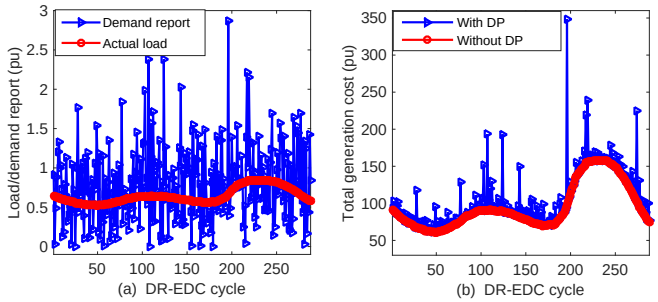


Fig. 6. Load, demand report, and generation cost over a day. (a) Total load and the demand report aggregate. (b) Total generation costs with and without DP protection in EDC.

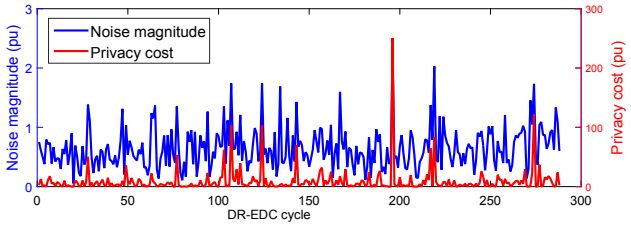


Fig. 7. Total noise magnitude and total privacy cost over a day.

total generation cost of DR-EDC is always higher than that of EDC without DP protection. This result is consistent with Lemma 3.

Fig. 7 shows the magnitude of total noise (i.e., absolute difference between the two curves in Fig. 6(a)) and the total privacy cost (i.e., difference between the two curves in Fig. 6(b)). We can observe that the total privacy cost is not always proportional to the magnitude of the total noise. This is because the total privacy cost is also affected by the distribution of noise among the buses. Intuitively, if a generator with a low generation cost curve $C_i(\cdot)$ is close to a load bus with a high noise for its demand report, the noise will not cause a significant increase in the generation cost.

C. Evaluation of Privacy Cost Sharing Approaches

1) Bus-level cost sharing: We compare the three bus-level cost sharing approaches discussed in Section VI-B, namely the Shapley cost (SC) and the two heuristic approaches using respectively noise magnitude (NM) and noise variance (NV) as weight to split the privacy cost among the buses. Each simulation lasts for 300 DR-EDC cycles. Fig. 8 shows the demand-report noises of the three load buses in four selected DR-EDC cycles, and the corresponding cost shares under the SC and NM approaches. In the first DR-EDC cycle, the buses use similar noises and the total privacy cost is almost equally shared between them. In the second cycle, the buses use different noises and their cost shares are roughly proportional to the noise magnitudes. In these two cycles, the two approaches of SC and NM yield similar results. In the third cycle, bus 2 uses positive noise, while the other two buses use negative noises. As a result, the Shapley cost of bus 2 is negative. This is because bus 2's presence in the coalition helps reduce the total generation cost, as its positive noise

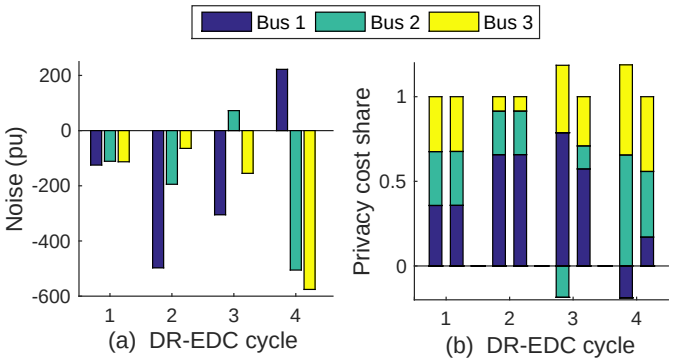


Fig. 8. Total noise amounts of buses in four DR-EDC cycles and the corresponding privacy cost shares under the SC and NM approaches. In each bar group of (b), the first and second bars are respectively the results of SC and NM.

offsets the negative noises of the other buses. Interestingly, therefore, in this particular cycle bus 2's noise helps make the overall demand report more accurate. Under the Shapley's principle, bus 2 should be rewarded. We see a similar result in the fourth cycle, where bus 1 is rewarded because its noise counteracts the noises of the other buses. We note that, under the SC approach, the aggregated cost share of a bus over a long time period is almost surely positive, since it is extremely unlikely for the noise of any bus to help reduce the overall inaccuracy all the time. We next illustrate this observation.

We compare the aggregated privacy cost shares over the 300 DR-EDC cycles computed by the three approaches. Fig. 9 shows the results. Consistent with our previous discussion, the aggregated Shapley cost is positive for every bus. Both the NM and NV approaches yield similar aggregated privacy cost shares as the Shapley costs. Specifically, the maximum per-bus deviations from the Shapley costs are 6.2% and 12.1% respectively for the NM and NV approaches. From Fig. 9, therefore, the NM approach appears to perform better. Note that, to compute the Shapley costs for the 5-bus system, the EDC problem in Eq. (4) needs to be solved 24 times. Moreover, as discussed in Section VI-B4, this number will increase exponentially with the number of load buses, which renders the Shapley cost approach infeasible for large power systems. In comparison, the NM approach has much lower computational time complexity.

2) Customer-level cost sharing: We follow the approach described in Section VI-C to further distribute the per-bus Shapley cost among the customers. Fig. 10 shows, for each bus, the ratio of per-customer aggregated cost in a privacy group to the sum of privacy costs of all the privacy groups. We can see that on a certain bus, the per-customer cost increases with the customer's required privacy, which is consistent with intuition. Note that the customers not requiring any DP protection share no privacy cost.

3) Network effects: We now show how the incremental cost sharing scheme to maintain the cost sharing fairness for customers. We set the number of customers choosing different privacy levels as $\{5, 5, 20, 8, 2\}$ at Bus 1, which is a realistic

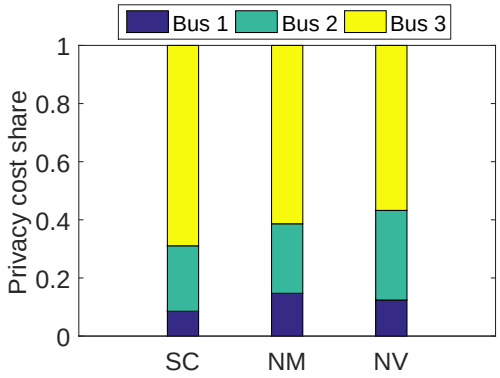


Fig. 9. Bus-level cost shares computed by the different approaches.

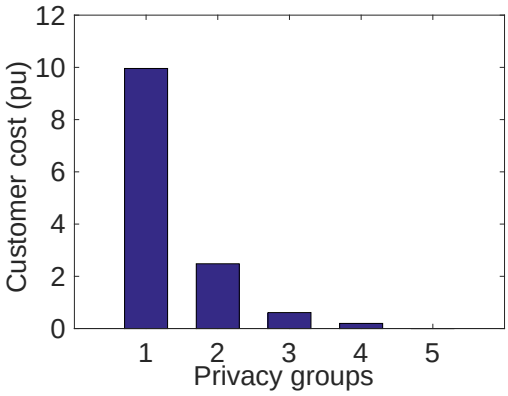


Fig. 11. The customer cost after applying the incremental cost sharing scheme.

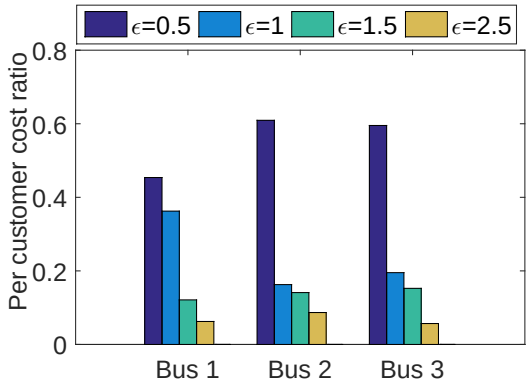


Fig. 10. Ratio of per-customer aggregated cost.

scenario, i.e., the customer's privacy level choices' distribution is similar to normal distribution. Due to the most customers are in group 3, the per-customer cost will be smaller without the incremental cost sharing scheme. However, in Fig. 11 we see that we can avoid the unfair cost sharing, i.e., the customers choosing higher privacy level $\epsilon = 1.5$ have higher privacy cost compared with customers choosing lower privacy level $\epsilon = 2.5$. Thus, the incremental cost sharing scheme ensures higher privacy level customers have higher cost, and thus the unfair cost sharing can be eliminated.

IX. Discussion

A. High-demand customer

The incremental privacy cost sharing scheme is based on the assumption that the higher level privacy group introduces higher privacy cost if the global sensitivity of all customers are similar. However, if there exists very demand customers, e.g., the industrial customer, choosing the same low privacy level as other residential customers, the high group privacy cost will be introduced and thus the low-demand customer in the group will also have to pay more privacy cost. In the following, we will explore this network effect and propose a solution to charge higher cost on the high-demand customers due to the high group cost introduced by them.

By Lemma 1, the noise variance in DP is decided by the global sensitivity once the privacy level is chosen. Thus, the global sensitivity affects the group's privacy cost. In our differentially private demand reporting scheme, the global sensitivity is set as the upper bound of the per-customer demand among all the customers in a privacy group. As a result, the customer with the highest demand (e.g., an industrial customer) will significantly affect the group's total privacy cost and the per-customer privacy costs. We now illustrate the impact of the high-demand customer on the privacy costs using numeric experiments based on the 5-bus system in Fig. 5. In our experiments, there is a high-demand customer who demands three times higher than other customers with equal demands. Fig. 12 shows the groups' total privacy costs when the high-demand customer joins different privacy groups. We can see that when the high-demand customer is in a group, the total privacy cost of the group increases.

From the above results, we can see that the presence of a high-demand customer (i.e., the demand upper bound is at least twice as that of other users) in a privacy group will significantly increase the group's total privacy cost. As the total privacy cost is equally shared among the customers in each privacy group, the high-demand can cause undesirable effects such as unfairness to other low-demand customers, e.g., residential customers, in the group. Specifically, these low-demand customers will pay higher privacy cost due to the presence of the high-demand customer in the same group.

A possible approach to preventing this undesirable network effect is to share the cost using the customers' demands as the weights. However, this approach fundamentally conflicts with the original goal of preserving customers' privacy by not revealing their demands. We now present an approach to alleviating the undesirable network effect. Specifically, we propose to divide the high-demand customer's demand upper bound into b equal sub-blocks, where the integer $b > 1$. We now use the sub-block from demand division as the weights to assign the cost in the group with high-demand customers.

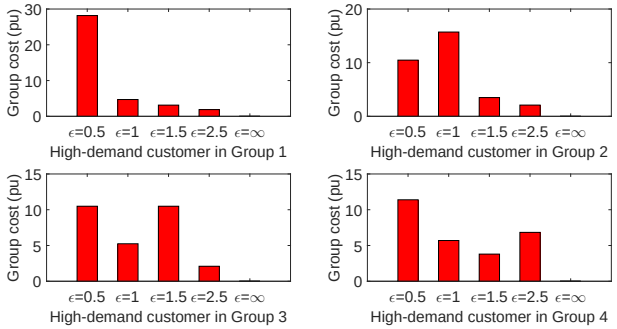


Fig. 12. The groups' privacy costs when the high-demand customer is in different groups.

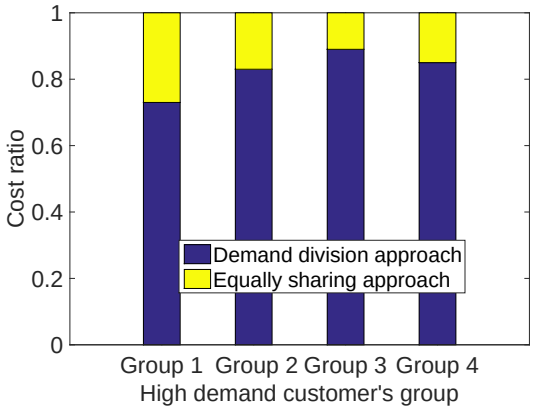


Fig. 13. The high-demand customer cost ratio between applying demand division approach and equally cost sharing approach.

Suppose there are N_i^k customers in group k at bus i. Let $d_{i,x}^k$ denote the demand upper bound of the high-demand customer x in group k at bus i, which is also the upper bound of the demands in the group. Let $d_{i,y}^k$ denote the upper bound of any other customer y's demand in group k at bus i, where $y \in \Phi_i^k$ and $y \neq x$. We define the demand sub-block after demand division is $\hat{d}_{i,x}^k = d_{i,x}^k/b < d_{i,x}^k$. If a customer in group k is a high-demand customer, i.e., $\hat{d}_{i,x}^k > d_{i,y}^k, \exists y \in \Phi_i^k$, and $y \neq x$, the additional demand is introduced to this group. We define $\hat{\Phi}_i^k$ the set of high demand customers in group k at bus i. Then the maximum demand sub-block is $\hat{d}_i^k = \max\{\hat{d}_{i,x}^k\}, x \in \hat{\Phi}_i^k$. Therefore, when sharing the cost in this group, we use the demand sub-block as the weight to decide the cost, i.e., for any low-demand customer $y \in \Phi_i^k$ but $y \notin \hat{\Phi}_i^k$, the cost is $c_{i,y}^k = c_i^k/||\Phi_i^k|| \cdot (1/\hat{d}_i^k)$ and for the high-demand customer $x \in \hat{\Phi}_i^k$, it should pay higher cost as $c_{i,x}^k = c_{i,y}^k + c_i^k \cdot (1 - 1/\hat{d}_i^k) \cdot \frac{\hat{d}_{i,x}^k}{\sum_{j \in \hat{\Phi}_i^k} \hat{d}_{i,j}^k}$. Then, the total cost for group k at bus i is still c_i^k, but instead of being charged as the same cost as other low-demand customers, the high-demand customer has to pay the additional cost introduced by its demand sub-blocks, which is the punishment for imposing high noises to this group.

Moreover, the incremental cost sharing scheme in Section VII-A can also be applied to all low-demand customers. To facilitate it, when deciding the cost for the high-demand customer, we should ensure the privacy cost of all other low-demand customers is between neighboring higher and lower privacy groups by reducing or adding $\alpha > 0$ amount of cost at the high-demand customer. Then the incremental cost sharing can be applied to all the low-demand customers in this group and customers in other groups.

We now evaluate the effectiveness of this approach. We use the cost ratio of high-demand customer between applying demand division approach and equally cost sharing approach as the metric. Similar to the simulation before, a high-demand customer that demands three times of power than other customers joins one of the four privacy groups in each simulation run. If the demand division approach is applied, the high-demand customer needs to pay additional cost. Fig. 13 shows the high-demand customer's cost ratio when the high-demand customer joins this group. The high-demand customer has to pay much higher cost due to more noises introduced by them compared with equally sharing the cost with other group members before.

X. Conclusion and Future Work

We analyzed the cost of differential privacy as increase of a grid's total generation cost when its EDC is given noisy demand reports, rather than the customers' true demand data, for the sake of the privacy protection. We then applied the principle of Shapley value to distribute this total privacy cost among different buses in the power system. We also studied the properties of the Shapley cost sharing scheme. To address large systems, we additionally proposed heuristic cost sharing algorithms that scale well to large grids, and compared their solutions to the corresponding Shapley value solutions. Moreover, we investigated interesting network effects of the per-customer cost sharing, and designed a truthful incremental cost-sharing scheme for pricing the privacy groups associated with a load bus. We also discussed the impact of the high-demand customer on other customers' cost. Simulations based on a 5-bus power system model illustrated the privacy cost, its Shapley cost shares, and corresponding cost shares according to the heuristic algorithms.

To improve the accuracy of the DP cost analysis, it is interesting for future work to extend our analysis and simulations to address line loss and/or AC power flow models. It is also interesting to design incentive programs with effective mechanisms to motivate customers to participate in the demand reporting. For instance, an interesting question is how to design the set of offered ϵ values such that all the customers are sure to pay less irrespective of their choice of the ϵ value, compared with the choice of not reporting their demand at all.

XI. Acknowledgment

This research was supported in part by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme, in part by the Energy Innovation Research Programme (EIRP, Award Nos. NRF2014EWTEIRP002-026), administered by the Energy Market Authority (EMA), in part by SUTD-ZJU IDEA programme, award number SUTD-ZJU (VP) 201805, in part

by Singapore Ministry of Education Tier 1 grant number SUTDT12017004, and in part by an NTU Start-up Grant.

REFERENCES

[1] "Illinois public act 094-0977," 2006, http://bit.ly/2asU2Fi.

[2] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley & Sons, 2012.

[3] N. Li, C. Zhao, and L. Chen, "Connecting automatic generation control and economic dispatch from an optimization view," *IEEE Trans. on Control of Network Systems*, vol. 3, no. 3, pp. 254–264, 2016.

[4] C.-L. Su and D. Kirschen, "Quantifying the effect of demand response on electricity markets," *IEEE Trans. Power Syst.*, vol. 24, no. 3, 2009.

[5] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *IEEE International Conference on Computer Communications (INFOCOM)*, 2014.

[6] C. Dwork, "Differential privacy," in *International Colloquium on Automata, Languages, and Programming (ICALP)*, 2006.

[7] E. Shi, R. Chow, T.-H. H. Chan, D. Song, and E. Rieffel, "Privacy-preserving aggregation of time-series data," in *Network and Distributed System Security Symposium (NDSS)*, 2011.

[8] G. Ács and C. Castelluccia, "I have a dream! (differentially private smart metering)," *Information Hiding*, vol. 6958, pp. 118–132, 2011.

[9] J. Won, C. Ma, D. Yau, and N. Rao, "Proactive fault-tolerant aggregation protocol for privacy-assured smart metering," in *IEEE International Conference on Computer Communications (INFOCOM)*, 2014.

[10] V. Gulisano, V. Tudor, M. Almgren, and M. Papatriantafilou, "Bes-differentially private and distributed event aggregation in advanced metering infrastructures," in *ACM Cyber-Physical System Security Workshop (CPSS)*, 2016.

[11] X. Lou, R. Tan, D. Yau, and P. Cheng, "Cost of differential privacy in demand reporting for smart grid economic dispatch," in *IEEE International Conference on Computer Communications (INFOCOM)*, 2017.

[12] C. Zhao, E. Mallada, and F. Dorfler, "Distributed frequency control for stability and economic dispatch in power networks," in *American Control Conference (ACC)*, 2015.

[13] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography Conference (TCC)*, 2006.

[14] S. Kotz, T. J. Kozubowski, and K. Podgorski, *The Laplace Distribution and Generalizations*. Birkhäuser, 2001.

[15] P. Kundur, *Power System Stability and Control*. McGraw-Hill, 1994.

[16] D. Cai, E. Mallada, and A. Wierman, "Distributed optimization decomposition for joint economic dispatch and frequency regulation," in *IEEE Conference on Decision and Control (CDC)*, 2015.

[17] X. Zhang, N. Li, and A. Papachristodoulou, "Achieving real-time economic dispatch in power networks via a saddle point design approach," in *IEEE Power & Energy Society General Meeting*, 2015.

[18] J. D. Glover, M. S. Sarma, and T. J. Overbye, *Power System Analysis and Design*, 5th ed. Cengage Learning, 2011.

[19] U.S. DoE, "The value of economic dispatch – a report to congress pursuant to section 1234 of the energy policy act of 2005," 2005, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/value.pdf.

[20] R. R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure," *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 473–484, 2014.

[21] F. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," *Workshop on Security and Trust Manag.*, 2010.

[22] "IEEE 14-bus system," http://icseg.iti.illinois.edu/ieee-14-bus-system/.

[23] L. S. Shapley, "A value for n-person games," *Annals of Mathematical Studies*, vol. 28, 1953.

[24] R. Stanojevic, N. Laoutaris, and P. Rodriguez, "On economic heavy hitters: Shapley value analysis of 95th-percentile pricing," in *ACM Internet Measurement Conference (IMC)*, 2010.

[25] S. S. Fatima, M. Wooldridge, and N. R. Jennings, "A linear approximation method for the shapley value," *Artificial Intellilgence*, vol. 172, no. 14, pp. 1673–1699, 2008.

[26] "Comed's hourly pricing program," https://hourlypricing.comed.com/.

[27] "Ameren, real-time pricing for residential customers," https://bit.ly/2EdquKb.

[28] "Static load profiles," 2015, http://on.sce.com/2aAHY3b.

[29] M. Roozbehani, M. Dahleh, and S. Mitter, "Volatility of power grids under real-time pricing," *IEEE Trans. Power Syst.*, vol. 27, no. 4, 2012.

[30] "Line loss," 2018, http://www.eia.gov/tools/faqs/faq.cfm?id=105&t=3.

APPENDIX: PROOF OF LEMMA 2

Proof. Denote by $\mathcal{E}$ the set of transmission lines and (i,j) the line connecting the bus i and bus j. Let Δx represent the derivation of x from its past steady-state value. Generators' primary control is described by [17]:

$$2H_i\Delta\dot{\omega}_i+D_i\Delta\omega_i=\Delta P_{M_i}-\sum\nolimits_{(i,j)\in\mathcal{E}} B_{ij}\Delta\theta_{ij},\ i\in\mathcal{G}, \quad (13)$$

$$D_i\Delta\omega_i = -\Delta P_{d_i} - \sum\nolimits_{(i,j)\in\mathcal{E}} B_{ij}\Delta\theta_{ij},\ i\in\mathcal{L}, \quad (14)$$

$$\Delta\dot{\theta}_{ij} = \Delta\omega_i - \Delta\omega_j,\ (i,j)\in\mathcal{E}, \quad (15)$$

$$\Delta\dot{P}_{M_i} = K_iR_i(L_i - \Delta P_{M_i} - R_i^{-1}\Delta\omega_i), \quad (16)$$

where ω_i is the grid frequency, H_i is the generator inertia, D_i is the load damping constant, P_{M_i} is the mechanical power input, P_{d_i} is the load, B_{ij} is the susceptance of (i,j), θ_{ij} is the difference of voltage phases difference between bus i and bus j, L_i is the reference signal from the LFC, K_i is the primary control gain, and R_i is the droop [15]. The LFC control law in the Laplace domain is $\widetilde{\Delta L_i} = -\frac{G_i}{s}\widetilde{\Delta\omega_i}$ [15], where s is the Laplace operator and G_i is the LFC gain. To simplify the analysis, we ignore the differences between ω_i's and consider a globally identical grid frequency ω. This simplification is safe as the differences are often tiny. It is often adopted in power system analysis [15]. By replacing ω_i and ω_j in Eqs. (13)-(16) with ω, summing Eq. (13) and Eq. (14), and applying the Laplace transform, we have

$$\widetilde{\Delta\omega} = \frac{1}{2Hs+D}\cdot(\widetilde{\Delta P_M} - \widetilde{\Delta P_d}), \quad (17)$$

where $H=\sum_{i\in\mathcal{G}} H_i$, $D=\sum_{i\in\mathcal{G}\cup\mathcal{L}} D_i$, $P_M=\sum_{i\in\mathcal{G}} P_{M_i}$, and $P_d=\sum_{i\in\mathcal{L}} P_{d_i}$. The Laplace transform of Eq. (16) is

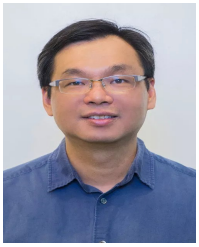
$$\widetilde{\Delta P_{M_i}} = -\frac{K_i}{s+K_iR_i}\cdot\widetilde{\Delta\omega} + \frac{K_iR_i}{s+K_iR_i}\cdot\widetilde{\Delta L_i}. \quad (18)$$

The $\widetilde{\Delta P_{M_i}}$ can be solved from Eqs. (17), (18), and the LFC control law $\widetilde{\Delta L_i} = -\frac{G_i}{s}\widetilde{\Delta\omega}$:

$$\widetilde{\Delta P_{M_i}} = \frac{\frac{K_i}{s+K_iR_i}\left(1+\frac{R_iG_i}{s}\right)}{2Hs+D+\sum\limits_{i\in\mathcal{G}}\frac{K_i}{s+K_iR_i}\left(1+\frac{R_iG_i}{s}\right)}\cdot\widetilde{\Delta P_d}. \quad (19)$$

At the beginning of an DR-EDC cycle, the generators' settings are updated such that they output $\widehat{\mathbf{p}}_0^g$ that is scheduled based on the noisy demand $\widehat{\mathbf{p}}^l = \mathbf{p}^l + \mathbf{n}$. Then, the LFC controls the generators to meet the actual load $\mathbf{p}^l$. This process is equivalent to that, the LFC controls the generators when there is a step change of load (i.e., $\mathbf{n}$) from $\widehat{\mathbf{p}}^l$ to $\mathbf{p}^l$ at the beginning of the EDC cycle. In the Laplace domain, this step change can be expressed by $\widetilde{\Delta P_d} = \sum_{i\in\mathcal{L}} n_i/s$. By replacing $\widetilde{\Delta P_d}$ in Eq. (19) with $\sum_{i\in\mathcal{L}} n_i/s$ and applying the Final Value Theorem, the steady-state value of ΔP_{Mi} in time domain is given by $\Delta P_{M_i}^{\infty} = \lim_{s\to 0} s\cdot\widetilde{\Delta P_{M_i}} = \frac{G_i}{\sum_{i\in\mathcal{G}} G_i}\cdot\sum_{i\in\mathcal{L}} n_i$. As discussed in Section V-A, LFC converges in a few LFC cycles. In the steady state after the convergence, generators' electricity power outputs equal their mechanical power inputs [15]. Thus, at the end of the EDC cycle, we have $\widehat{p}_i^g = \widehat{p}_{0,i}^g + \Delta P_{Mi}^{\infty}$. By applying this result to Eq. (6), we have Eq. (7). □

Xin Lou in Louin LouX is a Research Scientist at Advanced Digital Sciences Center (ADSC), a research center established by the University of Illinois at Urbana Champaign (UIUC) in Singapore. He is also a research affiliate at the Coordinated Science Laboratory (CSL) at UIUC. He was a postdoctoral Researcher (2016-2018) at ADSC. He received the Ph.D. (2016) degree in computer science from City University of Hong Kong, Hong Kong SAR and B.E. (2009) degree in telecommunication engineering from Sichuan University, China. His research interests include cyber-physical systems, deep learning for sensing and computing, nonlinear optimization and distributed algorithms.



David K.Y. Yau received the B.Sc. from the Chinese University of Hong Kong, and M.S. and Ph.D. from the University of Texas at Austin, all in computer science. He has been Professor at Singapore University of Technology and Design since 2013. Since 2010, he has been Distinguished Scientist at the Advanced Digital Sciences Centre, Singapore. He was Associate Professor of Computer Science at Purdue University (West Lafayette). He received an NSF CAREER award. He won Best Paper award in 2017 ACM/IEEE IPSN and 2010 IEEE MFI. His papers in 2008 IEEE MASS, 2013 IEEE PerCom, 2013 IEEE CPSNA, and 2013 ACM BuildSys were Best Paper finalists. His research interests include cyber-physical system and network security/privacy, wireless sensor networks, smart grid IT, and quality of service. He serves as Associate Editor of IEEE Trans. Network Science and Engineering and ACM Trans. Sensor Networks. He was Associate Editor of IEEE Trans. Smart Grid, Special Section on Smart Grid CyberPhysical Security (2017), IEEE/ACM Trans. Networking (2004-09), and Springer Networking Science (2012-2013); Vice General Chair (2006), TPC co-Chair (2007), and TPC Area Chair (2011) of IEEE ICNP; TPC co-Chair (2006) and Steering Committee member (2007-09) of IEEE IWQoS; TPC Track co-Chair of 2012 IEEE ICDCS; and Organizing Committee member of 2014 IEEE SECON.

Rui Tan (M'08-SM'18) is an Assistant Professor at School of Computer Science and Engineering, Nanyang Technological University, Singapore. Previously, he was a Research Scientist (2012-2015) and a Senior Research Scientist (2015) at Advanced Digital Sciences Center, a Singapore-based research center of University of Illinois at Urbana-Champaign (UIUC), a Principle Research Affiliate (2012-2015) at Coordinated Science Lab of UIUC, and a postdoctoral Research Associate (2010-2012) at Michigan State University. He received the Ph.D. (2010) degree in computer science from City University of Hong Kong, the B.S. (2004) and M.S. (2007) degrees from Shanghai Jiao Tong University. His research interests include cyberphysical systems, sensor networks, and ubiquitous computing systems. He received the Best Paper Awards from IPSN'17, CPSR-SG'17, Best Paper Runner-Ups from IEEE PerCom'13 and IPSN'14.

Peng Cheng (M'10) received the B.Sc. degree in automation and the Ph.D. degree in control science and engineering, from Zhejiang University, Hang Zhou, China, in 2004 and 2009, respectively. From 2012 to 2013, he worked as Research Fellow in Information System Technology and Design Pillar, Singapore University of Technology and Design. He is currently a Professor with the College of Control Science and Engineering, Zhejiang University, Hangzhou, China. His research interests include networked sensing and control, cyber-physical systems, and control system security.