# Privacy-Preserving Aggregation of Controllable Loads to Compensate Fluctuations in Solar Power

Jin Dong*, Teja Kuruganti*, Seddik Djouadi†, Mohammed Olama*, and Yaosuo Xue*
* Oak Ridge National Laboratory, Oak Ridge, TN 37831
† Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996
Email: {dongj, kurugantipv, olamahussemm, xuey}@ornl.gov, mdjouadi@utk.edu

***Abstract*—Cybersecurity and privacy are of the utmost importance for safe, reliable operation of the electric grid. It is well known that the increased connectivity/interoperability between all stakeholders (e.g., utilities, suppliers, and consumers) will enable personal information collection. Significant advanced metering infrastructure (AMI) deployment and demand response (DR) programs across the country, while enable enhanced automation, also generate energy data on individual consumers that can potentially be used for exploiting privacy. Inspired by existing works which consider DR, battery-based perturbation, and differential privacy noise adding, we novelly consider the aggregator (cluster) level privacy issue in the DR framework of solar photovoltaic (PV) generation following. Different from most of the existing works which mainly rely on the charging/discharging scheduling of rechargeable batteries, we utilize controllable building loads to serve as virtual storage devices to absorb a large portion of the PV genertaion while delicately keeping desired noisy terms to satisfy the differential privacy for the raw load profiles at the aggregator level. This not only ensures differential privacy, but also improves the DR efficiency in load following since part of the noisy signal in solar PV generation has been filtered out. In particular, a mixed integer quadratic optimization problem is formulated to optimally dispatch a population of on/off controllable loads to achieve this privacy-preserving DR service.**

## I. INTRODUCTION

An important feature of the smart grid is the demand response (DR) mechanism that provides customers with flexibility to meet their energy needs. Intermittent and volatile production of renewable energy leads to an unavoidable incorporation between customers and energy sources that increases the need for additional balancing resources. In addition to battery energy storage (BES), virtual storage devices such as thermostatically controlled loads (TCLs) play as an alternative storage to help restore demand-supply balance. However, significant advanced metering infrastructure (AMI) deployment and DR programs, while enable enhanced automation, also generate energy data on individual consumers that can potentially be used for exploiting privacy [1], [2]. There exist major concerns about consumers' privacy when aggregators provide DR services using controllable building loads, especially after an intruder gains access to the aggregated power consumption data or the aggregator releases this information to the public. According to a study by NIST [3], obtaining near-real-time data regarding energy consumption may infer when and how long a residence or facility is occupied, where people are in the structure, what they are doing, whats their favorite team, whats their political affiliation, and so on.

To protect the residential users' privacy from malicious attacks, many secure data aggregation schemes have been proposed in the literature, i.e., encryption mechanism, battery-based perturbations, and noise adding. Homomorphic encryption was utilized in [4], [5] to allow a semi-trust gateway to aggregate consumption reports in a specific residential area. End-to-end encryption is a straightforward way to hide the communication content and preserve users privacy, but at the same time heavily increases communication overhead and computational latency for lightweight embedded systems [6]. An alternative way is to bring uncertainty into the original raw data by directly adding noise signal, especially using the differential privacy mechanisms [7]. Broadly speaking, differential privacy is a mathematically provable paradigm for privacy-preserving data sharing [8]. It ensures that the outputs of neighboring datasets are indistinguishable from randomized noise. Various approaches based on differential privacy have been introduced in [9]–[11] for smart meter reading and appliance usage using directly noise addition.

Inspired by existing works which consider DR, battery-based perturbation, and differential privacy noise adding under different scenarios, we novelly consider the privacy issue in the DR framework of solar photovoltaic (PV) generation tracking. Different from most of the existing works that mainly rely on the charging/discharging scheduling of rechargeable batteries, we utilize controllable building loads to serve as virtual storage devices to track a pre-specified aggregated load profile so that the raw power consumption will be distorted and the differential privacy for personal information can be satisfied. The main objective of our work is to reduce both fluctuations in solar PV generation and potential privacy leakage while providing certain user satisfaction. To the best of our knowledge, we are

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan http://energy.gov/downloads/doe-public-access-plan.

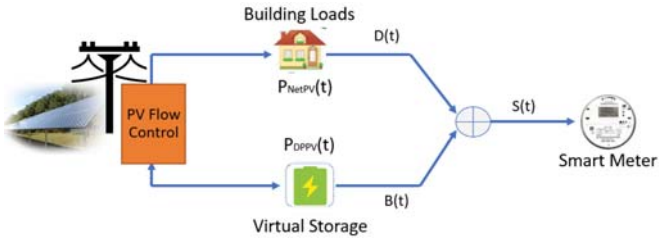


Fig. 1: PV-based perturbation mechanism

the first to study this challenging problem of increasing solar PV penetration level while providing privacy protection.

In this paper, we propose a hybrid method, which is a combination of battery-based perturbation and noise adding. We denote that, $D(t)$ and $B(t)$ in Fig. 1 correspond to base loads and differential privacy signal, respectively. On the one hand, by filtering out the high frequency components in PV generation, it relieves the pressure of generation following for slow-responsive controllable loads. On the other hand, by smartly picking the mid-high frequency components, desired differential privacy noise signal $B(t)$ is perfectly computed, and then implemented through virtual storage devices. The main privacy concern here is to ensure two aggregated datasets are indistinguishable by delicately keeping the inherent noisy signal inside local solar PV generation. At last, the performance of the proposed design is verified through controllable Heating, Ventilation and Air-Conditioning (HVAC) loads based on the DR control technique introduced in [12], [13].

The remainder of this paper is organized as follows. Section II introduces the background for differential privacy and problem formulation. Section III then derives the optimization formulation for aggregated HVAC loads. Section IV presents the simulation results to validate the tracking performance using a set of real temperature and solar power data. Finally, Section V summarizes the paper and presents the conclusions.

## II. Preliminary and Problem Formulation

In this section, we will discuss the basic principle for differential privacy and the building thermal model. By adding random noise, typically with Laplacian [14] distribution, to the measurement data submitted by the customers, the differential private aggregation scheme will not increase system complexity. On the one hand, this contributes to reducing the capital and maintenance cost by purchasing smaller size battery storage. On the other hand, considering the intermittent renewable resources, this privacy-in-the-loop strategy will contribute to absorbing the PV high frequency uncertain fluctuations and, therefore, reducing stress to the grid.

### A. Differential Privacy

Broadly speaking, differential privacy is a privacy-preserving mechanism, which is independent of the background knowledge of the adversary [8], [15]. It guarantees that the probabilities that two neighboring data sets that have the same output are quite close so that the probability dilation is bounded by $exp(\varepsilon)$. By doing so, the adversary can hardly infer a single data record by manipulating outputs. The definition and detailed description of the standard $\varepsilon$-differential privacy can be found in [15].

Mathematically, $\mathscr{M}$ satisfies $\varepsilon$-differential privacy, if for all possible data sets, any individual (say, Alex), and all possible result set $\mathbb{R} \subseteq \text{Range}(\mathscr{M})$:

$$\frac{Pr(\mathscr{M}(\text{DB with Alex}) \in \mathbb{R})}{Pr(\mathscr{M}(\text{DB without Alex}) \in \mathbb{R})} \leq e^{\varepsilon} \approx 1 \pm \varepsilon, \tag{1}$$

where DB is short for Database. Note that $\varepsilon$ is denoted as the privacy budget and specifies the privacy degree. Intuitively, a lower $\varepsilon$ means a better privacy and typically $\varepsilon = 0.1$.

*Definition 2.1:* Given an $n$-dimension dataset $D^n$, a randomized algorithm to answer query $A$ is $(\delta, \varepsilon)$-differentially private if $\forall x, y \in D^n$ that differs only in one element and all $S \in range(A)$,

$$Pr[A(x) \in S] \leq e^{\varepsilon} \times Pr[A(y) \in S] + \delta, \tag{2}$$

where $range(A)$ denotes the output range of $A$.

After reviewing differential privacy, a Baseline Aggregation scheme can be drawn to provide differential privacy for real-time aggregated data streams. The basic principle is to add independent Laplace noise into the aggregation result at each time slot [7], aiming at providing $\varepsilon$-differential privacy.

### B. Problem Formulation

In an aggregated control system, the power consumption data is transmitted to the controller. It is necessary that the information preserves a certain level of privacy such that an adversary or another curious aggregator cannot infer more information about the system states than what is intended.

The overall objective is to utilize the aggregated HVAC loads to compensate fluctuations in solar PV power as well as protecting the users' privacy without jeopardizing thermal comfort. In other word, we will utilize controllable loads to maximize the locally absorbed PV generation while providing adequate differential privacy covering noise signal. Hence, we need first to compute the minimum differential privacy noise signal corresponding to the specific solar PV generation, then ensure the controllable loads consume exactly desired amounts of energy (as illustrated by $P_{NetPV}(t)$ in Fig. 1) through DR algorithms.

*Problem 2.2:* (Privacy-preserving generation following problem). Given the dataset $D(t)$ and the query function $Q(\cdot)$ over $D(t)$ which returns $P(t)$ (i.e., $Q(D(t)) = P(t)$), we aim to devise a privacy-preserving algorithm $\mathscr{A}$ which extracts $B(t)$ (from local PV generation $L(t)$) as noise to the query result to hide $L(t)$ from adversaries such that $(\delta, \varepsilon)$-differential privacy is guaranteed with good $\delta, \varepsilon$.

## III. Privacy-preserving Generation Following

This section discusses the noise construction technique to provide sufficient differential privacy. It is followed by the control design, which relies on model predictive control (MPC) scheme to regulate the aggregated power consumption of a population of HVAC loads to track a desired profile.

### A. Differential Privacy Noise Calculation

In this subsection, to derive the necessary noise signal for differential privacy, we depart from exploring the definition of $(\varepsilon, \delta)$-differential privacy.

In the original derivation for differential privacy [7], Dwork presented a general protocol to implement differential privacy utilizing the concept of *global sensitivity* $\Delta Q$. Given a query set $Q \in \mathbb{Q}$, the global sensitivity $\Delta Q$ is the maximal $\mathscr{L}_1$ distance (difference) between the exact query results on any two neighboring datasets $D_1$ and $D_2$, i.e.

$$\begin{aligned} \Delta Q &= \max_{D_1, D_2} \|Q(D_1), Q(D_2)\|_1 \\ &= \max_{D_1, D_2} |Q(D_1) - Q(D_2)|, \end{aligned} \tag{3}$$

for all $D_1, D_2$ that differ in at most one element.

Informally, the sensitivity $\Delta Q$ is the maximum amount the result $Q(\cdot)$ can change, given any change to a single users' data.

*Lemma 3.1:* When $\Delta Q = 1$, the function $Q(\cdot)$ achieves $(\varepsilon, \delta)$-differential privacy if noise from the Laplacian distribution is added to it [7].

It should be mentioned that, although we focus on the Laplace noise in this paper, our approach is easily extendable to other mechanisms that satisfy requirements by differential privacy.

*Remark 3.2:* The $\Delta Q$ usually depends on the data domain $\mathbb{D}$ and the query set $Q$, but not the actual data. Therefore, we simply assume such a constant $\Delta Q$ is public knowledge to everyone, including the adversary.

The Laplace Mechanism, $M_L$, outputs a randomized result $R$ on dataset $D$, following a Laplace distribution with mean $Q(D)$ and magnitude $\frac{\Delta Q}{\varepsilon}$, i.e.,

$$Pr(M_L(Q, D) = R) \propto exp\left(\frac{\varepsilon}{\Delta Q} \|R - Q(D)\|_1\right). \tag{4}$$

This is equivalent to adding $m$-dimensional independent Laplace noise to each query in $Q$, that is, $M(Q, D) = Q(D) + Lap(\frac{\Delta Q}{\varepsilon})^m$, in which $Lap(\frac{\Delta Q}{\varepsilon})$ is a random variable following a zero-mean Laplace distribution with scale $\frac{\Delta Q}{\varepsilon}$. The Laplace noise is drawn from Laplace distribution with probability density function (PDF)

$$f(x) = \frac{1}{2\lambda} exp(-\frac{|x|}{\lambda}), \tag{5}$$

where the variance of $Lap(\lambda)$ is $2\lambda^2 = \frac{2\Delta Q^2}{\varepsilon^2}$. Since the Laplace noise injected into each of the $m$ query result is independent, the overall expected squared error of the query answers obtained by the Laplace mechanism is $\frac{2m\Delta Q^2}{\varepsilon^2}$ [16].

*Remark 3.3:* Note that the amount of error only depends on the sensitivity of the queries, regardless of the records in dataset $D$. Therefore, we can obtain the desired noise signal to ensure differential privacy (denoted as $P_{DPPV}(k)$) by sampling through $f(x)$ (defined in (5) and (4)), where $k$ represents time step.

*Remark 3.4:* $P_{DPPV}(k)$ corresponds to the desired noise signal $B(t)$ in Fig. 1.

After extracting this noise part from the total PV generation, we can easily compute the remaining net PV generation $P_{NetPV}(k)$ that needs to be locally consumed by aggregated controllable loads. $P_{NetPV}(k)$, which will play as a new reference profile to be followed by the DR program, is defined as follows.

$$P_{NetPV}(k) = P_{PV}(k) - P_{DPPV}(k). \tag{6}$$

### B. DR for $P_{DPPV}$

Due to the partially uncontrollable and stochastic nature of renewable resources, the variance of net load of distribution systems increases [17]. In effect, TCLs, such as HVAC units, have been used for virtual energy storage. Hence, the designed privacy noise signal $P_{DPPV}$ can be provided by such virtual storage devices.

The feasibility of this approach has been well recognized in the literature, for example in [12], [13], [18], [19].

### C. DR for $P_{NetPV}$

This section develops a centralized MPC-based DR strategy to locally absorb the net PV generation - $P_{NetPV}$.

*1) Building Thermal Model:* In this section, we describe the typical one-dimensional model used in this work and formulate the control strategy. The system model was widely utilized in the literature such as [13], [20], [21].

The system state is the room air temperature $q$. If we denote the state vector $X = [q]$, input $U = [Mode_{HVAC}]$ (HVAC ON/OFF status), and disturbances $V = [T_{out}, Q_{out}]$ (outdoor temperature and solar irradiance), we can rewrite the building thermal model into the state-space form as:

$$\dot{X} = AX + BU + GV. \tag{7}$$

State-space matrices $A, B, G$ can be obtained for any given building, and disturbance $V$ is recorded for that specific location.

We consider the problem where indoor temperature $x = q$ is required to remain within certain bounds of a constant deadband in the presence of the disturbance vector $V$. Moreover, we make the indoor temperature $x_j$ ($j$ corresponds to $j_{th}$ building) track a pre-assigned reference temperature set-points by minimizing the state error $e_j(k) := x_j(k) - X_r$ at each time step $k$, where $X_r$ is the temperature set-point.

MPC is implemented as a discretized building thermal model with sampling period $\triangle T = 10$ minute, $t_i = i\Delta T$ which yield the discrete-time model

$$x_{k+1} = A_k x_k + B_k u_k + G_k v_k. \tag{8}$$

After ensuring the differential privacy noise signal, we need to design optimal control signals to orchestrate the aggregate demand of HVAC systems follow the net PV power generation $P_{NetPV}$ without violating the temperature comfort requirement.

$$z(k) := \sum_{j=1}^{N_s} u_j(k) \approx P_{NetPV}(k), \tag{9}$$

where $N_s$ denotes total number of HVAC units and $u_j(k)$ denotes the control action taken for the $j_{th}$ HVAC unit at the $k_{th}$ time interval.

*2) Cost Functions:* We formulate the control strategy as an optimization problem, whose objective consists of two parts. The first part describes the performance of privacy protection while the second part characterizes the user comfort satisfaction ($e_i(k)$ denotes the temperature deviation from temperature setpoint).

$$J = \sum_{k=1}^{N_p} \Big\{ Q(z(k) - P_{NetPV}(k))^2 + R(\sum_{i=1}^{N_s} e_i(k)^2) \Big\}, \quad (10)$$

where $N_p$ represents the prediction horizon with $Q$ and $R$ being weighting factors.

*3) Constraints:* In the MPC problem, we have both states and control input constraints. For temperature state constraint, we set $x \in [22.5^\circ C, 23.5^\circ C]$. And for the discrete ON/OFF control signal, the binary inputs $u \in \{0, 1\}$. Notice here, "0" means HVAC OFF, while "1" means HVAC ON.

## IV. Performance Evaluation

In this section, we evaluate the proposed privacy-preserving aggregation algorithm through a numerical example. We consider a central coordinator that collects total PV generation, computes desired differential privacy noise signal, and allocates energy to a population of HVAC loads to minimize difference between total power consumption and net PV generation.

Based on the MPC design introduced in Sec. III-C, we utilize 100 buildings, each of which is equipped with identical building thermal model (8). It is worth mentioning that the simulation time is 432 time steps, which means 10 mins per time step for three days. Both PV generation and weather profiles are picked for these days from a local station.

### A. Differential Privacy Noise

The desired noise is generated by $Lap(\mu, b)$, with $\mu = 0$ and $b = \frac{\Delta Q}{\varepsilon}$ (corresponding to the raw PV generation measurement), and $\varepsilon = 0.1$. Figs. 2 and 3, respectively, illustrate the detailed noise signal for each time step and the overall histogram for the generated noise. From Fig. 3, we observe that Laplace noise is obtained. Then, the net PV generation $P_{NetPV}(k)$ profile is depicted in Fig. 4.

### B. Load Tracking Performance for $P_{NetPV}$

Based on the net PV generation profile, we present simulation results for the developed MPC strategy of all 100 buildings in Figs. 5 - 6. The indoor temperatures are plotted in Fig. 5. We can observe that the indoor temperatures are strictly bounded by the preassigned comfort band, utilizing discrete ON/OFF control signals. After checking the temperatures in bound, we need to evaluate the tracking performance depicted in Fig. 6. It can be seen from Fig. 6 that satisfied tracking performance has been achieved, in particular with the presence of highly dynamic solar PV generation after extracting the designed noise signal. Therefore, we claim that these 100 HVAC loads are well coordinated to track the PV generation using the developed optimal control strategy.

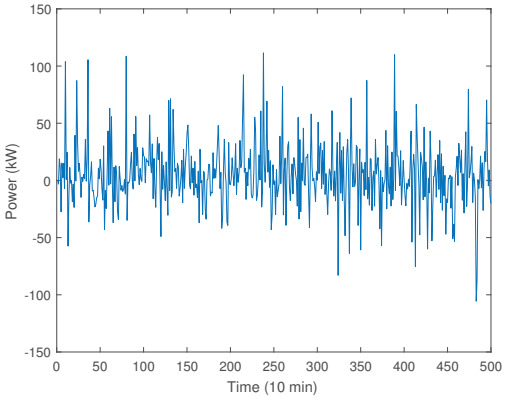


Fig. 2: Desired Laplacian noise

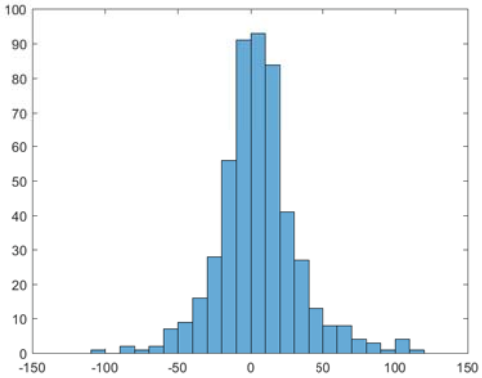

Fig. 3: Histogram of the Laplacian noise

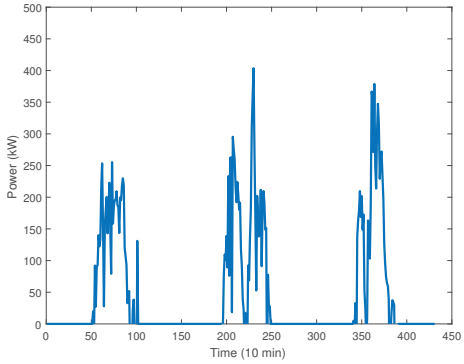


Fig. 4: Net reference PV power generation ($P_{NetPV}$)

## V. Conclusions and Future Works

In this paper, the privacy issues associated with DR that aim to improve security and efficiency of aggregated controllable loads for mitigating fluctuations in solar PV generation are addressed. Different from most of the existing works which mainly rely on the charging/discharging scheduling of

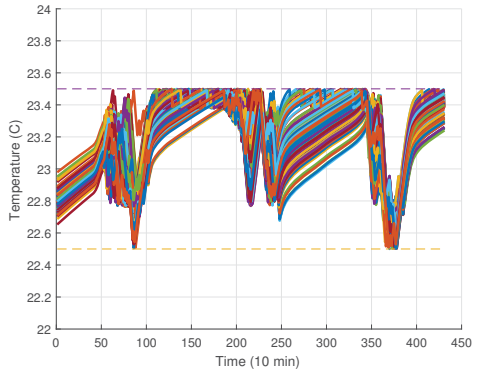


Fig. 5: Indoor temperature for 100 buildings when tracking $P_{NetPV}$ using MPC

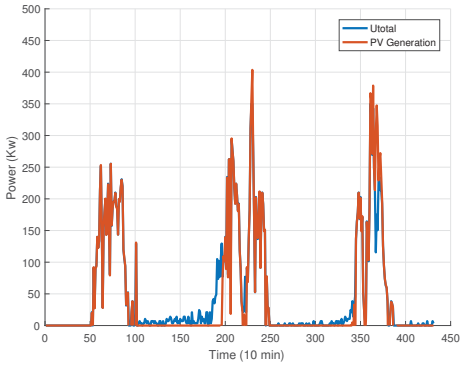


Fig. 6: Tracking the $P_{NetPV}$ signal using MPC control

rechargeable batteries, we utilize controllable building loads to serve as virtual storage devices to track a pre-specified aggregated load profile so that the raw power consumption will be distorted and the differential privacy for personal information can be guaranteed. A differential privacy based aggregation algorithm is proposed to compensate for fluctuations in solar power as well as to protect the users' privacy without jeopardizing user comfort. Considering the intermittent renewable resources, this privacy-in-the-loop strategy will contribute to filter out high frequency uncertain fluctuations into the grid. Optimal coordination of controllable loads is then investigated to simultaneously track both the load and noise profiles. A numerical example is provided to optimally dispatch an aggregate of on/off HVAC units to track the designed net PV generation signal after filtering out the privacy signal. It's worth mentioning that, this framework can be generalized to any controllable loads.

In our future work, a distributed cooperative optimization-based control algorithm will be combined with this framework to address the large-scale HVAC system control problem. Another interesting direction is to design a more complex privacy-preserving DR framework, whose objective is to ensure the privacy of each individual user under the aggregator.

## REFERENCES


[1] C. Horne, B. Darras, E. Bean, A. Srivastava, and S. Frickel, "Privacy, technology, and norms: The case of smart meters," *Social science research*, vol. 51, pp. 64–76, 2015.

[2] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, 2017.

[3] N. S. Grid, "Introduction to nistir 7628 guidelines for smart grid cyber security," *Guideline, Sep*, 2010.

[4] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[5] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 327–332.

[6] E. Liu and P. Cheng, "Achieving privacy protection using distributed load scheduling: A randomized approach," *IEEE Transactions on Smart Grid*, 2017.

[7] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *TCC*, vol. 3876. Springer, 2006, pp. 265–284.

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

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

[10] J. Won, C. Y. Ma, D. K. Yau, and N. S. Rao, "Privacy-assured aggregation protocol for smart metering: A proactive fault-tolerant approach," *Biological Cybernetics*, vol. 24, no. 3, pp. 1661–1674, 2016.

[11] 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.

[12] J. Dong, M. Olama, T. Kuruganti, J. Nutaro, Y. Xue, I. Sharma, and S. M. Djouadi, "Adaptive building load control to enable high penetration of solar PV generation," in *2017 IEEE Power & Energy Society General Meeting*, 2017.

[13] J. Dong, M. Olama, T. Kuruganti, J. Nutaro, C. Winstead, Y. Xue, and A. Melin, "Model predictive control of building on/off HVAC systems to compensate fluctuations in solar power generation," in *2018 9th IEEE International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*. IEEE, 2018, pp. 1–5.

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

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

[16] G. Yuan, Z. Zhang, M. Winslett, X. Xiao, Y. Yang, and Z. Hao, "Optimizing batch linear queries under exact and approximate differential privacy," *ACM Transactions on Database Systems (TODS)*, vol. 40, no. 2, p. 11, 2015.

[17] Y. Zhang, A. Melin, M. Olama, S. Djouadi, J. Dong, and K. Tomsovic, "Battery energy storage scheduling for optimal load variance minimization," in *2018 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2018, pp. 1–5.

[18] J. Brooks and P. Barooah, "Virtual energy storage through decentralized load control with quality of service bounds," in *Proc. of American Control Conference (ACC)*. IEEE, 2017, pp. 735–740.

[19] Y. Lin, P. Barooah, and J. L. Mathieu, "Ancillary services through demand scheduling and control of commercial buildings," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 186–197, 2017.

[20] J. L. Mathieu, S. Koch, and D. S. Callaway, "State estimation and control of electric loads to manage real-time energy imbalance," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 430–440, 2013.

[21] J. Dong, C. Winstead, J. Nutaro, and T. Kuruganti, "Occupancy-based HVAC control with short-term occupancy prediction algorithms for energy-efficient buildings," *Energies*, vol. 11, no. 9, p. 2427, 2018.