Comparative Analysis of Load Shaping Based Privacy Preservation Strategies in Smart Grid

Cihan Emre Kement, Hakan Gultekin, Bulent Tavli, *Senior Member*, *IEEE*, Tolga Girici, *Member*, *IEEE*, and Suleyman Uludag, *Member*, *IEEE*

***Abstract*—A key enabler for the smart grid is the fine grained monitoring of power utilization. Although such a mechanism is helpful in the optimization of the whole electricity generation, distribution, and consumption cycle, it also creates opportunities for the potential adversaries in deducing the activities and habits of the subscribers. In fact, by utilizing the standard and readily available tools of Non-Intrusive Load Monitoring (NILM) techniques on the metered electricity data, many details of customers' personal lives can be easily discovered. Therefore, prevention of such adversarial exploitations is of utmost importance for privacy protection. One strong privacy preservation approach is the modification of the metered data through the use of on-site storage units in conjunction with renewable energy resources. In this study, we introduce a novel mathematical programming framework to model eight privacy enhanced power scheduling strategies inspired and elicited from the literature. We employ all the relevant techniques for the modification of the actual electricity utilization (*i.e.*, on-site battery, renewable energy resources, and appliance load moderation). Our evaluation framework is the first in the literature, to the best of our knowledge, for a comprehensive and fair comparison of the load shaping techniques for privacy preservation. In addition to the privacy concerns, we consider monetary cost and disutility of the users in our objective functions. Evaluation results show that privacy preservation strategies in the literature differ significantly in terms of privacy, cost, and disutility metrics.**

***Index Terms*—Smart grid, privacy, load shaping, NILM, renewable energy, mixed integer programming, mixed integer quadratic programming, goal programming, multi-objective programming.**

Manuscript received January 31, 2017; revised April 21, 2017; accepted June 18, 2017.

C. E. Kement and T. Girici are with the Department of Electrical and Electronics Engineering, TOBB University of Economics and Technology, 06560, Ankara, Turkey (e-mail: cekement@etu.edu.tr, tgirici@etu.edu.tr).

H. Gultekin is with the Department of Industrial Engineering, TOBB University of Economics and Technology, 06560, Ankara, Turkey (e-mail: hgultekin@etu.edu.tr).

B. Tavli is with the Department of Electrical and Electronics Engineering, TOBB University of Economics and Technology, 06560, Ankara, Turkey (corresponding author; phone: +90-312-292-4074; fax: +90-312-292-4180; e-mail: btavli@etu.edu.tr).

S. Uludag is with the Department of Computer Science, Engineering and Physics, University of Michigan - Flint, MI, USA (e-mail: uludag@umich.edu).

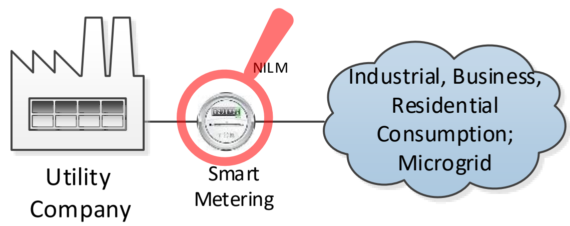


Fig. 1: Non-Intrusive Load Monitoring (NILM).

I. Introduction

RECENTLY, unprecedented global initiatives have been undertaken to upgrade the aging power grid with bidirectional power and information flow capabilities into what is known as the smart grid [1]–[3]. One of the crucial components of the smart grid is the Demand-Side Management (DSM) whose overarching goal is to enhance the efficacy through energy consumption scheduling [4]–[6]. An inevitable prerequisite of DSM methodologies is the access to consumption data [7], which may be viewed by many as a potential for privacy violation [8], [9]. Privacy is, in essence, the right to informational self-determination (*i.e.*, individuals must be able to determine for themselves when, how, to what extent and for what purpose information about them is communicated to others) [10]. The initial goal of collecting electricity usage information to generate an electricity profile has now become a source of inferring behavioral information [11]. Furthermore, there are well-known techniques to compromise the sanctity of the information of the energy consumer, known as Non-Intrusive Load Monitoring (NILM) where only one individual monitor at the metering unit is enough to decide the energy usage from the aggregate data [12], [13], as shown in Fig. 1. Note that the aggregate data may be abused by the utility or by unauthorized third parties.

To protect the customers' privacy against potential NILM-based privacy violations, two major categories of privacy preservation techniques have been proposed in the literature [10]. First, measured electricity is reported accurately without any distortion or obfuscation of the measured quantity via privacy preserving data handling (*e.g.*, data anonymization [14], data aggregation [15]–[17]). However, such privacy preservation requires either interacting with a trusted third party or requires other households to collaborate, therefore, rendering privacy to be at least partially compromised. Second, measured data itself can be modified to hide the actual electricity utilization within the household to mislead the inferring techniques even when all measured data is compromised [18].

Since its inception in [19], four major categories of modification of electricity utilization for privacy preservation have been proposed in the literature. The first approach is based on charging/discharging a battery in the household which modifies metered data to hide the salient characteristics of the actual electricity utilization in the household [19]–[24]. The second approach utilizes the concepts of information theory and signal processing to distort the metered data which is treated as an information sequence by modifying its characteristics [25], [26]. The third approach is to reduce the time granularity of the reporting interval which is intrinsically capable of erasing a significant amount of information in the metered data provided that the granularity is high (*e.g.*, tens of minutes) [27], [28]. The fourth approach is based on the idea of utilizing heating loads (*e.g.*, electric water and space heaters) as tools to modify the metered data which is similar to the first approach with batteries [29], [30]. Nevertheless, the on-site battery based approach is the earliest and the most widely utilized approach for privacy preservation through load shaping [10], [14], [19], [31], [32].

Our major contributions in this study are enumerated as follows:

1) We created a unified stochastic mathematical programming framework for a fair comparison of privacy-preserving strategies by means of on-site batteries, appliance moderation, and renewable energy resources (RERs).
2) We constructed Mixed Integer Programming (MIP) and Mixed Integer Quadratic Programming (MIQP) models for eight approaches in line with the spirit of specific techniques/algorithms reported in the literature (*i.e.*, all our strategies are inspired by the existing body of work in the literature [19]–[24] which are concisely summarized in Section II).
3) While our optimization framework is a novel contribution in and of itself, first in the literature to the best of our knowledge, another major contribution is the extensive experimental analysis through the numerical evaluations of our MIP and MIQP models.

The rest of the paper is organized as follows: We present a literature overview on privacy preservation through load shaping in Section II. In Section III, we develop our stochastic mathematical programming framework. Analysis and discussion of the performances of the strategies are presented in Section IV. Section V provides the concluding remarks.

II. Related Work

In this section, we provide synopses of the major papers in privacy-enhanced load scheduling from the literature that are the motivating approaches for our optimization framework of Section III.

One of the earliest studies on load shaping for privacy preservation by utilizing a battery is reported in [19]. By charging/discharging the battery, temporal changes in the electricity usage measured by the electric meter is kept at a single constant level as the battery charge level permits. When charge/discharge state of the battery does not permit the maintenance of the predetermined constant level, the privacy preservation strategy reveals the data until the necessary battery charge level is restored which is the reason why this algorithm is called the Best Effort (BE) algorithm.

Several algorithms are proposed to improve the BE algorithm, such as the Non Intrusive Load Leveling (NILL) algorithm [20] and the Tolerable Deviation (TD) algorithm [21]. Unlike the BE method, these algorithms allow the targeted metered load to vary. Furthermore, in TD algorithm, the metered load is allowed to take values within a range (*i.e.*, the target load can vary within a predetermined range). There are also two recovery states for the battery level to charge/discharge in both algorithms. In TD, if the battery level is too high then the target level is set to the minimum and if the battery level is too low then the target level is set to the maximum. Likewise, in NILL algorithm, metered load is adjusted to recover the battery's charge level.

In the stepping framework, metered load is kept at discrete values of a constant step size matching the battery charging/discharging rate (whichever is lower) so that the battery charging/discharging can be utilized efficiently [22]. Nevertheless, the main idea is again to keep the metered load constant as long as it is sustainable by the battery charge level.

Instead of devising indirect load hiding strategies, it is possible to directly minimize the information leakage from the metered load. In [23], a convex optimization framework is created with the objective of minimizing the L2 norm of the deviation between the metered load and the target load as an approximation to the mutual information metric.

In [24], load shaping using an on-site battery is investigated via online stochastic optimization. Three load shaping strategies are investigated to hide the household electricity usage. It is reported that the best proposed strategy minimizes the differences between the electricity usage of each appliance in different time instants (*i.e.*, L1 norm).

III. Problem Formulation

Our main purpose in this study is to create an optimization framework to be able to perform comparative analysis of the load shaping algorithms presented in the literature. Quantitative analysis of these algorithms operating optimally will serve the research community for the understanding of the performance bounds of these algorithms under fair and ideal conditions. Since we are not proposing a new algorithm we do not focus on the specific implementation details of the aforementioned algorithms, which will render our analysis incompatible with one another. Instead, we take the main ideas in each algorithm and build optimization models based on these ideas which will give us enough latitude to compare the main design philosophy of each algorithm.

A. Base Model

We first present our base model for privacy preservation followed by our specific models for each algorithm. Notations

TABLE I: Symbols and their descriptions.

Symbol	Description
T	Total number of time slots
t, τ	indices of time slots $[1, 2, \ldots, T]$
a	index of appliances
s	index of scenarios
i	index of goals
ρ^s	probability of scenario s
c_t	cost of electricity at time slot t ($/kWh)
NA	number of appliances
H_a	min. number of slots that appliance a must run for
α_a	operation time window start of appliance a
β_a	operation time window end of appliance a
E_a	min. amount of energy that appliance a must spend (kWh)
P_a^{max}	max. power that appliance a can draw when operating (kW)
P_a^{min}	min. power that appliance a can draw when operating (kW)
P_{gt}^s	power generated by renewable source at time slot t (kW)
$\phi_{a,t}$	penalty cost of appliance a for operating at time t
δ_a	penalty coefficient of appliance a
L_x	pre-determined power levels (kW)
γ_1	weight of cost reduction
γ_2	weight of disutility
γ_3	weight of privacy
ΔT	duration of one time slot
M	a big number
P^{max}	max. power capacity of the entire house (kW)
E_b^{init}	initial energy stored in the battery (kWh)
E_b^{max}	max. energy that can be stored in the battery (kWh)
R_{cb}^{max}	max. charge rate of the battery (kW)
R_{db}^{max}	max. discharge rate of the battery (kW)
η_c	charging efficiency of the battery
η_d	discharging efficiency of the battery
p_{ct}^s	power drawn from the grid at time t (kW)
d_{xt}^s	coefficients used for privacy
$p_{ca,t}^s$	power consumed by appliance a at time t (kW)
$p_{cb,t}^s$	power charged into battery at time t (kW)
$p_{db,t}^s$	power discharged from battery at time t (kW)
z_t^s	a binary variable

used in our models are given in Table I. In the following optimization models, the index s denotes the scenario index. Renewable output is typically random and each scenario corresponds to a different sample path for this output. Each scenario has a certain probability, ρ^s. Our aim is to minimize the expected value of the objective function as a deterministic equivalent to this stochastic problem. For this purpose, we generate a finite set of scenarios that is representative of the renewable output sample space. Details of scenario generation are provided in Section IV-A. Our objective function consists of three separate components:

1) Minimize the expected cost: $G_1(s) = \sum_{t=1}^{T} c_t \cdot p_{ct}^s$.
2) Minimize the disutility of consumers caused by late start of the appliances: $G_2(s) = \sum_{t=1}^{T} \sum_{a=1}^{NA} \phi_{a,t} \cdot p_{ca,t}^s$. In this objective, power usage in each time slot is multiplied with a coefficient ($\phi_{a,t}$) that increases geometrically with t, forcing appliances to operate at earlier time slots. Details of the disutility metric and determination of $\phi_{a,t}$ are given in Section IV-A.
3) Minimize the information leakage, thus, maximize the privacy: $G_3(s) = \sum_{t=1}^{T} F(t, s)$. Here, $F(t, s)$ denotes a measure for information leakage at time slot t under scenario s. We will use several different strategies for minimizing the information leakage that will be explained later in this section. $F(t, s)$ takes different forms depending on the strategy under consideration.

One way to deal with such multiple challenging objectives is to use the weighted sum of the objectives as

$$\sum_{s=1}^{S} \rho^s \left(\gamma_1 G_1(s) + \gamma_2 G_2(s) + \gamma_3 G_3(s) \right). \quad (1)$$

However, since each objective has a different metric (*e.g.*, dollars vs. time), in order for the summation to be logical, the weights (γ_i) must be adjusted carefully for each problem instance. To resolve this issue, we use a *goal programming* approach [33] to minimize the percentage deviation of each objective from its best possible value. In this approach, the model is first solved with each of the objectives, $G_i(s)$, as a single objective model. Let $G_i(s)^*$ denote the optimal objective function value of the corresponding single objective model. We calculate the percent deviation of this objective as

$$\frac{G_i(s) - G_i(s)^*}{G_i(s)^*}. \quad (2)$$

Then to generate different non-dominated solution alternatives, we use a minimax objective function that minimizes the sum of the maximum weighted deviations of the three objectives under all scenarios as follows:

$$\text{Minimize} \sum_{s=1}^{S} \rho^s \cdot \max_{i \in \{1,2,3\}} \left\{ \gamma_i \cdot \frac{G_i(s) - G_i(s)^*}{G_i(s)^*} \right\}. \quad (3)$$

Different weights lead to different nondominated solutions in this method. To linearize this nonlinear objective function (i) we define auxiliary decision variable Q^s to be equal to the $\max$ term in this equation, (ii) write Eq. (4) as the single objective function, and (iii) include Constraint (5) to have the goal programming formulation GP.

In this approach, we solve the models separately using each of the three objectives and attain $G_i(s)^*$ values. Then input these into the GP model and solve the goal programming formulation. Constraint (6) dictates that power usage of an appliance is zero outside its operation window. Constraint (7) makes sure that appliances do not exceed their maximum power limit. Constraint (8) ensures that appliances consume the energy necessary to complete their operation. Constraint (9) calculates the power drawn from the grid using the load of the appliances, power stored to and drawn from the battery and the power generated by the renewables. Constraints (10) and (11) make sure that the battery operates within its capacity $[0, E_b^{max}]$, while the battery's charge and discharge rates are limited by constraints (12) and (13), respectively. Constraint (14) is added to the problem to ensure that the initial and final energy levels of the battery are the same. Hence, there remains sufficient amount of energy in the battery for scheduling the next day's power consumption. Constraint (15) limits the power drawn from the grid at each time slot. Constraint (16) defines the sign restrictions on the decision variables.

In the following we will describe different strategies that can be used for maximizing privacy. Note that, some of these strategies are developed for online control of the system. However, in this study, we use the main ideas of the proposed

GP: Minimize
$$\sum_{s=1}^{S} \rho^s Q^s \tag{4}$$
Subject to:
$$\gamma_i \cdot \frac{G_i(s) - G_i(s)^*}{G_i(s)^*} \leq Q^s, \quad \forall s, i \in \{1,2,3\} \tag{5}$$
$$p^s_{ca,t} = 0, \quad \forall s, \forall t \notin [\alpha_a, \beta_a] \tag{6}$$
$$p^s_{ca,t} \leq P^{max}_a, \quad \forall a, t, s \tag{7}$$
$$\Delta T \cdot \sum_{t=1}^{T} p^s_{ca,t} = E_a, \quad \forall a, s \tag{8}$$
$$p^s_{ct} = \sum_{a=1}^{NA} p^s_{ca,t} + p^s_{cb,t}/\eta_c - p^s_{db,t}/\eta_d - P^s_{g,t}, \quad \forall t, s \tag{9}$$
$$E^{init}_b + \sum_{t=1}^{\tau} \Delta T \cdot p^s_{cb,t} - \sum_{t=0}^{\tau} \Delta T \cdot p^s_{db,t} \leq E^{max}_b, \quad \forall \tau, s \tag{10}$$
$$E^{init}_b + \sum_{t=1}^{\tau} \Delta T \cdot p^s_{cb,t} - \sum_{t=0}^{\tau} \Delta T \cdot p^s_{db,t} \geq 0, \quad \forall \tau, s \tag{11}$$
$$p^s_{cb,t} \leq R^{max}_{cb}, \quad \forall t, s \tag{12}$$
$$p^s_{db,t} \leq R^{max}_{db}, \quad \forall t, s \tag{13}$$
$$\sum_{t=1}^{T} p^s_{cb,t} = \sum_{t=1}^{T} p^s_{db,t}, \quad \forall s \tag{14}$$
$$p^s_{ct} \leq P^{max}, \quad \forall t, s \tag{15}$$
$$p^s_{ct}, p^s_{ca,t}, p^s_{cb,t}, p^s_{db,t} \geq 0 \tag{16}$$

Fig. 2: Mathematical Programming framework.

strategies within an optimization framework. The uncertainty caused by the renewable generation is handled by calculating the expected value of the objective function by considering different scenarios and their occurrence probabilities.

B. Best Effort Strategy

As described earlier, the main objective of the best effort strategy is to minimize the deviation of the power drawn from the grid in adjacent time slots [19]. Two alternative formulations can be developed for this purpose. In the first alternative, denoted as BE1, $F(t,s) = \left|p^s_{ct} - p^s_{c(t-1)}\right|$. The absolute value can be linearized by introducing two non-negative decision variables, d^s_{1t} and d^s_{2t}. Then, in GP $F(t,s)$ is replaced with (17) and constraint (18) is added to the model.

$$\textbf{BE1:} \quad F(t,s) = d^s_{1t} + d^s_{2t} \tag{17}$$
$$d^s_{1t} - d^s_{2t} = p^s_{ct} - p^s_{c(t-1)} \quad \forall s, t > 1 \tag{18}$$

In the second alternative, denoted as BE2, we use $F(t,s) = |p_{ct} - L^s|$ which minimizes the deviation from the average load of all time slots under each scenario. Here, L^s denotes this average load level in scenario s which is also a decision variable and determined by the optimization model. After linearizing the absolute value similar to the previous case, $F(t,s)$ is replaced with (17) and constraint (19) is added to GP.

$$\textbf{BE2:} \quad d^s_{1t} - d^s_{2t} = p^s_{ct} - L^s \quad \forall s, t \tag{19}$$

C. Tolerable Deviation Strategy

In this strategy, we want to keep the deviation of the power drawn from the grid within a certain limit of the target metered load [21], where the target is also a decision variable. That is, we want $p^s_{ct} \in [L^s - \nu, L^s + \nu]$ as long as possible and try to minimize the number of occurrences in which p^s_{ct} is not within these limits. Here, ν is a fixed parameter. This strategy can be formulated by defining a binary decision variable z^s_t that indicates whether p^s_{ct} is within the limits or not. Then, in GP $F(t,s)$ is replaced with (20) and constraints (21) and (22) are added to the model.

$$\textbf{TD1:} \quad F(t,s) = z^s_t \tag{20}$$
$$p^s_{ct} - L^s \leq \nu + M \cdot z^s_t \quad \forall s, t \tag{21}$$
$$-p^s_{ct} + L^s \leq \nu + M \cdot z^s_t \quad \forall s, t \tag{22}$$

where M is a large number. Note that, in TD1, a single level is used. However, it is also possible to use more than a single level as explained in [21]. An alternative model can be developed by introducing another binary decision variable y^s_t that indicates whether a new load level is used at time t or not. $F(t,s)$ is replaced with (23) and constraints (24) through (27) are added to the model.

$$\textbf{TD2:} \quad F(t,s) = z^s_t + y^s_t \tag{23}$$
$$p^s_{ct} - L^s_t \leq \nu + M \cdot z^s_t \quad \forall s, t \tag{24}$$
$$-p^s_{ct} + L^s_t \leq \nu + M \cdot z^s_t \quad \forall s, t \tag{25}$$
$$L^s_t - L^s_{(t-1)} \leq M \cdot y^s_t \quad \forall s, t > 1 \tag{26}$$
$$-L^s_t + L^s_{(t-1)} \leq M \cdot y^s_t \quad \forall s, t > 1 \tag{27}$$

D. Non Intrusive Load Leveling Strategy

In this strategy, the number of deviations of the power drawn from a level is minimized [20]. Although there are recovery modes in the original approach, these are not required in the optimization framework. Then, we can replace $F(t,s)$ with (20) and add constraints (28) and (29) to the model.

$$\textbf{NILL:} \quad p^s_{ct} - p^s_{c(t-1)} \leq M \cdot z^s_t \quad \forall s, t \tag{28}$$
$$-p^s_{ct} + p^s_{c(t-1)} \leq M \cdot z^s_t \quad \forall s, t \tag{29}$$

E. Stepping Strategy

In this strategy, we want the power drawn from the grid at a certain time slot to be equal to the power drawn in the previous time slot as much as possible [22]. If it is not possible to keep the same level, then we want the new level to be a specific step size (κ) higher or lower than its previous value.

To formulate this, we need two binary decision variables r^s_{1t} and r^s_{2t}. Variable r^s_{1t} (r^s_{2t}) indicates whether the new level is higher (lower) than the previous one or not. If both of them are zero, then there is no change in the level. This strategy can be formulated by replacing $F(t,s)$ with (30) and adding constraints (31) and (32) to the model. In (30) we minimize the total number of level changes as the primary objective and the deviation of the actual power drawn from the grid from the determined level as a secondary objective. To achieve this hierarchy, we multiply the secondary objective with a small constant, ε. Variables d^s_{1t} and d^s_{2t} are used to linearize $|p^s_{ct} - L^s_t|$.

$$\textbf{Stepping:}\quad F(t,s) = r^s_{1t} + r^s_{2t} + \varepsilon \cdot (d^s_{1t} + d^s_{2t}) \tag{30}$$

$$L^s_t - L^s_{(t-1)} = \kappa \cdot (r^s_{1t} - r^s_{2t}) \quad \forall s, t > 1 \tag{31}$$

$$d^s_{1t} - d^s_{2t} = p^s_{ct} - L^s_t \quad \forall s, t \tag{32}$$

F. Minimizing the L2 Norm Strategy

In this strategy, the L2 norm of the deviation between the metered load and the average load is minimized [23]. Let $\bar{L}^s$ denote the average load per time slot. Then, we use $F(t,s) = \left\| \frac{p^s_{ct} - \bar{L}^s}{\bar{L}^s} \right\|_2$ which is a non-linear function. We can replace $F(t,s)$ with (33) and add constraint (34) to the model to attain a quadratic formulation that can be solved to optimality by CPLEX.

$$\textbf{ML2N:}\quad F(t,s) = \lambda^s \tag{33}$$

$$\sum_{t=1}^{T} \left(\frac{p^s_{ct} - \bar{L}^s}{\bar{L}^s} \right)^2 \leq (\lambda^s)^2 \quad \forall s, t \tag{34}$$

G. Minimizing the L1 Norm Strategy

In this strategy, the total deviation of the metered loads of each appliance at a certain time slot from the metered loads at all the remaining time slots is minimized [24]. This can be achieved by using $F(t,s) = \sum_{a=1}^{NA} (\max_\tau \{p^s_{ca\tau}\} - p^s_{cat})$. By this formula, the maximum load as well as the deviation of the load at each time slot from this maximum is minimized for each appliance resulting in appliance loads with minimum deviation at different time slots. We can use z^s_a to linearize this nonlinear function. Then, $F(t,s)$ is replaced with (35) and constraint (36) is added to the model.

$$\textbf{ML1N:}\quad F(t,s) = \sum_{a=1}^{NA} (z^s_a - p^s_{cat}) \tag{35}$$

$$z^s_a \geq p^s_{cat} \quad \forall a, s, t \tag{36}$$

H. No Privacy Strategy

This strategy models the case where privacy preservation do not carry any weight. It is useful for providing a baseline case for comparisons which can be modeled by using the following constraint:

$$\textbf{NoPr:}\quad F(t,s) = 0 \quad \forall s, t. \tag{37}$$

IV. Numerical Analysis

In the first part of this section (subsection IV-A) we present our renewable model, temporal modeling parameters, appliance model, disutility model, and pricing model. In the second part (subsection IV-B), we define our privacy metrics. In the third part (subsection IV-C), we present our numerical analysis.

A. Models, Parameters, and Scenarios

We employ photovoltaic (PV) panels that produce energy depending on the random solar irradiance. Irradiance at each time slot is modeled by a bimodal distribution [34], which consists of two unimodal distributions. For each unimodal distribution Beta pdf is used, where $f_b(r)$ is the pdf of the solar irradiance (kW/m^2) and $\Gamma(.)$ is the Gamma Function.

$$f_b(r) = \begin{cases} \frac{\Gamma(\varrho+\zeta)}{\Gamma(\varrho)\Gamma(\zeta)} r^{\varrho-1}(1-r)^{\zeta-1}, & 0 \leq r \leq 1; \varrho, \zeta \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{38}$$

Parameters ϱ and ζ are calculated according to the mean (μ) and variance (σ^2) as $\zeta = (1-\mu)(\frac{\mu(1+\mu)}{\sigma^2} - 1)$ and $\varrho = \frac{\mu\zeta}{1-\mu}$, respectively. Given the irradiance, renewable power output at time t is modelled as $P^s_{gt}(s) = \eta \times S \times s$, where $\eta = 0.186$ is the efficiency and $S = 40m^2$ is the solar panel area. The mean and the variance of the solar irradiance vary with time, which are given in [34]. Using these values, ϱ and ζ values are computed for each time slot. Then 4000 sample paths of PV outputs (each of size T) are generated. These 4000 sample paths are candidate scenarios. K-means clustering is utilized to reduce the number of scenarios to 10, for ease of computation [24].

In our numerical tests, we use 5-minutes (1/12 hours) reporting intervals that corresponds to a total of $T = 288$ time slots. Please note that we are considering a Non-Intrusive Load Monitoring (NILM) technique in this paper. Unlike the intrusive approaches, NILM is based on approaches that make load inferences from the smart meter data. Please see [35] for our underlying privacy violation assumption. The frequency of the smart meter data, also known as time interval data, is our reference point in determining our T value. Based on our research from regulatory sources, utility company practices, smart meter manufacturer specifications, industry data analytic companies, government reports, white papers, and academic papers, we have concluded that the dominant interval for data collection from smart meters is between 5 minutes and 15 minutes, 288 times a day and 96 times per day, respectively. Please also note that our analyses are based on a rough consensus of many papers from the literature and we thus use similar parameters from these papers.

We consider appliances that are either time or power shiftable, or nonshiftable [36]. Appliance parameters are presented in Table II.

Disutility model is inspired from [37], where power use of an appliance is multiplied with a penalty coefficient at each time slot. This coefficient grows exponentially with time, forcing the optimal solution to move its power consumption to earlier time slots. More specifically, penalty cost of appliance

TABLE II: Appliances

Appliance	Shft	Eng Req (kWh)	Min Drn (h)	Power (kW)	Intrvl
Washing Machine	Time	0.7	3.5	0.2	19-23
Clothes Dryer	Time	2.1	1	2.1	20-23
Dishwasher	Time	1.42	2	0.71	14-16, 21-7
PHEV	Time	9.9	3	3.3	22-7
Water Heater	Power	13.75	2.5	5.5	0-8
Space Heater-day	Power	3	1	3	15-20
Space Heater-night	Power	3	1	3	3-8
Iron	Time	1	0.5	2	9-24
Vacuum Cleaner	Time	0.36	0.2	1.8	9-22
Phone Charger	Time	0.01	2	0.001	18-8
Tablet Charger	Time	0.06	5	0.006	18-20
Oven	Non	5.25	1.5	3.5	–
Stove	Non	2.4	2	1.2	–
Fridge	Non	1.32	24	0.055	–
Freezer	Non	0.48	24	0.02	–
Kettle	Non	0.5	0.25	2	–
Hair Dryer	Non	0.35	0.15	2.33	–
Lighting	Non	1	5	0.2	–
TV	Non	0.5	4	0.125	–
PC/Laptop	Non	0.2	3	0.065	–

a for operating at time t ($\phi_{a,t}$) is obtained by utilizing the penalty coefficient of appliance a (δ_a) as

$$\phi_{a,t} = \frac{(\delta_a)^{\beta_a - t}}{E_a} \quad \forall a, \forall t \in [\alpha_a, \beta_a]. \tag{39}$$

We utilized $\delta_a = 0.9$ in our analysis. For example, if $\alpha_a = 3$, $\beta_a = 6$, and $E_a = 1$ for a particular appliance a then $\phi_{a,3} = 0.7290$, $\phi_{a,4} = 0.8100$, $\phi_{a,5} = 0.9000$, $\phi_{a,6} = 1.0000$, and $\phi_{a,t} = 0 \quad \forall t \notin [3, 6]$. Assuming the appliance can complete its task in two time slots with full power, completion of the task in time slots 5 and 6 will result in 23.46% more disutility than the completion of the task in time slots 3 and 4.

Time of Use (TOU) pricing model is a commonly used model in the literature. Therefore, we utilize the pricing data of 07/04/2016 from *nyiso.com*. In this data set electricity prices change at different hours of the day. Fig. 3j shows a typical trace of the electricity price.

B. Privacy Performance Metrics

We compare the outputs of our optimization models with respect to three privacy criteria. Let us call $p_A(t)$ and $p(t)$ as the aggregate appliance load and the metered load, respectively. $p_A(t)$ is the actual appliance load, whereas $p(t)$ is the load that can be observed by the meter. NILM discovers appliances turning ON and OFF by detecting the changes in the load. Therefore we consider differential loads $\Delta p(t) = p(t) - p(t-1)$ and $\Delta p_A(t) = p_A(t) - p_A(t-1)$ in evaluating the privacy performance.

1) Number of Changes (N_C): Most of the NILM schemes are based on detecting the instantaneous load changes and matching them with known appliance load signatures. Hence, number of changes that can be observed in the metered load, formulated as $N_C = \sum_{t=2}^{T} I_{|\Delta p(t)|>c_0}$, is a suitable privacy performance metric [12], [20]. Here c_0 is the detectable change threshold, which is taken as 20 W. $I_{|\Delta p(t)|>c_0}$ is the indicator function that becomes one if the load change is higher than the threshold. Lower N_C implies better privacy performance.

2) Coefficient of Determination (COD): A good privacy scheme reduces the predictability of $\Delta p_A(t)$ from $\Delta p(t)$. First, the linear least squares (LLS) fit of the form $\Delta \hat{p_A}(t) = \varphi + \chi \Delta p(t), \forall t$ is computed that minimizes the mean square difference between the actual appliance load, $\Delta p_A(t)$, and the LLS fit, $\Delta \hat{p_A}(t)$ [19] [24]. Then the residual sum of squares, $SS_{res} = \sum_t (\Delta \hat{p_A}(t) - \Delta p_A(t))^2$, and the regression sum of squares, $SS_{req} = \sum_t (\Delta \hat{p_A}(t) - \overline{\Delta p_A(t)})^2$, are computed. Finally, the coefficient of determination is computed as $COD = 1 - \frac{SS_{res}}{SS_{res}+SS_{req}}$. A lower COD value implies better privacy protection.

3) Relative Entropy ($D(p||p_A)$): Relative entropy, $D(p||p_A) = \sum_{c \in \mathcal{C}} p_p(c) \log(\frac{p_p(c)}{p_{p_A(c)}})$ [19], [20], is a measure of the difference between the empirical probability mass functions (pmf) of differential metered and appliance loads. Here $p_p(c)$ and $p_{p_A(c)}$ are the pmf's of $\Delta p(t)$ and $\Delta p_A(t)$, respectively. To obtain these pmf's we divide the differential load range into bins of equal size (b). $p_p(i)$ is the fraction of load changes in $[ib, (i+1)b]$. Parameter b is taken to be 2 kW. Higher $D(p||p_A)$ implies better privacy performance.

4) Combined Privacy Metric (Pr_{comb}): In the presence of three different privacy measures we have defined, it may be hard to compare the presented models in terms of privacy. In order to level the playing field, we propose a *combined privacy metric*. This combined metric is formulated as $Pr_{comb} = \frac{(N_C)\times(CoD)}{D(p||p_A)}$. Lower Pr_{comb} implies a better privacy protection. When $p(t) = p_A(t), \forall t$, this means no privacy protection and Pr_{comb} becomes infinity. The latter corresponds to the case without renewable power and battery.

C. Comparative Analysis

All the models presented in Section III are solved using the generated test problems using 10 scenarios under the stochastic programming framework. We utilized the GAMS CPLEX 12.6.2 solver on a machine with an 8-core i7 CPU and 16 GB RAM. The results are given in Table III and Table IV. In these tables, each column represents a variation of priority weights ($\gamma_1, \gamma_2, \gamma_3$) which account for cost, disutility, and privacy coefficients, respectively. Each entry is a 5-tuple, [Cost, Disutility, N_C, COD, $D(p||p_A)$] representing five performance metrics. Furthermore, the combined metric values for all coefficient sets are presented in Table V.

For nonzero privacy weights ($\gamma_3 > 0$), *Stepping*, *NILL*, *BE1* and *TD2* are always the best four strategies. This can also be observed in Fig. 3, where appliance, metered, and battery power profiles are plotted for a single scenario. These strategies provide flat metered loads, therefore, significantly reduce the number of jumps in the metered load. If the privacy

TABLE III: Results with multiple weighted objectives [Cost, Disutility, N_C, COD, $D(p||p_A)$]

	Priority Weights $(\gamma_1, \gamma_2, \gamma_3)$			
Strategy	(1,1,1)	(10,1,1)	(1,1,10)	(1,10,1)
BE1	[15.12 3.26 **3** 0.016 **2.45**]	[13.91 6.63 9.99 **0.006** 1]	[15.81 3.33 **4** 0.009 2.07]	[15.58 2.73 7.30 0.126 0.26]
BE2	[13.80 2.98 73.60 0.489 0.14]	[12.72 4.09 79.89 0.571 0.19]	[14.52 3.13 40.52 0.537 0.16]	[14.63 2.65 54.98 0.191 0.22]
TD1	[**13.46** **2.90** 41.07 0.603 0.55]	[**12.44** **3.50** 49.79 0.600 0.59]	[**13.70** **2.96** 36.62 0.581 0.58]	[**13.94** **2.63** 42.25 0.571 0.50]
TD2	[15.07 3.54 3.80 0.062 0.62]	[13.75 5.90 7.82 0.086 0.79]	[15.39 4.51 10.06 0.009 0.88]	[15.80 2.74 4.54 0.010 0.64]
NILL	[15.31 4.19 **3.09** 0.021 1.46]	[14.17 5.32 **5** 0.051 **1.57**]	[15.59 4.77 **3.95** 0.009 1.22]	[15.90 2.85 **3.91** 0.010 **1.05**]
Stepping	[15.12 3.26 **3** 0.003 2.33]	[13.91 6.58 9.99 0.009 1.09]	[15.80 3.35 **4** **0.006** **2.17**]	[15.58 2.73 7.79 0.125 0.26]
L1	[15.42 3.33 95.18 **0.002** 0.32]	[12.64 3.93 89.92 0.025 0.27]	[15.78 4.87 98.18 0.009 0.35]	[16.05 2.87 93.76 **0.004** 0.32]
L2	[14.47 3.12 212.8 0.157 0.08]	[13.08 4.86 204.8 0.228 0.07]	[15.41 3.32 159.2 0.179 0.13]	[15.86 2.68 118 0.287 0.21]
NoPr	[12.81 2.76 63.01 0.498 0.18]	[12.35 3.30 61.82 0.604 0.31]	[12.81 2.76 63.01 0.498 0.18]	[13.25 2.62 58.53 0.413 0.20]

TABLE IV: Results with single objectives [Cost, Disutility, N_C, COD, $D(p||p_A)$]

	Priority Weights $(\gamma_1, \gamma_2, \gamma_3)$		
Strategy	(1,0,0)	(0,0,1)	(0,1,0)
BE1	[12.03 6.24 60.22 0.434 0.40]	[16.02 4.64 4.80 0.011 1.79]	[16.40 2.59 79.84 0.005 0.25]
BE2	[12.03 6.24 60.22 0.434 0.40]	[15.93 4.79 60.28 0.019 0.31]	[16.40 2.59 79.84 0.005 0.25]
TD1	[12.03 6.26 62.29 0.372 0.73]	[15.87 **4.29** 50.28 0.466 1.50]	[16.35 2.59 96.21 0.004 0.71]
TD2	[12.03 6.19 62.83 0.274 0.42]	[15.59 5.16 2.49 0.006 1.15]	[16.30 2.59 93.75 0.003 0.45]
NILL	[12.03 6.32 62.05 0.341 0.74]	[**15.43** 4.72 **2.00** 0.006 **2.11**]	[16.33 2.59 111.8 0.005 0.53]
Stepping	[12.03 6.23 63.03 0.270 0.44]	[16.10 4.93 4.61 0.014 1.70]	[16.25 2.59 91.41 0.073 0.40]
L1	[12.03 6.23 63.03 0.270 0.44]	[16.27 4.35 98.30 **0.002** 0.33]	[16.25 2.59 91.41 0.073 0.40]
L2	[12.03 6.33 60.42 0.446 0.38]	[16.08 4.52 5.39 0.251 0.31]	[16.35 2.59 92.48 0.006 0.49]
NoPr	[12.03 6.24 60.22 0.434 0.40]	[N/A]	[16.40 2.59 79.84 0.005 0.25]

TABLE V: Combined privacy metric with multiple weighted objectives

	Priority Weights $(\gamma_1, \gamma_2, \gamma_3)$						
Strategy	(1,1,1)	(10,1,1)	(1,1,10)	(1,10,1)	(1,0,0)	(0,0,1)	(0,1,0)
BE1	0.020	0.070	0.017	3.537	65.34	0.029	1.597
BE2	257.07	240.1	136.0	47.73	65.34	3.694	1.597
TD1	45.03	50.63	36.68	48.25	31.74	15.62	0.542
TD2	0.38	0.85	0.103	0.071	40.99	0.013	0.804
NILL	0.044	0.162	0.029	0.037	28.59	0.0056	1.055
Stepping	0.0004	0.082	0.011	3.745	38.68	0.038	16.68
L1	0.595	8.33	2.52	38.68	38.68	0.596	16.68
L2	417.58	667.06	219.2	161.3	70.91	4.364	1.132
NoPr	174.32	120.45	3324	120.9	65.34	[N/A]	1,597

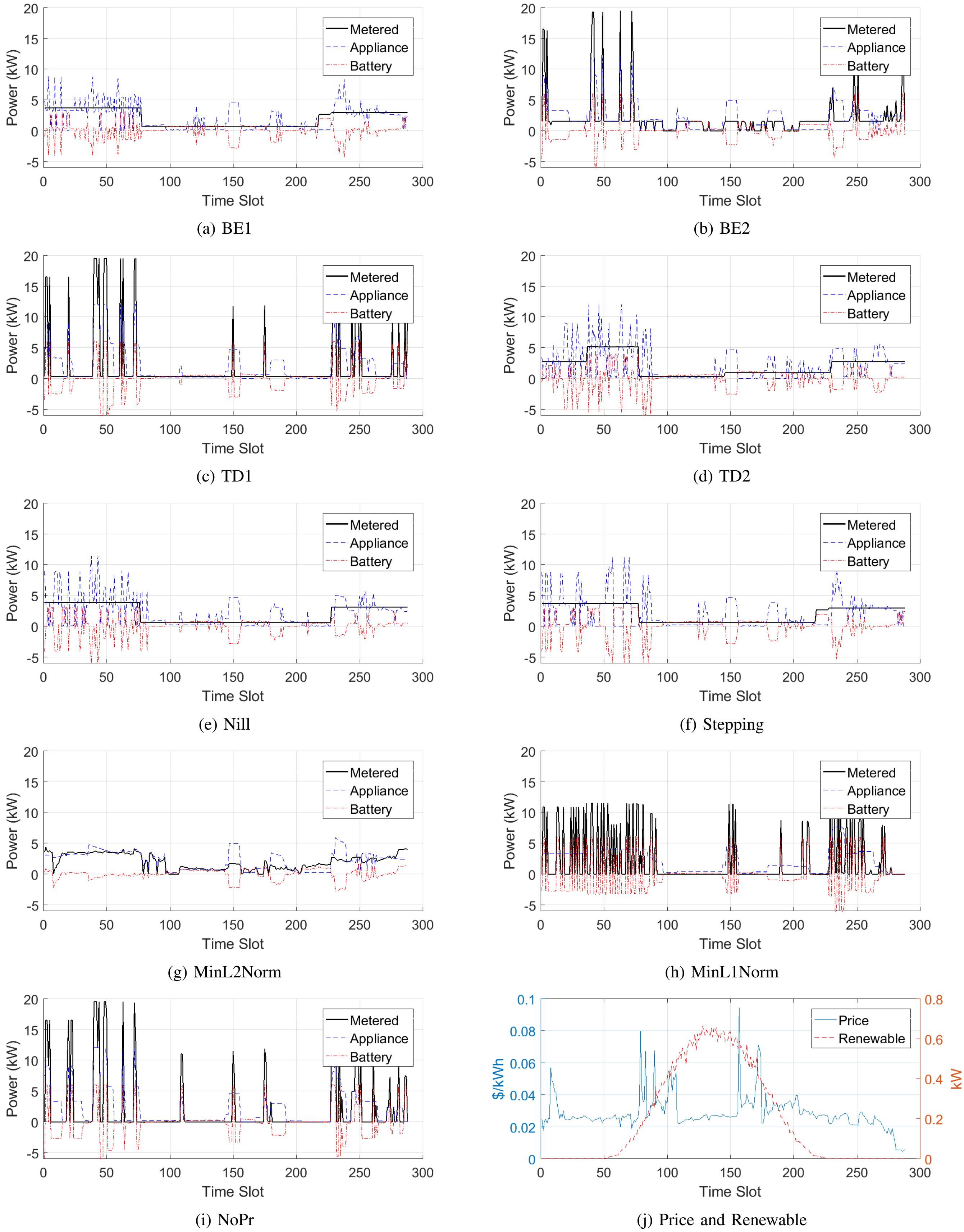
TABLE VI: Effects of PV module size [Cost, Disutility, N_C, COD, $D(p||p_A)$]

	PV Module Area (m^2)		
Strategy	0	40	80
BE1	[16.87 4.38 3.10 0.003 1.99]	[15.47 3.76 2.91 0.008 2.01]	[14.80 3.57 3 0.013 1.56]
BE2	[14.89 3.86 74.50 0.245 0.43]	[14 3.63 62.68 0.197 0.25]	[13.74 3.56 49.32 0.174 0.30]
TD1	[15.37 3.98 35.80 0.642 0.71]	[14.23 3.69 30.43 0.248 1.21]	[13.31 3.45 29.66 0.545 0.61]
TD2	[17.08 4.48 4.40 0.010 1.25]	[16.03 4.34 4.13 0.017 1.21]	[15.68 4.29 4.11 0.037 1.04]
NILL	[17.06 4.39 3.70 0.014 1.56]	[15.42 4.02 3.11 0.009 1.86]	[13.22 3.93 2.98 0.008 1.72]
Stepping	[16.87 4.30 4 0.005 1.88]	[15.46 3.68 3 0.005 2.77]	[14.79 3.75 3 0.006 1.50]
L1	[14.16 3.67 103.6 0.041 0.27]	[13.11 3.40 88.13 0.042 0.27]	[12.83 3.33 83.99 0.006 0.27]
L2	[15.74 4.08 221 0.095 0.02]	[14.73 3.82 203.3 0.129 0.06]	[14.32 3.71 183.8 0.142 0.13]

is at least as important as the other metrics, that is, the weight sets $(1,1,1)$ and $(1,1,10)$ are used, then the *Stepping* strategy has the best privacy performance. After determining the four better privacy-preserving strategies, we compare those in terms of cost and disutility. Table III reveals that these four strategies result in similar costs for all coefficient sets. *BE1* and *Stepping* perform slightly better in terms of disutility among the four privacy preserving algorithms.

BE1 and *Stepping* strategies require much less run time (a few minutes) among the top four privacy-preserving algorithms. On the other hand, NILL and TD2 strategies require several hours for runtime. *BE1* and *Stepping* strategies are also easier to implement as online algorithms [19], [22].

As it can be observed in Table IV, the overall minimum cost and disutility values are attained by all algorithms when the coefficient sets $(1,0,0)$ and $(0,1,0)$ are used, respectively. On the other hand, *NoPr* strategy provides the best cost and disutility values among all strategies for all coefficient sets in Table III. This is because, while other strategies sacrifice the cost and disutility objectives to improve the privacy, *NoPr*



(a) BE1
(b) BE2
(c) TD1
(d) TD2
(e) Nill
(f) Stepping
(g) MinL2Norm
(h) MinL1Norm
(i) NoPr
(j) Price and Renewable

Fig. 3: Metered, battery, and appliance power (Fig. 3a–3i) plus electricity price and renewable power (Fig. 3j).

focuses only on the cost and disutility. This is an expected trade-off between privacy and cost/disutility.

Fig. 3j presents a typical renewable power output, which is a linear function of the PV panel surface area. Table VI presents the performance metrics as a function of the PV panel surface area. As the surface area increases from 0 to $80m^2$, on the average more than 10% decrease in cost and disutility is attained. As for the privacy performance, renewable capacity does not have a significant effect on the best performing strategies (*i.e.*, *Stepping*, *NILL*, *BE1*, and *TD2*). Yet, strategies that perform poor in terms of privacy are significantly affected by the PV capacity (*e.g.*, more than 15% decrease in N_C is achieved for *BE2*, *TD1*, *L1*, and *L2*).

We have also run experiments by utilizing 15-minute slot durations and confirm that all our findings reported in this paper holds for both 5 minutes (T=288) and 15 minutes (T=96) intervals. The only noteworthy difference is that the N_C increases as slot time decreases, which is quite intuitive (*i.e.*, as the data collection interval increases from 5 to 15 minutes, the observed number of changes from time slot to time slot also naturally goes down) [27], [28].

V. Conclusion

Demand-side management techniques, considered as the low-hanging fruit of the smart grid efforts, rely heavily on optimization formulations, which in turn require collection and dissemination of fine-grained measurements and electricity usage data. The Achilles's heel of the aforementioned approaches is potential privacy violations. Load shaping with storage and distributed renewable energy sources for privacy preservation is one of the promising technical solutions. In this study, we present a comprehensive comparative analysis of prominent privacy preservation techniques based on load shaping. Our contributions are listed as follows:

1) We have developed a novel mathematical programming framework to model eight privacy preservation strategies. All our strategies are inspired by the techniques reported in the literature.
2) We have utilized all the mechanisms envisioned for load shaping to preserve privacy through a single, unified model (*i.e.*, renewable energy resources, on-site battery, and load moderation). To the best of our knowledge, our study and framework is the first such study in the literature for privacy preserving power scheduling.
3) We have presented a comprehensive performance analysis in terms of monetary cost, disutility, and various privacy metrics under fair and ideal conditions for the privacy preservation techniques in the literature.

We believe that the mathematical programming framework and the results of our analysis thereof are invaluable in understanding the fundamental performance bounds of the proposed approaches in the literature under ideal conditions. Furthermore, the results of this study serve as a stepping stone in developing insight and novel techniques on privacy preservation via load shaping in smart grid.

References

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[2] T. Strasser, P. Siano, and V. Vyatkin, "New trends in intelligent energy systems: An industrial electronics point of view," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2420–2423, Apr. 2015.

[3] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[4] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Trans. Ind. Informat.*, vol. 7, no. 3, pp. 381–388, Aug. 2011.

[5] R. Deng, Z. Yang, M.-Y. Chow, and J. Chen, "A survey on demand response in smart grids: Mathematical models and approaches," *IEEE Trans. Ind. Informat.*, vol. 11, no. 3, pp. 570–582, Jun. 2015.

[6] M. Alipour, B. Mohammadi-Ivatloo, and K. Zare, "Stochastic scheduling of renewable and CHP-based microgrids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1049–1058, Oct. 2015.

[7] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 425–436, Feb. 2016.

[8] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Sec. Priv.*, vol. 7, no. 3, pp. 75–77, May. 2009.

[9] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Perez, "Do not snoop my habits: preserving privacy in the smart grid," *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 166–172, May. 2012.

[10] S. Uludag, S. Zeadally, and M. Badra, *Techniques, Taxonomy, and Challenges of Privacy Protection in the Smart Grid*. Springer, Oct. 2015, pp. 343–390.

[11] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring Personal Information from Demand-Response Systems," *IEEE Security Privacy*, vol. 8, no. 1, pp. 11–20, Jan. 2010.

[12] G. W. Hart, "Nonintrusive appliance load monitoring," *Proc. IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.

[13] Z. Wang and G. Zheng, "Residential Appliances Identification and Monitoring by a Nonintrusive Method," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 80–92, Mar. 2012.

[14] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2010, pp. 238–243.

[15] C. I. Fan, S. Y. Huang, and Y. L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 666–675, Feb. 2014.

[16] F. Li, B. Luo, and P. Liu, "Secure and privacy-preserving information aggregation for smart grids," *Int. J. Secur. Netw.*, vol. 6, no. 1, pp. 28–39, Apr. 2011.

[17] F. Rassaei, W. S. Soh, and K. C. Chua, "Distributed scalable autonomous market-based demand response via residential plug-in electric vehicles in smart grids," *IEEE Trans. Smart Grid*, vol. PP, no. 99, pp. 1–1, 2016.

[18] A. O. Isikman, C. Altun, S. Uludag, and B. Tavli, "Power scheduling in privacy enhanced microgrid networks with renewables and storage," in *Proc. IEEE Ann. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2016, pp. 405–410.

[19] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGrid-Comm)*, Oct. 2010, pp. 232–237.

[20] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Oct. 2011, pp. 87–98.

[21] B. Ge and W. T. Zhu, "Preserving user privacy in the smart grid by hiding appliance load characteristics." ser. Lecture Notes in Computer Science, G. Wang, I. Ray, D. Feng, and M. Rajarajan, Eds., vol. 8300. Springer, 2013, pp. 67–80.

[22] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Oct. 2012, pp. 415–427.

[23] Y. Sun, L. Lampe, and V. W. S. Wong, "Combining electric vehicle and rechargeable battery for household load hiding," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2015, pp. 611–616.

[24] Z. Chen and L. Wu, "Residential appliance DR energy management with electric privacy protection by online stochastic optimization," *IEEE Trans. Smart Grid*, vol. 4, no. 4, pp. 1861–1869, Dec. 2013.

[25] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 190–195.

[26] P. Barbosa, A. Brito, and H. Almeida, "Defending against load monitoring in smart metering data through noise addition," in *Proc. Ann. ACM Symp. Appl. Comput. (SAC)*, Apr. 2015, pp. 2218–2224.

[27] G. Eibl and D. Engel, "Influence of data granularity on nonintrusive appliance load monitoring," in *Proc. ACM Workshop Inf. Hiding Multimedia Security (IH&MMSec)*, Jun. 2014, pp. 147–151.

[28] G. Eibl and D. Engel, "Influence of data granularity on smart meter privacy," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 930–939, Mar. 2015.

[29] D. Egarter, C. Prokop, and W. Elmenreich, "Load hiding of household's power demand," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2014, pp. 854–859.

[30] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, "Preventing occupancy detection from smart meters," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2426–2434, Sep. 2015.

[31] G. Kalogridis, R. Cepeda, S. Z. Denic, T. Lewis, and C. Efthymiou, "ElecPrivacy: Evaluating the privacy protection of electricity management algorithms," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 750–758, Dec. 2011.

[32] G. Kalogridis, M. Sooriyabandara, Z. Fan, and M. A. Mustafa, "Toward unified security and privacy protection for smart meter networks," *IEEE Syst. J.*, vol. 8, no. 2, pp. 641–654, Jun. 2014.

[33] T. Tanino, T. Tanaka, and M. Inuiguchi, *Multi-objective programming and goal programming: theory and applications*. Springer, 2013.

[34] M. Mazidi, A. Zakariazadeh, S. Jadid, and P. Siano, "Integrated scheduling of renewable generation and demand response programs in a microgrid," *Energ. Convers. Manage.*, vol. 86, pp. 1118–1127, Oct. 2014.

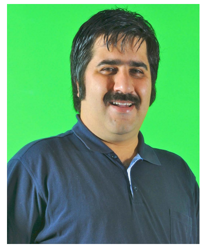
[35] L. Stankovic, V. Stankovic, J. Liao, and C. Wilson, "Measuring the energy intensity of domestic activities from smart meter data," *Applied Energy*, vol. 183, pp. 1565–1580, Dec. 2016.

[36] F. B. Saghezchi, F. B. Saghezchi, A. Nascimento, and J. Rodriguez, "Game theory and pricing strategies for demand-side management in the smart grid," in *Proc. Int. Symp. Commun. Syst. Netw. Digtl. Sign. Proc. (CSNDSP)*, Jul. 2014, pp. 883–887.

[37] A. H. Mohsenian-Rad and A. Leon-Garcia, "Optimal residential load control with price prediction in real-time electricity pricing environments," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 120–133, Sep. 2010.

Cihan Emre Kement has received his BS degree in Electrical and Electronics Engineering from Bilkent University, Ankara, Turkey, in 2011. He received his MS degree in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey, in 2014. He is currently a PhD candidate at TOBB University of Economics and Technology, Ankara, Turkey. His research interests include wireless communications, optimization and smart grid.

Hakan Gultekin is an Associate Professor at the Department of Industrial Engineering at TOBB University of Economics and Technology in Ankara, Turkey. He received his BS, MS and PhD degrees in Industrial Engineering from Bilkent University in Turkey. Before joining TOBB ETU he visited the University of Liege in Belgium for postdoctoral studies. He received a Career Award and a Project Performance Award from the Scientific and Technological Research Council of Turkey. His research interests include scheduling, optimization modeling, and exact and heuristic algorithm development, especially for problems arising in modern manufacturing systems, energy systems, and wireless sensor networks.



Bulent Tavli (S'97–M'05–SM'17) is a Professor at the Electrical and Electronics Engineering Department, TOBB University of Economics and Technology, Ankara, Turkey. He received his BS degree in Electrical and Electronics Engineering from the Middle East Technical University, Ankara, Turkey, in 1996. He received his MS and PhD degrees in Electrical and Computer Engineering from the University of Rochester, Rochester, NY, USA in 2002 and 2005, respectively. Wireless communications, networking, optimization, embedded systems, information security, and smart grid are his current research areas.

Tolga Girici (S'99–M'07) received his B.S. degree from Middle East Technical University, Ankara, Turkey in 2000 and Ph.D. degree from University of Maryland, College Park in 2007, both in Electrical Engineering. In 2005, he has spent six months as an intern at the Intelligent Automation Inc, Rockville, MD USA. He was a research assistant at the Fujitsu Labs, College Park MD USA in 2006-2007. He is currently an associate professor at TOBB University of Economics and Technology, Ankara, Turkey. He received a TUBITAK Career Award in 2010, and actively collaborates with industry. His research interests include resource allocation and optimization in next generation cellular wireless access networks, wireless ad hoc networks, smarty grid and tactical networks.

Suleyman Uludag (S'97–M'07) is an Associate Professor of Computer Science at the University of Michigan - Flint. His research interests have been around secure data collection, Smart Grid communications, Smart Grid privacy, Smart Grid optimization, demand response bidding privacy, Denial-of-Service in the Smart Grid, cybersecurity education and curriculum development, routing and channel assignment in Wireless Mesh Networks, Quality-of-Service (QoS) routing in wired and wireless networks, topology aggregation.