Assessing the Privacy Cost in Centralized Event-Based Demand Response for Microgrids

Areg Karapetyan, Syafiq Kamarul Azman, and Zeyar Aung
Deparment of Electrical Engineering and Computer Science
Masdar Institute of Science and Technology
54224 Abu Dhabi, United Arab Emirates
emails:{akarapetyan, mbinkamarulazman, zaung}@masdar.ac.ae

***Abstract*—Demand response (DR) programs have emerged as a potential key enabling ingredient in the context of smart grid (SG). Nevertheless, the rising concerns over privacy issues raised by customers subscribed to these programs constitute a formidable hurdle towards their effective deployment and utilization. This has driven extensive research to resolve the hindrance confronted, resulting in a number of methods being proposed for preserving customers' privacy. While these methods provide stringent privacy guarantees, only limited attention has been paid to their computational efficiency and performance quality. Under the paradigm of differential privacy, this paper initiates a systematic empirical study on quantifying the trade-off between privacy and optimality in centralized DR systems for maximizing cumulative customer utility. Aiming to elucidate the factors governing this trade-off, the privacy cost is evaluated in terms of changes in objective value of the DR optimization problem when effecting the employed privacy-preserving strategy based on Laplace mechanism. The analytical results presented herein are complemented with empirical findings, corroborated extensively by simulations with up to thousands of customers on a realistic 4-bus microgrid (MG) model embracing the underlying power distribution network properties and AC power flow constraints. By evaluating the privacy impact, this pilot study serves DR practitioners when considering the social and economic implications of deploying privacy-preserving DR programs in practice. Moreover, it stimulates further research to explore more efficient privacy solutions for energy procurement of MGs with bounded constant optimality guarantees.**

***Index Terms*—Demand response, differential privacy, microgrids, privacy-preserving energy management, randomized response, AC power flow equations, inelastic demands.**

I. Introduction

Proliferating environmental and economic concerns necessitate modernization of the aging power grid infrastructure into a more sustainable and optimized cyber-physical system, SG. MGs, reckoned as a vital contributor towards this transition, facilitate large scale deployment of renewable distributed generation (DG) and incorporation of new load types such as plug-in hybrid electric vehicles. However, the volatile nature of renewable energy (RE) sources, amplified uncertainty in load fluctuations along with increasing customer expectation for both power quality and quantity further complicate the energy management of MGs besetting with an intricate power allocation problem critical for maintaining system stability.

DR management has proven instrumental in resolving the problem confronted, offering efficient schemes for energy procurement and optimization of MGs suffering from power disbalance [1]. To achieve the desired system reliability, resilience and power quality, DR programs aim at establishing a mutually beneficial interaction framework for DR participants and aggregators where power generation drives the demand. With DR, customers are incentivized to shape and schedule their consumption profiles to flatten the peak demand, consequently deferring the cost of generation expansion and ancillary grid services. DR programs can be broadly categorized into two classes, price-based and event-based [2]. The latter are well suited for isolated MGs experiencing power generation shortage, on which the present work focuses [2], [3].

A. Background and Motivation

Increasing customer participation can potentially translate into elevated benefits for MG operators, as the availability and volume of controllable load reserves grows with the number of DR-capable devices. Towards realizing this prospect, customers' concerns over privacy could constitute a major threat [4]. DR programs with centralized control architecture, which are commonly deployed in practice [5], [6], entail information pertaining to customer loads and preferences as the inputs for optimization. This may limit customer participation severely since revealing such information infringes upon privacy [7]. Knowledge on the desired power valuation (utility) and electricity consumption characteristics of a customer empowers DR operators or potential eavesdroppers to exploit this marketable information to their own benefit. According to [8], the latter alone suffices to infer customer's appliances operated or even daily activities. More importantly, with this information an adversary participant may attempt to manipulate the DR outcome by misreporting own utility value for the sake of profit. In view of above arguments, deriving efficient privacy-aware strategies for solving large-scale DR problems under centralized control philosophy becomes vital.

While ensuring customer privacy, MG operators should also seek certain economic benefits or savings when deploying a DR scheme in practice. As long as the private information lies in the objective function or constraint matrix of the DR optimization problem these two objectives may conflict. Indeed, optimizing the DR management choosing to ignore customer input data as a privacy-preventive measure may lead to arbitrarily worse solutions when compared to optimal ones. The induced suboptimality gap typifies the cost of privacy, in

2324-9013/17 $31.00 © 2017 IEEE
DOI 10.1109/Trustcom/BigDataSE/ICESS.2017.276

a sense to be formalized in Section IV. Most of the extant literature on energy management of MGs, such as [7], [9] and [10], [11], approach this trade-off from one angle or the other leaving the privacy cost largely unexamined. Among these works, those dealing with the privacy aspect advocate approaches relying on cryptographic techniques and security protocols that may evoke substantial communication and computation overheads, thereby questioning their practicality in large-scale applications.

Recently, smart metering infrastructure sparked considerable research efforts [12]–[14] in response to privacy threats. Various schemes have been developed for securing smart meter data aggregation and customer demand reporting in SG. In [14] an efficient scheme is proposed with a quantifiable privacy metric. This is achieved by adding a randomly generated number to the measurement sent from the smart meter to the power provider, making it a simple and low complexity approach. The trade-off between economic benefit and privacy is evaluated in terms of error in the billed amount to SG operator. Nevertheless, the setting in these studies envisions smart metering primarily in the scope of electricity billing service rather than deployed within a DR optimization framework as in the case studied here. A simple yet effective privacy solution is presented in [15] for demand reporting by utilizing rechargeable batteries. Essentially, the batteries are used as a proxy between smart metering devices and household appliances to mask consumer demands in a non-intrusive manner (i.e., without introducing additional noise to data).

Privacy preservation is also evident in economic load dispatch control problem for minimizing generation cost [16]. Similar to [14], customer demands are altered by noise prior to reaching the control unit to enable the privacy. The increased generation cost attributed to privacy is assessed through small scale experiments based on a 5-bus power system with 200 customers only and a simplified grid model that omits AC power flow equations.

Against the background discussed, this study is set out to explore and quantify the interplay between privacy and optimality in centralized event-based DR programs through extensive empirical investigation on a realistic MG model. We further unravel the obscure relationship between privacy and DR parameters driving this trade-off, thus conducing to deeper understanding of the scales and dynamics of privacy phenomena in energy management optimization of MGs.

B. Contributions

Typically, in a DR management scheme, there is a single load-serving entity (LSE) or an operator of MG, which coordinates the decisions of subscribed customers. There is a high probability that an MG once initiated will be short of power, consequently resulting in significant voltage and frequency deviations, and leading to its instability. The LSE then invokes the featured event-based DR program to ensure the endurance of an MG. Constrained by the net satisfiable apparent generation and power flow equations, LSE is required to make control decisions in real time as to maximize the total utility of satisfied customers without violating their privacy. To ensure scalability, a computationally efficient privacy-preserving mechanism introduced in [17] is leveraged to this end, which provides a definite theoretical guarantee on the level of privacy and optimality. The privacy cost is quantified by benchmarking the maximized utility of this mechanism with that in the omniscient case, where customer privacy is not protected.

The major contribution of this preliminary study is centered on two salient features that differentiate it from the surveyed literature. First, particular emphasis is paid to establishing a realistic DR system with an accurate and reliable MG model capturing power flow and operational constraints (e.g., voltage limits, non-linear apparent power generation constraints, reactive power requirements) associated with the underlying distribution network. The importance and necessity of this were acknowledged in technical literature [18]–[20], which highlight that using a simplified MG model may lead to infeasible load management decisions in practice and thus impairs the credibility of the results produced. Second, power valuation, which is a core design parameter of an event-based DR, is regarded as information private to a customer. While various approaches were proposed for tackling privacy issues in demand reporting (e.g., the method in [15] relying on rechargeable batteries), the setting with private power valuations has not been studied properly. Taken together, these contributions illustrate and appraise the ramifications of deploying large-scale event-based DR programs in practice where privacy concerns are a priority.

As one demonstration, the proposed privacy-preserving DR scheme is applied to a 4-bus feeder from Canadian Benchmark distribution system (see Fig. 1 in Section III). The results indicate that enabling customers privacy in centralized event-based DR programs may degrade the optimality of the produced load management decisions severely as the number of customers continues to grow. Nevertheless, considering a more likely scenario with heterogeneous, slightly relaxed privacy levels varying among customers may smooth the impact. Also, it is inferred that the privacy cost is influenced by several DR parameters including customers' type (i.e., power consumption profile) and privacy level.

II. Preliminaries

A. Differential Privacy

When it comes to quantifying the extent of privacy of a customer participating in a DR program, this paper adheres to the notion of *differential privacy*. Originated from the research in [21] and defined by [22], differential privacy has evolved as a rigorous definition of privacy in computer science. As such, it can be interpreted as a guarantee that altering an individual record in the input set does not impact distribution of the computation outcomes significantly. In other terms, customers' private information becomes indistinguishable in the output of a differentially private algorithm. This yields a strong privacy

guarantee regardless of any auxiliary information the adversary may possess.

On the other hand, it is increasingly hard to derive efficient algorithms meeting such a stringent privacy guarantee [17]. As a consequence, many fundamental problems as those studied in [23], [24] have private solutions, while lacking efficient algorithms. For a certain class of combinatorial optimization problems several approximation algorithms are devised in [25] that retain differential privacy. *Laplace mechanism* and *exponential mechanism*, which by far are the most prevalent approaches practiced for differential privacy were introduced in [22] and [26], respectively. Unlike the former one, exponential mechanism runs in linear time of its output range, which might largely outweigh the number of customers, and thus is not suitable for the purpose of this study.

The framework of differential privacy represents information private to a customer as a set D referred to as *database*. Let $\mathcal{D}$ be the domain of all databases of interest. The basic idea underlying this framework is to draw an association between privacy and impact of an individual customer in the database. The impact, that is, changes that occur in the database when altering or deleting a customer's record is characterized by the concept of *neighboring databases*. Define databases $D \in \mathcal{D}$ and $D' \in \mathcal{D}$ to be neighboring if they are identical except a single record. Differential privacy is formalized by the definition below.

Definition 1 (Differential privacy [22])**.** *A randomized algorithm $\mathcal{A} : \mathcal{D} \to \mathbb{R}^n$ that maps databases to an output range $\mathcal{R}$ is (ϵ, δ)-differentially private if for every pair of neighboring databases $D \in \mathcal{D}$, $D' \in \mathcal{D}$ and $\forall\ S \subseteq \mathcal{R}$, $Pr[\mathcal{A}(D) \in S] \leq e^{\epsilon} \cdot Pr[\mathcal{A}(D') \in S] + \delta$, where $\epsilon > 0$ and $\delta \in [0, 1)$.*

Similarly, an algorithm $\mathcal{A}$ is ϵ-differentially private, if $\delta = 0$. The level of privacy is inversely commensurate with the value of ϵ. The smaller the ϵ, the higher is privacy level.

III. System Model and Assumptions

Towards defining the DR optimization problem under study formally, this section starts by modeling the system and its components. The adopted DR model envisions a single LSE procuring the responses of customers' demands over a finite decision horizon $\mathcal{T} \triangleq \{1, ..., m\}$. The decision horizon $\mathcal{T}$ is discretized into m equal periods with a duration corresponding to the required time resolution granularity at which DR management decisions are to be produced. At each time slot $t \in \mathcal{T}$, the net available generation capacity of MG is denoted by $C^t \in \mathbb{R}_+$.

A. Load Model

Consider a set of customers $\mathcal{N} \triangleq \{1, ..., n\}$ for a DR management scheme run by LSE. A customer $k \in \mathcal{N}$ is associated with a complex-valued power demand $S_k^t \in \mathbb{C}$ (composed of *active* and *reactive* power components) required for operating certain electric appliances at particular time instant $t \in \mathcal{T}$. Alongside the appliances, each customer may possess a small-scale local generation source (e.g., solar panel or wind turbine) and storage (e.g., battery). These energy resources, however, are designated primarily to serve own energy needs of a customer, and thus are not connected to MG. In the scope of current study, this design can be encapsulated into the aggregate customer power demand. In a sense, S_k^t captures the net load of customer k minus the available on-site generation at time t.

To allow effective DR application, diverse customer appliances should be taken into account [27]. The customers' demands here are categorized into two types according to their operation and energy consumption characteristics, *elastic* (divisible) and *inelastic* (indivisible). The demand of a customer possessing inelastic load can be either shed or fed completely. This models the electric appliances that can operate only under particular energy supply level (e.g., washing machine, vacuum cleaner). Different from the inelastic demands, an elastic load may be satisfied partially and adjusted to operate with different energy consumption levels (e.g., air conditioner, water heater).

B. Modeling the Distribution Network

To incorporate the power flow and voltage constraints into the DR optimization problem a model of the distribution network, resembling that of in [28], is established below. We shall confine our attention to radial (tree) distribution networks which are prevalent in practice [29].

The distribution system is represented by a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where each customer $k \in \mathcal{N}$ is located at a given node except the root. The set of nodes $\mathcal{V}$ denote the electric buses, whereas the set of edges $\mathcal{E}$ denote the distribution lines. The nodes in $\mathcal{V}$ are indexed by $\{0, 1, ..., |\mathcal{V}|\}$, where the node 0 denotes the collective generation source, with a fixed voltage and flexible power injection, which powers the entire MG. To empower RE penetration, the generation source is modeled to encompass a hybrid mix of traditional, RE supplies and energy storage units that could collectively have a variable (depending on the availability of RE and storage available) yet dispatchable capacity. An edge of $\mathcal{G}$ is represented by a tuple $(i, j) \in \mathcal{E}$ (or alternatively by e_j) where i is referred as the parent of j (i.e., i is the immediate upstream node from j to the root 0).

Let $V_i^t \in \mathbb{C}$ denote the voltage of node $i \in \mathcal{V}$ at time slot $t \in \mathcal{T}$. Define $I_{i,j}^t$ to be the current flowing through edge $(i, j) \in \mathcal{E}$ and with a slight abuse of notation, $\widehat{S}_{i,j}^t \in \mathbb{C}$ to be the transmitted power through that edge at time t. Similarly, let $z_{i,j} \in \mathbb{C}$ be the impedance of that edge. Denote by $v_i^t \triangleq |V_i^t|^2$ and $\ell_{i,j}^t \triangleq |I_{i,j}^t|^2$ the magnitude square of voltage and current, respectively. For each node $i \in \mathcal{V} \backslash \{0\}$, there is a set of customers attached to i, denoted by $\mathcal{N}_i$ such that $\mathcal{N} = \cup_{i \in \mathcal{V} \backslash \{0\}} \mathcal{N}_i$.

A power flow in a steady state is characterized by a set of power flow equations. In radial networks (which include paths) the Branch Flow Model (BFM) can be utilized to model them. It was first proposed by [30] in the context of AC *optimal power flow* (OPF) problem. The OPF is a fundamental problem in power systems concerned with optimizing certain

operational cost (e.g., minimizing power losses) subject to distribution networks physical and engineering constraints. Assuming v_0 and $\{z_{i,j}\}_{(i,j)\in\mathcal{E}}$ are given, the BFM is captured by the following set of equations for $\forall\ (i,j) \in \mathcal{E}$

$$\ell_{i,j}^t = \frac{|\widehat{S}_{i,j}^t|^2}{v_i^t}, \tag{1}$$

$$v_j^t = v_i^t + |z_{i,j}|^2 \ell_{i,j}^t - 2\mathrm{Re}(z_{i,j}^* \widehat{S}_{i,j}^t), \tag{2}$$

$$\widehat{S}_{i,j}^t = \sum_{l:(j,l)\in\mathcal{E}} \widehat{S}_{j,l}^t + \bar{s}_j^t + z_{i,j}\ell_{i,j}^t, \tag{3}$$

where $\bar{s}_j^t \in \mathbb{C}$ is the total load at node (i.e., bus) j at time $t \in \mathcal{T}$, $\mathrm{Re}(\chi)$ denotes the real component of a complex number $\chi \in \mathbb{C}$ and ψ^* denotes the complex conjugate of $\psi \in \mathbb{C}$. Equations (1) - (3), essentially, capture Ohm's law combined with the Kirchhoffs laws of electric flows and power flow definitions. Recall that in DR programs the net load at each bus is guided by the energy management decisions settled by LSE. That is, $\bar{s}_j^t = \sum_{k\in N_j} S_k^t x_k$, where x_k is the decision produced by LSE for customer $k \in \mathcal{N}$. Depending on customer's load type, x_k takes values either from $[0,1]$ or $\{0,1\}$. In more detail, for elastic loads $x_k \in [0,1]$, while for inelastic demands $x_k \in \{0,1\}$. Eqn. (3) now can be reformulated as

$$\widehat{S}_{i,j}^t = \sum_{l:(j,l)\in\mathcal{E}} \widehat{S}_{j,l}^t + \sum_{k\in N_j} S_k^t x_k + z_{i,j}\ell_{i,j}^t\,. \tag{4}$$

Besides power flow equations, for each node $i \in \mathcal{V}\backslash\{0\}$ and $t \in \mathcal{T}$ the following operational constrain should be satisfied

$$v_{\min} \le v_i^t \le v_{\max}\,, \tag{5}$$

where $v_{\min}, v_{\max} \in \mathbb{R}^+$ are the minimum and maximum allowable voltage magnitude square at any node, respectively. The setting studied here assumes a limited apparent power generation on MG and thus at each time step $t \in \mathcal{T}$

$$|\sum_{j:(0,j)\in\mathcal{E}} \widehat{S}_{0,j}^t| \le C^t\,. \tag{6}$$

Observe that BFM model is non-convex due to the quadratic equality constraints in Eqn.(1) and thus is computationally intractable in general. We therefore consider relaxing them to inequalities in Eqn. (7) to convexify the model.

$$\ell_{i,j} \ge \frac{|\widehat{S}_{i,j}|^2}{v_i}\,, \qquad \forall (i,j) \in \mathcal{E} \tag{7}$$

By analogous reasoning, the same relaxation is adopted in [19], [31]. Obviously, when the equality in (7) is attained then the relaxation is exact. In the sequel, using the established distribution model, the employed differentially private mechanism of [17] is applied to a 4-bus feeder of the Canadian Benchmark system depicted in Fig. 1.

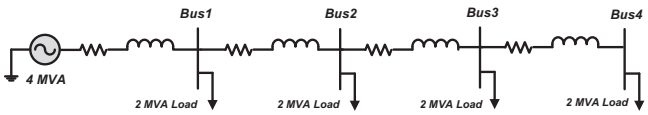

Fig. 1: A 4-bus feeder from Canadian benchmark distribution system.

C. Customer Preference Model

In a DR program where each subscribed customer is an independent decision maker, typically, responses to the incentives by LSE are modeled by a *utility function*. The response may vary depending on the particular time of a day (e.g. at peak and non-peak hours). Moreover, it may vary from customer to customer based on the consumption profile (i.e., when considering *residential* and *commercial* customers).

To simplify the exposition, the utility function is summarized by an non-negative *utility value* (power valuation) u_k^t associated with a customer $k \in \mathcal{N}$. This value quantifies the extent of satisfaction obtained (or alternatively, the payment) by customer k when own power demand is satisfied at time $t \in \mathcal{T}$. In the case with inelastic demands, if S_k^t is satisfied at time slot t, u_k^t is the perceived utility for customer k, otherwise zero utility is perceived. As for a customer $k' \in \mathcal{N}$ with an elastic load, a portion $b \in [0,1]$ of the power demand $S_{k'}^t$ drawn from MG (i.e., $bS_{k'}^t$ amount of power in aggregate) at time instant t imparts an utility of $b \cdot u_{k'}^t$.

D. Privacy-Preserving DR Scheme

This subsection exemplifies the configuration of the envisioned event-based DR system. Recall that it is required to protect customer sensitive information in the input data. In particular, this paper focuses on the case where utilities, which define objective function of the DR optimization problem, are the sensitive information to customers. That is, the private database at time t of the participating customers is $D = \{u_k^t\}_{k\in\mathcal{N}}$. Since only aggregate power demands are required by LSE, it is assumed that the customer loads can be protected in a non-intrusive manner by a method akin to that proposed in [15] relying on rechargeable batteries. In a sense, shifting between neighboring databases affects only the objective function of the DR problem leaving the constraint matrix unchanged.

In the envisioned DR program featuring a centralized control scheme, each customer declares his reactive and active power demand through the equipped smart metering infrastructure to LSE upon request (or periodically over a predetermined schedule). The smart meters operating on customer end are expected to be embedded with a fully-automated interface which responds to LSE control signals [32]. Therefore, it is to be assumed that LSE has complete control over the on/off and other relevant operations of its customers' demands. In order to prevent customer utilities from being exposed to LSE or a potential eavesdropper the adopted privacy strategy produces a perturbed utility value to obfuscate true valuation, which is then submitted to LSE. Section IV scopes a detailed explanation of this mechanism and provides provable guarantees on its privacy level.

As noted previously, devising computationally efficient differentially private algorithms with provable optimality guar-

antees is substantially difficult. In fact, it was shown in [17] that if one makes no assumptions on the sensitivity of the private data it is impossible to devise such an algorithm with non-trivial optimality guarantees. This necessitates the need for introducing the simplifying assumption stated hereunder that will be followed throughout this paper.

Assumption 1. *There exist positive* $u_{\max}$ *and* $u_{\min}$ *known to LSE apriori such that for* $\forall\ k \in \mathcal{N},\ t \in \mathcal{T}\quad u_{\min} \leq u_k^t \leq u_{\max}$.

We remark that Assumption 1 naturally holds in DR systems, since usually $u_{\min}$ and $u_{\max}$ are determined by LSE.

IV. Problem Formulation and Chosen Approach

A. Optimization Problem

Now that the system model is established the DR optimization problem can be formulated in an OPF framework by leveraging BFM. This engenders the *utility maximizing demand response* (UMDR) problem which is defined for a particular time $t \in \mathcal{T}$ by the following *quadratically constrained mixed integer programming* (QCMIP) problem.

$$\begin{aligned} (\text{UMDR}) \quad & \max_{x_k, v_i^t, \ell_{i,j}^t, \widehat{S}_{i,j}^t} \sum_{k\in\mathcal{N}} u_k^t x_k \\ \text{subject to} \quad & (2), (4), (5), (6), (7) \\ & x_k \in \{0,1\}, \qquad \forall\ k \in \mathcal{N} \end{aligned} \tag{8}$$

Here, x_k is a binary decision variable that takes value 1 if and only if the k-th customer's power demand S_k^t is satisfied and 0 otherwise. The UMDR problem aims at maximizing the overall net utility of customers while maintaining the apparent power generation C^t bound at time instant $t \in \mathcal{T}$, power flow equations and voltage levels.

Evidently, UMDR is NP-HARD, since the 0-1 classical knapsack problem is its special case. Relaxing binary (discrete) decision variables (x_k) to continuous ones in UMDR problem, such that $x_k \in [0,1]$, yields a *convex quadratic programming* problem denoted by UMDR_L. Aside from complexity, setting the decision variable (x_k) to be discrete or continuous alters the practical aspects of DR application. Concretely, the continuous case corresponds to customers having only elastic power demands, whereas the discrete case assumes customer set is comprised solely of inelastic loads.

B. Differentially Private Method

This subsection presents an efficient randomized mechanism, introduced by [17], to compute solutions of UMDR and UMDR_L problems privately. The method relies on a principle differential privacy technique which is explained in what follows.

Define a function $f : \mathcal{D} \to \mathbb{R}^n$ to be $\triangle$-sensitive if $||f(D) - f(D')||_1 \leq \triangle$ for $\forall$ neighboring $D, D' \in \mathcal{D}$. Let $Lap(\Omega)$ denote the Laplace transformation of Ω with a probability density function $f(x \mid \Omega) = \frac{1}{2\Omega} e^{-\frac{|x|}{\Omega}}$. Then, applying the Laplace mechanism to a $\triangle$-sensitive function $f(D)$ yields $f(D) + [\mu_1, \mu_2, ..., \mu_n]^T$, where $\mu_1, \mu_2, ..., \mu_n$ are n independent and identically distributed draws from $Lap(\frac{\triangle}{\epsilon})$ with $\epsilon > 0$.

Theorem 1 ([33]). *A randomized algorithm* $\mathcal{A}$ *that invokes the Laplace mechanism explained above is* ϵ*-differentially private.*

Instead of releasing the true customer valuations, the considered mechanism perturbs each customer's utility u_k^t independently by adding a noise drawn from the Laplace distribution that commensurates with the desired level of privacy. Define $\hat{u}_k^t \triangleq u_k^t + \text{Lap}(\frac{(u_{\max} - u_{\min})\sqrt{8n\log(\frac{1}{\delta})}}{\epsilon})$ to be the perturbed utility of customer $k \in \mathcal{N}$ at time $t \in \mathcal{T}$, where $\delta \in [0,1)$. Then, the private analog of UMDR_L problem (DR with elastic demands) defined for time slot $t \in \mathcal{T}$ is embodied by the following *convex programming problem*.

$$\begin{aligned} (\text{UMPDR})_\text{L} \quad & \max_{x_k, v_i^t, \ell_{i,j}^t, \widehat{S}_{i,j}^t} \sum_{k\in\mathcal{N}} \hat{u}_k^t x_k \\ \text{subject to} \quad & (2), (4), (5), (6), (7) \\ & x_k \in [0,1], \qquad \forall\ k \in \mathcal{N} \end{aligned} \tag{9}$$

Solving UMPDR_L problem non-privately results in a private solution to the original one. Note that any feasible solution to UMPDR_L is also feasible for UMDR_L. Denote by $X_\text{L}^* \subseteq \mathcal{N}$ an optimal solution of UMDR_L and by $\text{OPT}_\text{L} \triangleq \sum_{k\in X_\text{L}^*} u_k^t$ the corresponding total utility for time $t \in \mathcal{T}$. Set $\hat{X}_\text{L}^* \subseteq N$ to be an optimal solution of UMPDR_L and define $\text{OPT}_\text{L}^\text{DP} \triangleq \sum_{k\in\hat{X}_\text{L}^*} u_k^t$.

Theorem 2 ([17]). *An optimal solution* $\hat{X}_\text{L}^*$ *for* UMPDR_L *problem is* (ϵ, δ)*-differentially private feasible solution to* UMDR_L *that with high probability satisfies the following additive optimality bound* $\text{OPT}_\text{L}^\text{DP} \geq \text{OPT}_\text{L} - \alpha$ *where* $\alpha = \frac{4(u_{\max} - u_{\min})\sqrt{8n\log(\frac{n}{\delta})}}{\epsilon}$.

The proof of Theorem 2 can be consulted in [17].

The privacy cost in this study is defined in terms of the relative difference between OPT_L and $\text{OPT}_\text{L}^\text{DP}$. In a sense, it exemplifies the diminished objective value arising as a result of solving the DR optimization problem with inaccurate customers demands obfuscated by differentially private noise. For UMDR_L, the cost of privacy, denoted by $\Phi_\text{L} \in [0,1]$, is defined as

$$\Phi_\text{L} \triangleq \frac{\text{OPT}_\text{L} - \text{OPT}_\text{L}^\text{DP}}{\text{OPT}_\text{L}}\,. \tag{10}$$

When $\Phi_\text{L} = 0$, this represents the ideal desirable case when no cost is incurred on the optimality of the produced energy management decisions. The closer Φ_L to 1 the higher the privacy cost is and so is the optimality gap. For example, $\Phi_\text{L} = 0.4$ implies that incorporating the privacy-preserving method entails 40% loss of optimality. Following the logic of Eqn. (10), define Φ to be the privacy cost for UMDR problem.

V. Empirical Evaluation

To complement the analytic result in Theorem 2, this section evaluates the utilized differentially private mechanism empiri-

cally by applying it to a simulated 4-bus feeder from Canadian Benchmark distribution system, which appears in Fig.1. The objective is to investigate and quantify the privacy cost in the proposed event-based DR system. The CPLEX optimizer is invoked to obtain the close-to-optimal solutions numerically for UMDR, UMDR_L problems and their differentially private analogs.

A. Simulation Setup and Settings

The feeder, which is rated at 8.7MVA, 400A and 12.47KV, is simulated with an overall generation capacity of 4MVA and over 1500 customers allocated among the buses randomly. Each feeder section is a 700MCM Cu XLPE cable with impedance $z = 0.1529 + J0.1406\ \Omega/km$. Each customer has a specific power demand (including both active and reactive power) and a utility that is generated according to a probability preference model. Due to limited power supply, the customers may suffer from a reduction of generation capacity occasionally.

B. Case Studies

Various case studies are performed to evaluate the studied privacy-preserving mechanism under diverse scenarios with respect to the correlation between customer loads and utilities, consumption profile and privacy protection levels (i.e., ϵ). The following are settings for the case studies in this paper.

(i) *Utility-demand correlation*:
a) *Quadratic utility (Q)*: The utility of a customer is a quadratic function of the power demand in the form of $u_k^t(|S_k^t|) = a \cdot |S_k^t|^2 + b \cdot |S_k^t| + c, \quad \forall t \in \mathcal{T}$, where $a > 0, b, c \geq 0$ are preset constants.
b) *Uncorrelated setting (U)*: The utility of each customer is independent of the power demand and is generated randomly.

(ii) *Customer types*:
a) *Residential (R) customers*: The customer set is comprised of residential customers having small power demands ranging from 1500VA to 15KVA.
b) *Mixed (M) customers*: The customer set is comprised of a mix of commercial and residential customers. The former have big power demands ranging from 300KVA up to 1MVA and constitute no more than 10% of all customers chosen at random.

(ii) *Privacy protection levels*:
a) *Fixed (F) privacy level*: All the customers have uniform privacy protection level predetermined by LSE.
b) *Variable (M) privacy level*: Customers are allowed to choose the desired privacy protection level from a predefined set of values offered by LSE.

In this paper, the case studies will be represented by the aforementioned acronyms. For example, the case study named QMV stands for the one with mixed customers, quadratic utility-demand correlation and heterogeneous privacy levels.

C. Simulations with Homogeneous Privacy Levels

In this subsection the privacy cost is evaluated for case studies with homogeneous privacy levels, where each case study is analyzed considering changes in the set of customers. For each DR optimization problem (i.e., UMDR and UMDR_L), two different privacy levels are examined where the corresponding value of ϵ is set to 0.01 and 1 for all customers. As for the additive privacy parameter δ, the value is fixed to 0.5 for all case studies unless otherwise explicitly mentioned.

The privacy cost for UMDR_L is compared for different values of ϵ in Fig.2. The employed privacy method is applied to the UMDR_L problem (i.e., this corresponds to solving UMPDR_L with perturbed customer utilities) 30 times for each of the m number of customers, where m varies between 500 to 1500 in steps of hundred. For case studies with residential customers, m varies between 1000 to 1500 since with fewer customers the total load on MG is less than the supply thus resulting in trivial DR decisions. Each of 30 iterations yields random changes in demands and utilities of customers. The same set of experiments is conducted for UMDR problem, however, for brevity the results are omitted due to their close resemblance to those of UMPDR_L. The privacy cost

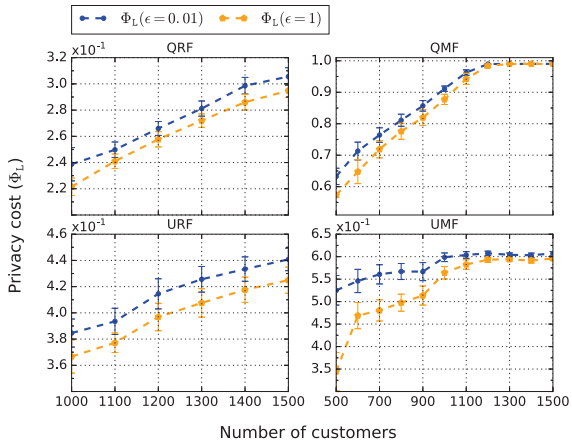

Fig. 2: The average privacy cost for UMDR_L against the number of customers at 95% confidence interval.

for UMDR is contrasted with that of UMDR_L in Fig. 3 considering a fixed number of customers. Here, the privacy level ϵ is varied from $5 \cdot 10^{-5}$ to 1 for 900 customers considering random changes in demands and utilities. One of the important findings observed is a common trend appearing in all the case studies performed. As can be inferred from Figs. 2 and 3, increasing ϵ reduces the optimality gap and hence the privacy cost. In other terms, the lower the privacy parameter ϵ (i.e., higher privacy guarantees) the higher is the privacy cost. This directly implies that the privacy cost increases with the noise magnitude since the Laplace noise added to each customer's utility increases when lowering ϵ. As illustrated in Fig. 2, on a MG with 500 customers the studied differentially private mechanism resulted in a privacy cost of 0.59 when $\epsilon = 1$ (i.e., the optimality of DR is decreased by

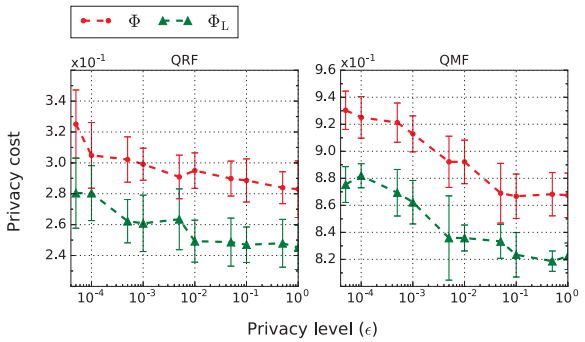

Fig. 3: The average privacy cost for UMDR and UMDR_L against ϵ at 95% confidence interval.

59%), whereas when $\epsilon = 0.1$ the privacy cost is about 0.63, considering the case study QMF.

Another important observation is that with increasing customer participation optimality of produced DR solutions degrades drastically. As depicted in Fig. 2, when the number of customers is small the privacy cost is only in order of 0.6 when considering case study QMF, while as the customer set cardinality grows privacy cost escalates approaching nearly 0.98. This highlights the necessity of devising efficient privacy-preserving mechanisms with a constant factor optimality guarantees.

Also, it is observed that the privacy cost is sensitive with respect to customer types. In particular, when increasing the number of customers the privacy cost grows slower for case studies with residential customers than in those with mixed industrial and residential customers. As portrayed in Fig. 2, the difference in privacy cost for case study QRF is about 0.08 when considering the number of customers ranging from 1000 to 1500. In contrast, for the same range the privacy cost increases nearly by 1.2 in case study QMF. In a sense, incorporation of privacy has more significant degrading effect on the optimality for scenarios with mixed customers as compared to those with only residential customers.

An auxiliary yet interesting result is the inferred loose coupling between customers' utilities and the privacy cost. Specifically, for case studies with residential customers the observed optimality loss is always more significant in scenarios with quadratic utilities than in those with uncorrelated ones. Surprisingly, the exact opposite correlation is evident in case studies with mixed customers. The reported privacy cost for case study URF with 1000 customers nears 0.37 when $\epsilon = 1$, as alluded by Fig. 2, while for case study QRF the privacy cost is only about 0.22 for the same parameters. As for case studies QMF and UMF, the recorded privacy cost is approximately 0.87 and 0.57, respectively when considering 1000 customers and privacy level of 1.

D. Dynamic Generation Capacity and Heterogeneous Privacy Levels

The previous subsection considered an MG with a fixed generation capacity and homogeneous privacy levels. Here simulations are performed considering an MG with generation capacity varying over time, which captures a case of hybrid system with renewable generation sources. Furthermore, in a real-world situation customers may desire different levels of privacy depending on their preferences and needs. Thus, the simulation studies performed in this section consider heterogeneous privacy levels. For residential customers, ϵ was generated randomly from the range $[0.5, 1]$, whereas for commercial customers from $[0, 0.1]$.

The time-varying generation capacity of MG C^t, that follows a Bernoulli process, is dynamically varied between 1MVA and 4MVA from time 0 to 10000 (seconds). To analyze the effect of heterogeneous privacy levels, the employed privacy-preserving DR scheme is applied to the feeder at each time of the occurring capacity fluctuation event. Overall, 1000 customers have been allocated among the 4 buses in a random fashion at each event. The observed privacy cost for UMDR problem is plotted in Fig 4. The privacy cost and absolute

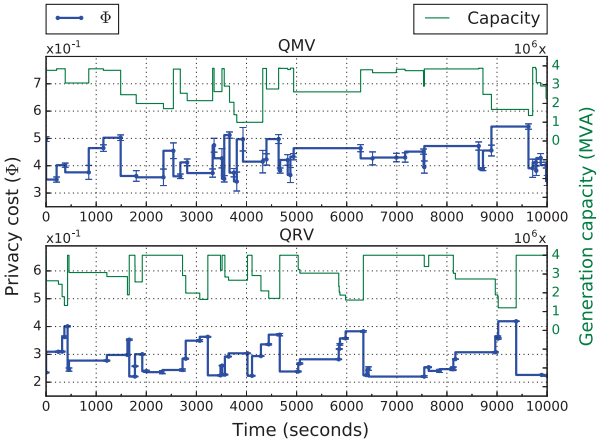

Fig. 4: The average privacy cost against the number of customers at 95% confidence interval considering dynamic generation capacity.

noise magnitude (per customer), which appear in Fig. 5, are evaluated considering changes in the number of customers, whereas MG generation capacity remains fixed at 4MVA. The results demonstrate that allowing flexible privacy levels, instead of flat ones, may considerably increase the optimality of the proposed DR management scheme but with a slight sacrifice in overall privacy guarantees. The average privacy cost plotted in Fig. 5 for case study QMV fluctuates around 0.4 when the number of customers changes, yet does not drift far away from that threshold. Conversely, in the scenarios with homogeneous privacy levels, appearing in Fig. 2, the privacy cost was sometimes as high as nearly 0.98.

VI. Conclusion

This paper studies the trade-off between privacy and optimality in centralized DR management of MGs. Under the framework of differential privacy, the privacy cost is quantified

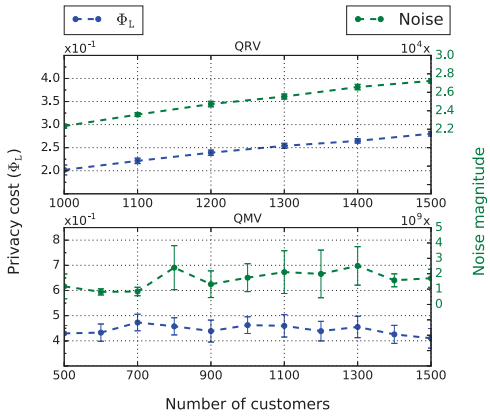

Fig. 5: The average privacy cost and absolute noise magnitude (per customers) as a function of the number of customers at 95% confidence interval.

empirically through extensive numerical simulations on a realistic MG system considering the power flow and operational constrains associated with the underlying power distribution network. The observed results illustrate the striking effect posed on the optimality of produced DR solutions when considering increasing customer participation. According to the findings, the optimality gap approaches nearly 98% in some cases, which urges the need for efficient privacy-preserving algorithms with constant theoretically-backed guarantees on their worst case performance. The major factors identified in this study that define the privacy-to-optimality trade-off in centralized event-based DR management of MGs include customers' type (i.e., power consumption magnitude) and privacy protection level.

REFERENCES

[1] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Transactions on Smart Grid*, vol. 1, pp. 82–88, June 2010.

[2] P. Siano, "Demand response and smart gridsa survey," *Renewable and Sustainable Energy Reviews*, vol. 30, pp. 461 – 478, 2014.

[3] W. Chen, X. Wang, J. Petersen, R. Tyagi, and J. Black, "Optimal scheduling of demand response events for electric utilities," *IEEE Transactions on Smart Grid*, vol. 4, pp. 2309–2319, Dec 2013.

[4] R. Hoenkamp, G. B. Huitema, and A. J. de Moor-van Vugt, "Neglected consumer: The case of the smart meter rollout in the netherlands, the," *Renewable Energy L. & Pol'y Rev.*, p. 269, 2011.

[5] S. Lu, N. Samaan, R. Diao, M. Elizondo, C. Jin, E. Mayhorn, Y. Zhang, and H. Kirkham, "Centralized and decentralized control for demand response," in *ISGT 2011*, pp. 1–8, Jan 2011.

[6] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," *IEEE Communications Surveys Tutorials*, vol. 17, pp. 152–178, Firstquarter 2015.

[7] Y. Gong, Y. Cai, Y. Guo, and Y. Fang, "A privacy-preserving scheme for incentive-based demand response in the smart grid," *IEEE Transactions on Smart Grid*, vol. 7, pp. 1304–1313, May 2016.

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

[9] D. Seo, H. Lee, and A. Perrig, "Secure and efficient capability-based power management in the smart grid," in *2011 IEEE 9th IPDPS*, pp. 119–126, May 2011.

[10] Z. Zhu, J. Tang, S. Lambotharan, W. H. Chin, and Z. Fan, "An integer linear programming based optimization for home demand-side management in smart grid," in *2012 IEEE PES ISGT*, pp. 1–5, Jan 2012.

[11] A. G. Tsikalakis and N. D. Hatziargyriou, "Centralized control for optimizing microgrids operation," *IEEE Transactions on Energy Conversion*, vol. 23, pp. 241–248, March 2008.

[12] X. He, X. Zhang, and C. C. J. Kuo, "A distortion-based approach to privacy-preserving metering in smart grids," *IEEE Access*, vol. 1, pp. 67–78, 2013.

[13] S. Wang, L. Cui, J. Que, D. H. Choi, X. Jiang, S. Cheng, and L. Xie, "A randomized response model for privacy preserving smart metering," *IEEE Transactions on Smart Grid*, vol. 3, pp. 1317–1324, Sept 2012.

[14] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Information Sciences*, vol. 370, pp. 355–367, 2016.

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

[16] X. Lou, R. Tan, D. Yau, and P. Cheng, "Cost of differential privacy in demand reporting for smart grid economic dispatch," tech. rep., 2016, http://publish.illinois.edu/cps-security/files/2016/12/dp-cost-techreport.pdf.

[17] J. Hsu, A. Roth, T. Roughgarden, and J. Ullman, "Privately solving linear programs," in *ICALP*, pp. 612–624, Springer, 2014.

[18] W. Shi, X. Xie, C. C. Chu, and R. Gadh, "Distributed optimal energy management in microgrids," *IEEE Transactions on Smart Grid*, vol. 6, pp. 1137–1146, May 2015.

[19] N. Li, L. Chen, and S. H. Low, "Demand response in radial distribution networks: Distributed algorithm," in *Proceedings of the 6th ASILOMAR*, pp. 1549–1553, Nov 2012.

[20] D. E. Olivares, C. A. Caizares, and M. Kazerani, "A centralized energy management system for isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 5, pp. 1864–1875, July 2014.

[21] I. Dinur and K. Nissim, "Revealing information while preserving privacy," in *Proceedings of the 22nd ACM SIGMOD-SIGART*, pp. 202–210, ACM, 2003.

[22] C. Dwork, F. McSherry, K. Nissim, and A. Smith, *Calibrating Noise to Sensitivity in Private Data Analysis*, pp. 265–284. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[23] A. Blum, K. Ligett, and A. Roth, "A learning theory approach to non-interactive database privacy," in *Proceedings of the 40th Annual ACM STOC*, pp. 609–618, ACM, 2008.

[24] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?," *SIAM Journal on Computing*, vol. 40, no. 3, pp. 793–826, 2011.

[25] A. Gupta, K. Ligett, F. McSherry, A. Roth, and K. Talwar, "Differentially private combinatorial optimization," in *Proceedings of the 21st Annual ACM-SIAM SODA*, pp. 1106–1125, 2010.

[26] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *48th Annual IEEE Symposium on FOCS'07*, pp. 94–103, IEEE, 2007.

[27] S. J. Kim and G. B. Giannakis, "Scalable and robust demand response with mixed-integer constraints," *IEEE Transactions on Smart Grid*, vol. 4, pp. 2089–2099, Dec 2013.

[28] A. Karapetyan, M. Khonji, C. K. Chau, K. Elbassioni, and H. Zeineldin, "Efficient algorithm for scalable event-based demand response management in microgrids," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[29] K. P. Schneider, Y. Chen, D. P. Chassin, R. Pratt, D. Engel, and S. Thompson, "Modern grid initiative distribution taxonomy final report," *PNNL-18035*, 2008.

[30] M. E. Baran and F. F. Wu, "Optimal capacitor placement on radial distribution systems," *IEEE Transactions on Power Delivery*, vol. 4, pp. 725–734, Jan 1989.

[31] S. H. Low, "Convex relaxation of optimal power flow part i: Formulations and equivalence," *IEEE Transactions on Control of Network Systems*, vol. 1, pp. 15–27, March 2014.

[32] M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "An algorithm for intelligent home energy management and demand response analysis," *IEEE Transactions on Smart Grid*, vol. 3, pp. 2166–2173, Dec 2012.

[33] C. Dwork, *Differential Privacy: A Survey of Results*, pp. 1–19. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.