2018 IEEE Conference on Decision and Control (CDC)
Miami Beach, FL, USA, Dec. 17-19, 2018

A Differentially Private Distributed Solution Approach to the Model Predictive Control of Building Clusters

Yingying Xiao, Xiaodong Hou, Jie Cai, and Jianghai Hu

Abstract— **Coordinated control of a cluster of buildings can lead to reduced energy usage and demand charge. However, it requires individual buildings to share local data, e.g., their energy demands. The leak of such data could potentially be used by third parties to infer sensitive information such as occupancy that could be used to the detriment of building occupants. In this paper, using the notion of differential privacy, a distributed algorithm based on the Alternating Direction Method of Multiplier (ADMM) algorithm is proposed for the coordinated control of building clusters that can provide guaranteed levels of privacy for individual buildings by adding noises to the data being exchanged. Theoretical bounds on the strength of noises needed to achieve given privacy levels are derived, and the performance suboptimality caused by the added noise is demonstrated through simulations.**

I. INTRODUCTION

According to the 2016 report from the U.S. Energy Information Administration [1], [2], buildings account for about 40% of the primary energy consumption and 75% of the electricity use within U.S. To reduce building energy consumption, a popular approach is the model predictive control (MPC) method [3], [4] as it can incorporate weather forecast, occupancy, lighting, etc., into controller design. For building systems with a large number of subsystems (buildings in the building clusters, thermal zones in individual buildings, and shared heating, ventilation and air-conditioning (HVAC) subsystems), the coordinated control of building subsystems could lead to significant energy saving while, however, the optimization problems that need to be solved on-line by MPC methods can become intractable.

Agent-based distributed algorithms provide a viable strategy for building clusters' coordination control as they are scalable and require lower engineering and implementation costs. Examples include the token-based scheduling [5], Nash-optimization enhanced algorithm [6], dual decomposition [7], ADMM-based algorithms [8], [9] and dynamic programming based approaches [10], to name a few. A common feature of these algorithms is that each agent (building, thermal zone, HVAC equipment, etc.) needs to share its data with other agents or the central coordinator to achieve collective control (sub)optimality. However, in many cases, the shared data contain (at least implicitly) sensitive information that, if leaked, could violate the privacy of or even bring harms to the agent. For example, to reduce peak demand, an individual building may be asked to release its energy usage data, which can be potentially exploited by a third party or an adversary to infer this building's occupancy profile.

The notion of *differential privacy* was originally proposed in the static database field [11], [12], [13]. Different from cryptography, differential privacy has a continuous rather than binary characterization of privacy, and differential privacy mechanisms that randomize private information by adding noises can guarantee privacy even when the adversary has all the side information [14], [15]. Recently, differential privacy has also been applied to control problems, e.g., filtering problem [16], electric vehicle charging schedule problem [17], distributed optimization problem [18], [19], consensus problem [20], [21], and distributed control [22].

In this paper, we study the differential privacy mechanisms for the agent-based MPC of building clusters with the objective to reduce the energy consumption and demand charge as well as maintain the privacy of individual building. The proposed solutions can also be applied to a single building with multiple thermal zones. Although the thermal dynamics are decoupled across different buildings, the objective function representing the total electricity bill depends on the decisions of all buildings. In the proposed agent-based solution framework, each building is represented by an agent responsible for maintaining local comfort; a central coordinating agent (coordinator) is responsible for information aggregation and for reducing the overall energy usage and demand charge. The solution algorithm is adapted from the ADMM algorithm, which requires constant information exchanges between building agents

This material is based upon work supported by the National Science Foundation under Grant No. 1329875.

Y. Xiao, X. Hou, and J. Hu are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907, USA {xiao106,hou39,jianghai}@purdue.edu.

J. Cai is with the School of Aerospace and Mechanical Engineering, University of Oklahoma, Norman, OK 73019, USA jcai@ou.edu.

978-1-5386-1394-8/18/$31.00 ©2018 IEEE

and the coordinator. For each building, its desired level of privacy can be ensured by adding noises of proper strength to its shared information. The required noise strength is determined via a sensitivity analysis of the shared information w.r.t. the private information.

The remainder of this paper is organized as follows. The MPC problem formulation and a distributed solution algorithm are described in Section II. Section III presents the differential privacy mechanism and the associated distributed algorithm. The results of a case study are given in Section IV. Section V concludes the paper.

Notation: For any integer $m \geq 1$, $\mathcal{I}_m$ denotes the index set $\{1, \ldots, m\}$ and $(x_i)_{i \in \mathcal{I}_m}$ is the column stack of all x_i's, $i \in \mathcal{I}_m$. We use $\mathbf{1}$ to denote the vector of proper size with all entries equal to 1, I for the identity matrix, $\| \cdot \|_2$ and $\| \cdot \|_\infty$ for the L_2 and L_∞ norm, respectively. Given a finite set S, its cardinality is represented as $|S|$. And $[A]_{ij}$ denotes matrix A's entry on the i-th row and j-th column. The "$\leq$" and "$\geq$" always represent entry-wise comparison.

II. MPC PROBLEM FORMULATION

In this section, the problem of building cluster control is formulated, and a distributed solution strategy without considering privacy is proposed. These results can also be applied to the problem of multi-zone building control.

A. Building cluster control as an optimization problem

Consider a building cluster consisting of multiple buildings indexed by $\mathcal{I}_m$ that are thermally decoupled but served by the same chiller. We consider cooling seasons only, as heating efficiency is relatively constant w.r.t. control strategies. For each building $i \in \mathcal{I}_m$, its thermal dynamics is given by

$$\begin{aligned} x_i(t+1) &= A_i x_i(t) - B_i u_i(t) + F_i w_i(t), \\ y_i(t) &= C_i x_i(t), \quad t = 0, 1, \ldots, \end{aligned}$$

where the state $x_i \in \mathbb{R}^{n_i}$ includes the temperatures of all thermal nodes, the output $y_i \in \mathbb{R}$ is the indoor air temperature, the controllable input $u_i \in \mathbb{R}$ represents the local sensible cooling supplied to building i, and the uncontrollable input w_i contains the (predicted) perturbations such as weather conditions. Note that different buildings are assumed to be thermally decoupled.

Given the prediction time horizon N, the problem is to minimize the building cluster's utility bill of electricity usage and demand charge during the predicted period while satisfying comfort and capacity constraints, formulated as follows:

$$\begin{aligned} \underset{\boldsymbol{u}_i,\, i \in \mathcal{I}_m}{\text{minimize}} \quad & r_{\text{elec}} \Big\| \sum_i \boldsymbol{u}_i \Big\|_2^2 + r_{\text{dem}} \Big\| \sum_i \boldsymbol{u}_i \Big\|_\infty^2 && \text{(1a)} \\ \text{subject to} \quad & \boldsymbol{y}_i = \boldsymbol{A}_i x_i(0) - \boldsymbol{B}_i \boldsymbol{u}_i + \boldsymbol{F}_i \boldsymbol{w}_i, && \text{(1b)} \\ & |\boldsymbol{y}_i - \boldsymbol{y}_{i,\text{set}}| \leq \boldsymbol{\tau}_i && \text{(1c)} \\ & \boldsymbol{u}_i \geq 0, \qquad i \in \mathcal{I}_m, && \text{(1d)} \\ & \sum_i \boldsymbol{u}_i \leq u_{\text{cap}} \mathbf{1}. && \text{(1e)} \end{aligned}$$

Here, $\boldsymbol{u}_i$ (resp. $\boldsymbol{w}_i$) is the stacked vector of $u_i(t)$ (resp. $w_i(t)$) for $t = 0, \ldots, N-1$; $\boldsymbol{y}_i$ (resp. $\boldsymbol{y}_{i,set}$) is the stacked vector of air temperature $y_i(t)$ (resp. its setpoint $y_{i,set}(t)$) for $t = 1, \ldots, N$; $\boldsymbol{A}_i$, $\boldsymbol{B}_i$ and $\boldsymbol{F}_i$ are matrices of proper sizes derived from building i's thermal dynamics. The constraints are induced from dynamics (1b), comfort (1c) with $\boldsymbol{\tau}_i$ specifying the maximum acceptable temperature deviation from its setpoint, and the chiller's cooling capacity (1e). During occupied hours, the corresponding entries in $\boldsymbol{\tau}_i$ are assigned a small value $\tau_{i,\text{in}} > 0$ to ensure indoor comfort delivery; in unoccupied periods, a larger value $\tau_{i,\text{out}} > \tau_{i,\text{in}}$ is used for energy saving. Thus, building i's occupancy determines $\boldsymbol{\tau}_i$, which further affects the solution $\boldsymbol{u}_i$ to the optimization problem (1).

In formulation (1), the two terms in the objective function correspond to bills from the electricity consumption at the price r_{elec} \$/kWh and the demand charge at the rate r_{dem} \$/kW, respectively. For simplicity, the chiller's power consumption is assumed to be a quadratic function of its total cooling load; however, the results can be easily extended to the cases of general convex functions. Typically, the demand rate r_{dem} is tens or even up to a hundred times of r_{elec} according to the survey in [23]. Thus, a smaller peak value may be preferred even at the expense of higher total electricity consumption.

Remark 1: By plugging the dynamics constraint (1b) into the comfort constraint (1c), the optimization problem (1) becomes a convex minimization problem with only linear inequality constraints.

B. Distributed solution using ADMM Algorithm

In problem (1), the constraints (1b)-(1d) are local, which together specify a local feasible set $\mathcal{F}_i$ for agent i's variable $\boldsymbol{u}_i$, while the constraint (1e) couples all the agents. By introducing copies $\boldsymbol{z}_i$ of each $\boldsymbol{u}_i$, problem (1) is equivalent to:

$$\begin{aligned} \underset{\boldsymbol{u}_i,\, \boldsymbol{z}_i,\, \forall i \in \mathcal{I}_m}{\text{minimize}} \quad & \sum_i f_i(\boldsymbol{u}_i) + g\Big(\sum_i \boldsymbol{z}_i \Big) \\ \text{subject to} \quad & \boldsymbol{u}_i = \boldsymbol{z}_i, \quad \forall i \in \mathcal{I}_m. \end{aligned}$$

Here, f_i is the convex indicator function of $\mathcal{F}_i$ that takes the value 0 on $\mathcal{F}_i$ and the value ∞ outside of it, and

$$g(\boldsymbol{p}) = r_{\text{elec}} \left\|\boldsymbol{p}\right\|_2^2 + r_{\text{dem}} \left\|\boldsymbol{p}\right\|_\infty^2$$

whose domain $\mathbf{dom}\, g = \{\boldsymbol{p} \,|\, \mathbf{0} \le \boldsymbol{p} \le u_{\text{cap}}\mathbf{1}\}$ is given by the chiller's capacity constraint (1e).

Applying the scaled ADMM algorithm [24] to the above problem, we obtain the iterations:

$$\begin{aligned} \boldsymbol{u}_i^{k+1} &= \Pi_{\mathcal{F}_i}(\boldsymbol{z}_i^k - \boldsymbol{\nu}_i^k),\ \forall i \in \mathcal{I}_m, && \text{(2a)} \\ \boldsymbol{z}^{k+1} &= \underset{\boldsymbol{z}_i,\, i \in \mathcal{I}_m}{\operatorname{argmin}} \Big\{ g\Big(\sum_i \boldsymbol{z}_i\Big) \\ &\qquad + \frac{\rho}{2}\sum_i \|\boldsymbol{z}_i - \boldsymbol{u}_i^{k+1} - \boldsymbol{\nu}_i^k\|_2^2 \Big\}, && \text{(2b)} \\ \boldsymbol{\nu}_i^{k+1} &= \boldsymbol{\nu}_i^k + \boldsymbol{u}_i^{k+1} - \boldsymbol{z}_i^{k+1},\ \forall i \in \mathcal{I}_m, && \text{(2c)} \end{aligned}$$

where $\rho > 0$ is an algorithm parameter and $\Pi_{\mathcal{F}_i}$ denotes the orthogonal projection operator onto the set $\mathcal{F}_i$.

The $\boldsymbol{u}$-update (2a) and $\boldsymbol{\nu}$-update (2c) can be efficiently computed in parallel while the $\boldsymbol{z}$-update (2b) requires collecting information from every agent and solving a high dimensional optimization problem. Next we use a procedure from [24] to simplify this step.

With $\boldsymbol{a}_i := \boldsymbol{u}_i^{k+1} + \boldsymbol{\nu}_i^k$ and $\bar{\boldsymbol{a}} := \sum_i \boldsymbol{a}_i/m$, the $\boldsymbol{z}$-update becomes

$$\begin{aligned} \underset{\bar{\boldsymbol{z}},\,(\boldsymbol{z}_i)_{i\in\mathcal{I}_m}}{\text{minimize}} \quad & g(m\bar{\boldsymbol{z}}) + \frac{\rho}{2}\sum_i \|\boldsymbol{z}_i - \boldsymbol{a}_i\|_2^2 \\ \text{subject to} \quad & m\bar{\boldsymbol{z}} = \sum_i \boldsymbol{z}_i. \end{aligned}$$

When $\bar{\boldsymbol{z}}$ is fixed, minimizing the second term in the objective function will result in

$$\boldsymbol{z}_i = \boldsymbol{a}_i - \bar{\boldsymbol{a}} + \bar{\boldsymbol{z}}. \tag{3}$$

Then the $\boldsymbol{z}$-update is reduced to minimize $g(m\bar{\boldsymbol{z}}) + (\rho m)/2\|\bar{\boldsymbol{z}} - \bar{a}\|_2^2$ with the decision variable $\bar{\boldsymbol{z}}$. After obtaining $\bar{\boldsymbol{z}}^{k+1}$, we have $\boldsymbol{z}_i^{k+1} = \big(\boldsymbol{u}_i^{k+1} + \boldsymbol{\nu}_i^k\big) - \big(\bar{\boldsymbol{u}}^{k+1} + \bar{\boldsymbol{\nu}}^k\big) + \bar{\boldsymbol{z}}^{k+1}$ as a consequence of (3). Therefore the corresponding $\boldsymbol{\nu}$-update becomes

$$\boldsymbol{\nu}^{k+1} = \bar{\boldsymbol{\nu}}^k + \bar{\boldsymbol{u}}^{k+1} - \bar{\boldsymbol{z}}^{k+1}.$$

Since all $\boldsymbol{\nu}_i^{k+1}$ are equal, we simply denote them by $\bar{\boldsymbol{\nu}}^{k+1}$. In sum, the iterations (2) can be simplified to

$$\begin{aligned} \boldsymbol{u}_i^{k+1} &= \Pi_{\mathcal{F}_i}(\boldsymbol{u}_i^k - \bar{\boldsymbol{u}}^k + \bar{\boldsymbol{z}}^k - \bar{\boldsymbol{\nu}}^k),\ \forall i \in \mathcal{I}_m && \text{(4a)} \\ \bar{\boldsymbol{z}}^{k+1} &= \underset{\bar{\boldsymbol{z}}}{\operatorname{argmin}} \Big\{ g\big(m\bar{\boldsymbol{z}}\big) + \frac{\rho m}{2}\|\bar{\boldsymbol{z}} - \bar{\boldsymbol{u}}^{k+1} - \bar{\boldsymbol{\nu}}^k\|_2^2 \Big\} && \text{(4b)} \\ \bar{\boldsymbol{\nu}}^{k+1} &= \bar{\boldsymbol{\nu}}^k + \bar{\boldsymbol{u}}^{k+1} - \bar{\boldsymbol{z}}^{k+1}, && \text{(4c)} \end{aligned}$$

where $\bar{\boldsymbol{u}} := \sum_i \boldsymbol{u}_i/m$, $\bar{\boldsymbol{z}}$ and $\bar{\boldsymbol{\nu}}$ have the same dimension as $\bar{\boldsymbol{u}}$. Note that the $\boldsymbol{u}$-update (4a) can be carried out locally while the $\bar{\boldsymbol{z}}$- and $\bar{\boldsymbol{\nu}}$-updates must be computed by the coordinator agent. See Algorithm 1 for details.

Algorithm 1 Distributed ADMM Algorithm

```
Initialize $\boldsymbol{u}^0$, $\bar{\boldsymbol{z}}^0$, $\bar{\boldsymbol{\nu}}^0$, and let $k \leftarrow 0$;
Coordinator broadcasts $\bar{\boldsymbol{u}}^0 - \bar{\boldsymbol{z}}^0 + \bar{\boldsymbol{\nu}}^0$ to all agents;
repeat
    for all $i \in \mathcal{I}_m$ do
        Agent $i$ computes $\boldsymbol{u}_i^{k+1}$ according to (4a) ;
    end for
    Coordinator collects $\boldsymbol{u}^{k+1}$ and computes $\bar{\boldsymbol{u}}^{k+1}$;
    Coordinator updates $\bar{\boldsymbol{z}}^{k+1}$ and $\bar{\boldsymbol{\nu}}^{k+1}$ by (4b)-(4c);
    Coordinator broadcasts $\bar{\boldsymbol{u}}^{k+1} - \bar{\boldsymbol{z}}^{k+1} + \bar{\boldsymbol{\nu}}^{k+1}$;
    $k \leftarrow k + 1$;
until certain convergence criteria are met
Return $\boldsymbol{u}_i^k$ for $i \in \mathcal{I}_m$.
```

III. DIFFERENTIALLY PRIVATE DISTRIBUTED SOLUTION

In Algorithm 1, each building agent i needs to transmit its local solution $\boldsymbol{u}_i$ to the coordinator at each iteration. By (4a), $\boldsymbol{u}_i$ is obtained by projecting onto the local feasible set $\mathcal{F}_i$ given by the constraints (1b)-(1d). As the comfort constraint (1c) depends on $\boldsymbol{\tau}_i$, so do $\mathcal{F}_i$ and the updated $\boldsymbol{u}_i$. As a result, the transmitted $\boldsymbol{u}_i$ by agent i contains information on $\boldsymbol{\tau}_i$ and ultimately the occupancy of building i. If the data $\boldsymbol{u}_i$ is compromised, e.g., due to inadvertent leaks or unauthorized access, a third party (which could be the coordinator, another building, or an external adversary) may be able to infer building i's occupancy. To prevent this, we adopt the differential privacy (DP) mechanism, where agent i transmits a noisy version $\tilde{\boldsymbol{u}}_i$ of $\boldsymbol{u}_i$ with sufficient noises such that an eavesdropper is incapable of figuring out whether building i is occupied or not at any time instant even with access to any side information such as $\boldsymbol{u}_i$.

A. Differentially private distributed solution algorithm

For our problem, the differential privacy mechanism randomizes the local information $\boldsymbol{u}_i$ as follows,

$$\mathcal{M}_i : \boldsymbol{u}_i \mapsto \tilde{\boldsymbol{u}}_i = \boldsymbol{u}_i + \boldsymbol{\eta}_i, \tag{5}$$

where $\tilde{\boldsymbol{u}}_i$ is the noisy information sent from agent i to the coordinator, and the random variable $\boldsymbol{\eta}_i \sim \mathcal{N}(0, \sigma_i^2 I_N)$ is the Gaussian noise added by agent i. The variance σ_i^2 will be determined later on. As $\boldsymbol{u}_i$ depends on $\boldsymbol{\tau}_i$, we can write $\mathcal{M}_i(\boldsymbol{u}_i)$ as $\mathcal{M}_i(\boldsymbol{\tau}_i)$. With differential privacy mechanism (5), the following Algorithm 2 can be obtained from Algorithm 1, which in general does not converge to any single point because of the random noises added.

Algorithm 2 Differentially Private Distributed ADMM Algorithm

```
Input $K$, $\sigma_i$;
Initialize $\boldsymbol{u}^0$, $\bar{\boldsymbol{z}}^0$, $\bar{\boldsymbol{\nu}}^0$, let $k \leftarrow 0$;
Coordinator broadcasts $\bar{\boldsymbol{u}}^0 - \bar{\boldsymbol{z}}^0 + \bar{\boldsymbol{\nu}}^0$;
repeat
  for all $i \in \mathcal{I}_m$ do
    Agent $i$ computes $\boldsymbol{u}_i^{k+1}$ according to (4a);
    Agent $i$ obtains $\tilde{\boldsymbol{u}}_i^{k+1}$ according to (5);
  end for
  Coordinator collects $\tilde{\boldsymbol{u}}^{k+1}$;
  Coordinator computes $\bar{\boldsymbol{u}}^{k+1} = \sum_i \tilde{\boldsymbol{u}}_i^{k+1}/m$;
  Coordinator updates $\bar{\boldsymbol{z}}^{k+1}$ and $\bar{\boldsymbol{\nu}}^{k+1}$ by (4b)-(4c);
  Coordinator broadcasts $\bar{\boldsymbol{u}}^{k+1} - \bar{\boldsymbol{z}}^{k+1} + \bar{\boldsymbol{\nu}}^{k+1}$;
  $k \leftarrow k + 1$;
until $k = K + 1$
Return $\boldsymbol{u}_i^k$.
```

The rest of this section will focus on finding the proper noise variance to achieve a given privacy level. First we present several standard definitions on differential privacy tailored to our problem.

Definition 1 (Adjacency): Two datasets $\boldsymbol{\tau}_i, \boldsymbol{\tau}_i' \in \mathbb{R}^N$ are called adjacent, denoted by Adj$(\boldsymbol{\tau}_i, \boldsymbol{\tau}_i')$, if and only if there exists $t \in \mathcal{I}_N$ such that $|[\boldsymbol{\tau}_i]_t - [\boldsymbol{\tau}_i']_t| \geq \beta_i$ and $[\boldsymbol{\tau}_i]_s = [\boldsymbol{\tau}_i']_s$ for all $s \neq t$.

The difference β_i determines the privacy granularity of the datasets that need to be protected. For the occupancy schedule $\boldsymbol{\tau}_i$ in the building cluster control problem, we can choose $0 < \beta_i < \tau_{i,\text{out}} - \tau_{i,\text{in}}$. Thus, two occupancy schedules are adjacent if and only if they have different occupancy at exactly one time instant. The objective is to make adjacent $\boldsymbol{\tau}_i$ and $\boldsymbol{\tau}_i'$ statistically almost indistinguishable based on the information $\tilde{\boldsymbol{u}}_i$.

Definition 2 (Differential Privacy): Given $\epsilon_i, \delta_i > 0$, a mechanism $\mathcal{M}_i$ is (ϵ_i, δ_i)-differentially private if and only if for any Adj$(\boldsymbol{\tau}_i, \boldsymbol{\tau}_i')$ and any subset $\mathcal{R}$ of $\mathbb{R}^N$,

$$\mathbb{P}(\mathcal{M}_i(\boldsymbol{\tau}_i) \in \mathcal{R}) \leq e^{\epsilon_i}\mathbb{P}(\mathcal{M}_i(\boldsymbol{\tau}_i') \in \mathcal{R}) + \delta_i,$$

where $\mathbb{P}$ is the probability in the given probability space.

Definition 3: (l_2-sensitivity) For a query $q_i : \boldsymbol{\tau}_i \mapsto \boldsymbol{u}_i$, its l_2-sensitivity under the adjacency relation Adj$(\boldsymbol{\tau}_i, \boldsymbol{\tau}_i')$ is defined as

$$\Delta_i := \max_{\text{Adj}(\boldsymbol{\tau}_i, \boldsymbol{\tau}_i')} \|q_i(\boldsymbol{\tau}_i) - q_i(\boldsymbol{\tau}_i')\|_2.$$

Define $\mathcal{Q}(x) := (1/\sqrt{2\pi})\int_x^\infty e^{\frac{-u^2}{2}} du$. We cite the following key result without proof.

Theorem 1 ([16]): Given $\epsilon_i > 0$, $0 < \delta_i < \frac{1}{2}$, the Gaussian mechanism $\mathcal{M}_i$ in (5) is (ϵ_i, δ_i)-differentially private if $\boldsymbol{\eta}_i \sim \mathcal{N}(0, \sigma_i^2 I_N)$ with

$$\sigma_i \geq \frac{\Delta_i}{2\epsilon_i}\big(M + \sqrt{M^2 + 2\epsilon_i}\big), \tag{6}$$

where Δ_i is the l_2-sensitivity of $\boldsymbol{u}_i$ w.r.t. $\boldsymbol{\tau}_i$ and $M = \mathcal{Q}^{-1}(\delta_i)$.

Theorem 1 provides a lower bound on the variance of the added noises to guarantee the (ϵ_i, δ_i)-privacy of $\boldsymbol{\tau}_i$.

B. l_2-sensitivity of local solution to occupancy schedule

With $\boldsymbol{b}_i^k := \boldsymbol{u}_i^k - \bar{\boldsymbol{u}}^k + \bar{\boldsymbol{z}}^k - \boldsymbol{\nu}^k$, the local update (4a) by agent i is obtained by solving the following problem:

$$\begin{aligned} \underset{\boldsymbol{u}_i}{\text{minimize}} \quad & \|\boldsymbol{u}_i - \boldsymbol{b}_i^k\|_2^2 \\ \text{s.t.} \quad & \boldsymbol{c}_i - \boldsymbol{\tau}_i \leq \boldsymbol{B}_i \boldsymbol{u}_i \leq \boldsymbol{c}_i + \boldsymbol{\tau}_i, \\ & \boldsymbol{u}_i \geq 0, \end{aligned} \tag{7}$$

where $\boldsymbol{c}_i = \boldsymbol{A}_i x_i(0) + \boldsymbol{F}_i \boldsymbol{w}_i - \boldsymbol{y}_{i,\text{set}}$ and

$$\boldsymbol{B}_i = \begin{bmatrix} C_i B_i & 0 & \cdots & 0 \\ C_i A_i B_i & C_i B_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_i A_i^{N-1} B_i & C_i A_i^{N-2} B_i & \cdots & C_i B_i \end{bmatrix},$$

or equivalently,

$$\begin{aligned} \underset{\boldsymbol{u}_i}{\text{minimize}} \quad & \tfrac{1}{2}\|\boldsymbol{u}_i - \boldsymbol{b}_i^k\|_2^2 \\ \text{s.t.} \quad & \underbrace{\begin{bmatrix} \boldsymbol{B}_i \\ -\boldsymbol{B}_i \\ -I \end{bmatrix}}_{\boldsymbol{\Phi}_i} \boldsymbol{u}_i \leq \underbrace{\begin{bmatrix} \boldsymbol{c}_i \\ -\boldsymbol{c}_i \\ 0 \end{bmatrix}}_{\mathbf{C}_i} + \underbrace{\begin{bmatrix} \boldsymbol{\tau}_i \\ -\boldsymbol{\tau}_i \\ 0 \end{bmatrix}}_{\mathbf{T}_i}, \end{aligned} \tag{8}$$

where $\boldsymbol{\Phi}_i \in \mathbb{R}^{3N \times N}$, $\mathbf{C}_i \in \mathbb{R}^{3N}$ and $\mathbf{T}_i \in \mathbb{R}^{3N}$.

The following result provides an upper bound on the sensitivity of $\boldsymbol{u}_i$ w.r.t. $\boldsymbol{\tau}_i$.

Proposition 1: Suppose the local optimization problem (4a) or (8) for agent i is always feasible. Then

$$\Delta_i \leq \frac{\tau_{i,\text{out}} - \tau_{i,\text{in}}}{\sigma_i}.$$

Here, $\sigma_i := \min_{\mathcal{A} \subset \mathcal{I}_{3N}}\{\sigma_{i,\mathcal{A}}\}$ where $\sigma_{i,\mathcal{A}}$ denotes the smallest (nonzero) singular value of the matrix $\boldsymbol{\Phi}_{i,\mathcal{A}}$ consisting of those rows of $\boldsymbol{\Phi}_i$ indexed by the subset $\mathcal{A} \subset \mathcal{I}_{3N}$.

Proof: Let $\boldsymbol{\tau}_i$ and $\boldsymbol{\tau}_i'$ be arbitrary such that Adj$(\boldsymbol{\tau}_i, \boldsymbol{\tau}_i')$. Denote by $\boldsymbol{u}_i$ and $\boldsymbol{u}_i'$ the corresponding solutions of problem (8), respectively. Define $\Delta \boldsymbol{u}_i := \boldsymbol{u}_i' - \boldsymbol{u}_i$ and

$$\Delta \mathbf{T}_i := \mathbf{T}_i' - \mathbf{T}_i = \begin{bmatrix} \boldsymbol{\tau}_i' - \boldsymbol{\tau}_i \\ -(\boldsymbol{\tau}_i' - \boldsymbol{\tau}_i) \\ 0 \end{bmatrix}.$$

We next find an upper bound of $\|\Delta \boldsymbol{u}_i\|_2$.

Since Problem (8) is assumed to be feasible, its solution $\boldsymbol{u}_i$ under the given $\boldsymbol{\tau}_i$ satisfies the KKT condition

$$\frac{\partial \mathcal{L}}{\partial \boldsymbol{u}_i} = \boldsymbol{u}_i - \boldsymbol{b}_i^k + \boldsymbol{\Phi}_i^\top \lambda_i = 0, \quad \text{(9a)}$$

$$\forall l \in \mathcal{I}_{3N}, \quad [\lambda_i]_l \left[\boldsymbol{\Phi}_i \boldsymbol{u}_i - \mathbf{C}_i - \mathbf{T}_i\right]_l = 0, \quad \text{(9b)}$$

$$\boldsymbol{\Phi}_i \boldsymbol{u}_i - \mathbf{C}_i - \mathbf{T}_i \leq 0, \quad \text{(9c)}$$

$$\lambda_i \geq 0, \quad \text{(9d)}$$

where $\mathcal{L}$ is the Lagrange function defined by

$$\mathcal{L}(\boldsymbol{u}_i, \lambda_i) = \frac{1}{2}\|\boldsymbol{u}_i - \boldsymbol{b}_i^k\|_2^2 + \lambda_i^\top \left(\boldsymbol{\Phi}_i \boldsymbol{u}_i - \mathbf{C}_i - \mathbf{T}_i\right).$$

The equation (9a) implies that

$$\boldsymbol{u}_i = \boldsymbol{b}_i^k - \boldsymbol{\Phi}_i^\top \lambda_i = \boldsymbol{b}_i^k - \boldsymbol{\Phi}_{i,\mathcal{A}}^\top \lambda_{i,\mathcal{A}}. \quad (10)$$

Here, $\mathcal{A} \subset \mathcal{I}_{3N}$ is the active pattern consisting of those indices at which λ_i has positive entries, and $\lambda_{i,\mathcal{A}}$ (resp. $\boldsymbol{\Phi}_{i,\mathcal{A}}$) consists of those entries of λ_i (resp. $\boldsymbol{\Phi}_i$) corresponding to $\mathcal{A}$. By the complementary slackness condition (9b), we must have

$$\boldsymbol{\Phi}_{i,\mathcal{A}} \boldsymbol{u}_i = \mathbf{C}_{i,\mathcal{A}} + \mathbf{T}_{i,\mathcal{A}}. \quad (11)$$

Without loss of generality, we assume that the active pattern $\mathcal{A}$ remains unchanged as $\mathbf{T}_i$ is gradually perturbed to become $\mathbf{T}_i'$, for otherwise we can break up the perturbation process into a finite number of stages each of which has a constant $\mathcal{A}$. As the upper bound we are about to develop applies for arbitrary $\mathcal{A}$, it provides a uniform bound over the whole perturbation process.

By the above assumption, we also have

$$\boldsymbol{u}_i' = \boldsymbol{b}_i^k - \boldsymbol{\Phi}_{i,\mathcal{A}}^\top \lambda_{i,\mathcal{A}}',$$
$$\boldsymbol{\Phi}_{i,\mathcal{A}} \boldsymbol{u}_i' = \mathbf{C}_{i,\mathcal{A}} + \mathbf{T}_{i,\mathcal{A}}'.$$

Substracting (10) and (11), we obtain

$$\Delta \boldsymbol{u}_i = -\boldsymbol{\Phi}_{i,\mathcal{A}}^\top \Delta \lambda_{i,\mathcal{A}}, \quad \text{(12a)}$$

$$\boldsymbol{\Phi}_{i,\mathcal{A}} \Delta \boldsymbol{u}_i = \Delta \mathbf{T}_{i,\mathcal{A}}, \quad \text{(12b)}$$

where $\Delta\lambda_{i,\mathcal{A}} := \lambda_{i,\mathcal{A}}' - \lambda_{i,\mathcal{A}}$. Suppose $\boldsymbol{\Phi}_{i,\mathcal{A}}$ has rank $r_{i,\mathcal{A}}$ and the singular value decomposition $\boldsymbol{\Phi}_{i,\mathcal{A}} = U_{i,\mathcal{A}} \Sigma_{i,\mathcal{A}} V_{i,\mathcal{A}}^\top$, where $U_{i,\mathcal{A}} \in \mathbb{R}^{|\mathcal{A}| \times r_{i,\mathcal{A}}}$ and $V_{i,\mathcal{A}} \in \mathbb{R}^{3N \times r_{i,\mathcal{A}}}$ have orthonormal columns, and $\Sigma_{i,\mathcal{A}} \in \mathbb{R}^{r_{i,\mathcal{A}} \times r_{i,\mathcal{A}}}$ is diagonal with diagonal entries being the nonzero singular values of $\boldsymbol{\Phi}_{i,\mathcal{A}}$. Let $\boldsymbol{\Phi}_{i,\mathcal{A}}^\dagger = V_{i,\mathcal{A}} \Sigma_{i,\mathcal{A}}^{-1} U_{i,\mathcal{A}}^\top$ be the Moore-Penrose inverse of $\boldsymbol{\Phi}_{i,\mathcal{A}}$. Then $\boldsymbol{\Phi}_{i,\mathcal{A}}^\dagger \boldsymbol{\Phi}_{i,\mathcal{A}} = V_{i,\mathcal{A}} V_{i,\mathcal{A}}^\top$ is the orthogonal projection matrix onto the column space of $V_{i,\mathcal{A}}$, or equivalently, the column space $\mathcal{V}$ of $\boldsymbol{\Phi}_{i,\mathcal{A}}^\top$. From (12a) we know that $\Delta \boldsymbol{u}_i \in \mathcal{V}$. Thus, by left multiplying (12b) with $\boldsymbol{\Phi}_{i,\mathcal{A}}^\dagger$, we have

$$\Delta \boldsymbol{u}_i = \boldsymbol{\Phi}_{i,\mathcal{A}}^\dagger \boldsymbol{\Phi}_{i,\mathcal{A}} \Delta \boldsymbol{u}_i = \boldsymbol{\Phi}_{i,\mathcal{A}}^\dagger \Delta \mathbf{T}_{i,\mathcal{A}}.$$

As a result,

$$\|\Delta \boldsymbol{u}_i\|_2 \leq \|\boldsymbol{\Phi}_{i,\mathcal{A}}^\dagger\|_2 \cdot \|\Delta \mathbf{T}_{i,\mathcal{A}}\|_2 = \frac{\|\Delta \mathbf{T}_{i,\mathcal{A}}\|_2}{\sigma_{i,\mathcal{A}}}, \quad (13)$$

where $\sigma_{i,\mathcal{A}}$ is the smallest singular value of $\boldsymbol{\Phi}_{i,\mathcal{A}}$.

As $\boldsymbol{\tau}_i$ and $\boldsymbol{\tau}_i'$ are adjacent, $\Delta \mathbf{T}_i$ has only two nonzero entries corresponding to respectively the lower and upper bounds of the comfort constraint of building i at some time t. As they cannot be active at the same time, we have $\|\Delta \mathbf{T}_{i,\mathcal{A}}\|_2 \leq \tau_{i,\text{out}} - \tau_{i,\text{in}}$. Plugging this into (13), we obtain the desired conclusion. ■

C. Privacy loss under multiple queries

In Section III-A, the noise strength in (6) can guarantee the specified (ϵ_i, δ_i)-privacy if the transmitted data $\tilde{\boldsymbol{u}}_i$ is intercepted once. However, Algorithm 2 requires agent i to send $\tilde{\boldsymbol{u}}_i$ to the coordinator in multiple iterations, essentially resulting in multiple queries on the same private dataset $\boldsymbol{\tau}_i$. To see how this affects the level of privacy protection, we cite the following result.

Theorem 2 (Adaptive composition [15]): Suppose the mechanism $\mathcal{M}_1 : \boldsymbol{\tau}_i \mapsto \tilde{\boldsymbol{u}}_i^k$ is (ϵ_1, δ_1)-differentially private and the mechanism $\mathcal{M}_2 : (\tau_i, \tilde{\boldsymbol{u}}_i^k) \mapsto \tilde{\boldsymbol{u}}_i^{k+1}$ is such that, for any fixed $\tilde{\boldsymbol{u}}_i^k$, $\mathcal{M}_2(\cdot, \tilde{\boldsymbol{u}}_i^k)$ is (ϵ_2, δ_2)-differentially private. Then the composite mechanism $\mathcal{M} : \boldsymbol{\tau}_i \mapsto (\tilde{\boldsymbol{u}}_i^k, \tilde{\boldsymbol{u}}_i^{k+1})$ preserves $(\epsilon_2 + \epsilon_2, \delta_1 + \delta_2)$-differential privacy.

The composite mechanism $\mathcal{M}$ is called the adaptive composition of mechanisms $\mathcal{M}_1$ and $\mathcal{M}_2$. The above result states that the privacy protection degrades linearly with the number of adaptive compositions. The following result sharpens this rather conservative estimate.

Theorem 3 (Advanced composition [15]): For any $\epsilon, \delta, \delta' \geq 0$, suppose $\mathcal{M} : \boldsymbol{\tau}_i \mapsto (\tilde{\boldsymbol{u}}_i^1, \tilde{\boldsymbol{u}}_i^2, \ldots, \tilde{\boldsymbol{u}}_i^k)$ is the adaptive composition of k mechanisms preserving (ϵ, δ)-differential privacy. Then $\mathcal{M}$ is $(\epsilon', k\delta + \delta')$-differentially private with $\epsilon' = \epsilon\sqrt{2k\log(1/\delta')} + k\epsilon(e^\epsilon - 1)$.

Using Theorem 3, the differential privacy level degrades at the rate $O(\sqrt{k})$ instead of $O(k)$ as the number k of adaptive compositions increases, provided that $\epsilon > 0$ is small. On the other hand, Theorem 3 in practice is still conservative for our proposed Algorithm 2.

IV. CASE STUDY RESULTS

In this section, we evaluate the performance of proposed algorithms on a case study consisting of three living offices (Fig. 1) in the Herrick Lab of Purdue University, West Lafayette. The three zones (offices) share one chiller for cooling and have almost identical thermal dynamics whose model was trained and validated by data collected from April 21 to May 20, 2015. The three zones have well insulated adjacent walls so

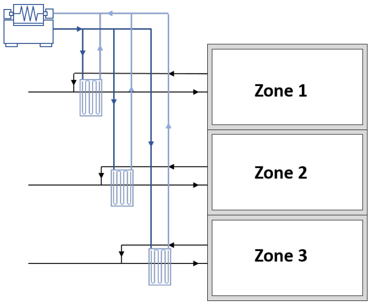

Fig. 1: Schematics of the three-zone case study building.

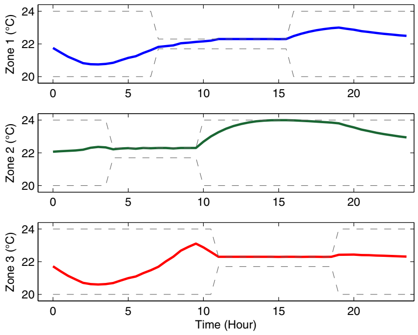

Fig. 2: Three zone temperatures with $\sigma_i \equiv 0.2$.

they are thermally decoupled and can be treated as three separate buildings. The sampling time is 30 minutes and the prediction horizon $N = 48$, i.e., one day.

To test the coordination ability of the proposed algorithms, we specify different temperature bounds (i.e., occupancy profiles) for the three zones, as indicated by the gray dashed lines in Fig. 2. Setting $\rho = 1$, $r_{\text{elec}} = 0.12$\$/kWh, $r_{\text{dem}} = 2.4$\$/kW, iteration number $K = 50$ and the noise standard deviation $\sigma_i \equiv 0$ and 0.2 respectively in Algorithm 2, the converged cooling loads for the zones and their sum are plotted in Fig. 3 and Fig. 4, respectively. Since the resulting zone temperatures in both case are close to each other, only one of them ($\sigma_i \equiv 0.2$) is shown in Fig. 2.

The coordinations across zones are evident. For the example in Fig. 3, zone 3's cooling request drops dramatically around 8:00 a.m. to help zone 1 meet its occupied period temperature starting at the same time; and the three zones cooperate between 3:00 a.m. and 12:00 p.m. to maintain a flat ($\sigma_i \equiv 0$) or relatively flat ($\sigma_i \equiv 0.2$) peak load (see Fig. 4). In both Fig. 3 and Fig. 4, compared to the result of $\sigma_i \equiv 0$, the cooling loads after adding noises with standard deviation $\sigma_i \equiv 0.2$ have similar shapes, although with small oscillations.

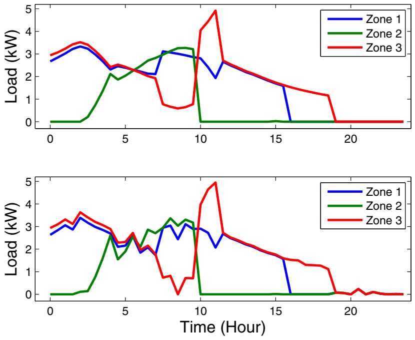

Fig. 3: Comparison of zone cooling loads obtained by Algorithm 2 for $\sigma_i \equiv 0$ (top) and $\sigma_i \equiv 0.2$ (bottom).

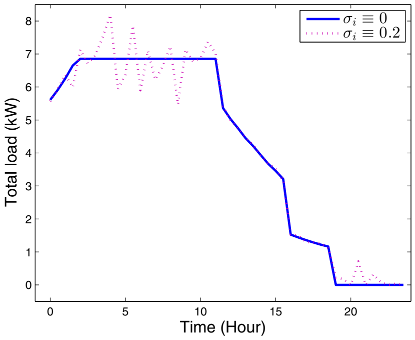

Fig. 4: Comparison of the total cooling loads obtained by Algorithm 2 for $\sigma_i \equiv 0$ and $\sigma_i \equiv 0.2$.

In addition to the control decision oscillations observed above, the performance of obtained solution also degrades as noise level increases, as shown in Fig. 5. For $\sigma_i \equiv 0.1$ and 0.2, the obtained solutions have reasonable suboptimality w.r.t. to the optimal case $\sigma_i \equiv 0$. However, with $\sigma_i \equiv 0.4$, the amplitude and oscillations of suboptimality becomes significant to the degree that the iterations barely result in performance improvement from the initial values. This can be partially explained by our choices of the prices r_{elec} and r_{dem}. The added noises to $\boldsymbol{u}_i$ directly affect the effort of the coordinator in optimizing the demand charge, which (112.76\$) accounts for roughly 61% of the total bill (185.87\$) when $\sigma_i \equiv 0$. In addition, the average value of $\boldsymbol{u}_i$ during the prediction horizon is around 1.39kW, which is not significantly higher than the noise standard deviation $\sigma_i \equiv 0.4$.

Note that the high electricity bill 185.87\$ is not a representative one-day bill for the following reason. Since the demand charge is monthly billed, the formulation (1) actually represents the MPC problem for the first day of each month, when there is no peak

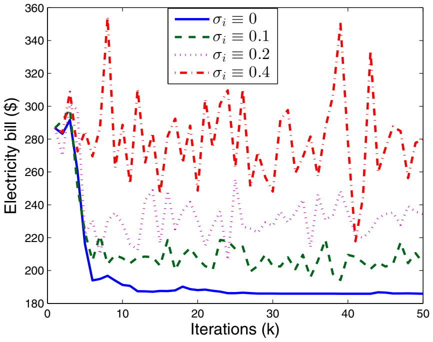

Fig. 5: Comparison of total bill for different noise levels.

load threshold produced within this billing cycle. But it can be easily extended for later days' control design by replacing the second term $r_{\text{dem}}\|\sum_i \boldsymbol{u}_i\|_\infty^2$ in (1a) by $r_{\text{dem}}\left(\|\sum_i \boldsymbol{u}_i\|_\infty - u_{\text{peak}}\right)^2$ where $u_{\text{peak}} \in \mathbb{R}$ is the peak load occurred in the past portion of current billing cycle, see [8]. Here the first day is only used to evaluate the performance of proposed algorithms.

V. CONCLUSIONS AND FUTURE WORKS

In this paper, we study the coordinated control of building clusters with the incorporation of differential privacy mechanisms. An (ϵ_i, δ_i)-differentially private distributed solution algorithm is proposed that randomizes the local information by adding Gaussian noises. Its effectiveness is demonstrated by the simulation results of a three-zone case study. A theoretical lower bound of the noise magnitude ensuring given privacy level is derived. Future research directions include obtaining the theoretical performance degradation caused by the added noises and the trade-off between privacy protection and performance optimality.

REFERENCES

[1] "How the united states uses energy, 2016," https://www.eia.gov/energyexplained/index.cfm?page=us_energy_use, accessed: 2018-03-18.

[2] "Electricity consumption in the united states was about 3.85 trillion kilowatthours (kwh) in 2016," https://www.eia.gov/energyexplained/index.cfm?page=electricity_use, accessed: 2018-03-18.

[3] F. Oldewurtel, A. Parisio, C. N. Jones, D. Gyalistras, M. Gwerder, V. Stauch, B. Lehmann, and M. Morari, "Use of model predictive control and weather forecasts for energy efficient building climate control," *Energy and Buildings*, vol. 45, pp. 15–27, 2012.

[4] J. Širokỳ, F. Oldewurtel, J. Cigler, and S. Prívara, "Experimental analysis of model predictive control for an energy efficient building heating system," *Applied energy*, vol. 88, no. 9, pp. 3079–3087, 2011.

[5] N. Radhakrishnan, Y. Su, R. Su, and K. Poolla, "Token based scheduling for energy management in building hvac systems," *Applied Energy*, vol. 173, pp. 67–79, 2016.

[6] P.-D. Moroşan, R. Bourdais, D. Dumur, and J. Buisson, "Building temperature regulation using a distributed model predictive control," *Energy and Buildings*, vol. 42, no. 9, pp. 1445–1452, 2010.

[7] Y. Ma, G. Anderson, and F. Borrelli, "A distributed predictive control approach to building temperature regulation," in *American Control Conference (ACC), 2011*. IEEE, 2011, pp. 2089–2094.

[8] J. Cai, J. E. Braun, D. Kim, and J. Hu, "General approaches for determining the savings potential of optimal control for cooling in commercial buildings having both energy and demand charges," *Science and Technology for the Built Environment*, vol. 22, no. 6, pp. 733–750, 2016.

[9] X. Hou, Y. Xiao, J. Cai, J. Hu, and J. Braun, "Distributed model predictive control via proximal jacobian ADMM for building control applications," in *American Control Conf.*, 2017, pp. 37–43, (Purdue Technical Report TR-ECE-17-02).

[10] V. Putta, D.-H. Kim, J. Cai, J. Hu, and J. E. Braun, "Dynamic programming based approaches to optimal rooftop unit coordination," *Science and Technology for the Built Environment*, vol. 21, no. 6, pp. 752–760, 2015.

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

[12] A. Friedman and A. Schuster, "Data mining with differential privacy," in *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2010, pp. 493–502.

[13] R. Chen, N. Mohammed, B. C. Fung, B. C. Desai, and L. Xiong, "Publishing set-valued data via differential privacy," *Proceedings of the VLDB Endowment*, vol. 4, no. 11, pp. 1087–1098, 2011.

[14] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*. Springer, 2008, pp. 1–19.

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

[16] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[17] 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.

[18] Z. Huang, S. Mitra, and N. Vaidya, "Differentially private distributed optimization," in *Proceedings of the 2015 International Conference on Distributed Computing and Networking*. ACM, 2015, p. 4.

[19] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via objective perturbation," in *American Control Conference (ACC), 2016*. IEEE, 2016, pp. 2061–2066.

[20] ——, "Differentially private average consensus with optimal noise selection," *IFAC-PapersOnLine*, vol. 48, no. 22, pp. 203–208, 2015.

[21] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753–765, 2017.

[22] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 118–130, 2017.

[23] J. Cai and J. Braun, "Assessments of demand response potential in small commercial buildings across the united states," *Energy and Buildings*, 2018, under review.

[24] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends® in Machine Learning*, vol. 3, no. 1, pp. 1–122, 2011.