This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

Fisher Information as a Measure of Privacy: Preserving Privacy of Households with Smart Meters Using Batteries

Farhad Farokhi and Henrik Sandberg

***Abstract*—In this paper, batteries are used to preserve the privacy of households with smart meters. It is commonly understood that data from smart meters can be used by adversaries to infringe on the privacy of the households, e.g., figuring out the individual appliances that are being used or the level of the occupancy of the house. The Cramér-Rao bound is used to relate the variance of the estimation error of any unbiased estimator of the household consumption from the aggregate consumption (i.e., the household plus the battery) to the Fisher information. Subsequently, optimal policies for charging and utilizing batteries are devised to minimize the Fisher information (in the scalar case and the trace of the Fisher information matrix in the multi-variable case) as a proxy for maximizing the variance of the estimation error of the electricity consumption by adversaries (irrespective of their estimation policies). The policies are chosen to respect the physical constraints of the battery regarding capacity, initial charge, and rate constraints. The results are demonstrated on real power measurement data with non-intrusive load monitoring algorithms.**

***Index Terms*—Data Privacy; Fisher Information; Estimation.**

I. Introduction

Smart meters have become common elements in modern electricity grids and are being more frequently used for metering and sensing purposes. However, data that is gathered from these meters can also be used by adversaries (such as criminals, advertising agencies, etc.) to infringe on the privacy of the households, e.g., figuring out the individual appliances that are being used or the level of the occupancy of the house [1]–[3]. Therefore, appropriate mechanisms are required to safeguard the privacy of the households with smart meters.

A common methodology to ensure the privacy of participants in large databases is differential privacy [4]–[8]. Differentially-private mechanisms often rely on adding noises with slow-decaying distributions, e.g., Laplace noise, to the outcome of queries. This ensures that the queries' statistics do not noticeably change in response to individual deviations in the entries of the database and thus an array of queries and responses cannot be used to learn a specific entry of the database. Differentially-private mechanisms have been previously utilized within the context of smart meters; see for example [9], [10]. However, implementing a differentially-private mechanism through adding an appropriate noise to the measurements collected by the smart meters remains impractical due to several reasons. First, in addition to being utilized for state estimation purposes by the grid operator, smart meters are currently used for measuring the household consumption for metering and billing purposes and thus adding noise (specifically one with a slow-decaying distribution) is not desirable from the perspective of the utility provider and the household. Second, adding noise results in an inferior estimation quality by the grid operator as also noted in [9]. Third, the specific nature of the utilized noise distributions, e.g., Laplace distribution, makes the optimal estimation problem cumbersome and increases the false alarm rate by the fault detection units (since sometimes faults are modelled as Laplace noises) [11], [12].

To combat the problems associated with adding noise to the measurements from smart meters, several studies have proposed using batteries to mask the household consumption [13]–[16]. Note that the effect of the battery can be modelled as a noise added to the household consumption but there are several important distinctions with the case of additive measurement noise. Firstly, the batteries have a finite capacity and thus noises with unbounded support, such as Gaussian and Laplace noises, cannot be implemented. Secondly, the measurements of the voltage and the current provided by the smart meter in this case are exact and thus estimation complexities and metering issues are all avoided.

In this paper, batteries are used to preserve the privacy of households. An adversary is considered that aims at estimating the household consumption, as closely as possible, from the aggregate consumption, i.e., the combined consumption of the household and the battery. The Cramér-Rao bound [17, p. 169] is used to relate the variance of the estimation error of unbiased estimators of the household consumption from the aggregate consumption by adversaries to the Fisher information, specifically the trace of the inverse of the Fisher information matrix. This allows us to use the Fisher information as a measure of privacy. Subsequently, optimal policies for charging and utilizing the batteries are devised to minimize the Fisher information as a proxy for maximizing the variance of the estimation error of the electricity consumption of the household irrespective of the estimation policy used by the adversary. This is done in a such a way that the physical constraints of the battery regarding its capacity, initial charge, and rate of charge/discharge are respected. At first, it is assumed that the policy of the battery cannot be a function of the household consumption; however, this assumption is

F. Farokhi is with the Department of Electrical and Electronic Engineering, University of Melbourne, Parkville, Victoria 3010, Australia. Email: ffarokhi@unimelb.edu.au

H. Sandberg is with the Department of Automatic Control, KTH Royal Institute of Technology, Stockholm, Sweden. Email: hsan@kth.se

The work of F. Farokhi was supported by a McKenzie Fellowship and an early career grant from Melbourne School of Engineering. The work of H. Sandberg was supported by the EU CHIST-ERA project COPES and the Swedish Civil Contingencies Agency through the CERCES project. The authors would like to thank Iman Shames for discussions.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

removed subsequently to significantly generalize the results. The framework is then partially extended to biased estimators. The price of charging and discharging the battery (due to, e.g., wear and tear) is considered and its effect on the optimal policy of the battery is investigated. Finally, we demonstrate the applicability of the devised method on real data from [18] while using a common non-intrusive load monitoring method from [19] for energy disaggregation in the presence and the absence of the battery. It is worth mentioning the presented framework can be used for more general privacy problems and the core results are not bound by the smart-metering literature.

To the best of our knowledge, this is the first time that the Fisher information and its interpretation through the Cramér-Rao bound are utilized within the context of privacy-aware mechanisms for smart metering. Within the statistics community, however, the use of Fisher information as a measure of privacy has been discussed previously [20]. In that study, minimizing the Fisher information over the set of density functions with constrained support sets to achieve a privacy-preserving policy was not discussed. Previously, other studies have utilized mutual information and entropy as well as the least mean square estimation error as a measure of privacy [13]–[15], [21]–[23]. The privacy measures based on mutual information do not provide a clear and tight lower-bound of the statistics of the estimation error by adversaries. Further, using them in this context requires *a priori* assumption on the distribution of the household consumption (which is not the case for the Fisher information). Also utilizing the framework of [23] requires the adversary to use the least mean square estimator (and restrict the distributions to be Gaussian) and does not provide general guarantees as opposed to the use of the Cramér-Rao bound.

Finally, we should mention that the probem of finding probability density functions that minimize the Fisher information has been discussed previously in various studies, e.g., see [24]–[26]. However, in those studies, scalar random variables are only considered. The results of this paper thus extends those problem formulations.

The rest of the paper is organized as follows. The problem formulation is presented in Section II. The optimal charging policies of the batteries without and with access to measurements of the household consumption are presented in Sections III and IV, respectively. Section V discusses biased estimators, extends the results to the case where the use of the battery is costly, and finally considers the case where the charging rate of the batteries is limited. The numerical results are presented in Section VI. Finally, the paper is concluded in Section VII.

II. Problem Formulation

Denote the energy consumption of a household at time instant $k \in \mathcal{T} := \{1, \dots, T\}$ by $s_k \in \bar{\mathcal{S}} \subseteq \mathbb{R}_{\geq 0}$. We can aggregate these variables into a vector to get $s = [s_1 \ \cdots \ s_T]^\top \in \mathcal{S} := \bar{\mathcal{S}}^T$. In what follows, we assume that this vector is deterministic. The deterministic nature of the vector implies that it is an arbitrary vector and with no requirements on its distribution. Further, it motivates the adversary's desire for seeking a point estimator (and thus the use of the Cramér-Rao bound, in what follows, for bounding its performance). The house has a battery that the occupants can use for meeting their demand as well as masking their energy consumption profile and thus preserving their privacy. The latter is done by ensuring that the part of the energy taken from the public grid cannot be used to construct accurate estimates of the household consumption. Let b_k denote the energy drawn from the battery at time instant $k \in \mathcal{T}$. If $b_k \geq 0$, the charge in the battery is being used to provide electricity to the house and if $b_k \leq 0$, the battery is being charged. We can aggregate these variables in a vector as $b = [b_1 \ \cdots \ b_T]^\top$. At the beginning of the horizon, we assume that the state of the charge of the battery is equal to c_0. The capacity of the battery is equal to c. Following the conservation of charge in the battery, we may define the set

$$\mathcal{B} := \{b \in \mathbb{R}^T \,|\, 0 \leq c_0 - \begin{bmatrix} \mathbb{1}_k^\top & 0_{T-k}^\top \end{bmatrix} b \leq c, \forall k \in \mathcal{T}\},$$

where $\mathbb{1}_k$ and 0_k denote a vector of ones and zeros of size k, respectively. Here, $\mathcal{B}$ denotes the set of all feasible vectors of charge/discharge commands b, i.e., the set of all battery uses for which the state of the charge does not go below zero or above the capacity. An equivalent representation of the set $\mathcal{B}$ is

$$\mathcal{B} := \Bigg\{ \begin{bmatrix} b_0 & \cdots & b_T \end{bmatrix}^\top \in \mathbb{R}^T \,| \\ -\sum_{i=1}^{k-1} b_i + (c_0 - c) \leq b_k \leq c_0 - \sum_{i=1}^{k-1} b_i, \forall k \in \mathcal{T} \Bigg\}.$$

The part of the energy consumption of the house that is acquired from the grid is $x = s - b$. In this paper, we use randomized policies for charging and utilizing the battery. Note that, if the capacity of the battery is infinitely large and its initial state of charge is large enough, one can use a deterministic policy that completely masks the household consumption (by keeping the aggregate consumption constant). However, in general, that is not possible and the deterministic nature of the policy might allow the procedure to be reversed by the adversary. This motivates the use of randomized policies. The policy for the charging/discharging the battery is a conditional density function $\gamma(\cdot|s) : \mathcal{B} \to \mathbb{R}_{\geq 0}$. This implies that $\mathbb{P}\{b \in \mathcal{B}'|s\} = \int_{b' \in \mathcal{B}'} \gamma(b'|s) \mathrm{d}b'$, for any Lebesgue-measurable set $\mathcal{B}' \subseteq \mathcal{B}$. The set of all admissible policies is restricted according to the following standing assumptions.

Assumption 1: $\gamma(b|s)$ is twice continuously differentiable in (b, s) over $\mathcal{B} \times \mathcal{S}$ and $\gamma(b|s) = 0$ for all $b \in \partial\mathcal{B}$. Further, γ is selected such that $\mathbb{P}\{b \in \mathbb{R}^T \setminus \mathcal{B} \,|\, s\} = 0$ for all $s \in \mathcal{S}$.

As discussed below, the first part of Assumption 1 is required for the validity of the Cramér-Rao bound (see Theorem 1). Alternatively, one can motivate this assumption by that the household does not want to assign a non-zero probability to the event that the battery is completely full or empty at all times in $\mathcal{T}$ as this reduces its flexibility in future decisions. The second part of Assumption 1 ensures that the state of the battery is feasible with probability one. This assumption can be replaced with the following stronger assumption.

Assumption 2: $\gamma(b|s)$ is twice continuously differentiable in (b, s) over $\mathbb{R}^T \times \mathcal{S}$. Further, γ is selected such that $\mathbb{P}\{b \in \mathbb{R}^T \setminus \mathcal{B} \,|\, s\} = 0$ for all $s \in \mathcal{S}$.

Lemma 1: Satisfaction of Assumption 2 implies satisfaction of Assumption 1.

Proof: Following Assumption 2, it can be deduced that $\gamma(b|s)$ is also continuous in b since it is continuously differentiable in b. Therefore, $\gamma(b|s) = 0$ for all $b \in \partial\mathcal{B}$ since $\gamma(b|s) = 0$ for all $b \in \mathbb{R}^T \setminus \mathcal{B}$. ∎

The probability density of x for a given s is then equal to

$$p(x|s) = \gamma(s - x|s),\ \forall x \in \mathcal{S} \oplus -\mathcal{B},$$

where $\oplus$ is defined as $\mathcal{X} \oplus \mathcal{Y} := \{x+y \text{ for all } x \in \mathcal{X}, y \in \mathcal{Y}\}$ for all sets $\mathcal{X}$ and $\mathcal{Y}$.

The adversary, or the attacker, is assumed to be a malicious agent that can access the smart meter measurements of the aggregate consumption of the household $x = s-b$ without any restrictions. To be able to figure out the individual appliances that are being used by the occupants or to find out the level of the occupancy of the house, the adversary seeks to construct an accurate estimate of s from this measurement. We assume that the adversary is going to use an unbiased estimator. However, we will briefly relax this assumption in Subsection V-A. In this paper, the Cramér-Rao bound is used to relate the variance of the estimation error of unbiased estimators of the household consumption from the aggregate consumption by adversaries to the Fisher information. This allows us to use the Fisher information as a measure of privacy without adding any extra assumptions on the sophistication of the adversary. The following result immediately follows from the use of the Cramér-Rao bound.

Theorem 1: Under either Assumption 1 or 2, for any unbiased estimate of s denoted by $\hat{s}(x)$, it holds that

$$\mathbb{E}\{\|s - \hat{s}(x)\|_2^2\} \geq \mathrm{Tr}(\mathcal{I}(s)^{-1}),$$

where $\mathcal{I}(s)$ is the Fisher information matrix defined as

$$\mathcal{I}(s) = \int_{x\in\{s\}\oplus-\mathcal{B}} p(x|s)\left[\frac{\partial \log(p(x|s))}{\partial s}\right]\left[\frac{\partial \log(p(x|s))}{\partial s}\right]^\top \mathrm{d}x.$$

Proof: For the sake of the space, the long proofs are moved to a technical note [27]. ∎

In this paper, it is desirable to find a charging policy for the battery that makes estimation of private activities of the household as hard as possible. Following Theorem 1, in order to make the task of constructing a point estimate of the household consumption s from the measurements of the aggregate consumption x difficult, we need to maximize the trace of the inverse of the Fisher information matrix. We formalized this problem without and with access to the measurements of the household consumption s in the following subsections.

A. Optimal Privacy-Preserving Policy when Consumption is not measured

In this case, the charging policy of the user is independent of s, i.e., $\gamma(b|s) = \gamma(b)$. This case is interesting when the household itself does not have access to the accurate predictions of the future consumption. The Fisher information matrix can be simplified to

$$\begin{aligned}\mathcal{I}(s) &= \int_{x\in\{s\}\oplus-\mathcal{B}} \gamma(s-x)\left[\frac{\partial \log(\gamma(s-x))}{\partial s}\right] \\ &\qquad\times\left[\frac{\partial \log(\gamma(s-x))}{\partial s}\right]^\top \mathrm{d}x \\ &= \int_{b\in\mathcal{B}} \gamma(b)\left[\frac{\partial \log(\gamma(b))}{\partial b}\right]\left[\frac{\partial \log(\gamma(b))}{\partial b}\right]^\top \mathrm{d}b.\end{aligned}$$

Not that, in this case, $\mathcal{I}(s)$ is no longer a function of s and is thus denoted by $\mathcal{I}$. Let Γ denotes the set of all density functions $\gamma(\cdot)$ that satisfy Assumption 1.

Problem 1: Find γ^* such that $\gamma^* \in \mathrm{argmax}_{\gamma\in\Gamma} \mathrm{Tr}(\mathcal{I}^{-1})$.

For scalar problems, i.e., when $T = 1$, this problem is equivalent to $\gamma^* \in \mathrm{argmin}_{\gamma\in\Gamma} \mathcal{I}$ because the mapping $x \mapsto 1/x$ is deceasing over $\mathbb{R}_{\geq 0}$ and the Fisher information is non-negative. In the multivariate case, it can be shown that

$$\mathrm{Tr}(\mathcal{I}^{-1}) = \sum_{i=1}^{T} \frac{1}{\lambda_i(\mathcal{I})} \geq \frac{T^2}{\sum_{i=1}^{T}\lambda_i(\mathcal{I})} = T^2\mathrm{Tr}(\mathcal{I})^{-1}, \quad (1)$$

where the inequality follows from that the mapping $x \mapsto 1/x$ is convex over $\mathbb{R}_{\geq 0}$ and $\lambda_i(\mathcal{I}) \geq 0$ for all i since $\mathcal{I}$ is positive semi-definite. Since directly maximizing the cost function $\mathrm{Tr}(\mathcal{I}^{-1})$ is difficult in general, we can instead aim at maximizing the lower bound $T^2\mathrm{Tr}(\mathcal{I})^{-1}$ to achieve a sub-optimal solution.

Remark 1: It is worth mentioning that the lower-bound in (1) is only tight for scalar problems, i.e., $T = 1$. This can add an additional layer of relaxation to the Cramér-Rao bound that can be shown to be only attainable for a family of exponential distributions [28]. A future direction for research could be to find tighter convex lower-bounds for the original cost function $\mathrm{Tr}(\mathcal{I}^{-1})$.

Problem 2: Find γ^* such that $\gamma^* \in \mathrm{argmin}_{\Gamma} \mathrm{Tr}(\mathcal{I})$.

In the next subsection, we extend this problem formulation to the case where the measurements of the household consumption are available. We assume there that the entire vector s is available. This might violate causality (underlying that the actions of the battery can only depend on the measurements of the household consumption in the current and previous time instants) as the sequence of the appliances to be used is not known in advance. However, recent innovations in scheduling appliances for reducing the electricity price (see, e.g., [29]) can benefit us by providing an estimate of the energy consumption for most of the day. In addition, the proposed strategy can be implemented in a receding horizon fashion based on possibly inaccurate estimates of the energy consumption in which case an estimate of the future household consumption is required.

B. Optimal Privacy-Preserving Policy when Consumption is measured

In this case, the Fisher information matrix is a function of s. Therefore, maximizing $\mathrm{Tr}(\mathcal{I}(s)^{-1})$ is not properly-defined. Instead, we maximize the cost function

$$\mathcal{J}' := \int_{s\in\mathcal{S}} \mathrm{Tr}(\mathcal{I}(s)^{-1})p(s)\mathrm{d}s,$$

where $p(s)$ is the weight associated with s, i.e., how eager the user is to make the estimation difficult at s. Without loss of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

generality, we can assume that $\int_{s\in\mathcal{S}} p(s)\mathrm{d}s = 1$. With some abuse of notation, Γ denotes the set of all *conditional* density functions $\gamma(\cdot|s)$ that satisfy Assumption 1.

Problem 3: Find γ^* such that $\gamma^* \in \mathrm{argmax}_{\gamma\in\Gamma}\, \mathcal{J}'$.

Similarly, using (1), it can be shown that

$$\int_{s\in\mathcal{S}} \mathrm{Tr}(\mathcal{I}(s)^{-1})p(s)\mathrm{d}s \geq T^2 \int_{s\in\mathcal{S}} \mathrm{Tr}(\mathcal{I}(s))^{-1}p(s)\mathrm{d}s \geq T^2\left(\int_{s\in\mathcal{S}} \mathrm{Tr}(\mathcal{I}(s))p(s)\mathrm{d}s\right)^{-1},$$

where the second inequality follows from the Jensen's inequality [30] and the earlier observation that the mapping $x \mapsto 1/x$ is convex over $\mathbb{R}_{\geq 0}$. Define

$$\mathcal{J} := \int_{s\in\mathcal{S}} \mathrm{Tr}(\mathcal{I}(s))p(s)\mathrm{d}s.$$

Noting that maximizing the cost function $\mathcal{J}'$ is difficult in general, we opt for maximizing its lower bound $T^2/\mathcal{J}$ to find a sub-optimal solution.

Problem 4: Find γ^* such that $\gamma^* \in \mathrm{argmin}_{\gamma\in\Gamma}\, \mathcal{J}$.

With the problem formulations in hand, we are ready to calculate the optimal policies for utilizing the batteries. This is the topic of the next sections.

III. Optimal Privacy-Preserving Policy when Consumption is not measured

In this section, we consider the case that the charging policy of the battery is not a function of the energy consumption of the house s. The first step to solving the problem is to show that the trace of the Fisher information matrix is a convex function of γ. To do so, we need to define the support of a density function γ as $\mathrm{supp}(\gamma) := \{b|\gamma(b) > 0\}$. Let $\mathcal{P} \subseteq \Gamma$ be a set such that, for all $\gamma_1, \gamma_2 \in \mathcal{P}$, $\mathrm{supp}(\gamma_1) \setminus \mathrm{supp}(\gamma_2)$ has a zero Lebesgue measure. This is the set of all density functions that assign non-zero probabilities to the same set of charging/discharging commands (with an exception of measure zero sets that are insignificant).

Proposition 1: $\mathrm{Tr}(\mathcal{I})$ is a convex function of the density function γ over the set of density functions $\mathcal{P}$.

Proof: See [27]. ∎

Motivated by Proposition 1, we search for the minimizer of $\mathrm{Tr}(\mathcal{I})$ over the set of all density functions γ that are at most over a measure-zero set equal to zero in $\mathrm{int}(\mathcal{B})$.

A. Scalar Cases

For the scalar problem, i.e., the single time step problem $T = 1$, Problems 1 and 2 are identical. Further, the problems admit an explicit solution that is presented in the next theorem.

Theorem 2: $\gamma^*(b) = \frac{2}{c}\cos^2(\pi(b - c_0 + c/2)/c)\mathbb{1}_{c_0 - c \leq b \leq c_0}$ solves Problems 1 and 2 for $T = 1$.

Proof: See [27]. ∎

The next theorem uses the Cramér-Rao bound to calculate the lower-bound on the performance of any unbiased estimator of s that receives the measurement $x = s - b$.

Theorem 3: $\mathbb{E}\{(s - \hat{s}(x))^2\} \geq c^2/(4\pi^2)$ for any unbiased estimate of s denoted by $\hat{s}(x)$ when $T = 1$.

Proof: See [27]. ∎

This corollary shows that, for the optimal charging policy, the quality of the estimation by the adversary degrades as the capacity of the battery increases and thus the privacy is better retained with high charging capacities. Interestingly, the initial charge of the battery does not play any role.

B. Greedy Multivariate Case

For the case where $T > 1$, an interesting heuristic is to assume that a greedy algorithm is used. When using the greedy policy, in each step, the user solves the scalar problem in the previous subsection for that step without considering its consequence on future decisions. As a result, $\gamma(b) = \gamma_1(b_1)\gamma_2(b_2|b_1)\cdots\gamma_T(b_T|b_1,\dots,b_{T-1})$, where

$$\gamma_k(b_k|b_1,\dots,b_{k-1}) = \frac{2}{c}\cos^2\!\left(\frac{\pi}{c}\left(b - c_0 + c + \sum_{i=1}^{k-1} b_i\right) - \frac{\pi}{2}\right) \times \mathbb{1}_{c_0 - c - \sum_{i=1}^{k-1} b_i \leq b \leq c_0 - \sum_{i=1}^{k-1} b_i},$$

for all $1 \leq k \leq T$. In the next subsection, we show that the greedy method is in fact optimal in the sense of Problem 2.

C. Multivariate Case

We start by solving Problem 1 in the next theorem. In what follows, the notation $D^2u(b)$ is adopted to denote the Hessian of the function $u(b)$.

Theorem 4: Let γ^* denote the solution of Problem 1. Then, it satisfies the following partial differential equation with $u(b) = \sqrt{\gamma^*(b)}$:

$$\begin{cases} \mathrm{Tr}(\mathcal{I}^{-2}D^2u(b)) + \mu u(b) = 0, & b \in \mathcal{B}, \\ u(b) = 0, & b \in \partial\mathcal{B}. \end{cases} \tag{2}$$

Here, μ is selected such that $\int_{b\in\mathcal{B}} u(b)^2\mathrm{d}b = 1$ and $\mathrm{supp}(u(b)) = \mathrm{int}(\mathcal{B})$.

Proof: See [27]. ∎

Remark 2: In (4) and throughout the rest of this section, μ is the Lagrange multiplier associated with the equality constraint $\int_{b\in\mathcal{B}} u(b)^2\mathrm{d}b = 1$ (which ensures that $\gamma(b) = u(b)^2$ is a probability density function). In several cases, we have calculated this value explicitly (see, e.g., Theorem 2 and Corollary 1). In general, however, we should iteratively change the value of the multiplier (following the approach of primal-dual optimization algorithms) to find an appropriate value.

Remark 3: The non-linearity of the partial differential equation in (2) follows from that $\mathcal{I}$ in $\mathrm{Tr}(\mathcal{I}^{-2}D^2u(b))$ is a function of $u(b)$. Further, Theorem 4 only provides a necessary condition, i.e., the solution of Problem 1 satisfies (2); however, the reverse does not necessarily hold.

In this section, we prove that the greedy algorithm in the previous subsection is actually the solution of Problem 2.

Theorem 5: The solution of Problem 2 is given by $\gamma^*(b) = u(b)^2$, where $u(b)$ is the solution of the linear partial differential equation

$$\begin{cases} \nabla^2 u(b) + \mu u(b) = 0, & b \in \mathcal{B}, \\ u(b) = 0, & b \in \partial\mathcal{B}. \end{cases} \tag{3}$$

Here, μ is selected such that $\int_{b\in\mathcal{B}} u(b)^2\mathrm{d}b = 1$ and $\mathrm{supp}(u(b)) = \mathrm{int}(\mathcal{B})$.

Proof: See [27]. ∎

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

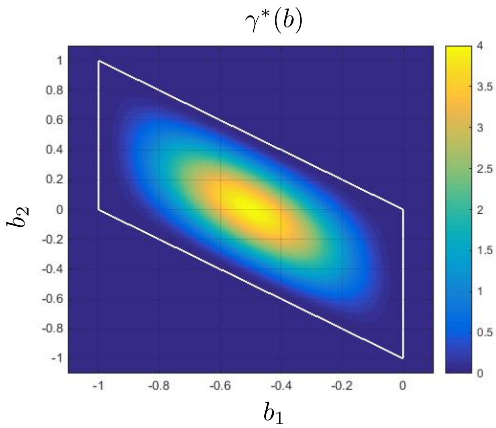

Fig. 1. The probability density function $\gamma^*(b)$ versus $b = (b_1, b_2) \in \mathcal{B}$. The boundaries of the feasible set $\mathcal{B}$ are shown by white lines.

The partial differential equation in (3) is a special case of the Schrödinger equation. This knowledge can be used to solve the partial differential equation explicitly.

Corollary 1: The solution of Problem 2 is given by

$$\gamma^*(b) = \left(\frac{2}{c}\right)^T \prod_{k=1}^{T} \cos^2\left(\pi\left(b_k - c_0 + c/2 + \sum_{i=1}^{k-1} b_i\right)/c\right) \times \mathbb{1}_{c_0 - c - \sum_{i=1}^{k-1} b_i \leq b \leq c_0 - \sum_{i=1}^{k-1} b_i}.$$

Proof: Following [31], we know that the solution of (3) is unique. The rest easily follows from showing that the provided density function satisfies the partial differential equation and its boundary conditions. ■

Remark 4 (Separation of Variables and Greedy Method): Alternatively, we can solve the Schrödinger equation in (3) using the separation of variables technique. To do so, we can assume that the solution inside $\mathrm{int}(\mathcal{B})$ takes the special form of $u(b) = u_1(b_1)u_2(b_1 + b_2)\cdots u_T(b_1 + \cdots + b_T)$. This gives

$$\begin{aligned}\nabla^2 u(b) =& u_1''(b_1)u_2(b_1 + b_2)\cdots u_T(b_1 + \cdots + b_T) \\ &+ 2u_1(b_1)u_2''(b_1 + b_2)\cdots u_T(b_1 + \cdots + b_T) \\ &+ \cdots \\ &+ Tu_1(b_1)u_2(b_1 + b_2)\cdots u_T''(b_1 + \cdots + b_T).\end{aligned}$$

Let $\mu_1, \ldots, \mu_T \in \mathbb{R}$ be such that $\mu = \mu_1 + \cdots + \mu_T$. Thus, the partial differential equation in (3) can be decomposed into T ordinary differential equations of the form $u_i''(b_1 + \cdots + b_i) + (\mu_i/i)u_i(b_1 + \cdots + b_i) = 0$, which can be solved following the same approach as in the proof of Theorem 2. This is intuitively why the greedy method is optimal.

Corollary 2: For the optimal policy in Corollary 1, $\mathbb{E}\{\|s - \hat{s}(x)\|_2^2\} \geq \mathrm{Tr}(\mathcal{I}^{-1}) = \kappa c^2$ for any unbiased estimate of s denoted by $\hat{s}(x)$, where κ is equal to $\mathrm{Tr}(\mathcal{I}^{-1})$ when $c = 1$.

Proof: See [27]. ■

Example 1: Now, we illustrate the optimal charging policy of the battery in a simple example with horizon $T = 2$. Let us fix $c_0 = 0$ and $c = 1$. Figure 1 shows the probability density function $\gamma(b)$ versus $b = (b_1, b_2) \in \mathcal{B}$. The boundaries of the feasible set $\mathcal{B}$ are shown by white lines.

Note that the dimension of the vector s rises with T and therefore the error variance $\mathbb{E}\{\|s - \hat{s}(x)\|_2^2\}$ (and its lower bound $\mathrm{Tr}(\mathcal{I}^{-1})$) is expected to naturally increase with higher T. We can scale $\mathrm{Tr}(\mathcal{I}^{-1})$ with T^2 to account for this fact.

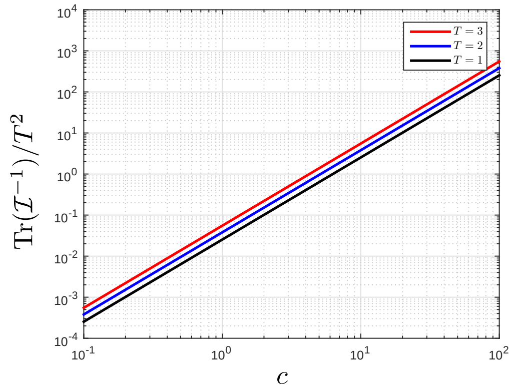

Fig. 2. The scaled lower bound of the variance of the estimation error of all unbiased estimators $\mathrm{Tr}(\mathcal{I}^{-1})/T^2$ as a function of the battery capacity c for $T = 1, 2, 3$.

Figure 2 illustrate $\mathrm{Tr}(\mathcal{I}^{-1})/T^2$, which is the lower bound of the scaled variance of the estimation error of all unbiased estimators and thus a measure of privacy, as a function of the battery capacity c for various horizons T. As expected, with increasing c, the estimation error worsens, which is a desirable outcome from the prospective of the household as it helps to preserve its privacy.

IV. Optimal Privacy-Preserving Policy when Consumption is Measured

Now, we extend the results of the previous section to the case where the charging policy of the battery can be a function of the energy consumption of the house s. With slight abuse of notation, let $\mathcal{P} \subseteq \Gamma$ be a set such that, for all $\gamma_1, \gamma_2 \in \mathcal{P}$, $\mathrm{supp}(\gamma(\cdot|s)) \setminus \mathrm{supp}(\gamma'(\cdot|s))$ has a zero Lebesgue measure for all $s \in \mathcal{S}$.

Proposition 2: $\mathcal{J}$ is a convex function of the conditional density function $\gamma(\cdot|s)$ over the set of density functions $\mathcal{P}$.

Proof: See [27]. ■

Again, motivated by this result, we search for the minimizer of $\mathcal{J}$ over the set of all density functions γ that are at most over a measure-zero set equal to zero inside $\mathrm{int}(\mathcal{B})$.

A. Scalar Case

Again, we start with the scalar case. The next theorem provides the solution in this case.

Theorem 6: Let γ^* denote the solution of Problem 3. Then, it satisfies the following partial differential equation with $u(b, s) = \sqrt{\gamma^*(b|s)}$:

$$\begin{cases} \dfrac{\partial^2 u(b,s)}{\partial b^2} + 2\dfrac{\partial^2 u(b,s)}{\partial b \partial s} + \dfrac{\partial^2 u(b,s)}{\partial s^2} & \\ \qquad\qquad + \mu(s)\mathcal{I}(s)^2 u(s,b) = 0, & b \in \mathcal{B}, \\ u(b,s) = 0, & b \in \partial\mathcal{B}. \end{cases} \tag{4}$$

Here, $\mu(s)$ is selected so that $\int_{b \in \mathcal{B}} u(b,s)^2 \mathrm{d}b = 1$ for all $s \in \mathcal{S}$ and $\mathrm{supp}(u(\cdot, s)) = \mathrm{int}(\mathcal{B})$.

Proof: See [27]. ■

Corollary 3: $\gamma^*(b|s) = \frac{2}{c}\cos^2(\pi(b - c_0 + c/2)/c)\mathbb{1}_{c_0 - c \leq b \leq c_0}$ solves Problem 3 for $T = 1$.

Proof: See [27]. ■

Note that the solution of Problem 3 may not be unique due to non-concavity of the cost function. Therefore, there might

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

exists another solution that is a function of s unlike the one in Corollary 3.

Theorem 7: The solution of Problem 4 is given by $\gamma^*(b|s) = u(b,s)^2$, where $u(b,s)$ is the solution of the linear partial differential equation

$$\begin{cases} \dfrac{\partial^2 u(b,s)}{\partial b^2} + 2\dfrac{\partial^2 u(b,s)}{\partial b \partial s} + \dfrac{\partial^2 u(b,s)}{\partial s^2} \\ \qquad\qquad +\mu(s)u(s,b) = 0, \quad b \in \mathcal{B}, \\ u(b,s) = 0, \qquad\qquad\qquad b \in \partial\mathcal{B}. \end{cases} \tag{5}$$

Here, $\mu(s)$ is selected so that $\int_{b\in\mathcal{B}} u(b,s)^2 \mathrm{d}b = 1$ for all $s \in \mathcal{S}$ and $\mathrm{supp}(u(\cdot,s)) = \mathrm{int}(\mathcal{B})$.

Proof: See [27]. ■

Corollary 4: $\gamma^*(b|s) = \frac{2}{c}\cos^2(\pi(b-c_0+c/2)/c)\mathbb{1}_{c_0-c\le b\le c_0}$ solves Problem 4 for $T=1$.

Proof: See [27]. ■

Remark 5: For the scalar case, one of the solution of Problem 3 coincides with the solution of Problem 4. However, due to the non-concavity of the cost function of Problem 3, this problem can have other solutions as well.

Remark 6: It is interesting to note that the optimal charging policy is independent of s; therefore, the lack of this information does not create any inefficiencies. Further, the choice of the weight function $p(s)$ does not change the optimal policy.

B. Multivariate

Now, we can extend the results to the case where $T > 1$. In this subsection, we only focus on Problem 4. The solution of Problem 3 can be calculated following the same recipe as in the previous section resulting in a nonlinear partial differential equation that cannot be efficiently solved for large horizons.

Theorem 8: The solution of Problem 4 is given by $\gamma^*(b|s) = u(b,s)^2$, where $u(b,s)$ is the solution of the linear partial differential equation

$$\begin{cases} \displaystyle\sum_{i=1}^{T} \dfrac{\partial u(b,s)}{\partial b_i^2} + 2\dfrac{\partial^2 u(b,s)}{\partial b_i \partial s_i} + \dfrac{\partial^2 u(b,s)}{\partial s_i^2} \\ \qquad\qquad +\mu(s)u(b,s) = 0, \quad b \in \mathcal{B}, \\ u(b,s) = 0, \qquad\qquad\qquad b \in \partial\mathcal{B}. \end{cases} \tag{6}$$

Here, $\mu(s)$ is selected such that $\int_{b\in\mathcal{B}} u(b,s)^2 \mathrm{d}b = 1$ and $\mathrm{supp}(u(\cdot,s)) = \mathrm{int}(\mathcal{B})$ for all $s \in \mathcal{S}$.

Proof: See [27]. ■

It is easy to show that γ^* in Corollary 1 satisfies the conditions of Theorem 8 and is thus the solution of Problem 4. This can be proved following the same reasoning as in Corollary 4.

V. Extensions

In this section, we consider three extensions of the framework. We start by considering biased estimators. Then, we study the case where using the battery is penalized by a cost function. Finally, we consider the case where the charging and discharging rate of the battery is limited.

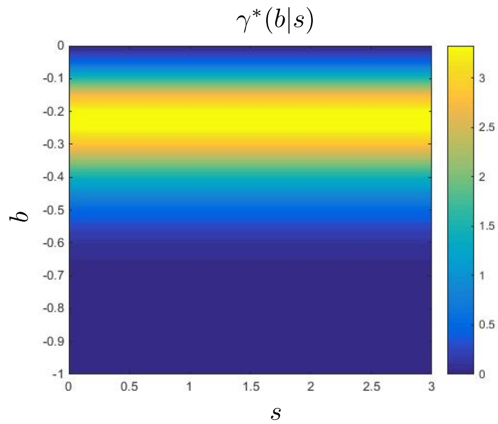

Fig. 3. The conditional probability density function $\gamma^*(b|s)$ for $b \in \mathcal{B}$ and $s \in \mathcal{S}$ in the case where $f(b,s) = 0.5(s-b)$.

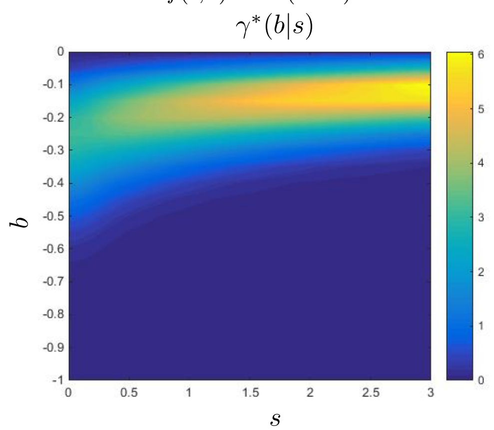

Fig. 4. The conditional probability density function $\gamma^*(b|s)$ for $b \in \mathcal{B}$ and $s \in \mathcal{S}$ in the case where $f(b,s) = 0.5(s-b)^2$.

A. Considering Biased Estimators

In this section, we briefly consider the case where the adversary uses a biased estimator.

Theorem 9: Under either Assumption 1 or 2, for any estimate of s denoted by $\hat{s}(x)$, it holds that

$$\mathbb{E}\{\|s-\hat{s}(x)\|_2^2\} \ge \mathrm{Tr}\left(\frac{\partial\psi(s)}{\partial s}\mathcal{I}(s)^{-1}\frac{\partial\psi(s)}{\partial s}^\top\right) + (\psi(s)-s)^2,$$

where $\psi(s) = \mathbb{E}\{\hat{s}(x)\}$.

Proof: The proof is similar to that of Theorem 1, which can be found in [27]. ■

For scalar case when the consumption is not measured, the problem is exactly the same as before since $\mathrm{Tr}((\partial\psi(s)/\partial s)\mathcal{I}(s)^{-1}(\partial\psi(s)/\partial s)^\top) = \psi'(s)^2/\mathcal{I}$. For a fixed $\psi(\cdot)$, the problem of maximizing $\psi'(s)^2/\mathcal{I} + (\psi(s)-s)^2$ is equivalent to the problem of minimizing $\mathcal{I}$.

B. Considering the Cost of Using Batteries

In some cases, the household might be interested in reducing its electricity bill in addition to preserving its privacy or to reduce the battery's wear and tear. In this case, the problem of interest changes to

$$\gamma^* \in \operatorname*{argmin}_{\gamma\in\Gamma} \left[\mathcal{J} + \int_{s\in\mathcal{S}}\int_{b\in\mathcal{B}} f(b,s)\gamma(b|s)p(s)\mathrm{d}b\mathrm{d}s\right], \tag{7}$$

where $f : \mathcal{B}\times\mathcal{S} \to \mathbb{R}$ denotes the cost associated with the use of the battery. This is an extension of Problem 4. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

cost function of the optimization problem (7) is convex over $\mathcal{P}$ thanks to Proposition 2 and the fact that the additional term due to the cost of using the battery is linear in $\gamma(\cdot|s)$.

Theorem 10: Let $T = 1$. The solution of (7) is given by $\gamma^*(b|s) = u(b,s)^2$, where $u(b,s)$ is the solution of the linear partial differential equation

$$\begin{cases} \dfrac{\partial^2 u(b,s)}{\partial b^2} + 2\dfrac{\partial^2 u(b,s)}{\partial b \partial s} + \dfrac{\partial^2 u(b,s)}{\partial s^2} \\ \qquad\qquad +(f(b,s)+\mu(s))u(s,b) = 0, \quad b \in \mathcal{B}, \\ u(b,s) = 0, \qquad\qquad\qquad\qquad\qquad b \in \partial\mathcal{B}. \end{cases} \tag{8}$$

Here, $\mu(s)$ is selected so that $\int_{b\in\mathcal{B}} u(b,s)^2 \mathrm{d}b = 1$ for all $s \in \mathcal{S}$ and $\mathrm{supp}(u(\cdot,s)) = \mathrm{int}(\mathcal{B})$.

Proof: The proof is similar to that of Theorem 7, which can be found in [27]. ∎

Let us define two special functions

$$\mathrm{Ai}(x) = \frac{1}{\pi}\int_0^\infty \cos(t^3/3 + xt)\mathrm{d}t,$$

$$\mathrm{Bi}(x) = \frac{1}{\pi}\int_0^\infty \left[\exp(-t^3/3 + xt)\sin(t^3/3 + xt)\right]\mathrm{d}t.$$

These are called the Airy functions and are used to construct the optimal charging policy of the battery.

Corollary 5: Let $f = \alpha b + \beta s$. Then,

$$\gamma^*(b|s) = \kappa_1 \mathrm{Ai}\bigg(-\frac{\mu_0 + \alpha b}{\alpha^{2/3}}\bigg) + \kappa_2 \mathrm{Bi}\bigg(-\frac{\mu_0 + \alpha b}{\alpha^{2/3}}\bigg),$$

where κ_1, κ_2, and μ_0 are chosen so that $\gamma^*(c_0 - c|s) = 0$, $\gamma^*(c_0|s) = 0$, and $\int_{c_0-c}^{c_0} \gamma^*(b|s)\mathrm{d}b = 1$.

Proof: See [27]. ∎

Example 2: Consider the scalar case when the battery has access to the household consumption. Let us fix $c_0 = 0$ and $c = 1$. Here, a cost associated with the use of the battery or the combined consumption of the house (the household consumption and the battery use). Figure 3 shows the conditional probability density function $\gamma(b|s)$ for $b \in \mathcal{B}$ and $s \in \mathcal{S}$ in the case where $f(b,s) = 0.5(s-b)$. As expected from Corollary 5, the optimal policy is independent of s. In this case, the battery's charging is kept low with a high probability to reduce the combined consumption of the house. Figure 4 illustrates the conditional probability density function in the case where $f(b,s) = 0.5(s-b)^2$. The probability density function is generated by numerically solving the partial differential equation in (8). In this case, we cannot separate $f(b,s)$ into separate parts for s and b and thus the policy becomes a function of s. For small s, preserving the privacy seems to be more important (as the density is closer to the case without f); however, as s rises, the consumption is kept small.

C. Considering Rate Limits

In this section, we assume that the rates b_k must belong to the range $[\underline{b}, \overline{b}]$ with constants $\underline{b} \le \overline{b}$. In this case, the set $\mathcal{B}$ changes to

$$\mathcal{B} = \bigg\{ \begin{bmatrix} b_0 & \cdots & b_T \end{bmatrix}^T \in \mathbb{R}^T \,|\, \forall k \in \mathcal{T} \\ -\max(\underline{b}, \sum_{i=1}^{k-1} b_i + (c_0 - c)) \le b_k \le \min(\overline{b}, c_0 - \sum_{i=1}^{k-1} b_i) \bigg\}.$$

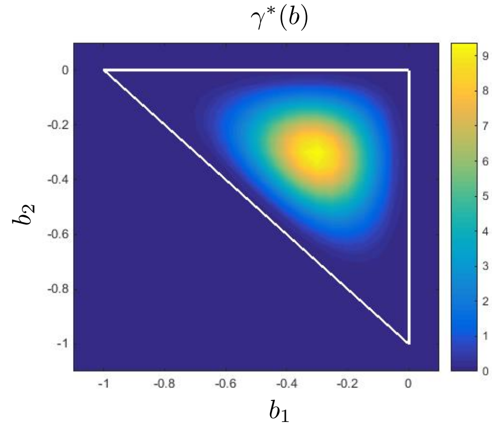

Fig. 5. The probability density function $\gamma^*(\underline{b})$ versus $b = (b_1, b_2) \in \mathcal{B}$ for the case with rate limits of $\underline{b} = -\infty$ and $\overline{b} = 0$. The boundaries of the feasible set $\mathcal{B}$ are shown by white lines.

In this case, the Greedy method, stemming from the separation of the variables, is no longer the solution of Problem 2 because the optimal charging policy needs to consider the effect of the current decisions on future. Therefore, the previously derived partial differential equations need to be solved numerically. This is demonstrated in the following numerical example.

Example 1 (Cont'd): Again assume that $c_0 = 0$ and $c = 1$. Here, we add the extra assumption that $\underline{b} = -\infty$ and $\overline{b} = 0$. This means that the battery can only be charged (because, e.g., the occupants need the battery to be fully charged at night). Figure 5 shows the probability density function $\gamma^*(b)$ versus $b = (b_1, b_2) \in \mathcal{B}$. The probability density function is generated by numerically solving the partial differential equation in (3). The boundaries of the feasible set $\mathcal{B}$ are shown by white lines. The lack of symmetry in the distribution (note the distortion of the shape close to the line defined by the equation $b_1 + b_2 = 1$) implies that the decision making about b_1 and b_2 cannot be separated; thus, the greedy method is no longer optimal.

VI. Numerical Example

In this section, we validate our results against the state-of-the-art adversary who wants to learn private information from measurements of the household consumption. Noting that we have not optimized the charging policy of the battery against this particular adversary, it is interesting to observe that we can still obtain good results.

We demonstrate the applicability of the derived method on real data from the REDD[1] database [18]. Here, we are using the low frequency data from the first house in the REDD database. In this database, the consumption of the various appliances is measured every 3-4 seconds. This data in conjunction with the consumption of the entire house is used for training and verification purposes. The consumption of the entire house is measured every second. The data is for the period of April 23–May 21, 2011. The part of the data prior to April 30th is used for training and the rest for validation purposes. We have selected the top 5 appliances in energy consumption for disaggregation purposes, namely, fridge, microwave, socket (in the kitchen), light, and dish washer.

[1] http://redd.csail.mit.edu/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2667702, IEEE Transactions on Smart Grid

For disaggregation, we have used the NILMTK[2] toolbox in Python [32]. We have used a frequently utilized disaggregation method called Factorial Hidden Markov Model (FHMM). This method was originally proposed in [33] and was used for energy disaggregation in [19]. This method has also been used by the researchers contributing to the REDD database [18]. We set the resolution of the charging/discharging policy of the battery (i.e., the duration of each time instant for setting the actions of the battery) to be one hour.

A widely utilized measure of accuracy for energy disaggregation is f-score. This measure takes values between zero and one with one denoting perfect disaggregation. To present the description of the f-score, we need to define a few concepts. Let TP denote the number of time instances in which the appliance was correctly classified on (true positive), FP denote the number of time instances in which the appliance was mistakenly classified on (false positive), and FN denote the number of time instances in which the appliance was mistakenly classified off (false negative). Then, we have

$$\text{f-score} := \frac{1}{1+(\mathrm{FN}+\mathrm{FP})/(2\mathrm{TP})}.$$

Clearly, as the number of the mistakes, i.e., FP and FN, grows, the f-score of the method decreases. To put the following discussion into perspective, an f-score that is, respectively, equal to $1/2$ and $1/3$ means that the number of the false positive and false negatives (mistakes by the method) is equal to twice and four times the number of the correct positives. Therefore, the performance of the energy disaggregation method drops rapidly as its f-score reduces.

Figure 6 illustrates the f-score of various appliances without a battery and in the presence a battery. For the case where the battery is present, the charging policy of Corollary 1 is utilized. As expected, with increasing the capacity of the battery, the f-score for almost all the appliances decreases. The socket reacts differently as its f-score does not seem be influenced by the battery. This is due to the special pattern of its consumption. During the whole observation window, the appliance connected to the socket is continuously on (with occasional spikes). Therefore, the utilized disaggregation algorithm (learning from the data before April 30th) always assumes that the appliance is on irrespective of the battery's demand.

VII. Conclusions and Future Work

In this paper, optimal policies for charging and utilizing batteries are devised to minimize the trace of the Fisher information matrix so as to maximize the variance of the estimation error of the electricity consumption irrespective of the estimation policy used by adversaries. This ensures that the privacy of the households with smart meters is preserved. The use of the Fisher information as a measure of privacy, as opposed to the mutual information, provides a meaningful performance guarantee against the adversary through the use of the Cramér-Rao bound. This interpretation is useful as we might not be able to model the adversary. Parts of the results of this paper are extended to general privacy problems in [34].

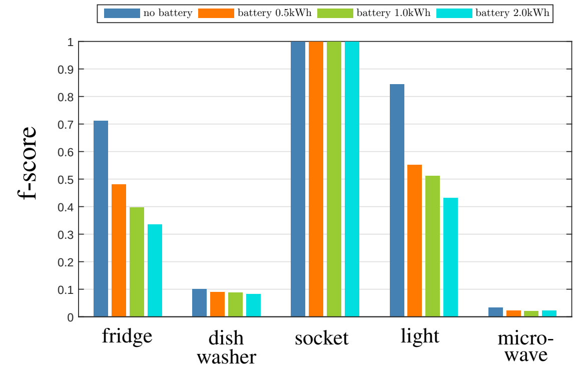

Fig. 6. F-score of various appliances without a battery for masking the consumption and in the presence a battery.

However, the extension is at an early stage and only consider the case where the distribution of the additive constrained noise is not a function of the private data. Future work can focus on taking into account the causality assumption when the measurements of the household consumption are available.

[2] https://github.com/nilmtk/nilmtk

References

[1] G. W. Hart, "Residential energy monitoring and computerized surveillance via utility power flows," *IEEE Technology and Society Magazine*, vol. 8, no. 2, pp. 12–16, 1989.

[2] A. Zoha, A. Gluhak, M. A. Imran, and S. Rajasegarar, "Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey," *Sensors*, vol. 12, no. 12, pp. 16838–16866, 2012.

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

[4] C. Dwork, "Differential privacy: A survey of results," in *Theory and Applications of Models of Computation: 5th International Conference, TAMC 2008, Xi'an, China, April 25-29, 2008. Proceedings* (M. Agrawal, D. Du, Z. Duan, and A. Li, eds.), pp. 1–19, Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[5] C. Dwork, "Differential privacy," in *Encyclopedia of Cryptography and Security* (H. C. A. van Tilborg and S. Jajodia, eds.), Boston, MA: Springer US, 2011.

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

[7] S. Han, U. Topcu, and G. J. Pappas, "Differentially private convex optimization with piecewise affine objectives," in *Proceedings of the 53rd IEEE Conference on Decision and Control*, pp. 2160–2166, 2014.

[8] Z. Huang, Y. Wang, S. Mitra, and G. E. Dullerud, "On the cost of differential privacy in distributed control systems," in *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, pp. 105–114, ACM, 2014.

[9] H. Sandberg, G. Dán, and R. Thobaben, "Differentially private state estimation in distribution networks with smart meters," in *Proceedings of the 54th IEEE Conference on Decision and Control*, pp. 4492–4498, 2015.

[10] G. Ács and C. Castelluccia, "I have a DREAM! (DiffeRentially privatE smArt Metering)," in *Information Hiding: 13th International Conference, IH 2011, Prague, Czech Republic, May 18-20, 2011, Revised Selected Papers* (T. Filler, T. Pevný, S. Craver, and A. Ker, eds.), pp. 118–132, Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.

[11] F. Farokhi, J. Milosevic, and H. Sandberg, "Optimal state estimation with measurements corrupted by Laplace noise," in *Proceedings of the 55th IEEE Conference on Decision and Control*, 2016.

[12] L. R. G. Carrillo, W. J. Russell, J. P. Hespanha, and G. E. Collins, "State estimation of multiagent systems under impulsive noise and disturbances," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 1, pp. 13–26, 2015.

[13] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 232–237, 2010.

[14] O. Tan, D. Gunduz, 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.

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

[16] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1932–1935, 2011.

[17] J. Shao, *Mathematical Statistics*. Springer Texts in Statistics, Springer-Verlag New York, 2003.

[18] J. Z. Kolter and M. J. Johnson, "REDD: A public data set for energy disaggregation research," in *Workshop on Data Mining Applications in Sustainability (SIGKDD)*, vol. 25, pp. 59–62, 2011.

[19] H. Kim, M. Marwah, M. Arlitt, G. Lyon, and J. Han, *Unsupervised Disaggregation of Low Frequency Power Measurements*, ch. 64, pp. 747–758. 2011.

[20] H. Anderson, "Efficiency versus protection in a general randomized response model," *Scandinavian Journal of Statistics*, pp. 11–19, 1977.

[21] T. Tanaka and H. Sandberg, "SDP-based joint sensor and controller design for information-regularized optimal LQG control," in *Proceedings of the 54th IEEE Conference on Decision and Control*, pp. 4486–4491, 2015.

[22] E. Akyol, C. Langbort, and T. Basar, "Privacy constrained information processing," in *Proceedings of the 54th IEEE Conference on Decision and Control*, pp. 4511–4516, IEEE, 2015.

[23] F. Farokhi, H. Sandberg, I. Shames, and M. Cantoni, "Quadratic Gaussian privacy games," in *roceedings of the 54th IEEE Conference on Decision and Control*, pp. 4505–4510, 2015.

[24] J.-F. Bercher and C. Vignat, "On minimum Fisher information distributions with restricted support and fixed variance," *Information Sciences*, vol. 179, no. 22, pp. 3832–3842, 2009.

[25] E. Uhrmann-Klingen, "Minimal Fisher information distributions with compact-supports," *Sankhyā: The Indian Journal of Statistics, Series A (1961-2002)*, vol. 57, no. 3, pp. 360–374, 1995.

[26] P. J. Huber, *Robust Statistics*. Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, 1981.

[27] F. Farokhi and H. Sandberg, "Fisher information as a measure of privacy: Preserving privacy of households with smart meters using batteries," Technical Note, 2016. https://dl.dropboxusercontent.com/u/36867745/PrivacySmartMetering.pdf.

[28] R. Wijsman, "On the attainment of the cramér-rao lower bound," *The Annals of Statistics*, pp. 538–542, 1973.

[29] K. C. Sou, J. Weimer, H. Sandberg, and K. H. Johansson, "Scheduling smart home appliances using mixed integer linear programming," in *Proccedings of the 50th IEEE Conference on Decision and Control and European Control Conference*, pp. 5144–5149, IEEE, 2011.

[30] J. L. W. V. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Mathematica*, vol. 30, no. 1, pp. 175–193, 1906.

[31] A. S. Mohamed and H. A. Atia, "Separation of the Schrödinger operator with an operator potential in the Hilbert spaces," *Applicable Analysis*, vol. 84, no. 1, pp. 103–110, 2005.

[32] N. Batra, J. Kelly, O. Parson, H. Dutta, W. Knottenbelt, A. Rogers, A. Singh, and M. Srivastava, "NILMTK: An open source toolkit for non-intrusive load monitoring," in *Fifth International Conference on Future Energy Systems (ACM e-Energy)*, 2014.

[33] Z. Ghahramani and M. I. Jordan, "Factorial hidden Markov models," *Machine learning*, vol. 29, no. 2-3, pp. 245–273, 1997.

[34] F. Farokhi and H. Sandberg, "Optimal constrained additive noise distribution minimizing Fisher information for ensuring privacy," Submitted to the *American Contriol Conference*, 2016. https://dl.dropboxusercontent.com/u/36867745/ACC2016Privacy.pdf.