Privacy Preserving Rechargeable Battery Policies for Smart Metering Systems

(Invited Paper)

Simon Li
Department of Electrical and Computer Engineering
University of Toronto
Email: simonli@ece.utoronto.ca

Ashish Khisti
Department of Electrical and Computer Engineering
University of Toronto
Email: akhisti@ece.utoronto.ca

Aditya Mahajan
Department of Electrical and Computer Engineering
McGill University
Email: aditya.mahajan@mcgill.ca

***Abstract*—We consider a setup where a rechargeable battery is used to partially mask the load profile of a user from the utility provider in a smart-metered electrical system. We focus on the case of i.i.d. load profile, use mutual information as our privacy metric, and characterize the optimal policy as well as the associated leakage rate.**

Our approach is based on obtaining single-letter expression for the leakage rate for a class of battery policies and providing a converse argument for establishing the optimality.

I. Introduction

Smart meters are becoming a critical part of modern electrical grids. They deliver fine-grained household power usage measurements to utility providers. This information allows them to implement changes to improve the efficiency of the electrical grid. However, despite the promise of savings in energy and money, there is potentially a loss of privacy. Anyone with access to the load profile may employ data mining algorithms to infer details about the private activities of the user [1]–[4].

In this paper, we investigate one possible solution to the privacy problem. Using a rechargeable battery, the user can distort the load profile generated by the appliances by charging and discharging the battery. Due to the proliferation of rechargeable batteries, energy harvesting devices and electric vehicles, the strategy of using these devices to partially obfuscate the user's load profile is becoming more feasible. As we discuss below, a number of recent works have studied this approach in the literature.

A. Related Works

We consider a similar setup to [7] which introduces using mutual information as a privacy metric then considers an instance of the problem with binary alphabets. The setup is extended in [8], [9] where the multi-letter mutual information optimization problem is reformulated as a Markov Decision Process. The results in this paper mirror that of [10] where the optimal single-letter information leakage rate and policy is characterized using Markov Decision Theory. In this paper, we provide the proofs using purely information theoretic arguments which may be of interest in its own right. In other related works, rate-distortion type approaches for studying privacy-utility tradeoffs in smart grid systems have been studied in [11]–[14]. These works are not directly related to the present setup.

II. Problem definition

We consider a smart metering system as shown in Fig. 1 where at each time a residence generates an aggregate demand that must either be satisfied by charges in the battery or by drawing power from the grid. $\{X_t\}_{t\geq 1}$, $X_t \in \mathcal{X}$ where $\mathcal{X} := \{0, 1, 2, \dots, m_x\}$ denotes the (exogeneous) i.i.d. power demand process distributed according to Q_X. $\{Y_t\}_{t\geq 1}$, $Y_t \in \mathcal{Y}$, denotes the energy consumed from the grid where $\mathcal{Y} := \{0, 1, 2, \dots, m_y\}$ and $\{S_t\}_{t\geq 1}$, $S_t \in \mathcal{S}$ denotes the energy stored in the battery where $\mathcal{S} := \{0, 1, 2, \dots, m_s\}$ and the initial charge S_1 of the battery is distributed according to probability mass function P_{S_1}.

We assume that $m_x \leq m_y$ so that the system is guaranteed to be able to satisfy the demand at any time by drawing solely from the grid i.e. $Y_t = X_t$, $\forall t$. While in general, the alphabets $\mathcal{X}$ and $\mathcal{Y}$ can be any finite subset of the integers – where negative values of X and Y would model a situation where energy (possibly generated from an alternative energy source) is sold back to the utility provider – it is more realistic to for them to be a contiguous interval. In this case, without further assumptions on the battery size, the alphabets would have to satisfy $\mathcal{X} \subset \mathcal{Y}$ in order to guarantee that energy is not wasted and the power demand can always be satisfied. Nonetheless, our results generalize to these cases.

We assume an ideal battery that has no conversion losses or other inefficiencies. Therefore, the following conservation equation must be satisfied at all time instances:

$$S_{t+1} = S_t - X_t + Y_t. \tag{1}$$

The energy management system observes the power demand and battery charge and consumes energy from the grid according to a randomized *charging policy* $\mathbf{q} = (q_1, q_2, \dots)$. In particular, at time t, given $(x^t,\ s^t, y^{t-1})$, the history of demand, battery charge, and past consumption, the battery policy chooses the level of current consumption Y_t to be y with probability $q_t(y \mid x^t, s^t, y^{t-1})$. For a randomized charging policy to be feasible, it must satisfy the conservation

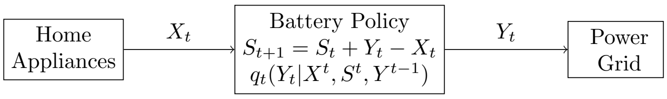

Fig. 1: System Diagram. The user demand is denoted by X_t, the grid consumption by Y_t, and the battery state by S_t. The battery policy is denoted by the conditional distribution $q(Y_t|X^t, S^t, Y^{t-1})$. The battery policy effectively defines a channel with memory from the residence to the utility provider.

equation (1), so given the current power demand and battery charge (x_t, s_t), the feasible values of grid consumption are defined by

$$\mathcal{Y}_\circ(s_t - x_t) = \{y \in \mathcal{Y} : s_t - x_t + y \in \mathcal{S}\}.$$

Thus, we require that

$$\begin{aligned} &q_t(\mathcal{Y}_\circ(s_t - x_t) \mid x^t, s^t, y^{t-1}) \\ &:= \sum_{y \in \mathcal{Y}_\circ(s_t - x_t)} q_t(y \mid x^t, s^t, y^{t-1}) \\ &= 1. \end{aligned}$$

The set of all such feasible strategies is denoted by $\mathcal{Q}_A$. A battery policy effectively defines a channel with memory between a residence and the utility provider (as portrayed in Fig. 1).

The quality of a charging policy depends on the amount of information leaked under that policy. This notion is captured by mutual information $I^{\mathbf{q}}(S_1, X^T; Y^T)$ evaluated according to the joint probability distribution on (S^T, X^T, Y^T) induced by the sequence $\mathbf{q}$:

$$\begin{aligned} &\mathbb{P}^{\mathbf{q}}(S^T = s^T, X^T = x^T, Y^T = y^T) \\ &= P_{S_1}(s_1) P_{X_1}(x_1) q_1(y_1 \mid x_1, s_1) \\ &\times \prod_{t=2}^{T} \Big[\mathbb{1}_{s_t}\{s_{t-1} - x_{t-1} + y_{t-1}\} \\ &\qquad Q(x_t) q_t(y_t \mid x^t, s^t, y^{t-1}) \Big]. \end{aligned} \tag{2}$$

Given a policy $\mathbf{q} = (q_1, q_2, \dots) \in \mathcal{Q}_A$, we define the worst case information leakage *rate* as follows:

$$L_\infty(\mathbf{q}) := \limsup_{T \to \infty} \frac{1}{T} I^{\mathbf{q}}(S_1, X^T; Y^T). \tag{3}$$

Remark II.1. The random variable S_1 in the mutual information terms do not affect the asymptotic rate. It will be clear in the sequel that this simplifies the analysis.

We are interested in the following optimization problem:

Problem A. *Given the alphabet $\mathcal{X}$ and distribution Q_X of the power demand, the alphabet $\mathcal{S}$ of the battery, the initial distribution P_{S_1} of the battery state, and the alphabet $\mathcal{Y}$ of the demand: find a battery charging policy $\mathbf{q} = (q_1, q_2, \dots) \in \mathcal{Q}_A$ that minimizes the leakage rate $L_\infty(\mathbf{q})$ given by* (3).

III. Stationary Posterior Policies

The simplest class of policies are stationary and memoryless, conditioning only on the current battery state and power demand:

$$q(y|x, s). \tag{4}$$

As such evaluating the leakage rate (3) even for this simplified class of policies requires numerical approaches, see e.g., [7], [13]. Our key insight is that if we further impose a certain invariance condition we can obtain a closed form expression for the leakage rate. Interestingly we will see that this class of policies also includes a globally optimal policy. Our proposed class preserves the following property:

$$\mathbb{P}(S_2 = s_2 | Y_1 = y_1) = \mathbb{P}(S_1 = s_2),\ \forall s_2 \in \mathcal{S}, y_1 \in \hat{\mathcal{Y}} \tag{5}$$

where $\hat{\mathcal{Y}} := \{y : P_{Y_1}(y_1) > 0\}$ for some initial battery state distribution $\mathbb{P}_{S_1}$. This invariance condition implies that $S_t \perp Y_{t-1}$ and also that $\mathbb{P}_{S_t} = \mathbb{P}_{S_1},\ \forall t$. By exploiting this property, we can obtain single-letter achievable leakage rates as follows:

Lemma III.1. *Given an instance of Problem A with i.i.d. power demand $Q_X(x)$ and initial battery state distribution $\mathbb{P}_{S_1}$, if the stationary memoryless policy $\mathbf{q} = (q, q, \dots) \in \mathcal{Q}_A$ satisfies the invariance property* (5)*, then*

$$L_\infty(\mathbf{q}) = I^{\mathbf{q}}(S_1, X_1; Y_1),$$

where $(S_1, X_1, Y_1) \sim \mathbb{P}_{S_1}(s_1) Q(x_1) q(y_1|x_1, s_1)$.

Proof. The invariance property and the memorylessness of $\mathbf{q}$ implies that $(Y_t, X_t, S_t) \perp Y^{t-1},\ \forall t$. Therefore we have

$$\begin{aligned} \frac{1}{T} I^{\mathbf{q}}(S_1, X^T; Y^T) &\overset{(a)}{=} \sum_{t=1}^{T} \frac{1}{T} I^{\mathbf{q}}(S^t, X^T; Y_t | Y^{t-1}) \\ &\overset{(b)}{=} \sum_{t=1}^{T} \frac{1}{T} I^{\mathbf{q}}(S_t, X_t; Y_t | Y^{t-1}) \\ &\overset{(c)}{=} I^{\mathbf{q}}(S_1, X_1; Y_1),\ \forall T \end{aligned}$$

where (a) is due to the chain rule of mutual information and the fact that S^t is a deterministic function of (S_1, X^{t-1}, Y^{t-1}) given by the battery update equation (1), (b) is due to the memoryless condition (4), and (c) is due to the invariance property (5). ☐

We will next develop some further properties of the invariance condition (5). Let us define an auxillary random variable $W_t := S_t - X_t$ where $W_t \in \mathcal{W} := \mathcal{S} - \mathcal{X}$ and for $w \in \mathcal{W}$, let

$$\mathcal{D}(w) := \{(x, s) \in \mathcal{X} \times \mathcal{S} : s - x = w\}.$$

Lemma III.2. *An initial battery distribution $\mathbb{P}_{S_1}$ and a stationary memoryless policy $\mathbf{q} = (q, q, \dots)$ satisfies the invariance property* (5) *iff for each $(s_2, y_1) \in \mathcal{S} \times \mathcal{X}$, we have*

$$\mathbb{P}_{S_1}(s_2) Q(y_1) = \sum_{(\tilde{x}, \tilde{s}) \in \mathcal{D}(s_2 - y_1)} q(y_1 | \tilde{x}_1, \tilde{s}_1) Q(\tilde{x}_1) \mathbb{P}_{S_1}(\tilde{s}_1). \tag{6}$$

Proof. (If) Note that since the rhs is equal to the joint $\mathbb{P}^{\mathbf{q}}(S_2 = s_2, Y_1 = y_1)$, the systems of equations in the Lemma implies that $S_2 \perp Y_1$ and $\mathbb{P}^{\mathbf{q}}_{S_2} = \mathbb{P}_{S_1}$ which is the invariance property (5).

(Only if) Assuming the invariance property to be true, since $S_1 - X_1 = S_2 - Y_1$ given by the battery update equation (1) we must have $\mathbb{P}^{\mathbf{q}}_{Y_1}(y_1) = Q(y_1),\ \forall y_1 \in \mathcal{X}$. Using Bayes rule and the definition of the joint distribution we recover the statement in the Lemma. $\square$

Lemma III.2 implies that the alphabet for $\{Y_t\}_{t>0}$ must be limited to $\mathcal{X}$ and $\mathbb{P}^{\mathbf{q}}_{Y_t} = Q$. In addition, Eq. (6) provides an explicit condition that must be satisfied by the stationary memoryless policies for any fixed $\mathbb{P}_{S_1} \in \mathcal{P}_S$. Note that these are essentially $|\mathcal{W}|$ linear constraints. It should be clear that these constraints are always feasible. For example, using the policy $Y_t = X_t$, any $\mathbb{P}_{S_1}$ will satisfy the invariance property (5). However, this will maximize the leakage rate. We next discuss a policy that turns out be optimal.

A. Optimal Policy

Lemma III.3. *Given a fixed $\mathbb{P}_{S_1}$ and $W_1 = S_1 - X_1$, the optimal policy $\mathbf{q}^* = (q^*, q^*, \dots)$ satisfying the invariance property III.2 is*

$$q^*(y|x,s) = \begin{cases} \frac{Q(y)P_{S_1}(y+s-x)}{P_{W_1}(s-x)} & \text{if } y \in \mathcal{X} \cap \mathcal{Y}_\circ(s-x) \\ 0 & \text{otherwise} \end{cases}$$

achieving a leakage rate of

$$L_\infty(\mathbf{q}^*) = I(S_1 - X_1; X_1)$$

where $(S_1, X_1) \sim \mathbb{P}_{S_1}(s_1)Q(x_1)$.

Proof. By definition, $q^*(y|x,s) \geq 0,\ \forall s \in \mathcal{S}, x \in \mathcal{X}, y \in \mathcal{X} \cap \mathcal{Y}_\circ(s-x)$. Next, we show that q^* is properly normalized.

$$\begin{aligned} &\sum_{\tilde{y} \in \mathcal{X} \cap \mathcal{Y}_\circ(s-x)} Q(\tilde{y}) P_{S_1}(\tilde{y} + s - x) \\ &= \sum_{(\tilde{x}, \tilde{s}) \in \mathcal{D}(s-x)} Q(\tilde{x}) P_{S_1}(\tilde{s}) \\ &= \text{Denominator of } q^*(\mathcal{Y}_\circ(s-x)|x,s), \end{aligned}$$

where the second step follows by substituting $\tilde{x} = \tilde{y}$ and $\tilde{s} = \tilde{y} + s - x$ and observing that $\tilde{s} - \tilde{x} \in \mathcal{D}(s-x)$. Therefore, $\mathbf{q}^*$ is admissible. The invariance property can be verified using Lemma III.2 or as follows:

$$\begin{aligned} &\mathbb{P}^{\mathbf{q}^*}(S_2 = s_2, Y_1 = y_1) \\ &\overset{(a)}{=} \mathbb{P}^{\mathbf{q}^*}(S_2 = s_2, Y_1 = y_1, W_1 = s_2 - y_1) \\ &\overset{(b)}{=} \mathbb{P}^{\mathbf{q}^*}(Y_1 = y_1, W_1 = s_2 - y_1) \\ &= \mathbb{P}^{\mathbf{q}^*}(Y_1 = y_1 | W_1 = s_2 - y_1) \mathbb{P}(W_1 = s_2 - y_1) \\ &\overset{(c)}{=} \mathbb{P}^{\mathbf{q}^*}(Y_1 = y_1 | X_1 = y_1, S_1 = s_2) \mathbb{P}(W_1 = s_2 - y_1) \\ &= q(y_1|y_1, s_2) \mathbb{P}(W_1 = s_2 - y_1) \\ &= Q(y_1) \mathbb{P}_{S_1}(s_2) \end{aligned}$$

where (a) and (b) use the fact that $S_2 - Y_1 = W_1$ holds from the battery update equation, (c) is because $q^*(y|x,s)$ only depends on (x,s) via $s - x$ and the last equality follows from the definition of q^*. The last equality shows that the invariance property is satisfied.

To show optimality, fix $\mathbb{P}_{S_1}$ and let $\mathbf{q}$ be any policy satisfying Lemma III.2 and consider the following inequalities:

$$\begin{aligned} L_\infty(\mathbf{q}) &\overset{(a)}{=} I(S_1, X_1; Y_1) \\ &\overset{(b)}{\geq} I(W_1; Y_1) \\ &= H(W_1) - H(W_1 + Y_1 | Y_1) \\ &\overset{(c)}{=} H(W_1) - H(S_2) \\ &\overset{(d)}{=} H(W_1) - H(S_1) \\ &\overset{(e)}{=} H(S_1 - X_1) - H(S_1 - X_1 | X_1) \\ &= I(S_1 - X_1; X_1) \end{aligned}$$

(a) is due to Lemma III.2, (b) is due to the data processing inequality, (c) and (d) are due to the battery update equation (1) and the invariance property of $\mathbf{q}$, and (e) is by definition.

The achievability proof is completed by noting that under $\mathbf{q}^*$, we have $Y_t - W_t - (X_t, S_t)$ and so the lower bound is obtained. $\square$

Proposition III.1. *Minimizing over the initial battery distribution $\mathbb{P}_{S_1}$ in Lemma III.3 we obtain the optimal leakage rate in the class of policies satisfying the invariance property III.2.*

Remark III.1. The limitation of this achievability scheme requires that the battery have a specific distribution over the battery's initial states. However, this loss of generality is operationally insignificant since the user can start off by randomly charging the battery from an external source.

B. Converse

So far we have shown that the policy in Lemma III.3, is optimal for the class of invariance policies that satisfy (5). We will now prove an information theoretic converse that establishes that the stated policy is globally optimal among all policies in $\mathcal{Q}_A$. This provides the counterpart of the result in [10], but avoids the use of the dynamic programming framework. Consider the following inequalities: for any admissible policy $\mathbf{q} \in \mathcal{Q}_A$ we have

$$\begin{aligned} &I(S_1, X^T; Y^T) \geq \sum_{t=1}^T I(S_t, X_t; Y_t | Y^{t-1}) \geq \sum_{t=1}^T I(W_t; Y_t | Y^{t-1}) \\ &= H(W_1) - H(W_1|Y_1) + H(W_2|Y_1) - H(W_2|Y^2) + \cdots \\ &\overset{\text{(a)}}{=} H(W_1) - H(S_2|Y_1) + H(S_2 - X_2|Y_1) - H(S_3|Y^2) + \cdots \\ &= H(W_1) + \sum_{t=2}^T I(W_t; X_t | Y^{t-1}) - H(W_T | Y^T) \end{aligned}$$

where (a) is because S_{t+1} is an invertible function of W_t given Y_t. Now, taking the limit $T \to \infty$ to obtain a lower bound to the leakage rate we have

$$\begin{aligned}
&L_\infty(\mathbf{q}) = \lim_{T\to\infty} \frac{1}{T} I(S_1, X^T; Y^T) \\
&\geq \lim_{T\to\infty} \frac{1}{T}\left[H(W_1) + \sum_{t=2}^{T} I(W_t; X_t|Y^{t-1}) - H(W_T|Y^T)\right] \\
&\overset{(a)}{=} \lim_{T\to\infty} \frac{1}{T}\left[\sum_{t=2}^{T} I(W_t; X_t|Y^{t-1})\right] \\
&\overset{(b)}{\geq} \min_{P_S \in \mathcal{P}_S} I(S-X; X).
\end{aligned}$$

(a) is because the entropy of any discrete random variable is bounded and (b) follows from the observation that every term in the summation is only a function of the posterior $P(S_t|Y^{t-1})$. Therefore, minimizing each term over a $P_S \in \mathcal{P}_S$ results in a lower bound to the optimal leakage rate which is achievable using Proposition III.1.

IV. Conclusions

In this paper, we provide a single-letter characterization of the optimal private information leakage rate using information theoretic arguments. While the result was already established in [10], the proof provided in this paper is based on more elementary arguments and avoids the use of the dynamic programming framework. Our proof shows that the optimal leakage rate is achieved using a class of stationary memoryless policies that preserve the posterior distribution of the battery state. We believe that the techniques discussed here also extend to continuous valued input and output alphabets.

References

[1] A. Predunzi, "A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel," in *Proc. IEEE Power Eng. Society Winter Meeting, New York*, Jan. 2002.

[2] G. W. Hart, "Nonintrusive appliance load monitoring," Proceedings IEEE, vol. 80, no. 12, pp. 1870-1891, Dec. 1992.

[3] H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A novel method to construct taxonomy of electrical appliances based on load signatures," IEEE Trans. user Electronics, vol. 53, no. 2, pp. 653-660, May 2007.

[4] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in Proc. 2nd ACM Workshop Embedded Sensing Systems for Energy-Efficiency in Building, ser. BuildSys 10. New York, NY, USA: ACM, 2010, pp. 61-66.

[5] P. Harsha and M. Dahleh, "Optimal management and sizing of energy storage under dynamic pricing for the efficient integration of renewable energy," in Power Systems, IEEE Transactions on, 30(3):1164-1181, May 2015.

[6] 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 Smart Grid Commun. Conf., Gaithersburg, Maryland, 2010.

[7] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proc. IEEE Int'l Conf. Acoust. Speech Sig. Proc. Prague, Czech Republic*, May 2011.

[8] S. Li, A. Khisti, and A. Mahajan, "Structure of optimal privacy-preserving policies in smart-metered systems with a rechargeable battery," Proceedings of the IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pp. 1-5, Stockholm, Sweden, June 28-July 1, 2015.

[9] J. Yao and P. Venkitasubramaniam, "On the Privacy of an In-Home Storage Mechanism," 52nd Allerton Conference on Communication, Computation and Control, Monticello, IL, October 2013.

[10] S. Li, A. Khisti, A. Mahajan, "Privacy-Optimal Strategies for Smart Metering Systems with a Rechargeable Battery," online, http://arxiv.org/abs/1510.07170,

[11] S. Rajagopalan, L. Sankar, S. Mohajer, and V. Poor, "Smart meter privacy: A utility-privacy framework," in 2nd IEEE International Conference on Smart Grid Communications, 2011.

[12] L. Sankar, S.R. Rajagopalan, and H.V. Poor, "An Information-Theoretic Approach To Privacy," in Proc. 48th Annual Allerton Conf. on Commun., Control, and Computing, Monticello, IL, Sep. 2010, pp. 1220-1227.

[13] D. Gunduz and J.Gomez-Vilardebo, "Smart meter privacy in the presence of an alternative energy source," in *2013 IEEE International Conference on Communications (ICC)*, June 2013.

[14] J. Gomez-Vilardebo and D. Gunduz, "Privacy of smart meter systems with an alternative energy source," in Proc. IEEE Int'l Symp. on Inform. Theory, Istanbul, Turkey, Jul. 2013, pp. 2572-2576.