Online Energy Management Strategy Design for Smart Meter Privacy Against FHMM-based NILM

Yang You and Tobias J. Oechtering
KTH Royal Institute of Technology, Stockholm, Sweden

***Abstract*—We consider the privacy-preserving problem for smart grid consumers where the adversary employs a factorial hidden Markov model based inference for load disaggregation. An online convex optimization framework is further proposed for the privacy-preserving energy management strategy design. With certain specific assumptions, the derived online energy management strategy is shown to have a sublinear dynamic regret and a sublinear dynamic fit, which means our proposed online algorithm has the asymptotic performance with the optimal offline dynamic benchmark. The performance of the design approach is finally illustrated in numerical experiments.**

***Index Terms*—Smart meter privacy, privacy-preserving, non-intrusive load monitoring, factorial hidden Markov model, online convex optimization.**

I. Introduction

In future smart grids, smart meters are essential components to deliver information about consumers' energy demand to the energy provider (EP). This information can help the EP to improve the prediction on the future energy demands and therefore to increase the efficiency of the whole smart grid [1]. However, this benefit is at a cost of privacy of consumers, since an adversary (this could be a legitimate receiver of the data, e.g., the energy grid operator) can use standard energy load disaggregation algorithms.

Regarding this issue, different approaches have been proposed previously. One approach is to modify the smart metering data before it is sent to the EP by using off-the-shelf methods, such as obfuscation [2], anonymization [3], and data aggregation [4]. The major limitation of these methods is that they hide the real energy flow in the grid so that these methods fail if the legitimate receiver of the data requires exact measurements. Moreover, the adversary (even a compromised EP) may decide to install a sensor for directly monitoring the energy request of a household or a business. The EU General Data Protection Regulation (GDPR) [5] calls for an authorized data recipient to hold and process only the data absolutely necessary for the completion of its duties as well as limiting the access to personal data to those needed to act out the processing [5]. To achieve this, GDPR advocates for innovative privacy-by-design approaches as considered here. Using an energy storage such as rechargeable battery [6]–[10], or an alternative energy supply such as renewable energy source [11]–[13], the actual consumer profile can be modified by a privacy-enhancing energy management strategy.

Recently, the non-intrusive load monitoring (NILM) [14] load disaggregation algorithms have been significantly advanced. Instead of intrusively monitoring the energy consumption of the individual appliances, the NILM algorithm can achieve the load disaggregation based on the analysis of voltage and current waveforms measured at the electrical services entry point. The hidden Markov model (HMM) and its variants have been widely used for the NILM algorithms [15]–[17]. In particular, as an extension of the basic HMM, the authors in [18] propose an additive factorial hidden Markov model (FHMM) for the NILM algorithms, where the aggregated energy consumption of the consumer is modeled as an additive form of each appliance's energy consumption. However, due to its efficiency on the load disaggregation, the NILM algorithm has brought more privacy risks in the meanwhile. To protect the consumers' privacy against the NILM algorithms, different privacy-preserving schemes have been proposed previously [19]–[21].

In this paper, we consider a smart privacy-preserving problem against NILM load disaggregation techniques which apply FHMM based inference. We show that the privacy-preserving problem is equivalent to finding an energy management strategy that minimizes the joint log-likelihood of the energy request sequence and the appliances' operating state sequence given the FHMM parameters. With the assumption that the energy consumption profile can only be known causally, we propose an online convex optimization (OCO) approach to design the corresponding online energy management strategy. We further show that the designed online energy management strategy have sublinear dynamic regret and sublinear dynamic fit with some specific assumptions, which theoretically guarantees the performance of our proposed algorithm.

Accordingly, the contribution of this paper can be accordingly summarized as follows: (i) We formulate a privacy-preserving problem and propose the privacy-by-design approach for the case where the adversary applies FHMM based inference for load disaggregation; (ii) We provide an online convex optimization framework for the energy management strategy design, which is more reasonable when considering the realistic system and is also computationally more efficient. (iii) We proved the performance of our proposed online algorithm is theoretically guaranteed under certain conditions.

II. Background on FHMM-based NILM

In this section, we propose a privacy-preserving problem against the FHMM-based NILM adversary. In more details,

978-1-7281-6127-3/20/$31.00 ©2020 IEEE

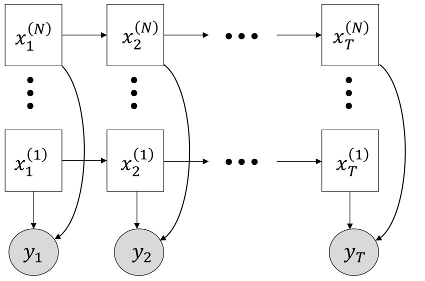

Fig. 1. Graphical structure of factorial HMM

the NILM problem is formulated as a inference problem under FHMM framework. And we further propose the energy management scheme that can preserve consumers' privacy.

A. Basic HMM for Individual Appliance

Assuming the appliance can operate at K different states, and the operating state cannot be directly measured. At each time step, an operating state emits a certain amount of power consumption. Given an operating state i, we further assume the corresponding power consumption follows the Gaussian distribution with mean μ_i and standard deviation σ_i. In this case, we consider an HMM with the hidden state $X_t \in \mathcal{X} = \{1, 2, ..., K\}$ to be the operating states of an appliance, and the observation variable Y_t represents the continuous power consumption with $Y_t \sim \mathcal{N}(\mu_i, \sigma_i)$. Accordingly, the HMM for an individual appliance is then fully characterized by the following parameters:

- Transition matrix $A \in \mathbb{R}^{K \times K}$ with the element A_{ij} represent the stationary transition probability of an appliance transfer from state i at time t to state j at time $t+1$:
$$A_{ij} = P_{X_{t+1}|X_t}(x_{t+1} = j | x_t = i), \tag{1}$$
- Prior distribution of initial state $\pi_i = P_{X_1}(x_1 = i)$, where π_i represents the probability that an appliance is initially in state i.
- All possible emission distributions $B = \{\mathcal{N}(\mu_i, \sigma_i)\}_{i=1}^K$, where each of the Gaussian distribution $\mathcal{N}(\mu_i, \sigma_i)$ represents the emission distribution of the hidden state i.

Thus, fitting the basic HMM to an individual appliance requires learning the above parameters, which has been widely studied and developed in the NILM area [15]–[17].

B. FHMM Modeling for Multiple Appliances

Assuming there are N appliances in a household, the NILM problem can be formulated as a FHMM inference problem by combining all individual basic HMM models [18]. The schematic is shown as Fig. 1, where the superscript indicates the index of appliance and the subscript indicates the time index. As shown in the figure, the hidden state sequence $\{x_t^{(n)}\}_{t=1}^T, \forall n \in \{1, ..., N\}$ represents the operating state sequence of the n-th appliance over time horizon T. At time step t, the operating states of all N appliances lead to an aggregated power consumption y_t. Thus, the sequence $\{y_t\}_{t=1}^T$ is regarded as the observation sequence for our FHMM.

By using the same notation as the basic HMM, we define $\theta^{(1:N)} = \{\pi^{(1:N)}, A^{(1:N)}, B^{(1:N)}\}$ as the parameters that fully characterize our FHMM. In this case, the joint log-likelihood of our FHMM can be written as:

$$\begin{aligned} \mathcal{L}(\mathbf{y}, \mathbf{x}^{(1:N)} | \theta^{(1:N)}) = & \sum_{n=1}^{N} \log P(x_1^{(n)} | \pi^{(n)}) \\ & + \sum_{t=2}^{T} \sum_{n=1}^{N} \log P(x_t^{(n)} | x_{t-1}^{(n)}, A^{(n)}) \\ & + \sum_{t=1}^{T} \log P(y_t | x_t^{(1:N)}, B^{(1:N)}) \end{aligned} \tag{2}$$

where $\mathbf{y} = \{y_t\}_{t=1}^T$ and $\mathbf{x}^{(n)} = \{x_t^{(n)}\}_{t=1}^T, \forall n \in [1, N]$. Given the parameters $\theta^{(1:N)}$ are known, the NILM problem then becomes the problem of inferring the most likely underlying operating state sequences $\mathbf{x}^{(1:N)}$, i.e., find the hidden state sequences that maximize the following joint log-likelihood:

$$\mathbf{x}^{*(1:N)} = \arg\max_{\mathbf{x}^{(1:N)}} \mathcal{L}(\mathbf{y}, \mathbf{x}^{(1:N)} | \theta^{(1:N)}). \tag{3}$$

C. Privacy Preserving Against the FHMM Inference adversary

In the following, we propose the privacy-preserving energy management problem against the adversary that employs an unauthorized FHMM inference, i.e., the adversary tries to solve (3) for the purpose of energy load disaggregation. Due to privacy reason, the consumer wishes to hide this true operating state sequence $\mathbf{x}^{*(1:N)}$ against the adversary. Thus, given $\mathbf{x}^{*(1:N)}$, an energy management unit (EMU) should design an energy request sequence $\mathbf{y}$ that minimizes the joint log-likelihood defined in (2):

$$\mathbf{y}^* = \arg\min_{\mathbf{y}} \mathcal{L}(\mathbf{y}, \mathbf{x}^{*(1:N)} | \theta^{(1:N)}). \tag{4}$$

In this case, given the modified energy request sequence $\mathbf{y}^*$, the true operating state sequences $\mathbf{x}^{*(1:N)}$ will lead to the minimum joint log-likelihood, which is the worst case for the adversary.

On noticing the first two terms in (2) are not affected by $\mathbf{y}$, the optimization problem in (4) can be equivalently transformed to the following problem:

$$\mathbf{y}^* = \arg\min_{\mathbf{y}} \sum_{t=1}^{T} \log P(y_t | x_t^{(1:N)}, B^{(1:N)}), \tag{5}$$

where the RHS of the equation is fully paramterized by the emission distributions $B^{(1:N)}$. For the HMM-based energy load disaggregation, we assume the adversary follows the common model with Gaussian emission distribution for each individual appliance. At time step t, given the independent assumption between different appliances, the aggregated energy request y_t is also normally distributed, i.e., $y_t \sim$

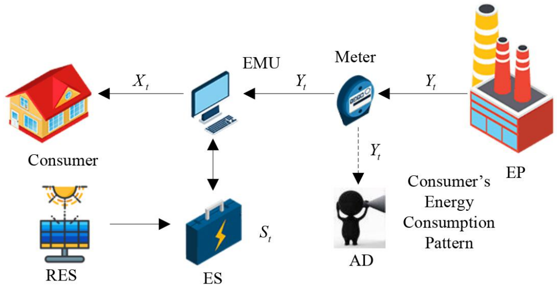

Fig. 2. System Model

$\mathcal{N}(\sum_{n=1}^{N}\mu_{x_t}^{(n)}, \sum_{n=1}^{N}(\sigma_{x_t}^{(n)})^2)$, where $\mu_{x_t}^{(n)}$ and $\sigma_{x_t}^{(n)}$ denote the mean and standard deviation of the operating state of n-th appliance at time t. Accordingly, $\log P(y_t|x_t^{(1:N)}, B^{(1:N)})$ can be expressed by:

$$\log\frac{1}{\sqrt{2\pi\sum_{n=1}^{N}(\sigma_{x_t}^{(n)})^2}} - \frac{1}{2\sum_{n=1}^{N}(\sigma_{x_t}^{(n)})^2}(y_t - \sum_{n=1}^{N}\mu_{x_t}^{(n)})^2. \tag{6}$$

On combining the above results, we end up with the following privacy preserving problem.

Proposition 1. *The privacy preserving problem in (5) is equivalent to the following optimization problem:*

$$\boldsymbol{y}* = \arg\min_{\boldsymbol{y}} \sum_{t=1}^{T}[-\frac{1}{2\sigma_t^2}(y_t - \mu_t)^2], \tag{7}$$

where $\mu_t = \sum_{n=1}^{N}\mu_{x_t}^{(n)}$ and $\sigma_t^2 = \sum_{n=1}^{N}(\sigma_{x_t}^{(n)})^2$.

III. Privacy-Preserving Problem Formulation

A. System Model

Consider a smart metering system as shown in Fig. II. At time step t, denote consumers' actual energy consumption by $z_t \in \mathcal{Z} = [z_{min}, z_{max}]$ and the energy request by $y_t \in \mathcal{Y} = [0, y_{max}]$. The energy storage (ES), e.g., a rechargeable battery, has a finite capacity with its instantaneous storage level denoted by $s_t \in \mathcal{S} = [0, s_{max}]$, and we further assume the battery capacity is larger than the maximum actual energy consumption, i.e., $s_{max} > z_{max}$. The instantaneous energy consumption z_t should always be satisfied by supplies from either EP or ES without wasting energy. Then, the ES level evolves as:

$$s_{t+1} = s_t + y_t - z_t. \tag{8}$$

In addition, to guarantee $0 \leq s_t \leq s_{max}$, the energy request y_t should be chosen within the following feasible set:

$$\begin{aligned}&\overline{\mathcal{Y}}(\,z_t, s_t)\\&= \{y_t \in \mathcal{Y} : \max\{0, z_t - s_t\} \leq y_t \leq s_{max} + z_t - s_t\},\end{aligned} \tag{9}$$

where the lower bound $z_t - s_t$ ensures that the energy supply y_t provides at least the rest energy when ES level s_t cannot solely satisfy the consumer demand; and the lower bound 0 is because no energy can be sold back to the grid; the upper bound is due to the constraints of finite maximum ES capacity and that no energy should be wasted. In addition, we assume that the ES also has access to a renewable energy source (RES), which can provide a constant amount of energy R in total at each time step, and the RES is shared by M consumers. However, the energy amount R produced by the RES is limited at each time step. Thus, we require each consumer can only request energy from the RES when it is essential to guarantee the performance of its individual energy management strategy. Assuming the adversary is applying the above FHMM model to infer on the consumer's energy consumption pattern for all N appliances over a certain time period T, i.e., $\{x_1^n, x_2^n, ..., x_T^n\}, \forall n \in [1, N]$. Thus, the corresponding privacy-preserving problem is given by:

$$\min_{y_t \in \overline{\mathcal{Y}}(z_t, s_t), \forall t} \sum_{t=1}^{T} l_t(y_t), \tag{10}$$

where $l_t(y_t) = -\frac{1}{2\sigma_t^2}(y_t - \mu_t)^2$.

Solving such a problem via offline optimization methods requires full knowledge of the time-varying function $l_t(\cdot)$ over the T-time horizon, and this knowledge is usually hard to be acquired since the consumer's energy consumption behavior is usually unable to be predicted. On the other hand, the complexity solving this problem via offline approaches grows rapidly with the growth of T and the complexity of system dynamics. In this case, we next propose an OCO approach to solve this problem.

IV. Online Privacy-Preserving Energy Management Strategy Design

A. OCO Problem Formulation

We first define a new time-varying feasible set for the energy request:

$$\hat{\mathcal{Y}}(z_t, s_t) = \{y_t \in \mathcal{Y} : y_t \in [\max\{0, z_t - s_t\}, +\infty)\}. \tag{11}$$

To maintain the hard energy request constraint (10), we further another time-varying constraint as following:

$$g_t(y_t) = y_t + s_t - z_t - s_{max} \leq 0, \forall t. \tag{12}$$

In this case, the original energy request constraint (9) is decomposed to constraints (11) and (12).

It is easy to verify that both of the objective function $l_t(\cdot)$ and the constraint function $g_t(\cdot)$ are convex functions, and the set $\hat{\mathcal{Y}}(z_t, s_t)$ is also convex. We further make a relaxation that we can allow temporal violations of constraint (12) but a long-term constraint $\sum_{t=1}^{T} g_t(y_t) \leq 0$ must be satisfied instead, i.e., we may allow to waste an amount of energy at certain time steps, but we require the total amount of requested energy stays the same in a long term. Under the OCO context, z_t is unknown when we make the decision. Thus, to ensure the consumer's actual energy demand is satisfied, we restrict the set $\hat{\mathcal{Y}}(z_t, s_t)$ as following:

$$\hat{\mathcal{Y}}(z_{max}, s_t) = \{y_t \in \mathcal{Y} : y_t \in [\max\{0, z_{max} - s_t\}, z_{max}]\}, \tag{13}$$

We we restrict the maximum amount of energy request to be z_{max} for the sake of reducing the load of the whole grid. In this case, we propose the following OCO problem:

$$\min_{y_t \in \hat{\mathcal{Y}}(z_{max}, s_t), \forall t} \sum_{t=1}^{T} l_t(y_t) \quad s.t. \sum_{t=1}^{T} g_t(y_t) \le 0. \tag{14}$$

At each time step, the EMU selects an energy request $y_t \in \hat{\mathcal{Y}}(z_{max}, s_t)$ and incurs a time-varying loss $l_t(y_t)$ and a time-varying penalty $g_t(y_t)$.

In order to measure the performance of the OCO algorithms of the above problem, two metrics are considered here: **dynamic regret** and **dynamic fit**. The dynamic regret is defined as:

$$\mathbf{Reg}_T = \sum_{t=1}^{T} l_t(y_t) - \sum_{t=1}^{T} l_t(y_t^*), \tag{15}$$

where the sequence of optimal dynamic solutions $\mathbf{y}^* = \{y_t^*\}_{t=1}^T$ is defined as:

$$y_t^* = \operatorname*{arg\,min}_{y_t \in \hat{\mathcal{Y}}(z_{max}, s_t)} \; l_t(y_t) \;\; s.t. \; g_t(y_t) \le 0. \tag{16}$$

Accordingly, the dynamic regret represents the difference between the online loss of an OCO algorithm and that of the best dynamic solution as defined in (16).

Remark 1. *The definition in (16) represents the best dynamic solution for problem (14) with one-slot-ahead information of the cost and the constraint available, which is thus a sub-optimal solution to problem (14). But the dynamic regret still has the advantage of being more suitable and flexible for the online energy management policy design problem compared to the static regret [22].*

Lemma 1. *The strictly feasible optimal solution for problem (16) exists at each time step, i.e., there exist a $\hat{y}_t \in \hat{\mathcal{Y}}(z_{max}, s_t)$ such that $g_t(\hat{y}_t) < 0, \forall t \in [1:T]$.*

Proof: The lemma holds on observing: (i). When $z_{max} > s_t$, $z_{max} - s_t < s_{max} + x_t - s_t$ given $s_{max} > z_{max}$. (ii). When $z_{max} \le s_t, s_{max} + x_t - s_t \ge z_{min} > 0$. □

Besides, the dynamic fit is introduced to measure the accumulated violation of constraints, which is defined as $\mathbf{Fit}_T = \big[\sum_{t=1}^{T} g_t(y_t)\big]^+$. In this case, a desirable OCO is the one that can yield a sub-linear regret and sub-linear dynamic fit, i.e., $\lim_{T\to\infty} \frac{\mathbf{Reg}_T}{T} \to 0$ and $\lim_{T\to\infty} \frac{\mathbf{Fit}_T}{T} \to 0$.

B. Main Results

1) Algorithm Design: We now consider the per-slot problem of (14) with current objective function $l_t(y_t)$, current constraint $g_t(y_t) \le 0$ and the current action set $\hat{\mathcal{Y}}(z_{max}, s_t), \forall t \in [1, T]$. Let λ_t denote the Lagrange multiplier associated with the constraint $g_t(y_t) \le 0$, the partial Lagrange function of this per-slot problem thus can be expressed by:

$$L_t(y_t, \lambda_t) = l_t(y_t) + \lambda_t g_t(y_t) \tag{17}$$

To solve this online Lagrangian problem, we first take gradient ascent to update the dual iterate:

$$\lambda_{t+1} = [\lambda_t + \mu \nabla_{\lambda_t} L_t(y_t, \lambda_t)]^+ = [\lambda_t + \mu g_t(y_t)]^+, \tag{18}$$

where μ is a positive stepsize. Then take the following proximal gradient descent to update the primal variable y_{t+1}, given primal iterate y_t and dual iterate λ_{t+1}:

$$y_{t+1} = \operatorname*{arg\,min}_{y \in \hat{\mathcal{Y}}(z_{max}, s_{t+1})} \nabla l_t(y_t)(y - y_t) + \lambda_{t+1} g_t(y) + \frac{(y - y_t)^2}{2\alpha}, \tag{19}$$

where α is a positive stepsize and $\nabla l_t(y_t)$ denotes the gradient of primal objective function $l_t(\cdot)$ at point y_t. And the action y_{t+1} will incur the corresponding $l_{t+1}(y_{t+1})$ and $g_{t+1}(y_{t+1})$, which can be used for the updating in the next iteration.

The authors in [23] show that by iteratively apply the above updating rules, an OCO problem in the same form with (14) but with time-invariant action set can be solved with sublinear dynamic regret and dynamic fit under certain assumptions. However, in our problem the action set $\hat{\mathcal{Y}}(z_{max}, s_t), \forall t \in [1, T]$ varies according to the time and is determined by y_{t-1}, which is the action from the last time step.

In the following, we propose an online energy management algorithm that deals with the time-varying action set, which later can be shown to guarantee the sublinear dynamic regret and dynamic fit under certain conditions.

Algorithm 1: Online Privacy-Preserving Energy Management

```
Initialization: Primal iterate $y_1 \in \hat{\mathcal{Y}}(z_{max}, s_1)$, dual
  iterate $\lambda_1$ and proper stepsizes $\alpha, \mu$. At $t = 1$, take
  energy request $y_1$, observe the loss $l_1(y_1)$, the constraint
  $g_1(y_1)$ and the battery level $s_2$.
for t=1:T do
    Update the dual iterate $\lambda_{t+1}$ by (18);
    if $s_{t+1} \ge s_t$ then
        Update primal iterate $y_{t+1}$ by solving (19);
    else if $z_{max} \le s_t, z_{max} \le s_{t+1}$ then
        Update primal iterate $y_{t+1}$ by solving (19) within
          the set $y_{t+1} \in [0, z_{max}]$;
    else if $z_{max} \le s_t, z_{max} > s_{t+1}$ then
        Update primal iterate by solving (19) within the
          set $y_{t+1} \in [0, z_{max}]$ and request energy from the
          RES with the amount $z_{max} - s_{t+1}$;
    else
        Update primal iterate by solving (19) within the
          set $y_{t+1} \in [z_{max} - s_t, z_{max}]$ and request energy
          from the RES with the amount $s_t - s_{t+1}$;
    Execute the energy request $y_{t+1}$, observes the loss
      $l_{t+1}(y_{t+1})$, the constraint $g_{t+1}(y_{t+1})$;
    Calculate the battery level according to
      $s_{t+2} = s_{t+1} + y_{t+1} - x_{t+1}$. Let $s_{t+2} = s_{max}$, if
      $s_{t+2} > s_{max}$;
end
```

2) Performance Analysis: Before investigating the performance, we first propose the following conditions, which can be easily verified for our problem:

Condition 1: At each time step t, both the gradient of $l_t(y_t)$ and $g_t(y_t)$ are bounded on $\hat{\mathcal{Y}}(z_{max}, s_t)$, i.e.,$|\nabla l_t(y_t)| \le L, \forall y_t \in \hat{\mathcal{Y}}(z_{max}, s_t), t \in [1,T]$ and $|g_t(y_t)| \le G, \forall y_t \in \hat{\mathcal{Y}}(z_{max}, s_t), t \in [1,T]$, where L and G denote the maximum upper bound of the gradient over all time horizon, and the maximum upper bound of $|g_t(\cdot)|$ over all time horizon respectively.

Condition 2: At each time step t, the radius of the feasible set $\hat{\mathcal{Y}}(z_{max}, s_t)$ is bounded, i.e., $|y_t - y'_t| \le R_1, \forall y_t, y'_t \in \hat{\mathcal{Y}}(z_{max}, s_t), t \in [1,T]$. Also, the absolute difference between the elements in the two consecutive feasible sets at time step t and $t+1$ is also bounded, i.e., $|y_{t+1} - y_t| \le R_2, \forall y_t \in \hat{\mathcal{Y}}(z_{max}, s_t), y_{t+1} \in \hat{\mathcal{Y}}(z_{max}, s_{t+1})$. We further define $R = max\{R_1, R_2\}$.

In addition, we provide the following definitions on the slack constant and the maximum constraint variation:

Definition 1: The slack constant ϵ is defined as:

$$\epsilon = \min_t \max_{y_t \in \hat{\mathcal{Y}}(z_{max}, s_t)} (-g_t(y_t)), \forall t \in [1,T]. \tag{20}$$

Definition 2: The maximum variation of consecutive constraint is defined as:

$$v(g) = \max_t \max_{y_{t+1} \in \hat{\mathcal{Y}}(z_{max}, s_{t+1})} [g_{t+1}(y_{t+1}) - g_t(y_{t+1})]^+. \tag{21}$$

Given the above definitions, the following lemma provide the conditions that guarantee the existence of an upper bound of the maximum constraint variation.

Lemma 2. *The slack constant ϵ satisfies $\epsilon > v(g)$ if $z_{max} < 2z_{min}$.*

Proof: See the longer version of this paper [24] for the details of the proof. □

We next provide upper bound on the dynamic fit and regret.

Proposition 2. *Given Condition 1-2, Lemma 1-2 and the dual iterate initialization $\lambda_1 = 0$, the dynamic fit of our online energy management algorithm is upper bounded as below according to:*

$$\textbf{\textit{Fit}}_T \le G + \frac{2LR/\mu + R^2/2\alpha\mu + G^2/2}{\epsilon - v(g)} \tag{22}$$

Proof: See [24] for the details of the proof. □

Theorem 1. *Given Condition 1-2, Lemma 1-2 and the dual iterate initialization $\lambda_1 = 0$, the dyamic regret of our online energy management algorithm is bounded by:*

$$\begin{aligned}\textbf{\textit{Reg}}_T \le & \frac{R\sum_{t=1}^{T}|y_t^* - y_{t-1}^*|}{\alpha} + \frac{\alpha L^2 T}{2} + \frac{\mu G^2(T+1)}{2} + \frac{R^2}{2\alpha} \\ & + \bar{\lambda}\sum_{t=1}^{T} \max_{y_{t+1} \in \hat{\mathcal{Y}}(z_{max}, s_{t+1})} [g_{t+1}(y_{t+1}) - g_t(y_{t+1})]^+,\end{aligned} \tag{23}$$

where $\bar{\lambda} = \mu \times (G + \frac{2LR/\mu + R^2/2\alpha\mu + G^2/2}{\epsilon - v(g)})$.

Proof: See [24] for the details of the proof. □

Corollary 1. *According to the results in [23], given the primal and dual stepsizes chosen as $\alpha = \mu = \mathcal{O}(T^{-\frac{1}{3}})$, the dyanmic fit is then upper bounded by $\textbf{\textit{Fit}}_T = \mathcal{O}(T^{\frac{2}{3}})$, and the dynamic regret is upper bounded by:*

$$\begin{aligned}\textbf{\textit{Reg}}_T = & \mathcal{O}\big(\max\{T^{\frac{2}{3}}, T^{\frac{1}{3}}\sum_{t=1}^{T}|y_t^* - y_{t-1}^*|, \\ & T^{\frac{1}{3}}\sum_{t=1}^{T} \max_{y_{t+1} \in \hat{\mathcal{Y}}(z_{max}, s_{t+1})} [g_{t+1}(y_{t+1}) - g_t(y_{t+1})]^+\}\big).\end{aligned} \tag{24}$$

Remark 2. *To ensure the above regret bound is sublinear, we need to have $\sum_{t=1}^{T}|y_t^* - y_{t-1}^*| = \mathcal{O}(T^{2/3})$ and $\sum_{t=1}^{T} \max_{y_{t+1} \in \hat{\mathcal{Y}}(z_{max}, s_{t+1})} [g_{t+1}(y_{t+1}) - g_t(y_{t+1})]^+ = \mathcal{O}(T^{2/3})$. To this end, we set the number of switches of dynamic optimal solution as $\sum_{t=1}^{T} \mathbb{I}_{y_t^* \neq y_{t-1}^*} \le T^{2/3}$ and the switches of constraint as $\sum_{t=1}^{T} \mathbb{I}_{g_{t+1}^* \neq g_t^*} \le T^{2/3}$. And this condition can be guaranteed for our smart metering system, since the change of the consumer's energy consumption behavior is much slower than the sampling frequency of the smart metering data. On the other hand, as stated above, the variation of dynamic optimal solution and maximum constraint variation are bounded. In this case, the sublinear dynamic regret can be achieved for our online privacy-preserving energy management strategy.*

V. Numerical Results

In this section, we provide the numerical results to demonstrate the performance of our proposed online privacy-preserving energy management strategy. We consider the setting where the consumer's actual energy consumption z_t takes value from the set $[30, 59]$, and the ES capacity is 100. The aggregated mean value μ_t can take value from the set $\{40, ..., 50\}$, and the aggregated variance σ_t takes value from $\{1, 2, 3, 4, 5\}$. We consider the time horizon with length $T = 500$, the stepsize μ in (18) is set as $50/t^{1/3}$, and the stepsize α in (19) is set as $0.5/t^{1/3}$.

In Fig. 3, we compare the dynamic regret between our proposed online privacy-preserving energy management algorithm and the privacy-unaware online energy management strategy[1]. And we use the sequence of per-slot dynamic optimal solutions given by (16) as the offline benchmark. As shown in the figure, the dynamic regret of our proposed online privacy-preserving algorithm grows sublinearly and much slower than the dynamic regret of the privacy-unaware random energy management strategy, which means our proposed online privacy-preserving energy management strategy can robustly provide a privacy enhancement over a long term. While as shown in Fig. 4, the dynamic fit of our proposed algorithm also grows sublinearly and much smaller compared to the random energy management strategy which does not consider the violation of constraint (12).

[1] For this privacy-unaware strategy, the EMU randomly decide the energy request y_t which only satisfies the constraint (13) in an online fashion instead of trying to optimize the privacy measure.

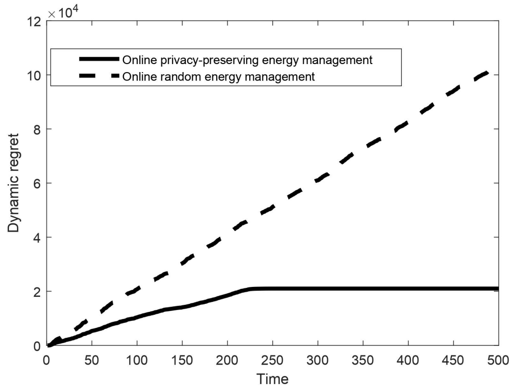

Fig. 3. Dynamic regret comparison

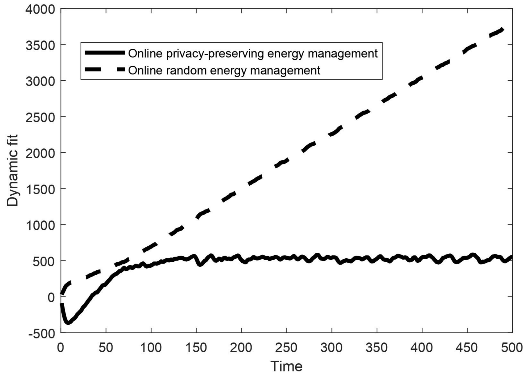

Fig. 4. Dynamic fit comparison

VI. Conclusion

In this work, we have shown the privacy-preserving problem under the FHMM inference based load disaggregation framework is equivalent to the design problem of the energy management strategy that minimizes the the joint log-likelihood of the energy request sequence and the appliances' operating state sequence given the FHMM parameters. Using the OCO framework, an online energy management strategy is designed and is conditionally guaranteed to have the same asymptotic performance as the offline dynamic benchmark. Compared to the traditional offline energy management algorithms, our online privacy-preserving energy management algorithm is more suitable for the realistic system and is also computationally more efficient.

References

[1] Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan 2012.

[2] Y. Kim, E. C. H. Ngai, and M. B. Srivastava, "Cooperative state estimation for preserving privacy of user behaviors in smart grid," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2011, pp. 178–183.

[3] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 First IEEE International Conference on Smart Grid Communications*, Oct 2010, pp. 238–243.

[4] J. M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *2010 IEEE International Conference on Communications Workshops*, May 2010, pp. 1–5.

[5] "The EU General Data Protection Regulation," Available online: https://eugdpr.org/.

[6] S. Li, A. Khisti, and A. Mahajan, "Privacy-optimal strategies for smart metering systems with a rechargeable battery," in *2016 American Control Conference (ACC)*, July 2016, pp. 2080–2085.

[7] J. Yao and P. Venkitasubramaniam, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct 2013, pp. 115–122.

[8] Y. You, Z. Li, and T. J. Oechtering, "Optimal privacy-enhancing and cost-efficient energy management strategies for smart grid consumers," in *2018 IEEE Statistical Signal Processing Workshop (SSP)*, 2018, pp. 826–830.

[9] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 486–495, Jan 2015.

[10] O. Tan, J. Gómez-Vilardebó, and D. Gündüz, "Privacy-cost trade-offs in demand-side management with storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1458–1469, 2017.

[11] G. Giaconi and D. Gündüz, "Smart meter privacy with renewable energy and a finite capacity battery," in *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, July 2016, pp. 1–5.

[12] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-cost trade-off in a smart meter system with a renewable energy source and a rechargeable battery," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 2687–2691.

[13] O. Tan, D. Gündüz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, 2013.

[14] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[15] Z. Guo, Z. J. Wang, and A. Kashani, "Home appliance load modeling from aggregated smart meter data," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 254–262, 2015.

[16] S. Makonin, F. Popowich, I. V. Bajić, B. Gill, and L. Bartram, "Exploiting hmm sparsity to perform online real-time nonintrusive load monitoring," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2575–2585, 2016.

[17] W. Kong, Z. Y. Dong, J. Ma, D. J. Hill, J. Zhao, and F. Luo, "An extensible approach for non-intrusive load disaggregation with smart meter data," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3362–3372, 2018.

[18] J. Kolter and T. Jaakkola, "Approximate inference in additive factorial hmms with application to energy disaggregation," in *Artificial intelligence and statistics*, 2012, pp. 1472–1482.

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

[20] H. Kim, M. Marwah, M. Arlitt, G. Lyon, and J. Han, "Unsupervised disaggregation of low frequency power measurements," in *Proceedings of the 2011 SIAM international conference on data mining*. SIAM, 2011, pp. 747–758.

[21] D. Mashima and A. Roy, "Privacy preserving disclosure of authenticated energy usage data," in *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2014, pp. 866–871.

[22] W. Ma, J. Wang, V. Gupta, and C. Chen, "Distributed energy management for networked microgrids using online admm with regret," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 847–856, 2018.

[23] T. Chen, Q. Ling, and G. B. Giannakis, "An online convex optimization approach to proactive network resource allocation," *IEEE Transactions on Signal Processing*, vol. 65, no. 24, pp. 6350–6364, 2017.

[24] Y. You and T. J. Oechtering, "Online energy mangement strategy design for smart meter privacy against fhmm-based nilm," available online: https://people.kth.se/~oech/sgc20.pdf, 2020.