On the Privacy-Cost Tradeoff of Battery Control Mechanisms in Demand Response: Selective Information Protection

Jiyun Yao, Parv Venkitasubramaniam,
Lehigh University, USA
{jiy312,parv.v}@lehigh.edu

***Abstract*—Perfect knowledge of a user's power consumption profile by a utility is a violation of privacy and can be detrimental to the successful implementation of demand response systems. It has been shown that an in-home energy storage system which provides a viable means to achieve the cost savings of instantaneous electricity pricing without inconvenience can also be used to maintain the privacy of a user's power profile. The optimization of the tradeoff between privacy and cost savings that can be provided by a finite capacity battery with zero tolerance for delay is known to be equivalent to a Partially Observable Markov Decision Process with non linear belief dependent rewards. In this paper, we assume a user is only interested in hiding some basic information such as his presence/absence, or a particular usage pattern and study the model with multiple levels of battery state, demand and price, and propose a "revealing state" approach to enable computation of a class of battery control policies that aim to maximize the achievable privacy of in-home demands. Numerical results based on real electricity and pricing data show that our proposed strategy performs close to the upper bound of the optimal tradeoff between privacy preserving and cost saving.**

***Index Terms*—Privacy, Storage, Entropy, Scheduling, Utility, Demand Response, Random Walk**

I. Introduction

Renewable energy share of global electricity production was estimated to reach 21.7% at the end of 2012 and this number has been rising every year [1]. Due to increased volatility of renewable energy and the emergence of flexible load scheduling through energy management systems, grid operators have already begun to rely on *demand response* technology to match the temporal generation profile [2].

One of the major drawbacks using demand response systems that require two way communications between the consumers and utility is the violation of consumer's privacy due to transmission of fine grained usage data to the utilities. Prior research on the perils of Non-intrusive Load Monitoring [3], [4] using smart meters have demonstrated that even without a prior knowledge of household activities or prior training, it is possible to extract complex usage patterns from smart meter data using off-the-shelf statistical methods.

Different approaches have been proposed to hide the information revealed through smart metering data. Encryption methods are studied in [5], [6]. In the absence of encryption, [7], [8] propose "distorting" the data to prevent information retrieval by shifting loads or filtering energy usage data.

In this work, the in-home storage mechanism can be used to provide privacy in both the short and long time scale with a zero tolerance on delay. Recent experiments by ABB and GM in the United States [9] have demonstrated the viability for small scale storage to supply up to 3 hours of electricity usage for a group of 2-3 homes. Their experiment demonstrated the cost effectiveness of such a system for small scale deployment.

A simple stochastic battery policy using a storage device at home to distort the instantaneous energy consumption is studied in [10]. But the fact that eavesdropper can use the observation to estimate the past energy consumption is neglected. Another recent approach to address the privacy preserving and cost saving tradeoff in [11] defines the privacy as the "flatness" of power consumption profile and proposed an online control algorithm. We note that "flatness" of a power profile is an implicit measure of privacy.In our previous work [12], a formal mathematical framework is introduced using a specific class of Markov modeled systems. We use Shannon's equivocation [13] to characterize the uncertainty of the demand from the utility's perspective and define it as privacy. Then we show that the optimal tradeoff between privacy protection and cost savings exists and it is the result of a Partially Observable Markov Decision Process with non linear belief dependent rewards (ρ-POMDP).

In this work, The framework proposed in [12] is shown to be applicable even when users only desire selective information protection such as presence/absence of activity or specific usage patterns they wish to hide. In addition, We propose a class of battery charging policies based on minimizing the frequency of "revealing states so as to obtain an achievable privacy-cost savings tradeoff for users. This class of policies is designed for a general model with multiple levels of battery state, demand and price that any practical system can be reasonably approximated by. We use numerical simulations to demonstrate that it preforms close to the optimal tradeoff between privacy preserving and cost saving.

The remainder of the paper is structured as follows. Section II introduces the mathematical model and describes the variables. In section III, we propose an extension of theρ-POMDP framework to study selective privacy in the application. In section IV, we describe the *revealing state* approach to optimize a certain class of strategies designed for multiple level systems. Analysis on these strategies is given to serve as an achievable lower bound of optimal tradeoff. Sections V and VI give a numerical example and conclusion respectively.

II. MODEL

Consider a household consumer with a battery that can store energy. The user has certain energy requirements and can be satisfied by direct purchase from the grid or by discharging the battery. Time and energy levels are assumed to be discretized. Specifically, let $t = 1, 2, \cdots$ denote the time slots over an infinite horizon. Let $B_1, B_2, \cdots, B_t, \cdots$ denote the sequence of discrete random variables characterizing battery process over the time horizon. Likewise, the user's demand for power and the instantaneous price at time t are modeled using two i.i.d. process and denoted by D_t with $p_i^D = \Pr\{D_t = i\}$ and P_t with $p_i^P = \Pr\{P_t = i\}$ respectively. A pictorial representation of the energy and information flow is shown in Fig.1. The assumption of integer demand and prices are

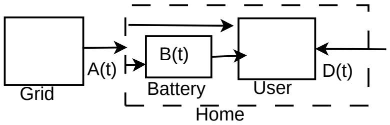

Fig. 1: A graphical representation of the model

merely for convenience of explanation and easy expression. Our approach and results are easily extended to general price and demand values.

A_t denotes the units of electricity purchased by the user at time t. Let $Q_t = \{q_t(d,b,a) = Pr\{A_t = a|D_t = d, B_t = b\}, d \in \mathcal{D}, b \in \mathcal{B}, j \in \mathcal{A}\}$ denote the probability distribution of purchasing A_t units of power given D_t units of demand and battery level B_t. Let μ_t denote the function that maps all available knowledge at time t to the probability distribution Q_t, and let $\mu = \{\mu_1, \mu_2, \cdots\}$ define the policy of the user in determining the level of energy to be purchased.

Since the energy levels are modeled as discrete quantities, the battery efficiency is assumed to be perfect. Though not perfect, it does capture the influence of a controllable storage to minimize information leakage through in-out traffic analysis, which is the primary purpose of this work. We require that all demand must be met immediately from a combination of direct purchase and battery discharging (zero delay inconvenience). So the battery level evolves:

$$B_t = B_{t-1} + A_{t-1} - D_{t-1} \tag{1}$$

We assume that only A_t and P_t are observable to the utility. The goal of an eavesdropper is to estimate the full history of user's demands using all observations. Therefore the eavesdropper will use later observations to have better estimation of previous demand. We also assume the strategy used by the controller μ is known to the eavesdropper while the realization of the randomness used by the controller is unavailable to the eavesdropper. We quantify the privacy of user energy demand from an external eavesdropper using conditional entropy:

$$\mathcal{P}(\mu) = \liminf_{t\to\infty} \frac{\mathbb{E}(H(D_1, \cdots, D_t|A_1, \cdots, A_t, P_1, \cdots, P_t))}{t} \tag{2}$$

where the expectation is over the demand and price evolution process. The entropy is computed based on the posterior distribution generated by the policy given the set of observations. The decision of the controller should take into account that actions in a particular state will reveal information about previous demands.

The instantaneous cost saving at time t is $u(D_t, B_{t+1}, A_t, P_t) = D_tP_t - A_tP_t$. We consider an infinite horizon average cost saving model in this work. The average cost saving per time slot is given by:

$$\mathcal{U}(\mu) = \liminf_{t\to\infty} \frac{\mathbb{E}(\sum_t u(D_t, B_{t+1}, A_t, P_t))}{t} \tag{3}$$

where the expectation is over the realization of the demand and price evolution and the probabilistic strategy at each time slot. The expression of expected cost saving function is simple, but the involvement of battery level introduces a time varying component. In order to study the tradeoff between cost savings and privacy, we define a weighted reward function:

$$\mathcal{R}(\mu, \lambda) = \lambda\mathcal{P}(\mu) + (1-\lambda)\mathcal{U}(\mu) \tag{4}$$

The ρ-POMDP Formulation: The optimization of the net weighted reward (4) across a time horizon was expressed as a solution to a ρ-POMDP in [12] which is given by the following Bellman equation:

$$J^* + \omega(\pi^{\mathbf{pr}}) = \sup_Q\{R_\lambda(\pi^{\mathbf{pr}}, Q) + \sum_a \gamma(a)\omega(\pi^{\mathbf{po},a}Q)\} \tag{5}$$

where the instantaneous reward at time t is:

$$\begin{aligned} R_\lambda(\pi_t^{pr}, Q_t) &= \lambda\left[H(\pi_t^{\mathbf{po}}) + H_D - H(\pi_t^{\mathbf{pr}})\right] \\ &+ (1-\lambda)\sum_{d,b,a}[\pi_t^{pr}(d,b)q_t(d,b,a)u(d,b,a,P_t)] \end{aligned} \tag{6}$$

and $\pi_t^{\mathbf{pr}} = \mathbf{Pr}(D_t, B_t|A^{t-1}, P^{t-1})$, the prior current observation probability distribution of demand and battery. $\pi_t^{\mathbf{po}} = \mathbf{Pr}(D_t, B_t|A^t, P^t)$, the post current observation probability distribution of demand and battery. $\omega(\pi^{\mathbf{pr}}) = \lim_{t\to\infty}[V_t(\pi^{\mathbf{pr}}) - tJ^*]$, where:

$$\begin{aligned} \frac{V_t(\pi^{\mathbf{pr}})}{t} &= \sup_Q\{R_\lambda(\pi^{\mathbf{pr}}, \mathbf{Q}) \\ &+ \sum_a \gamma_t(a)[V_{t-1}(\pi_t^{\mathbf{po},a}, \mathbf{Q}) - V_t(\pi^{\mathbf{pr}})] + \frac{V_t(\pi^{\mathbf{pr}})}{t}\} \end{aligned}$$

III. Privacy of Selective Information Eavesdropper

In some scenarios, a user may not be interested in hiding the complete usage pattern in a home. Selective information such as whether there is a high power device running or whether the house is empty or occupied alone may be sufficient– privacy has always been a subjective idea. In the subsequent argument we show that the framework described in [12] can be adapted to study the privacy of a deterministic function of demands as well. More specifically, we will show that the selective privacy is expressible as a sum of causal instantaneous rewards.

Assuming the user's requirement is not the protection of the demand process D^n but instead the protection of the sequence of functions $\rho(D_1)...\rho(D_t)...$, where $\rho : \mathcal{D} \to \Omega$.

A simple example when $\rho(d) = \mathbb{1}_{\{d>0\}}$ which could indicate whether a user is present or absent. Similarly a function $\rho(d) = 1$ if $d > D_{th}$ and $\rho(d) = 0$ if $d \leq D_{th}$ can be used to represent the timing of high electricity demands.

Using similar techniques as in [12] and we get:

$$\mathcal{P}_\rho(\mu) = \frac{1}{n}\sum_{t=1}^{n}[H_{\rho(D_t)} + H(A_t|A^{t-1}, P^t, \rho^t(D)) - H(A_t|A^{t-1}, P^t)] \tag{7}$$

where $H_{\rho(D_t)}$ is the entropy rate of $\rho(D_t)$. The average selective information privacy protection of a given policy in a finite time horizon can be numerically calculated by (7) while the upper bound can also be provided by rate distortion method.

Based on the described framework, our key objective is to provide computable solutions for the general model with multiple levels of battery, price and demand that any practical system can be approximated by. The resulting strategy should be close to the optimum and converge to the optimum when battery capacity is infinite. In the subsequent discussion, we propose a "Battery Centering" policy which aims to exploit the fact that minimum information is revealed when the purchase can be made probabilistically independent of demand.

IV. A "Revealing State" Approach

In the entropy based stochastic control problem described in the Section II, the battery and demand process are estimated together using the electricity purchase along the complete time horizon. If the battery reaches the maximum or minimum level, the choices of purchase action are limited and the battery state is revealed. Such a situation is named *revealing state* which is undesirable. If the battery is at a medium level, the purchase action needs not be constrained by either battery or demand. This is a desirable situation named *hiding state*. In order to minimizes the frequency of revealing states and maximizes the frequency of hiding states between revealing states, we designed a certain class of strategies showed in Algorithm 1, named *Battery Centering* strategy.

In the battery centering strategy, we classify the system state into three stages $S(t) \in \{0, 1, 2\}$. Assuming that battery starts from a medium level b_0 in stage 0, the electricity purchase action is made according to a probability distribution (8) which is independent of battery level and demand until the battery reaches its maximum or minimum.

$$\pi_a^A(p) = \Pr\{a_t = a | P_t = p, p \in \mathcal{P}\} \tag{8}$$

Then, the system transfers to stage 1 if battery reaches maximum or stage 2 if battery reaches minimum. When system is in stage 1 or 2, the electricity purchase is respectively large enough or small enough so that the battery level can traverse back to the medium point b_0 to go back to stage 0 again.

```
Initialization $B_0 = b_0$, go to Stage 0;
while in Stage 0 do
    generate $a_t$ according to distribution $\pi_a^A(p)$;
    if $B_t + a_t - D_t \in \mathcal{B}$ then
        purchase $A_t = a_t$ and stay in Stage 0;
    else if $B_t + a_t - D_t > B_{\max}$ then
        purchase $A_t = B_{\max} - B_t + D_t$, go to Stage 1;
    else
        purchase $A_t = B_{\min} - B_t + D_t$, go to Stage 2;
    end
end
while in Stage 1 do
    if $B_t - D_t \geq b_0$ then
        purchase $A_t = 0$, stay in Stage 1;
    else
        purchase $A_t = b_0 - B_t + D_t$, go to Stage 0;
    end
end
while in Stage 2 do
    if $B_t + D_{\max} - D_t \leq b_0$ then
        purchase $A_t = D_{\max}$, stay in Stage 2;
    else
        purchase $A_t = b_0 - B_t + D_t$, go to Stage 0;
    end
end
```

Algorithm 1: ”Battery Centering” Strategies

Theorem 1. *The battery level evolution in every stage of Algorithm 1 is equivalent to a bounded random walk process:*
Stage 0: $B_{t+1} = B_1 + X_1^0 + ... + X_t^0$, *where* $\Pr(X_t^0 = x) = \sum_{a,d,p|a-d=x}[\pi_a^A(p) p_d^D p_p^P]$
Stage 1: $B_{t+1} = B_1 + X_1^1 + ... + X_t^1$, *where* $\Pr(X_t^1 = x) = p_{-x}^D$
Stage 2: $B_{t+1} = B_1 + X_1^2 + ... + X_t^2$, *where* $\Pr(X_t^2 = x) = p_{D_{\max}-x}^D$

This Theorem follows if we treat the difference of battery level in every time slot as the random step.

Theorem 1 ensures that the movement of the states can be modeled as a random walk. According to the result in Chapter 2, [14], the distance between a random walk at time t and the original position at time 0 is $O(t)$ if it is a biased walk or $O(\sqrt{t})$ if it is an unbiased walk. Therefore, in order to reduce the frequency of ”revealing” state, we design $\pi_a^A(p)$ in such a way that $\mathbb{E}a = \mathbb{E}D$. In addition, as the equivalent random walk in stage 0 is unbiased, we want to maximize $\min\{|B_{\max} - b_0|, |B_{\min} - b_0|\}$ to increase the staying time in stage 0 which results in $b_0 = \frac{1}{2}(B_{\max} + B_{\min})$.

Following Theorem 1, the battery level process in stage 0 is equivalent to a random walk process with step move $X_t^0 = a_t - D_t$. Therefore, we have an estimation of battery level at time t: $\Pr(B_t - b_0 = k) \simeq \frac{1}{\sqrt{2\pi\sigma_{X_0^0}^2 t}} \exp\{-\frac{k^2}{2\pi\sigma_{X_0^0}^2 t}\}$ according to Central Limit Theorem [14]. Noticing that a_t is independent of D_t, which leads to $\sigma_{X_t^0}^2 = \sigma_{a_t}^2 + \sigma_{D_t}^2$. With these argument, we can notice that the increase of σ_a will lead the increase of $\Pr(B_t - b_0 \geq B_{\max} - b_0$ or $B_t - b_0 \leq B_{\min} - b_0)$.

Theorem 1 and its consequences show reducing the variance of X_t^0 will reduce the speed of battery level going towards the limit and increase the time spent at stage 0. Therefore, minimizing $\sigma_{X_t^0} = \sigma_{a_t}$ can minimize the frequency of system traversing from one stage to another, the situation reveals the system states to the eavesdropper. Such an approach would work very well if cost savings were not a consideration. In order to trade cost savings for privacy, the electricity purchase needs to depend on the price, which would in turn increase σ_{a_t}.

To optimize the tradeoff between privacy and cost savings is equivalent to optimize privacy protection with different minimum cost savings constraint. The optimization of privacy with cost savings constraint using the battery centering strategies can be solved by a linear programming (9) to minimize σ_a given equality constraint $\mathbb{E}a = \mathbb{E}D$ and inequality constraint $\mathbb{E}ap \leq s$, where s sweeps from $\mathbb{E}DP_{\min}$ to $\mathbb{E}D\mathbb{E}P$.

$$\text{minimize} \sum_{a \in \mathcal{A}, i \in \mathcal{P}} (a - \mathbb{E}D)^2 \pi_a^A(i) p_i^P \tag{9}$$

$$\text{subject to} \sum_{a \in \mathcal{A}, i \in \mathcal{P}} a \pi_a^A(i) p_i^P = \mathbb{E}D, \sum_{a \in \mathcal{A}, i \in \mathcal{P}} ap \pi_a^A(i) p_i^P \leq s$$

The average selective information privacy protection of a given policy in a finite time horizon can be numerically calculated by (7) while the upper bound can be derived using the rate distortion approach described in [12].

V. A Numerical Example

In this section, we validate our theoretical results through numerical simulations. We use real electricity usage and pricing data to show how the greedy algorithm derived by optimizing the weighted reward at each step and our proposed battery centering algorithm work in selective information protection scenario.

The electricity usage data of a home [15] and the time-of-use pricing data published by NY ISO [16] are used to numerically validate our framework and algorithms. The electricity usage is discretized into 20 levels and price is discretized into 10 levels. We assume that an electricity storage is available to provide both privacy protection and cost savings. Both the system and eavesdropper treat the demand process D_t and price process P_t as i.i.d..

We studied selective information leakage on the same data where the selective information function $\rho(D_t)$ is defined as:

$$\rho(D_t) = \begin{cases} 0 & \text{if } D_t < 200W \\ 1 & \text{if } 200W \leq D_t \leq 1000W \\ 2 & \text{if } D_t > 1000W \end{cases} \tag{10}$$

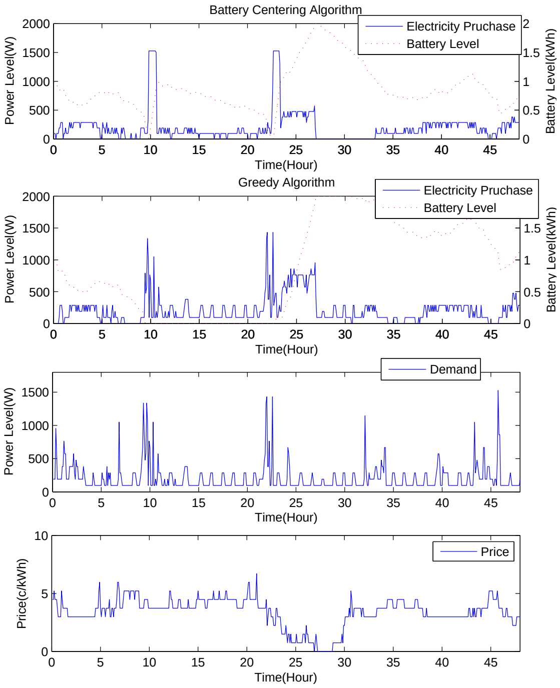

Fig. 2: The system activity in a real life case with energy storage with 2 kWh battery

Fig. 2 presents the activity of the energy storage system with capacity of 2 kWh using the battery centering algorithm and the greedy algorithm. As it is a relatively small electricity consumer with a peak power consumption of only 1.5 kW, a battery with 2 kWh is reasonable in this case. With battery centering algorithm, the privacy was well protected as the battery level touched its limit only twice and revealing states occurred on an average about 4 times in a total 48 hours. The privacy $\mathcal{P}/H_{\rho(D_t)} = 0.854$ while the cost is reduced by 22.87%. However, with the same cost savings requirement, the greedy algorithm performed worse, $\mathcal{P}/H_{\rho(D_t)} = 0.803$.

Fig. 3 presents the selective information protection and cost savings tradeoff of the greedy algorithm and battery centering algorithm when the battery capacity is 0.5, 2, 4 kWh based on numerical computation method of selective information protection described in (7). Upper bound is provided by the rate distortion technique. It shows that our proposed battery centering algorithm can provide better selective information protection compared to the greedy algorithm and both algorithms can provide good selective information protection with large capacity battery. The relatively worse performance when battery capacity is limited is due to the fact that the battery centering algorithm is not explicitly designed to treat demand levels differently, and the rate distortion upper bound exacerbates the eavesdroppers weak prior information.

VI. Conclusion

In this work, we studied a privacy of selective information problem in demand response system using a general model with multiple levels of energy storage, demand and price. Using the idea of reducing the frequency of revealing state, we designed a certain class of strategies for privacy protection and cost savings. Using such strategies, battery behavior is equivalent to a bounded random walk process and expected privacy and cost savings are analyzed to serve as an achievable lower bound. Numerical example is provided as demonstration with an upper bound which shows the closeness of our strategy to the optimum when battery capacity is large.

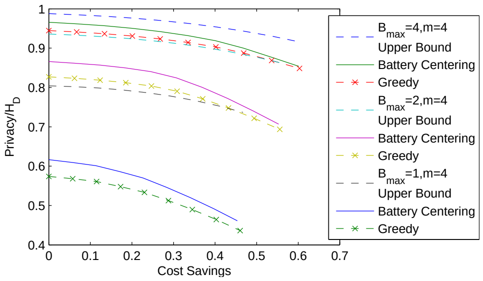

Fig. 3: selective information protection - Cost savings for a real system

Although the policy that solves the optimal tradeoff between privacy and cost savings remains unsolved, we believe that our policy given by revealing state approach is close to optimum enough. Investigating the impact of arbitrage costs and battery depreciation are interesting topics for future research.

VII. Acknowledgements

This work was supported in part by the National Science Foundation through the grants CNS-1117701 and CCF-1149495. These results have been submitted to *IEEE CDC 2014*.

References

[1] REN2013, *Renewables 2013: Global status report*. Paris: REN21 Secretariat, 2013.

[2] U.S. Department of Energy, "The Smart Grids: An Introduction," 2009.

[3] F. Sultanem, "Using Appliance Signatures for Monitoring Residential Loads at Meter Panel Level," *IEEE Trans. Power Delivery*, vol. 6, no. 4, pp. 1380–1385, Oct 1991.

[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 Buildings*, New York, NY, 2010, pp. 61–66.

[5] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids using Homomorphic Encryption," in *Proc. IEEE 1st Intl. Conf. on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010, pp. 327–332.

[6] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *Proc. IEEE 1st Intl. Conf. on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010, pp. 238–243.

[7] 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 1st Intl. Conf. on Smart Grid Communications*, Gaithersburg, MD, Oct. 2010, pp. 232–237.

[8] R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart Meter Privacy: A Utility-Privacy Tradeoff Framework," in *Proc. IEEE 2nd Intl. Conf. on Smart Grid Communications*, Brussels, Belgium, Oct. 2011.

[9] L. Schmidt and A. Thomas; Ligi, *GM, ABB Demonstrate Chevrolet Volt Battery Reuse Unit*. http://media.gm.com/, Nov. 2012.

[10] D. Varodayan and A. Khisti, "Smart Meter Privacy Using a Rechargeable Battery: Minimizing the Rate of Information Leakage," in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, Prague, Czech Republic, Apr. 2011.

[11] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Optimal privacy-preserving energy management for smart meters," in *Proc. IEEE INFOCOM 2014*. Toronto, Canada: IEEE, 2014.

[12] 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*. IEEE, 2013, pp. 115–122.

[13] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, 1949.

[14] G. F. Lawler and V. Limic, *Random Walk: A Modern Introduction*. Cambridge University Press, Jul. 2010. [Online]. Available: http://books.google.com/books?id=UBQdwAZDeOEC

[15] 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), San Diego, CA*, 2011.

[16] N. Y. I. S. Operator, *Real-Time LBMP - Zonal*. http://www.nyiso.com/, 2014.