2016 American Control Conference (ACC)
Boston Marriott Copley Place
July 6-8, 2016. Boston, MA, USA

Event-Based Information-Theoretic Privacy: A Case Study of Smart Meters

Shuo Han, Ufuk Topcu, George J. Pappas

Abstract— **Traditional information-theoretic privacy uses the mutual information rate as a metric of privacy for protecting the input data stream sent by participating users; a low information rate implies that the *entire* input data stream cannot be correctly inferred from the output with high probability. In many applications such as smart metering, however, the private *event* (e.g., whether the user is having dinner within a particular time slot) that a user does not wish to reveal may only be associated with part of the data stream, which can still be inferred correctly by adversaries under a low information rate. To this end, we propose a new information-theoretic metric that can provide event-based privacy guarantees. As a case study, we consider the problem of protecting the privacy in user's home energy usage profile with the aid of an internal energy storage device (e.g., a rechargeable battery). Through charging and discharging, the energy storage device is capable of altering the real-time energy usage profile and masking distinctive patterns that may be of interest to adversaries. We evaluate the new privacy metric under the best-effort control policy, which tries to keep the reported energy usage constant through compensation from the storage device. Through simulations, we show that the new privacy metric can be computed numerically and gives a nontrivial privacy guarantee.**

I. Introduction

With the advance in real-time computing and sensing technology, a growing number of user-based cyber-physical systems start to utilize user data for more efficient operation. This typically involves a central authority who collects user information for the purpose of system analysis and decision making. In power systems, for example, the utility company is able to collect real-time power consumption data from individual households through advanced metering infrastructures (i.e., "smart meters") in order to improve the demand forecast accuracy and facilitate the operation of power plants [1].

By sharing their data, however, individual customers are exposed to the risk that the central authority or a potential eavesdropper can learn about information (e.g., personal daily activities) that the customers did not intend to share. Concerns on such privacy issues have been raised [15] and start to become one major hindrance to effective user participation [9]. The possibility of decoding user's private information from real-time energy usage has been demonstrated in the research area of nonintrusive load monitoring [5], [8], [11], [12]. By making use of features in the consumption profile of different appliances, nonintrusive load monitoring techniques are able to disaggregate the consumption of individual appliances from the total energy consumption profile. The detailed energy usage of individual appliances may often be considered private by the users; for example, the usage of a microwave oven is strongly correlated to the time of dining. Although the goal of nonintrusive load monitoring is to provide users with detailed consumption information in order to improve user awareness and lead to reduction in future energy consumption (e.g., by encouraging users to upgrade to more energy efficient appliances), the capability of learning about such detailed information from aggregate consumption also makes the users vulnerable to undesirable usage of their private information by potential adversaries.

There have been approaches that propose to protect the privacy of users by making use of an energy storage device whose state is invisible to the outside adversaries [14]. The energy storage device serves as a buffer, which allows the user to alter their reported energy usage profile (i.e., actual power drawn from the power grid) through charging and discharging. The energy storage device can be in the form of a physical battery or, more abstractly, any kinds of flexible loads. Throughout the paper, we will often simply use the term *battery* to refer to a generic energy storage device.

One major challenge in developing solutions for protecting privacy is that the specific algorithm used by potential adversaries for learning about user's private information is often unknown. In order to provide strong privacy guarantees that are independent from the adversaries, researchers have proposed different rigorous frameworks for privacy protection. Among others, two popular frameworks for privacy are differential privacy and information-theoretic privacy.

Differential privacy was first proposed for publishing statistics of a database consisting of user information [6], [7]. In its original setting, differential privacy is capable of hiding the participation of any user in the database, since participation in the database may be linked to user privacy (e.g., in the case of a database of patients infected by a certain disease). The participation of any single user is captured through a binary relation called adjacency relation and can be viewed as an *event* (i.e., whether a user has participated or not). By defining different adjacency relations, differential privacy allows us to capture the private event that we wish to hide from adversaries [13]. In the context of smart metering, for example, an event can be the activation of a certain appliance during a specific time slot, which may be associated to a user's private activities. In other words, differential privacy can be considered as an event-based framework of privacy.

S.H. and G.J.P. are with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104. {hanshuo,pappasg}@seas.upenn.edu. U.T. is with the Department of Aerospace Engineering and Engineering Mechanics, University of Texas at Austin, Austin, TX 78712. utopcu@utexas.edu. This work was supported in part by the NSF (CNS-1239224) and TerraSwarm, one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA.

On the other hand, traditional information-theoretic privacy does not usually handle private events; the framework views the input data and output statistics as input and output of a communication channel [16]. The metric of privacy is defined as the mutual information between the input and output; less mutual information implies that the output preserves more privacy of the input containing user information.

Both differential privacy and information-theoretic privacy have been applied for preserving the privacy of real-time smart meter data in the presence of an energy storage device. For differential privacy, the presence of constraints in physical systems poses a new challenge in applying existing algorithms that were previously used for publishing statistics of a database. In the framework of differential privacy, a privacy-preserving algorithm typically works by adding noise to the output. In order to guarantee differential privacy, the noise must be independent of the current state (i.e., charging level) of the battery, because information on the battery state can be used to infer the true energy consumption profile. However, there may be situations where the battery does not hold enough charge in order to provide the amount of noise required for preserving privacy [3], [20]. On the other hand, information-theoretic privacy is capable of handling physical constraints, since it does not restrict the noise to a particular form [10], [17]–[19]. However, the framework is not based on private events so that it may not provide satisfactory guarantees. As we will discuss in Section II-C, the mutual information rate used in previous literature only gives a lower bound on the probability of error when an adversary wants to infer the *entire* input sequence over time. In practice, the adversary may only be interested in *events* associated with certain part of the input sequence (e.g., energy usage at some particular time during the day). As a result, the privacy guarantee provided by the mutual information rate can be too optimistic, since it is easier to infer part of the input sequence correctly than the entire sequence.

Contribution: In this paper, we propose a new information-theoretic metric of privacy that can provide guarantees for event-based privacy. It retains the flexibility of traditional information-theoretic privacy (for handling physical constraints in the case of smart metering) while adding the capability of defining private events as in differential privacy. For the case of smart meters with energy storage, we show how this new metric can be computed numerically by analyzing the privacy of a specific battery control policy named the best-effort charging policy, which is a policy that tries to hold the reported energy usage constant. Numerical results show that the new metric yields nontrivial privacy guarantees; in particular, the presence of an energy storage device makes it more difficult for an adversary to learn about user energy consumption from the smart metering data.

II. Problem Formulation

In this section, we start by describing the model of system that uses an energy storage device (e.g., rechargeable battery) for protecting the privacy of information contained in the energy usage profile reported by the smart meter. We propose a new privacy metric based on private *events*, in contrast to previous information-theoretic measures that use mutual information rate and are not event-oriented. Rather than designing the battery control policy, we focus on analyzing the privacy guarantee given by a chosen policy named the best-effort policy, which tries to maintain the reported energy usage constant through compensation from the battery.

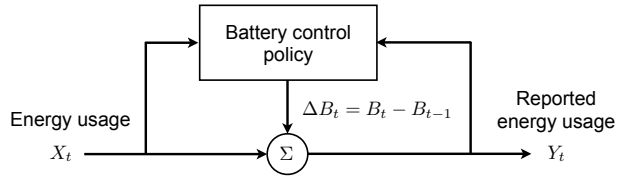

Fig. 1. System model. The battery control policy decides the change ΔB_t in the charging level based the history of the true energy usage X_t and reported energy usage Y_t.

A. Privacy protection using an energy storage device

We consider the problem over an infinite time horizon in which the time slots are indexed by $t \in \{0, 1, \dots\}$. The (discrete) user energy consumption over time is denoted by a *stochastic process* $\{X_t\}$, where $X_t \in \{0, \dots, n\}$ is the energy consumption during time slot t, and n is the maximum consumption; the charging level of the rechargeable battery during time slot t is denoted by $B_t \in \{0, 1, \dots, m\}$, where m is the capacity of the battery. The quantity B_0 is a *random variable* and denotes the initial charging level of the battery. The actual energy drawn from the power grid (i.e., the energy consumption measured by the smart meter) is denoted by Y_t for $t \in \{1, 2, \dots\}$, which is given by

$$Y_t = X_t + B_t - B_{t-1}. \tag{1}$$

In other words, the smart meter measurement corresponds to the sum of the user energy consumption X_t and the change $(B_t - B_{t-1})$ of the energy stored in the battery as illustrated in Fig. 1. We consider that Y_0 is also given as a *random variable*. For simplicity, we will denote the infinite sequences $\{X_t\}$ and $\{Y_t\}$ by X and Y, respectively.

For the purpose of preserving privacy of the user consumption X_t, the charging level B_t needs to be controlled according to a certain policy that only depends on the history $\{X_1, X_2, \dots, X_t\}$, $\{B_0, B_1, \dots B_{t-1}\}$, and $\{Y_0, Y_1, \dots, Y_{t-1}\}$. In this paper, we consider the *best-effort* policy proposed by McLaughlin et al. [14] for its simplicity. The best-effort policy chooses B_t as

$$B_t = [Y_{t-1} - X_t + B_{t-1}]_0^m, \tag{2}$$

where the notation $[\cdot]_0^m$ denotes the truncation operation defined as

$$[x]_0^m = \begin{cases} x, & 0 \le x \le m, \\ 0, & x < 0, \\ m, & x > m. \end{cases}$$

If the truncation $[\cdot]_0^m$ in (2) is removed, then B_t satisfies

$$Y_{t-1} = X_t + B_t - B_{t-1}.$$

From (1), we obtain that $Y_t = Y_{t-1}$ in the absence of battery capacity constraints $0 \le B_t \le m$. In other words, the best-effort policy (2) chooses the charging level B_t to make Y_t as close to Y_{t-1} as possible under the battery capacity constraints, hence the name "best-effort". Throughout the paper, we assume that the attacker knows the description of the random process X (but not its instantiation, which our goal is to keep private), the battery capacity m, and the battery control policy being used.

B. Mutual information as a metric of privacy

From an information-theoretic point of view, the effect of the rechargeable battery can be viewed as a communication channel, whose input sequence is the user energy consumption $X = \{X_t\}$ and output sequence is the smart meter measurement $Y = \{Y_t\}$. As a result, the problem of preserving privacy for smart metering can be viewed more generally as preserving the privacy between the input and output of the channel. Previous work on information-theoretic privacy uses the mutual information rate

$$I(X;Y) \triangleq \lim_{t\to\infty} \frac{1}{t} I(X_1, X_2, \ldots, X_t; Y_1, Y_2, \ldots, Y_t)$$

as a metric for privacy; smaller $I(X;Y)$ implies more privacy, and the goal of designing the battery control policy is usually to minimize $I(X;Y)$.

Before proposing our new metric of privacy, we would like to discuss the connection between the mutual information rate $I(X;Y)$ and privacy, which has not been discussed in previous work on information-theoretic privacy. Suppose the goal of the adversary is to learn about the entire input sequence X from the output sequence Y. In particular, the adversary tries to build an estimator $\hat{X}(Y)$ of X, where $\hat{X}$ is a function of the output Y. One way to quantify the performance of the estimator $\hat{X}$ is the probability of error

$$P_e \triangleq \mathbb{P}(\hat{X}(Y) \neq X). \tag{3}$$

Using Fano's inequality from information theory [4], we know that P_e is related to $I(X;Y)$ as follows. For any estimator $\hat{X}$, we have

$$H(P_e) + P_e \log_2(|\mathcal{X}| - 1) \ge H(X) - I(X;Y), \tag{4}$$

where $H(P_e) \triangleq -P_e \log_2 P_e - (1-P_e)\log_2(1-P_e)$ is the binary entropy function, $\mathcal{X}$ is the set of alphabets of X, and $|\mathcal{X}|$ is the cardinality of $\mathcal{X}$. In our case, we have $|\mathcal{X}| = n+1$. A weaker version of the Fano's inequality can be obtained as

$$P_e \ge \frac{H(X) - I(X;Y) - 1}{\log_2 |\mathcal{X}|} \tag{5}$$

by noting the fact that $H(P_e) \le 1$. Both $H(X)$ and $|\mathcal{X}|$ in inequality (5) are constants. As a result, smaller $I(X;Y)$ implies that it is more difficult to infer X correctly from the output Y. If the probability of error (3) is viewed as a fundamental quantification of privacy, then inequality (5) establishes the fact that the mutual information (or equivalently, the conditional entropy) can be used as a metric of privacy. The privacy guarantee given by (5) is a strong guarantee, since the lower bound holds regardless of the estimation algorithm that an adversary may use.

C. Problem statement

In many cases, however, the goal of the adversary is not to infer the entire input sequence X from the output Y. Instead, the adversary may be interested only in some part of X. In the context of smart metering, for example, the adversary may want to infer the energy usage X_t for some particular time slot t (but the specific t is unknown to the user who reports their energy usage). To this end, we consider the quantity

$$\begin{aligned}\bar{I}(X;Y) &\triangleq \sup_t I(X_t;Y) \\ &= \sup_t \lim_{T\to\infty} I(X_t; Y_1, Y_2, \ldots, Y_T).\end{aligned} \tag{6}$$

Later, we will show that the supremum and limit in (6) exist. Using the interpretation of privacy by Fano's inequality (5), the quantity $\bar{I}(X;Y)$ gives a lower bound on

$$\bar{P}_e \triangleq \inf_t \mathbb{P}(\hat{X}_t(Y) \neq X_t),$$

which corresponds to a lower bound on the probability of error for inferring X_t from Y for *any* time slot t. Our choice of the privacy metric (6) is inspired by the framework of differential privacy, which focuses on the privacy of *events*. The quantity $\bar{I}(X;Y)$ can be viewed as a metric for the privacy related to a particular event, which is the amount of energy usage within any single time slot t in the context of smart metering.

In this paper, we intend to solve problems related to the privacy metric $\bar{I}(X;Y)$ in the context of smart metering with internal energy storage controlled by the best-effort policy as described in Section III. Firstly, we would like to know whether $\bar{I}(X;Y)$ is well-defined (i.e., whether the supremum and limit in (6) exist). Secondly, we would like to compute $\bar{I}(X;Y)$ for the best-effort policy, at least numerically.

III. Event-based Information Privacy

In this section, we show that the quantity $\bar{I}(X;Y)$ for describing event-based privacy is well-defined. Namely, both the supremum and the limit in the definition (6) of $\bar{I}(X;Y)$ exist. Since it is generally difficult to obtain $\bar{I}(X;Y)$ in closed form, we also discuss the numerical computation of $\bar{I}(X;Y)$. In particular, we show that computation of the supremum that appears in $\bar{I}(X;Y)$ can be made numerically feasible under certain assumptions on the initial states of the system.

Proposition 1. *The limit and supremum in the definition (6) of $\bar{I}(X;Y)$ exist.*

Proof: In order to show that the supremum and limit in the definition of $\bar{I}(X;Y)$ exist, we start by considering

the mutual information

$$I(X_t; Y_1, Y_2, \ldots, Y_T)$$

for outputs of a finite length T. We first show that $I(X_t; Y_1, Y_2, \ldots, Y_T)$ grows monotonically with T for any given t. Namely, for any t and $T_1 < T_2$, we have

$$I(X_t; Y_1, Y_2, \ldots, Y_{T_1}) \leq I(X_t; Y_1, Y_2, \ldots, Y_{T_2}).$$

This can be shown using a property of mutual information: for any random variables X, Y, and Z, we have $I(X;Y) \leq I(X;Y,Z)$. Next, we show that $I(X_t; Y_1, Y_2, \ldots, Y_T)$ is upper bounded. From the definition of mutual information, we have

$$I(X_t; Y_1, Y_2, \ldots, Y_T) = H(X_t) - H(X_t | Y_1, Y_2, \ldots Y_T).$$

Since $H(X_t) < \infty$ and $H(X_t | Y_1, Y_2, \ldots, Y_T) \geq 0$, we know that

$$I(X_t; Y_1, Y_2, \ldots, Y_T) \leq H(X_t) < \infty.$$

As a result of monotonicity and boundedness, we know that the limit

$$\lim_{T \to \infty} I(X_t; Y_1, Y_2, \ldots, Y_T)$$

in (6) exists from the monotone convergence theorem. The boundedness also ensures that $\sup_t I(X_t; Y)$ in (6) exists. ■

Generally, it is difficult to obtain $\bar{I}(X;Y)$ in closed form. Instead, we seek numerical methods for computing $\bar{I}(X;Y)$. In order to compute $\bar{I}(X;Y)$ numerically, we need to evaluate both the limit and the supremum in the definition (6). The limit can be approximated by choosing T to be large enough; on the other hand, it is generally difficult to evaluate $\sup_t I(X_t; Y)$. In the following, we will show that, in the problem of smart metering with energy storage, we can obtain

$$\sup_t I(X_t; Y) = \lim_{t \to \infty} I(X_t; Y) \tag{7}$$

under some further assumptions. The relation (7) allows approximating the supremum by choosing t to be large enough, hence approximating $\bar{I}(X;Y)$ if we can compute $I(X_t; Y_1, Y_2, \ldots, Y_T)$.

In the problem of smart metering, the random process (B_t, Y_t) forms a discrete-time Markov chain, where the transition probabilities are given by

$$\mathbb{P}(B_t, Y_t | B_{t-1}, Y_{t-1}) = \begin{cases} \mathbb{P}(X_t = x_t), & B_t = [Y_{t-1} - x_t + B_{t-1}]_0^m, \\ & Y_t = x_t + B_t - B_{t-1}, \\ 0 & \text{otherwise}, \end{cases} \tag{8}$$

according to the dynamics (1) and (2).

Proposition 2. *The Markov chain (B_t, Y_t) defined in (8) is irreducible.*

Proof: We prove this by showing separately that the state $(0,0)$ is reachable from any state, and any state is reachable from the state $(0,0)$.

We first prove the reachability of the state $(0,0)$ from any state $(B_0, Y_0) = (b, y)$.

- Case 1: $y = 0$. Choose $X_\tau = 1$ for all $1 \leq \tau \leq b$, and it can be seen from (8) that $(B_b, Y_b) = (0,0)$.
- Case 2: $y > 0$. Choose $X_\tau = 0$ for $\tau \geq 1$ until $(B_\tau, Y_\tau) = (m, 0)$. The existence of such τ can be shown as follows. Note that we have $B_\tau > B_{\tau-1}$ whenever $B_{\tau-1} < m$ from (8). Once we have $B_\tau = m$ for some τ, choosing $X_{\tau+1} = 0$ yields $(B_{\tau+1}, Y_{\tau+1}) = (m, 0)$. Then, the reachability of $(0,0)$ follows from case 1.

We then prove the reachability of any state $(B_0, Y_0) = (b, y)$ from the state $(0,0)$.

- Case 1: $y > 0$. Choose $X_1 = y$, which yields $(B_1, Y_1) = (0, y)$. Then, choose $X_{\tau+1} = y - 1$ for all $1 \leq \tau \leq b$, which yields $(B_{\tau+1}, Y_{\tau+1}) = (b, y)$.
- Case 2: $y = 0$. From case 1, we know that the state $(B_t, Y_t) = (m, n)$ is reachable. Choose $X_{t+1} = 0$, which yields $(B_{t+1}, Y_{t+1}) = (m, 0)$; choose $X_{t+\tau+1} = 1$ for $1 \leq \tau \leq m - b$, which yields $(B_{t+\tau+m-b+1}, Y_{t+\tau+m-b+1}) = (b, 0)$.

■

The irreducibility of the Markov chain (B_t, Y_t) ensures that (B_t, Y_t) has a unique stationary distribution, which we will denote by π.

Proposition 3. *If the distribution of (B_0, Y_0) is the stationary distribution π of the Markov chain (B_t, Y_t), then we have $\sup_t I(X_t; Y) = \lim_{t \to \infty} I(X_t; Y)$.*

Proof: Using the fact that π is the stationary distribution of (B_t, Y_t), we know that the distribution of (B_t, Y_t) is π for any t. As a result, we have

$$I(X_t; Y_1, Y_2, \ldots, Y_T) = I(X_{t+1}; Y_2, Y_3, \ldots, Y_{T+1})$$

for any t and T. Then, we can obtain

$$I(X_t; Y_1, Y_2, \ldots, Y_T) \leq I(X_{t+1}; Y_1, Y_2, \ldots, Y_{T+1}) \tag{9}$$

using the property of mutual information used in the proof of Proposition 1. The inequality (9) implies that

$$\lim_{T \to \infty} I(X_t; Y_1, Y_2, \ldots, Y_T) \leq \lim_{T \to \infty} I(X_{t+1}; Y_1, Y_2, \ldots, Y_{T+1}),$$

and hence

$$I(X_t; Y) \leq I(X_{t+1}; Y) \tag{10}$$

by using the fact

$$\lim_{T \to \infty} I(X_{t+1}; Y_1, Y_2, \ldots, Y_T) = \lim_{T \to \infty} I(X_{t+1}; Y_1, Y_2, \ldots, Y_{T+1}).$$

The result follows from the monotonicity (10) of $I(X_t; Y)$. ■

From a practical point of view, the assumption that the initial states (B_0, Y_0) follow the stationary distribution is not particularly restrictive. It can be shown that the Markov chain

(B_t, Y_t) is also aperiodic, since for any state the transition probability of returning to the state itself is always nonzero (by choosing $X_t = Y_{t-1}$). As a result of aperiodicity, we can imagine a practical situation as follows: the system has evolved for long enough time to settle at the stationary distribution, after which the potential adversary starts to collect outputs from the system.

Finally, we note that the new privacy metric that we have proposed can be potentially applied beyond the case of smart meters. We can view the battery charging dynamics (1) and (2) as a nonlinear dynamical system whose states are (B_t, Y_t), control input is X_t, and output is Y_t. The goal is to protect the privacy of the input X_t when an adversary has access to the output Y_t but not all the internal states such as B_t. The new privacy metric gives a lower bound on the probability of error for inferring any single entry of inputs X from all the outputs Y.

IV. Numerical Results

In this section, we show numerical results on computing the privacy metric $\bar{I}(X;Y)$. Throughout the section, we assume that (B_0, Y_0) follows the stationary distribution as described in Section III. We consider the case that X_t is an i.i.d. process with the uniform distribution

$$\mathbb{P}(X_t = x_t) = \frac{1}{n+1}, \quad x_t = 0, 1, \ldots, n.$$

Using the results from Section III, we know that we can approximate $\bar{I}(X;Y)$ by computing $I(X_t; Y_1, Y_2, \ldots, Y_T)$ for large enough t and T. Denote by $p(x_t, y_1, \ldots, y_T)$ the joint distribution $\mathbb{P}(X_t = x_t, Y_1 = y_1, \ldots, Y_T = y_t)$ of $(X_t, \{Y_\tau\}_{\tau=1}^T)$. In all the following simulations, we compute the mutual information $I(X_t; Y_1, Y_2, \ldots, Y_T)$ from its definition

$$I(X_t; Y_1, Y_2, \ldots, Y_T) = \sum_{x_t, y_1, \ldots, y_T} p(x_t, y_1, \ldots, y_T) \log \frac{p(x_t, y_1, \ldots, y_T)}{p(x_t) p(y_1, \ldots, y_T)}.$$

Recall from (1) and (2) that (B_t, Y_t) is a function of $\{X_\tau\}_{\tau=1}^t$ and (B_0, Y_0). We can obtain the joint distribution of $(\{X_\tau\}_{\tau=1}^T, \{B_\tau\}_{\tau=1}^T, \{Y_\tau\}_{\tau=1}^T)$ and then marginalize to obtain the joint distribution of $(X_t, \{Y_\tau\}_{\tau=1}^T)$. The stationary distribution π can be obtained by solving the linear system $\pi = \pi P_{(B,Y)}$, in which $P_{(B,Y)}$ is the transition probability matrix whose entries are given by (8).

It should be mentioned that computing the mutual information from its definition can be quite expensive because the number of probability masses in the joint distribution of $(\{X_\tau\}_{\tau=1}^T, \{B_\tau\}_{\tau=1}^T, \{Y_\tau\}_{\tau=1}^T)$ is $(m+1)(n+1)^{T+1}$. (There are $(m+1)$ possibilities for B_0, $(n+1)$ possibilities for Y_0, and $(n+1)$ possibilities for each X_τ.) In the following simulations, we restrict ourselves to relatively small m and n for tractability. In the future, we plan to explore approximate numerical methods such as sampling-based methods that have been previously used for estimating mutual information [2].

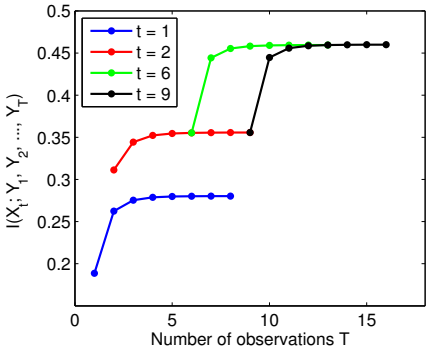

Fig. 2. The mutual information $I(X_t; Y_1, Y_2, \ldots, Y_T)$ as a function of the number of observations T. Different curves correspond to different choices of t.

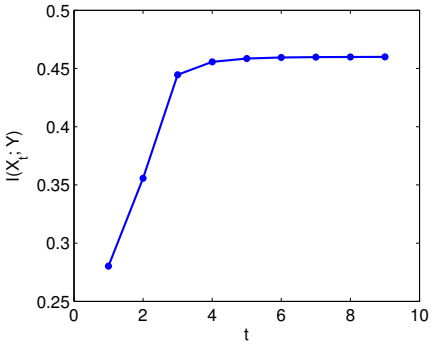

Fig. 3. The mutual information $I(X_t; Y)$ as a function of t ($n = 1$ and $m = 1$).

Fig. 2 shows the mutual information $I(X_t; Y_1, Y_2, \ldots, Y_T)$ as a function of the number of observations T, in which we choose $n = 1$ and $m = 1$. For each curve, we start computing $I(X_t; Y_1, Y_2, \ldots, Y_T)$ with $T = t$ and keep increasing T until $I(X_t; Y_1, Y_2, \ldots, Y_T)$ stops changing (up to a tolerance of 10^{-4}). For any given t, we note that $I(X_t; Y_1, Y_2, \ldots, Y_T)$ grows monotonically with T $(T \geq t)$ and eventually converges, exactly as what is described in Section III. We record the values of $I(X_t; Y_1, Y_2, \ldots, Y_T)$ at the point it converges and use them as approximations to $I(X_t; Y)$.

Fig. 3 shows how $I(X_t; Y)$ (using the approximate values obtained from Fig. 2) changes as a function of t. It can be seen that $I(X_t; Y)$ grows monotonically with t, which is the same as what is described in Proposition 3. From Fig. 3, we consider that $I(X_t; Y)$ has reached convergence at $t = 9$, which gives us $\bar{I}(X;Y) = 0.460$.

Fig. 4 shows how the mutual information $I(X_t; Y)$ changes under different battery capacities m. For visualization, the curve in Fig. 3 is also included in Fig. 4 for comparison. It can be seen that $\bar{I}(X_t; Y)$ decreases as m increases. Intuitively, it is easier to hide information about the input X_t with a larger battery, since the battery can provide more buffer for flattening out the patterns in X_t so that these patterns do not appear in the output Y_t.

In the end, we list in Table I the privacy guarantee expressed in the probability of error $P_e = \mathbb{P}(\hat{X}_t(Y) \neq X_t)$,

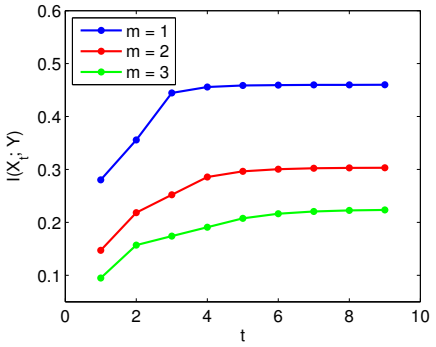

Fig. 4. The mutual information $I(X_t;Y)$ as a function of t. Different curves correspond to different choices of m. For all curves, we choose $n = 1$.

TABLE I

m	n	$\bar{I}(X;Y)$	Lower bound on $\mathbb{P}(\hat{X}_t(Y) \neq X_t)$
1	1	0.460	0.124
2	1	0.303	0.188
3	1	0.224	0.229
2	2	0.565	0.234

which is computed from the original Fano's inequality (4). For $n = 1$, we have $|\mathcal{X}| = 2$, and the entropy $H(X_t) = 1$ for all t. It can be seen that when the battery capacity is 3 times the maximum total energy consumption within a single time slot, the probability of error for an adversary to infer about X_t is at least 0.229. Note that the best privacy guarantee in this case is $P_e = 0.5$, which corresponds random guess without any additional information on X_t other than its distribution. We keep the ratio between the maximum consumption and battery capacity but increased the quantization level ($m = 2$ and $n = 2$). The result of computation is also listed in Table I. It can be seen that the probability of error has increased significantly to 0.234 compared to 0.124 in the case of $m = 1$ and $n = 1$. The simulation results have shown that our metric of privacy $\bar{I}(X;Y)$ defined in (6) can be numerically computed, and the metric yields nontrivial privacy guarantees (i.e., a strictly positive probability of inference error).

V. Conclusions and Future Work

We propose a new information-theoretic metric of event-based privacy for systems that process data streams from users. The new metric combines the benefits of both differential privacy and traditional information-theoretic privacy based on the information rate. As a case study, we consider the problem of collecting real-time home energy usage profiles (e.g., from smart meters) while protecting the privacy of participating individual households by controlling an internal energy storage device. The private event that we consider is the amount of energy usage within any single time slot, and we would like to protect the privacy of this event even when the adversary has access to the smart meter recordings. Through numerical simulations, we demonstrate that the best-effort battery control policy gives nontrivial privacy guarantees by evaluating the policy under the new privacy metric. As expected, the level of privacy improves as the amount of storage increases.

Currently, our method for evaluating the new privacy metric is only limited to a small number of discretization levels for both the input (energy usage) and internal states (battery capacity). Future work will be focused on scalable numerical methods (e.g., sampling-based methods) that are able to compute the privacy metric for larger number of discretization levels.

References

[1] The Benefits of Smart Meters. `http://www.cpuc.ca.gov/PUC/energy/Demand+Response/benefits.htm` (retrieved: March 19, 2014).

[2] D. M. Arnold, H.-A. Loeliger, P. O. Vontobel, A. Kavčić, and W. Zeng. Simulation-based computation of information rates for channels with memory. *IEEE Transactions on Information Theory*, 52(8):3498–3508, 2006.

[3] M. Backes and S. Meiser. Differentially private smart metering with battery recharging. In *Data Privacy Management and Autonomous Spontaneous Security*, pages 194–212. Springer, 2014.

[4] T. M. Cover and J. A. Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[5] R. Dong, L. J. Ratliff, H. Ohlsson, and S. S. Sastry. Energy disaggregation via adaptive filtering. In *Annual Allerton Conference on Communication, Control, and Computing*, pages 173–180, 2013.

[6] C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography*, pages 265–284. Springer, 2006.

[7] C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Theoretical Computer Science*, 9(3-4):211–407, 2013.

[8] G. W. Hart. Nonintrusive appliance load monitoring. *Proceedings of the IEEE*, 80(12):1870–1891, 1992.

[9] R. Hoenkamp, G. B. Huitema, and A. J. C. de Moor-van Vugt. The neglected consumer: The case of the smart meter rollout in the Netherlands. *Renewable Energy L. & Pol'y Rev.*, page 269, 2011.

[10] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. Lewis, R. Cepeda, et al. Privacy for smart meters: Towards undetectable appliance load signatures. In *IEEE International Conference on Smart Grid Communications*, pages 232–237, 2010.

[11] H. Kim, M. Marwah, M. Arlitt, G. Lyon, and J. Han. *Unsupervised Disaggregation of Low Frequency Power Measurements*, chapter 64, pages 747–758.

[12] J. Z. Kolter and M. J. Johnson. Redd: A public data set for energy disaggregation research. In *Workshop on Data Mining Applications in Sustainability*, volume 25, pages 59–62, 2011.

[13] J. Le Ny and G. J. Pappas. Differentially private filtering. *IEEE Transactions on Automatic Control*, 59(2):341–354, 2014.

[14] S. McLaughlin, P. McDaniel, and W. Aiello. Protecting consumer privacy from electric load monitoring. In *ACM Conference on Computer and Communications Security*, pages 87–98, 2011.

[15] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010.

[16] L. Sankar, S. Kar, R. Tandon, and H. V. Poor. Competitive privacy in the smart grid: An information-theoretic approach. In *IEEE International Conference on Smart Grid Communications*, pages 220–225, 2011.

[17] 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*, 31(7):1331–1341, 2013.

[18] D. Varodayan and A. Khisti. Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 1932–1935, 2011.

[19] J. Yao and P. Venkitasubramaniam. The privacy analysis of battery control mechanisms in demand response: Revealing state approach and rate distortion bounds. In *IEEE Conference on Decision and Control*, pages 1377–1382, 2014.

[20] J. Zhao, T. Jung, Y. Wang, and X. Li. Achieving differential privacy of data disclosure in the smart grid. In *IEEE INFOCOM*, pages 504–512, 2014.