Differentially Private Load Restoration for Microgrids with Distributed Energy Storage

Shourya Bose and Yu Zhang
Department of Electrical and Computer Engineering
University of California, Santa Cruz
{shbose, zhangy}@ucsc.edu

***Abstract*—Distributed energy storage systems (ESSs) can be efficiently leveraged for load restoration (LR) for a microgrid (MG) in island mode. When the ESSs are owned by third parties rather than the MG operator (MGO), the ESS operating setpoints may be considered as private information of their respective owners. Therefore, efforts must be put forth to avoid the disclosure through adversarial analysis of load setpoints. In this paper, we consider a scenario where LR takes place in a MG by determining load and ESS power injections through the solution of an AC optimal power flow (AC-OPF) problem. Since the charge/discharge mode at any given time is assumed to be private, we develop a differentially-private mechanism which restores load while maintaining privacy of ESS mode data. The performance of the proposed mechanism is demonstrated for a 33-bus MG.**

I. Introduction

Power distribution systems face constant risk of outage due to various factors [1] such as extreme weather conditions, system misconfiguration, overloading, etc. In this context, effective load restoration (LR) for electricity end users becomes an important but challenging task. A specific type of power network suitable for this purpose is the microgrid (MG). It is a geographically localized distribution system containing both loads and distributed energy resources (DERs). Federated control of MGs enables automatic LR when external supply of power is interrupted. A key element of a MG is the microgrid controller (MGC), which is a central computer that controls loads and DERs. Upon loss of external power, the MGC needs to provide new setpoints for all controllable and networked elements within the MG. If the setpoints are chosen appropriately, desired LR performance can be achieved [2].

MG operations are fundamentally distributed processes that are coordinated by the MGC. It is of paramount importance to ensure privacy of the data for all participating users. Some examples of user data include voltage and current values, operating modes and setpoints, a list of appliances being operated, etc. Leakage of private data during MG operation can lead to loss of trust, user attrition, and liabilities on part of a microgrid operator (MGO), thereby posing a threat to increased adoption of MGs for ensuring security and reliability of future power grids. The book [3] is an in-depth reference for various privacy concerns in MGs and smart grids.

Conventional distributed approaches for MG operation such as primal-dual gradient methods [4] and model-free machine-learning methods [5] provide a certain degree of privacy thanks to the locality of data. However, those methods do not guarantee that adversarial agents with strong computational capabilities cannot infer private data from local information such as voltage values. To overcome this shortcoming, we utilize the framework of *differential privacy* (DP) [6] to address data privacy in MG operation. DP posits that in order to protect the identity of individuals in a dataset, a carefully calibrated noise should be added to the response of any query on the dataset. The noise parameters are chosen to ensure that the noisy response makes it difficult to infer the presence or absence of an individual's data in the dataset. Since DP is an *information theoretic* concept, it is not vulnerable to adversaries with massive computational power.

Literature Review: Extensive efforts have been carried out on the topic of LR in MGs. Existing approaches include feedforward control of distributed generation [7], risk-limiting approach [8], robust model-predictive control [9], bi-level optimization approach [10], as well as reinforcement learning based control [11]. Comparatively, DP has received little attention as a framework for analyzing privacy in power systems. [12] considers differentially private distributed optimization to schedule charging of electrical vehicles. [13] investigates differential privacy of load data against aggregation queries. [14] develops a differentially private DC-OPF solver which exploits the structure of the underlying optimization problem to ensure privacy of load setpoints. However, privacy of generation data in a LR setting, which is indispensable for MGs with multiple producers or prosumers, has not received enough study. Especially, privacy issues have not analyzed for distribution systems modeled with the nonlinear AC Power Flow (AC-PF) equations.

Contributions: In this work, we formulate a load restoration problem for a MG equipped with energy storage systems (ESSs) over multiple time steps. The charge/discharge mode of each ESS on every time step is treated as a private datum, for which we leverage DP to obfuscate its value. The resulting load setpoints may not be feasible, and we propose a post-processing procedure to restore feasibility while ensure monotonicity in load restoration. Finally, performance of the proposed approach is demonstrated through extensive simulations tested on a 33-bus MG.

This work was supported in part by the Faculty Research Grant and the Chancellor's Fellowship of UC Santa Cruz, Seed Fund Award from CITRIS and the Banatao Institute at the University of California, and the Hellman Fellowship.

Notation: The symbols $\mathbb{R}$ and $\mathbb{R}_+$ denote the set of real numbers and non-negative real numbers, respectively. The notation $[N]$ denotes the set $\{1, \cdots, N\}$. The probability of event A is given by $\mathbb{P}[A]$. Vectors and matrices are denoted in boldface. $\mathbf{0}_m$ and $\mathbf{1}_m$ represent the m-dimensional vector of all zeros and ones. $(\mathbf{a})_j$ is the j^{th} element of vector $\mathbf{a}$. The condition $\mathbf{a} \sim_1 \mathbf{b}$ is true if and only if these two vectors differ only at one entry (i.e. $\|\mathbf{a}-\mathbf{b}\|_0 = 1$). For a sequence of vectors $\{\mathbf{a}_k\}_{k\in\mathcal{K}}$, the expression $\texttt{stack}(\mathbf{a}_k, \mathcal{K})$ represents the stacked vector $[\mathbf{a}_1^\top, \mathbf{a}_2^\top, \cdots, \mathbf{a}_{|\mathcal{K}|}^\top]^\top$.

II. Problem Statement

A. Differential Privacy

In this section, we briefly describe DP that ensures privacy of datasets manipulated by an algorithm. Let $\mathcal{D}$ denote the data space of a single user. A *dataset* $\mathbf{d} \in \mathcal{D}^n$ contains data of n users. A *query* $\mathcal{F} : \mathcal{D}^n \mapsto \mathbb{R}^k$ provides k 'responses' based on a given dataset. A *mechanism* $\mathcal{M}$ is a stochastic function of a query, i.e. $\mathcal{M}(\mathbf{d}) = g(\mathcal{F}(\mathbf{d}), \mathbf{w})$, where $\mathbf{w}$ is a random vector drawn from a specific distribution. A common class of mechanisms are ones which simply add noise to the query output, i.e. $\mathcal{M}(\mathbf{d}) := \mathcal{F}(\mathbf{d}) + \mathbf{w}$, to which we restrict our attention. A mechanism $\mathcal{M}$ is said to be ε-differentially private (ε-DP) if for some $\varepsilon > 0$,

$$\mathbb{P}[\mathcal{M}(\mathbf{d}) \in U] \leq e^{\varepsilon}\mathbb{P}[\mathcal{M}(\mathbf{d}') \in U]$$
$$\forall U \subseteq \mathbb{R}^k, \ \ \forall \mathbf{d}, \mathbf{d}' \in \mathcal{D}^n \text{ such that } (\mathbf{d} \sim_1 \mathbf{d}').$$

Note that smaller values of ε ensure higher privacy (see details in Section 2.3 of [15]). As given by the following theorem, post-processing preserves DP.

Theorem 1 (Prop. 2.1, [15]): Let $\mathcal{M} : \mathcal{D}^n \mapsto \mathbb{R}^k$ be an ε-DP mechanism, and let $\mathcal{G} : \mathbb{R}^k \mapsto \mathbb{R}^m$ be an arbitrary randomized mapping. Then, $\mathcal{G} \circ \mathcal{M}$ is ε-DP.

Based on the Laplace distribution, the popular Laplace mechanism is ε-DP (cf. Thm. 3.6, [15]). A centered Laplace random variable $X \sim \text{Lap}(b)$ $(b > 0)$ has the probability density function $f_X(x) = \frac{1}{2b}e^{-\frac{|x|}{b}}$, $\forall x \in \mathbb{R}$. X is zero mean and has variance $2b^2$. The Laplace mechanism $\mathcal{M}(\mathbf{d}) = \mathcal{F}(\mathbf{d}) + \mathbf{w}$ selects each noise element $(\mathbf{w})_i$ independently and identically distributed (i.i.d.) such that $(\mathbf{w})_i \sim \text{Lap}\left(\frac{\Delta}{\varepsilon}\right)$, where Δ is the l_1-sensitivity of the query, defined as

$$\Delta := \max_{\mathbf{d}, \mathbf{d}' \in \mathcal{D}^n : (\mathbf{d} \sim_1 \mathbf{d}')} \|\mathcal{F}(\mathbf{d}) - \mathcal{F}(\mathbf{d}')\|_1 .$$

Theorem 2 (Thm. 3.6, [15]): The Laplace mechanism is ε-DP.

B. Load Restoration Problem

We consider an island-mode MG with multiple ESSs and loads. The MG can be represented as a directed graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ where $\mathcal{N} := [N]$ denotes the set of *nodes* or *buses*, and $\mathcal{E} := [E]$ denotes the set of *branches* or *lines*. We assume that the MG has a *radial* topology, i.e. $\mathcal{G}$ is a tree. $\mathcal{N} = \mathcal{N}^{\text{ESS}} \cup \mathcal{N}^{\text{L}}$, wherein the two disjoint sets $\mathcal{N}^{\text{ESS}}$ and $\mathcal{N}^{\text{L}}$ represent ESS and load buses, respectively. We denote the sizes of these sets as $N_E := |\mathcal{N}^{\text{ESS}}|$ and $N_L := |\mathcal{N}^{\text{L}}|$ (with $N = N_L + N_E$). For the scenario of a load attached to an ESS, it can be modeled by allocating them adjacent buses connected by an impedance-free line. To focus on privacy of ESS data, we do not include distributed generation sources in the MG, although they can be easily incorporated into our model.

The LR problem is formulated over a time horizon $\mathcal{T} := [T]$, and the variable $t \in \mathcal{T}$ indicates the time step. On time step t, $\mathbf{p}_t \in \mathbb{R}^N$ and $\mathbf{q}_t \in \mathbb{R}^N$ denote real and reactive bus injections while $\mathbf{P}_t \in \mathbb{R}^E$ and $\mathbf{Q}_t \in \mathbb{R}^E$ are real and reactive line flows. $\mathbf{v}_t \in \mathbb{R}_+^N$ and $\mathbf{l}_t \in \mathbb{R}_+^E$ denote squared magnitude of nodal voltage phasors and line current phasors, respectively. $\mathbf{s}_t \in \mathbb{R}^{N_E}$ denotes the state-of-charge (SoC), and $\mathbf{d}_t \in \{0,1\}^{N_E}$ denotes the discharge/charge mode of each ESS, where 0 indicates discharge while 1 indicates charge mode. We maintain the convention that power injected into the MG has a positive sign, while power withdrawn from the MG has a negative sign.

We collect the aforementioned variables over the entire time horizon as $\mathbf{p} := \texttt{stack}(\mathbf{p}_t, \mathcal{T})$, $\mathbf{q} := \texttt{stack}(\mathbf{q}_t, \mathcal{T})$, $\mathbf{P} := \texttt{stack}(\mathbf{P}_t, \mathcal{T})$, $\mathbf{Q} := \texttt{stack}(\mathbf{Q}_t, \mathcal{T})$, $\mathbf{v} = \texttt{stack}(\mathbf{v}_t, \mathcal{T})$, $\mathbf{l} := \texttt{stack}(\mathbf{l}_t, \mathcal{T})$, $\mathbf{s} := \texttt{stack}(\mathbf{s}_t, [T+1])$, and the *mode vector* $\mathbf{d} := \texttt{stack}(\mathbf{d}_t, \mathcal{T})$. The voltages, currents, injections and branch flows on every time step are related through a convex second-order cone (SOC) relaxation of the nonconvex *DistFlow* AC-PF equations. Under mild conditions, such a relaxation is exact for radial networks (cf. Thm. 1, [16]). For any time step $t \in \mathcal{T}$, the equations are given as

$$\sum_{\substack{i \in \mathcal{N}: \\ b=(i,j)\in\mathcal{E}}} (\mathbf{P}_t)_b = (\mathbf{p}_t)_j + \sum_{\substack{k \in \mathcal{N}: \\ b'=(j,k)\in\mathcal{E}}} (\mathbf{P}_i)_{b'} - r_{b'}(\mathbf{l}_t)_{b'} \tag{1a}$$
$$\sum_{\substack{i \in \mathcal{N}: \\ b=(i,j)\in\mathcal{E}}} (\mathbf{Q}_t)_b = (\mathbf{q}_t)_j + \sum_{\substack{k \in \mathcal{N}: \\ b'=(j,k)\in\mathcal{E}}} (\mathbf{Q}_i)_{b'} - x_{b'}(\mathbf{l}_t)_{b'} \tag{1b}$$
$$(\mathbf{v}_t)_i - (\mathbf{v}_t)_j = 2(r_b(\mathbf{P}_t)_b + x_b(\mathbf{Q}_t)_b) - |z_b|^2(\mathbf{l}_t)_b \tag{1c}$$
$$(\mathbf{v}_t)_i(\mathbf{l}_t)_b \geq (\mathbf{P}_t)_b^2 + (\mathbf{Q}_t)_b^2, \tag{1d}$$

where $z_b := r_b + jx_b$ is the impedance of branch $b \in \mathcal{E}$. Note that (1a)-(1b) hold for all $j \in \mathcal{N}$, while (1c)-(1d) hold for all branches $b = (i,j) \in \mathcal{E}$.

We assume that ESS operators have provided vector $\mathbf{d}$ to the MGO *a priori*. For a given $\mathbf{d}$, the LR problem uses the *DistFlow* equations alongside other constrains to maximize restored load by setting load setpoints and charge/discharge amount corresponding to the decisions in $\mathbf{d}$. Because the exact load demand of the users may not be known *a priori*, we use forecasts $\hat{\mathbf{p}}, \hat{\mathbf{q}} \in \mathbb{R}^{N_L T}$ in place of the actual demand values. To this end, we define the load *pickup* vector $\mathbf{r}_t$ as

$$(\mathbf{r}_t)_i := \frac{(\mathbf{p}_t)_i}{(\hat{\mathbf{p}}_t)_j} \overset{[a]}{=} \frac{(\mathbf{q}_t)_i}{(\hat{\mathbf{q}}_t)_j}, \tag{2}$$
$$\text{index } i \in \mathcal{N} \text{ corresponds to load bus } j \in [N_L],$$

wherein $[a]$ follows from the assumption of constant power factor for all loads. If oversatisfaction of load demand is allowed, $\mathbf{r} := \texttt{stack}(\mathbf{r}_t, \mathcal{T})$ takes values in $[0, c]^{N_L T}$, where $c \geq 1$ denotes the maximum value of the pickup. In this work, we let $c = 1$.

Let $\mathbf{p}^E$ and $\mathbf{q}^E$ denote the sub-vectors of $\mathbf{p}$ and $\mathbf{q}$ corresponding to the ESS buses, respectively. Let $\mathbf{p}^{\text{ch}}$ and $\mathbf{p}^{\text{dis}}$ denote the ESS charge and discharge powers, respectively. Both vectors have the same size as $\mathbf{p}^E$. In addition, let $\mathbf{s}^{\text{init}} \in \mathbb{R}^{N_E}$ represent the initial SoC vector. To this end, the load restoration problem is formulated as

$$\mathcal{LR}(\mathbf{d}) := \mathbf{r}^* \in \underset{\{\mathbf{r},\mathbf{p}^{\text{ch}},\mathbf{p}^{\text{dis}},\mathbf{p},\mathbf{q},\mathbf{P},\mathbf{Q},\mathbf{v},\mathbf{l},\mathbf{s}\}}{\operatorname{argmax}} \quad \boldsymbol{\xi}^\top \mathbf{r} \tag{3}$$

$$\text{s.t.} \quad \text{(1a)-(1d)} \tag{3a}$$

$$\underline{\mathbf{v}} \leq \mathbf{v} \leq \bar{\mathbf{v}} \tag{3b}$$

$$\mathbf{0}_{ET} \leq \mathbf{l} \leq \bar{\mathbf{l}} \tag{3c}$$

$$\mathbf{0}_{N_L T} \leq \mathbf{r} \leq \mathbf{1}_{N_L T} \tag{3d}$$

$$(\mathbf{r}_t)_j \leq (\mathbf{r}_{t+1})_j, \forall j \in [N_L], \forall t \in [T-1] \tag{3e}$$

$$0 \leq (\mathbf{p}_t^{\text{ch}})_j \leq (\mathbf{d}_t)_j \bar{p}^{\text{ch}}, \forall j \in [N_E], \forall t \in \mathcal{T} \tag{3f}$$

$$0 \leq (\mathbf{p}_t^{\text{dis}})_j \leq (1-(\mathbf{d}_t)_j) \bar{p}^{\text{dis}}, \forall j \in [N_E], \forall t \in \mathcal{T} \tag{3g}$$

$$\mathbf{p}^E = -\mathbf{p}^{\text{ch}} + \mathbf{p}^{\text{dis}} \tag{3h}$$

$$\underline{\mathbf{q}}^E \leq \mathbf{q}^E \leq \bar{\mathbf{q}}^E \tag{3i}$$

$$(\mathbf{s}_{t+1})_j = (\mathbf{s}_t)_j + \Gamma^{\text{ch}}(\mathbf{p}_t^{\text{ch}})_j - \Gamma^{\text{dis}}(\mathbf{p}_t^{\text{dis}})_j; \;\; \mathbf{s}_1 = \mathbf{s}^{\text{init}}$$
$$\forall j \in [N_E], \forall t \in \mathcal{T} \tag{3j}$$

$$\underline{\mathbf{s}} \leq \mathbf{s} \leq \bar{\mathbf{s}}. \tag{3k}$$

The objective function in (3) maximizes the total pickup for all load buses, with each individual pickup weighted by the vector $\boldsymbol{\xi} \in \mathbb{R}_+^{N_L T}$. Constrains (3b)-(3c) limit nodal voltages and line currents within their safe operational limits. Constrain (3d) restricts the pickups to $[0,1]$. Constrain (3e) ensures *monotonic load restoration*, i.e. loads once picked up may not be dropped. Constrains (3f) and (3g) set limits for the ESS charge and discharge powers while ensuring *complementarity*, i.e. the ESS may either charge or discharge on a given time step, but not both. Constrain (3h) prescribes that the total power output of ESSs equal the sum of charge and discharge powers, while constrain (3i) places bounds on the reactive power the ESS inverters can produce. Constrain (3j) describes the temporal evolution of ESS SoC, with Γ^{ch} and Γ^{dis} denoting charge power-to-SoC and SoC-to-discharge power conversion factors, respectively. Lastly, constrain (3k) restricts the SoC of all ESSs within their upper and lower bounds.

Problem (3) is a convexified AC-OPF problem that can be solved via off-the-shelf convex solvers. $\mathcal{LR}$ is implemented at the MGC, which receives $\mathbf{d}$ from all ESSs and generates the optimal pickup $\mathbf{r}^*$ for all the loads. We assume that $\mathbf{d}$ is feasible for $\mathcal{LR}(\mathbf{d})$, and we refer to such $\mathbf{d}$ as *$\mathcal{LR}$-feasible*. In practice, the MGC can test feasibility of any provided $\mathbf{d}$, and reject infeasible ones. It is also assumed that the initial SoC vector $\mathbf{s}^{\text{init}}$ allows for at least one $\mathcal{LR}$-feasible value of $\mathbf{d}$.

III. Differentially Private Mechanism Design for $\mathcal{LR}(\mathbf{d})$

In this section, we discuss various aspects of making the LR problem deferentially private.

Algorithm 1: Approximation of $\Delta_{\mathcal{LR}}$

```
Input: mechanism $\mathcal{LR}$, $\mathbf{d}^{\text{init}} \in \mathcal{D}^n$, tolerance $\mathtt{tol} > 0$
Output: approx. $l_1$-sensitivity $\Delta_{\mathcal{LR}}$ of mechanism $\mathcal{LR}$
set $\mathbf{d}^{(0)} = \mathbf{d}^{\text{init}}$, $k = 0$, and $\Delta_{\mathcal{LR}} = -\infty$
do
    set $\delta_j^{(k)} := \left\| \frac{\partial \mathcal{LR}(\mathbf{d}^{(k)})}{\partial (\mathbf{d}^{(k)})_j} \right\|_2, \;\; \forall j \in [N_E T]$
    set $j^* = \operatorname{argmax}_{j \in [N_E T]} \left\{ \delta_j^{(k)} \right\}$
    set $(\tilde{\mathbf{d}}^{(k)})_i := \begin{cases} (\mathbf{d}^k)_i & i \neq j^* \\ 1 - (\mathbf{d}^k)_i & i = j^* \end{cases}, \;\; \forall i \in [N_E T]$
    if $\tilde{\mathbf{d}}^{(k)}$ is $\mathcal{LR}$-feasible then
        set $\mathbf{d}^{(k+1)} = \tilde{\mathbf{d}}^{(k)}$
    else
        set $\mathbf{d}^{(k+1)} = \mathring{\mathbf{d}}$ where $\mathring{\mathbf{d}}$ satisfies
          $\widehat{\mathcal{LR}}(\tilde{\mathbf{d}}^{(k)}) = \mathcal{LR}(\mathring{\mathbf{d}})$
        set $\delta_{j^*}^{(k)} = -\infty$
    end
    if $\Delta_{\mathcal{LR}} < \delta_{j^*}^{(k)}$ then set $\Delta_{\mathcal{LR}} = \delta_{j^*}^{(k)}$
    set $k = k + 1$
while $\left\{ \left\| \mathcal{LR}(\mathbf{d}^{(k-1)}) - \mathcal{LR}(\mathbf{d}^{(k)}) \right\|_1 \geq \mathtt{tol} \right\}$;
return $\Delta_{\mathcal{LR}}$
```

A. Trust Architecture

To implement DP in a real system, identification of trusted as well as potentially adversarial agents within the system becomes paramount. In the context of the LR problem, we assume that the MGC, operated by the MGO, is a trusted arbiter for all MG participants. Furthermore, we assume that all problem parameters of (3) (except $\mathbf{d}$) are known to all participants in the MG. However, vector $\mathbf{d}$ is supposed to be the private data of the ESS operators. To protect the privacy of $\mathbf{d}$ by avoiding its inference from the optimal pickup $\mathbf{r}^*$, the MGC adds noise to it as stipulated by DP. This can be represented by the mechanism $\mathcal{M}^{\mathcal{LR}}(\mathbf{d}) := \mathcal{LR}(\mathbf{d}) + \mathbf{w}$. From Theorem 2, we see that for $\varepsilon > 0$, letting $(\mathbf{w})_i \sim \operatorname{Lap}\left(\frac{\Delta_{\mathcal{LR}}}{\varepsilon}\right)$ makes the mechanism $\mathcal{M}^{\mathcal{LR}}$ ε-DP, where

$$\Delta_{\mathcal{LR}} := \max_{\check{\mathbf{d}}, \check{\mathbf{d}}' \in \{0,1\}^{N_E T} : (\check{\mathbf{d}} \sim_1 \check{\mathbf{d}}')} \left\| \mathcal{LR}(\check{\mathbf{d}}) - \mathcal{LR}(\check{\mathbf{d}}') \right\|_1 . \tag{4}$$

The resulting $\tilde{\mathbf{r}} := \mathcal{M}^{\mathcal{LR}}(\mathbf{d})$ may not be $\mathcal{LR}$-feasible. Thus, we run a post-processing procedure $\mathcal{FR}(\tilde{\mathbf{r}})$ which yields a new pickup $\hat{\mathbf{r}}$, and a corresponding $\mathcal{LR}$-feasible $\hat{\mathbf{d}}$. The MGC then withdraws power from the ESSs according to $\hat{\mathbf{d}}$ and restores load according to $\hat{\mathbf{r}}$. By Theorems 1 and 2, $\mathcal{FR}(\mathcal{M}^{\mathcal{LR}}(\mathbf{d}))$ is ε-DP. Next, we will discuss the calculation of $\Delta_{\mathcal{LR}}$ and the feasibility restoration operator $\mathcal{FR}$.

B. Calculation of $\Delta_{\mathcal{LR}}$

Due to the structure of the pickup vector, we have $\Delta_{\mathcal{LR}} \leq N_L T$. However, setting $\Delta_{\mathcal{LR}} = N_L T$ is excessively conservative since this would require the existence of $\mathbf{d}' \sim_1 \mathbf{d}''$ such that $\mathcal{LR}(\mathbf{d}') = \mathbf{0}_{N_L T}$ and $\mathcal{LR}(\mathbf{d}'') = \mathbf{1}_{N_L T}$, which may

Algorithm 2: $\widehat{\mathcal{LR}}(\mathbf{d})$: Generation of $\mathcal{LR}$-Feasible Mode Vector

```
Input: mode vector $\mathbf{d}$
Output: $\widehat{\mathcal{LR}}(\mathbf{d}) := \mathcal{LR}(\mathbf{d}^{(u)})$ where $\mathbf{d}^{(u)}$ is $\mathcal{LR}$-feasible
set $\mathbf{d}^{(0)} = \mathbf{d}$ and $u = 0$
while $\mathbf{d}^{(u)}$ is not $\mathcal{LR}$-feasible do
    randomly select $j \in [N_E T]$ under uniform distribution
    $(\mathbf{d}^{(u+1)})_i := \begin{cases} (\mathbf{d}^{(u)})_i & i \neq j \\ 1 - (\mathbf{d}^{(u)})_i & i = j \end{cases}, \ \forall i \in [N_E T]$
    set $u = u + 1$
end
return $\mathcal{LR}(\mathbf{d}^{(k)})$
```

not exist. Therefore, we propose a heuristic for calculation of $\Delta_{\mathcal{LR}}$ in Algorithm 1. Given the mechanism $\mathcal{LR}$ and $\mathbf{d}^{\text{init}}$, the proposed algorithm generates a sequence of $\{\mathbf{d}^{(k)}\}_k$ wherein for a given $\mathbf{d}^{(k)}$, $\mathbf{d}^{(k+1)}$ is generated such as to increase the value of $h(\mathbf{d}^{(k)}, \mathbf{d}^{(k+1)}) := \left\| \mathcal{LR}(\mathbf{d}^{(k)}) - \mathcal{LR}(\mathbf{d}^{(k+1)}) \right\|_1$ while trying to ensure that $\mathbf{d}^{(k)} \sim_1 \mathbf{d}^{(k+1)}$. This is done by calculating $\delta_j^{(k)}$, which is the sensitivity of $\mathcal{LR}(\mathbf{d}^{(k)})$ to the j^{th} index of $\mathbf{d}^{(k)}$, for all $j \in [N_E T]$. This is followed by generation of an intermediate vector $\tilde{\mathbf{d}}^{(k)}$ by flipping the $j^{*\text{th}}$ bit of $\mathbf{d}^{(k)}$ where j^* is the index that maximizes $\delta_j^{(k)}$. If $\tilde{\mathbf{d}}^{(k)}$ is $\mathcal{LR}$-feasible, then $\mathbf{d}^{(k+1)}$ is set equal to $\tilde{\mathbf{d}}^{(k)}$ and $h(\mathbf{d}^{(k)}, \mathbf{d}^{(k+1)})$ is tested as a candidate for $\Delta_{\mathcal{LR}}$. If $\tilde{\mathbf{d}}^{(k)}$ is not $\mathcal{LR}$-feasible, Algorithm 2 is used to convert $\tilde{\mathbf{d}}^{(k)}$ into a $\mathcal{LR}$-feasible $\mathbf{d}^{(k+1)}$ by randomly flipping bits at various indices and checking for feasibility. However, $h(\mathbf{d}^{(k)}, \mathbf{d}^{(k+1)})$ is not tested as a candidate for $\Delta_{\mathcal{LR}}$ since $\mathbf{d}^{(k)} \sim_1 \mathbf{d}^{(k+1)}$ does not hold.

C. Feasibility Restoration Operator $\mathcal{FR}(\mathbf{r})$

For a given $\mathbf{r}$, the feasibility restoration operator $\mathcal{FR}(\mathbf{r})$ is defined by the following problem. It calculates the minimum-norm perturbation $\hat{\boldsymbol{\rho}} \in \mathbb{R}^{N_L T}$ such that $\mathbf{r} + \hat{\boldsymbol{\rho}}$ is feasible, i.e. $\mathcal{LR}(\hat{\mathbf{d}}) = \mathbf{r} + \hat{\boldsymbol{\rho}}$ for some mode vector $\hat{\mathbf{d}}$. Correspondingly, $\mathbf{r} + \hat{\boldsymbol{\rho}}$ is the actual pickup delivered by the MGC.

$$\mathcal{FR}(\mathbf{r}) := \hat{\mathbf{d}}, \hat{\boldsymbol{\rho}} \in \underset{\mathbf{d}, \boldsymbol{\rho}, \mathbf{p}^{\text{ch}}, \mathbf{p}^{\text{dis}}, \mathbf{p}, \mathbf{q}, \mathbf{P}, \mathbf{Q}, \mathbf{v}, \mathbf{l}, \mathbf{s}}{\operatorname{argmin}} \|\boldsymbol{\rho}\|_2 \tag{5}$$

$$\text{s.t. (3a)-(3c), (3f)-(3k)} \tag{5a}$$

$$\mathbf{0}_{N_L T} \leq \mathbf{r} + \boldsymbol{\rho} \leq \mathbf{1}_{N_L T} \tag{5b}$$

$$(\mathbf{r}_t)_j + (\boldsymbol{\rho}_t)_j \leq (\mathbf{r}_{t+1})_j + (\boldsymbol{\rho}_{t+1})_j, \quad \forall j \in [N_L], \forall t \in [T-1] \tag{5c}$$

$$\mathbf{d} \in \{0, 1\}^{N_E T}. \tag{5d}$$

(5) is a mixed-integer program, which may become intractable as the number of binary variables increases. However, many practical workarounds have been devised for efficiently solving mixed-integer problems, including branch-and-bound methods and continuous reformulations [17], which can be used for efficiently computing $\mathcal{FR}(\mathbf{r})$.

TABLE I
SIMULATION SETUP: SYSTEM PARAMETERS

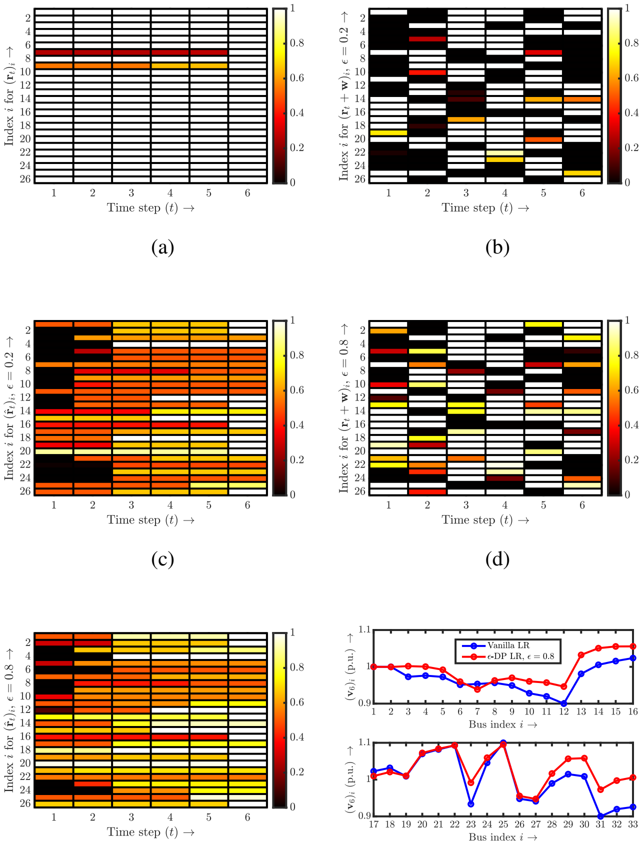
Parameter	Value
N_E, N_L, N, E	7, 26, 33, 32
$\underline{v}$, $\bar{v}$, $\bar{l}$	0.9 p.u, 1.1 p.u, ∞ (for all buses and lines)
$\mathcal{N}^{\text{ESS}}$	$\{2, 7, 12, 17, 23, 27, 31\}$
$\underline{s}$, $\bar{s}$, $\bar{p}^{\text{ch}}$, $\bar{p}^{\text{dis}}$	0.3594MWh, 3.5940MWh, 1.1980MW, 1.1980MW
Γ^{ch}, Γ^{dis}	0.90h, 1.11h

Note that for $\hat{\mathbf{d}}, \hat{\boldsymbol{\rho}} = \mathcal{FR}(\mathcal{M}^{\mathcal{LR}}(\mathbf{d}))$, in general $\hat{\mathbf{d}} \neq \mathbf{d}$, i.e. the mode vector implemented by the MGC is different from the one requested by ESS operators. This is a consequence of post-processing with $\mathcal{FR}$ which cannot use $\mathbf{d}$ to protect its privacy, and must instead only use $\mathcal{M}^{\mathcal{LR}}(\mathbf{d})$. Calculation of probabilistic guarantees on the accuracy of $\hat{\mathbf{d}}$ with respect to $\mathbf{d}$ is out of scope of the present work.

IV. SIMULATION RESULTS

In this section, we demonstrate the performance of differentially private LR through simulations. We use the 33-bus radial feeder test case 'case33bw' in MATPOWER [18], which prescribes network topology, branch parameters, and load demand, to emulate the MG. We consider a scenario with 7 ESSs having identical system parameters, which (alongside other values) are listed in Table I. For convex problems and the mixed-integer counterparts, the Gurobi solver [19] was used to find a solution, interfaced with MATLAB through CVX [20]. For the system under consideration, Algorithm 1 yielded the value $\Delta_{\mathcal{LR}} = 1.2863$. The generated mode vectors $\mathbf{d}^{(k)}$ were unique up to $k = 12$, and then started oscillating between two values on successive time steps. On no iteration k did the vector $\mathbf{d}^{(k)}$ fail to be $\mathcal{LR}$-feasible, and therefore the mechanism $\widehat{\mathcal{LR}}$ was never called.

We carry out simulation over 6 time steps, i.e. $T = 6$. Every element of $\mathbf{s}^{\text{init}}$ is chosen uniformly at random from $[0.7\bar{s}, 0.9\bar{s}]$ and then fixed for all simulations. The initial $\mathbf{d}$ is chosen from a binomial distribution with parameter 0.4. Figure 1a shows the pickup values for non-private LR, with most loads on all time steps receiving full load satisfaction. Figures 1b and 1d show the noisy pickup values for $\varepsilon = 0.2$ and $\varepsilon = 0.8$, respectively, while Figures 1c and 1e show the post-processed pickup values for said values of ε. Comparing Figures 1b and 1d, it is evident that a lower value of ε leads to addition of more noise to the LR output, thereby providing better privacy protection. The flip side of noise addition can be seen in the suboptimality of LR in the DP setting. Compared to Figure 1a, the pickup of loads in Figures 1c and 1e is lower, and this loss of LR performance can be viewed as a trade-off for privacy of the ESS mode vector. Furthermore, comparison of Figure 1b with Figure 1c (and Figure 1d with Fig 1e) clearly demonstrates the effectiveness of post-processing, as the post-processed pickups show monotonic load restoration. By contrast, the pickups without post-processing do not demonstrate the same. For $\varepsilon = 0.2$, the initial $\mathbf{d}$ differed from the implemented $\hat{\mathbf{d}}$ in



(a)

(b)

(c)

(d)

(e)

(f)

Fig. 1. The comparisons between non-private LR and DP-LR for different values of ε: (a) Pickup values for non-private LR; (b) and (d) Noisy pickup values before post-processing for $\varepsilon = 0.2, 0.8$, respectively; (c) and (e) Post-processed pickup values for $\varepsilon = 0.2, 0.8$, respectively; and (f) Nodal voltages for non-private LR and DP-LR for $\varepsilon = 0.8$.

29 out of 42 indices, while for $\varepsilon = 0.8$ they differed in 24 indices. This shows empirically that lower values of ε lead to a higher deviation of $\hat{\mathbf{d}}$ from $\mathbf{d}$.

Figure 1f compares the nodal voltage quantities under non-private LR with that of DP-LR on the last time step ($t = 6$). Again, the effectiveness of post-processing can be clearly seen, as the voltage profile in both cases respect the voltage upper and lower bounds over all time steps.

V. Conclusion

In this paper, we considered the emerging issue of differential privacy in load restoration for multi-user MGs. We designed a differentially private mechanism which ensures privacy of ESS charge/discharge mode by calculating the optimal pickup vector and then perturbing it with carefully chosen noise. We further proposed a post-processing step to restore feasibility, and validated our results through simulations. The simulations demonstrated empirically that there exists a tradeoff between privacy and LR performance. Topics of further research involve finding bounds on the accuracy of the proposed mechanism, and results which exploit the network structure and parameters.

References

[1] H. Haes Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, "A survey on power system blackout and cascading events: Research motivations and challenges," *Energies*, vol. 12, no. 4, 2019.

[2] G. Razeghi, F. Gu, R. Neal, and S. Samuelsen, "A generic microgrid controller: Concept, testing, and insights," *Applied Energy*, vol. 229, pp. 660–671, 2018.

[3] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, *Smart grids: security and privacy issues*. Springer, 2017.

[4] Q. Zhang, Y. Guo, Z. Wang, and F. Bu, "Distributed optimal conservation voltage reduction in integrated primary-secondary distribution systems," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3889–3900, 2021.

[5] Q. Zhang, K. Dehghanpour, Z. Wang, and Q. Huang, "A learning-based power management method for networked microgrids under incomplete information," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1193–1204, 2020.

[6] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 265–284.

[7] J.-Y. Park, J. Ban, Y.-J. Kim, and X. Lu, "Supplementary feedforward control of dgs in a reconfigurable microgrid for load restoration," *IEEE Transactions on Smart Grid*, pp. 1–1, 2021.

[8] F. Shen, Q. Wu, J. Zhao, W. Wei, N. D. Hatziargyriou, and F. Liu, "Distributed risk-limiting load restoration in unbalanced distribution systems with networked microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4574–4586, 2020.

[9] S. Cai, Y. Xie, Q. Wu, and Z. Xiang, "Robust mpc-based microgrid scheduling for resilience enhancement of distribution system," *International Journal of Electrical Power & Energy Systems*, vol. 121, p. 106068, 2020.

[10] Q. Zhang, Z. Ma, Y. Zhu, and Z. Wang, "A two-level simulation-assisted sequential distribution system restoration model with frequency dynamics constraints," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 3835–3846, 2021.

[11] S. Yao, J. Gu, H. Zhang, P. Wang, X. Liu, and T. Zhao, "Resilient load restoration in microgrids considering mobile energy storage fleets: A deep reinforcement learning approach," in *2020 IEEE Power Energy Society General Meeting (PESGM)*, 2020, pp. 1–5.

[12] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2017.

[13] F. Zhou, J. Anderson, and S. H. Low, "Differential privacy of aggregated dc optimal power flow data," in *2019 American Control Conference (ACC)*, 2019, pp. 1307–1314.

[14] V. Dvorkin, F. Fioretto, P. Van Hentenryck, P. Pinson, and J. Kazempour, "Differentially private optimal power flow for distribution grids," *IEEE Transactions on Power Systems*, vol. 36, no. 3, pp. 2186–2196, 2021.

[15] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy." *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.

[16] L. Gan, N. Li, U. Topcu, and S. H. Low, "Exact convex relaxation of optimal power flow in radial networks," *IEEE Transactions on Automatic Control*, vol. 60, no. 1, pp. 72–87, 2015.

[17] S. A. Gabriel, M. Leal, and M. Schmidt, "Solving binary-constrained mixed complementarity problems using continuous reformulations," *Computers & Operations Research*, vol. 131, p. 105208, 2021.

[18] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.

[19] Gurobi Optimization, LLC, "Gurobi Optimizer Reference Manual," 2021. [Online]. Available: https://www.gurobi.com

[20] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Mar. 2014.