Quantifying the Utility-Privacy Tradeoff in the Smart Grid

Roy Dong, Student Member, IEEE, Alvaro A. Cárdenas, Member, IEEE, Lillian J. Ratliff, Student Member, IEEE, Henrik Ohlsson, Member, IEEE, and S. Shankar Sastry, Fellow, IEEE

Abstract—The modernization of the electrical grid and the installment of smart meters come with many advantages to control and monitoring. However, in the wrong hands, the data might pose a privacy risk. In this paper, we consider the tradeoff between smart grid operations and the privacy of consumers. We analyze the tradeoff between smart grid operations and how often data is collected by considering a direct-load control example using thermostatically controlled loads, and we give simulation results to show how its performance degrades as the sampling frequency decreases. Additionally, we introduce a new privacy metric. This privacy metric assumes a strong adversary model, and fixes a definition of a privacy breach. Then, using results from detection theory, we can give an upper bound on the adversary’s ability to enact a privacy breach, independent of the algorithm he uses. Combining these two results allows us to directly consider the tradeoff between better load control and consumer privacy.

Index Terms—privacy, smart grid, direct load control, cyber-physical systems

I. INTRODUCTION

DATA collected by the smart grid enables a multitude of advantages to all parties, including better efficiency in energy distribution, more reliability, and giving electric utility customers more choices and transparency in their energy consumption. Smart grid data, however, also raises the issue of data privacy. Energy usage data will be collected at larger scales and at unprecedented levels of granularity. Monitoring energy consumption at high granularity can allow the inference of detailed information about consumers’ lives. This includes the times they eat, when they watch TV, and when they take a shower. Such information is highly valuable and will be sought by many parties, including advertising companies, law enforcement, and criminals.

In response to these concerns, governments, researchers, and standard organizations are working on privacy standards and policies to guide advanced metering infrastructure (AMI) deployments. Researchers have considered the issue of data privacy in smart grid infrastructures, and have proposed novel mechanisms for protecting the collected data (encryption, access control, and cryptographic commitments) by anonymization and aggregation, by preventing inferences and re-identification from databases that allow queries from untrusted third parties, and by differential privacy.

While all these previous proposals have strong contributions, none of them has addressed the Fair Information Practice (FIP) principle of data minimization. The NISTIR 7628 expresses the data minimization principle in the smart grid context as:

Limit the collection of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.

This same principle is included in several smart grid privacy recommendations including those published by the North American Energy Standards Board, DOE, the Texas Legislature and Public Utility Commission, and the California Public Utilities Commission (CPUC).

Electric utilities who want to follow these privacy recommendations do not have a sound reasoning principle to help them decide how much data is too little or too much. Our goal in this paper is to start discussing scientifically sound principles that can help determine how much data to collect in order to achieve a certain level of functionality of the grid, and how much privacy is granted to consumers under this data collection policy.

To successfully enact the data minimization principle, we must be able to quantify two things. First, we must model the tradeoff between how often data is collected and performance of smart grid operations. Second, we must understand the tradeoff between how much data is collected and the inference an adversary can make about a consumer’s private information.

In this paper, our goal is to analyze these tradeoffs in the context of electricity load shaping (demand-response). To quantify how much data is needed for smart grid operations, we consider how the performance of proposed direct load control (DLC) mechanisms change as fewer and fewer measurements are received by the controller. To quantify the privacy risk in these mechanisms, we use recent results in nonintrusive load monitoring (NILM) to give guarantees on when NILM algorithms will not be able to infer the device usage of a consumer from observing the aggregate power consumption of a building, acting as a certificate of privacy for the consumer.

This paper extends ideas presented in our previous work, where we used model predictive control (MPC) methods on a highly stylized DLC model to reduce unexpected demand across time, and analyzed the likelihood of the demand exceeding certain bounds as a function of the sampling rate. In contrast, in this paper we consider a more realistic DLC...
model and provide a formal definition of privacy that allows us to quantify the privacy of different sampling policies.

We note that our work is complementary to other privacy policies being researched. Our analysis helps determine how much data to collect and how often it should be collected. Once this is in place, encryption, anonymization and aggregation techniques can be employed in tandem.

The closest previous work to the ideas in this paper is the work of Sankar, Kar, Tandon, and Poor [16], which considers the utility and privacy tradeoffs from smart grid data. Their approach, however, focuses on the quality of collected data (by using quantization, and coding theory); while in this paper we focus on the quantity of collected data (or more precisely, the sampling interval). To the best of our knowledge, this is the first paper considering a concrete model of smart grid operations and the tradeoff between its performance and the privacy of its consumers.

The rest of the paper is organized as follows. In Section II, we outline a DLC model studied in recent literature and consider how different sampling policies affect its performance. In Section III we describe our metric for privacy, inspired by the recent literature in NILM, provide a strong adversary model, and give guarantees on when this adversary can infer private information about the consumer. Finally, in Section IV we conclude and discuss directions for future work.

II. DIRECT LOAD CONTROL PERFORMANCE

In this section, we consider the effects of lower sampling rates on smart grid operations. In particular, we focus on a direct load control (DLC) application using thermostatically controlled loads (TCLs) to manage load imbalances. As mentioned in Section I, for this paper, we restrict our scope to consider data sampling policies. Other ways to alter the privacy of a consumer participating in an advanced metering infrastructure (AMI) include adding noise to data, modifying how data is aggregated, and the duration of data retention. Such investigations are outside the scope of this paper, but are an active topic of research [5], [6], [7], [8], [9], [16], [17].

DLC has been a promising future direction for the smart grid for a variety of reasons. By controlling loads which can be modified without much impact on consumer satisfaction, we can delay many costs by shifting loads from peak demand and compensating for real-time load imbalances. Additionally, as renewable energy penetration increases, the generation side of power is becoming more uncertain.

TCLs, which are often heating, ventilation, and air conditioning (HVAC) systems for buildings, have been a promising avenue for the implementation of DLC policies. They have become a recent topic of study [18], [19] due to the fact that buildings have a thermal inertia and can, in essence, store energy. Power consumption can be deferred and shifted while resulting in an imperceptible change in temperature.

Additionally, such DLC policies are being deployed today. For example, Pacific Gas & Electric deployed the SmartAC program in Spring 2007 [20]. Another provider of demand response (DR) services has recruited over 1.25 million residential customers in DLC programs, and has deployed over 5 million DLC devices in the United States. In California, they have successfully curtailed over 25 MW of power consumption since 2007 [21]. As these programs are being deployed on a large scale, it is important to consider the privacy aspects of these programs.

In this paper, our development focuses on air conditioning for notational simplicity, but similar statements can be made for heaters.

A. Thermostatically controlled load model

The model outlined in this section closely mirrors the model presented in [22]. There are other TCL and DLC models in the literature, e.g. [23], [24], and our analysis can similarly be applied to these models as well.

Let $I$ denote the set of TCLs participating in a DLC program. We model each TCL $i \in I$ as a discrete-time difference equation:

$$\theta_i(k+1) = a_i\theta_i(k)+(1-a_i)[\theta_{a,i}(k)-m_i(k)\theta_{g,i}]+\epsilon_i(k)$$

(1)

In the above equations, $\theta_i(k)$ is the internal temperature of TCL $i$ at time $k$, $\theta_{a,i}$ is the ambient temperature around TCL $i$, and $\epsilon_i$ is a noise process. The term $a_i = \exp(-h/(R_iC_i))$, where $h$ is the sampling period, $R_i$ is the thermal resistance of TCL $i$, and $C_i$ is the thermal capacitance of TCL $i$. The $\theta_g$ term is the temperature gain when a TCL is in the ON state, and $\theta_{trans,i}$ is the energy transfer rate of TCL $i$. Let $P_i$ denote the power consumed by TCL $i$ when it is in the ON state.

The local control for TCL $i$ is modeled by the variable $m_i$. We assume the local controller does a basic ON/OFF hysteresis control based on its setpoint and deadband. For a cooling TCL, this is defined as:

$$m_i(k+1) = \begin{cases} 
0 & \text{if } \theta_i(k+1) < \theta_{set,i} - \delta_i/2 \\
1 & \text{if } \theta_i(k+1) > \theta_{set,i} + \delta_i/2 \\
m_i(k) & \text{otherwise}
\end{cases}$$

(2)

In these equations, $\theta_{set,i}$ and $\delta_i$ are the temperature setpoint and deadband of TCL $i$, respectively. If $m_i(k) = 1$, then we say that TCL $i$ is in the ON state at time $k$, and similarly $m_i(k) = 0$ means that $i$ is in the OFF state at $k$.

B. Direct load control objective

We consider DLC policies that attempt to compensate for load imbalances and defer demands from peak times by switching TCLs between the ON state and the OFF state. The marginal cost of peak loads and unexpected load imbalances is responsible for a large portion of the preventable costs in the electricity grid; for a more detailed treatment of the benefits and impact of a DLC policy which can shave demand, we refer the reader to [25].

Formally, we consider the load imbalance as an exogenous variable. In particular, the centralized DLC operator is given some desired power trajectory $P_{des}$ for the TCLs. The goal of the operator is to minimize the root-mean-square (RMS) error between the actual power consumed by the TCLs and the signal $P_{des}$, i.e. it wishes to minimize $\|\sum_{i \in I} P_i m_i - P_{des}\|_2$. 
C. Direct load control capabilities

To achieve the DLC objective, we assume the DLC operator has the capability of telling TCLs to switch modes between ON and OFF. This has the effect of tightening the deadband for TCLs. More explicitly, if a TCL is issued a command to switch from OFF to ON, the TCL turns on its air conditioner for TCLs. More formally, if a TCL is issued a command to ON and OFF. This has the effect of tightening the deadband

At time \( k + 1 \), the estimator uses the observation if it is available. If no measurement is available, it evolves the estimates according to the dynamics with known parameters \( \alpha \), under the assumption that \( \epsilon_i(k) = 0 \). These estimates are used to issue control commands. Our controller takes a binning approach, as seen in recent research \[ 13, 22 \]. Each TCL is assigned to a bin based on its thermal state relative to its deadband, and whether or not it is in the ON or OFF state.

More formally, let \( N_{\text{bin}} \) be an even number denoting the number of bins our controller uses. For the ON states, we assign \( N_{\text{bin}}/2 \) bins, and for the OFF states, we assign \( N_{\text{bin}}/2 \) bins. Then, for each \( i \in \mathbb{Z} \), we define the following functions. First, we define the function \( \phi_i : \mathbb{R}_+ \to \mathbb{R} \) as:

\[
\phi_i(\theta) = \left[ \theta - (\theta_{\text{set},i} - \delta_i/2) \right]/\delta_i \tag{5}
\]

This function normalizes \( \theta \) so, if \( \theta \) is in the deadband, then \( \phi_i(\theta) \) lies in the interval \([0, 1]\). Next, define the function \( \psi_i : \mathbb{R}_+ \to \{ 0, 1, 2, \ldots, N_{\text{bin}}/2 \} \) as:

\[
\psi_i(\theta) = \begin{cases} 
1 & \text{if } 0 \leq \phi_i(\theta) < 1/(N_{\text{bin}}/2) \\
2 & \text{if } 1/(N_{\text{bin}}/2) \leq \phi_i(\theta) < 2/(N_{\text{bin}}/2) \\
\vdots & \\
N_{\text{bin}}/2 & \text{if } 1 - 1/(N_{\text{bin}}/2) \leq \phi_i(\theta) < 1 \\
0 & \text{otherwise}
\end{cases} \tag{6}
\]

This function evenly partitions the interval \([\theta_{\text{set},i} - \delta_i/2, \theta_{\text{set},i} + \delta_i/2] \) into \( N_{\text{bin}}/2 \) bins of length \( \delta_i/(N_{\text{bin}}/2) \), and assigns 0 if \( \theta \) lies outside this interval. Bins are indexed by an integer in \([1, 2, \ldots, N_{\text{bin}}/2]\) and a state in \{ON, OFF\}. Thus, if the state of TCL \( i \) at time \( k \) is \( (\theta_i(k), m_i(k)) \), it will be assigned to bin \( \psi_i(\theta_i(k), m_i(k)) \) at time \( k \). The number of TCLs in bin \( (n, m) \) at time \( k \) is:

\[ \sum_{i \in \mathbb{Z}} \mathbb{1}(\psi_i(\theta_i(k)) = n) = n \] and \( m_i(k) = m \).

Also, note that a TCL may not fall into any bin; this corresponds to when the TCL’s thermal state is out of its deadband. Since we are considering deadband tightening strategies to maintain customer satisfaction, if a TCL is outside its deadband, we assume we cannot issue control commands to it.

Based on its estimate of how many TCLs are in each bin, the controller issues a command to each bin, stating what fraction of the TCLs in each bin should switch states. Here, for simplicity, we assume that every TCL consumes the same amount of power when on, i.e. \( P_i = P \) for all \( i \in \mathbb{Z} \).

More concretely, the controller switches TCLs at time \( k \) based on the mismatch between the estimated power consumed \( \left( \sum_{i \in \mathbb{Z}} \hat{m}_i(k) \right) P \) at time \( k \) and the desired power consumption \( P_{\text{des}}(k) \) at time \( k \). For example, suppose that it is time \( k \). The estimated number of TCLs in the ON state is \( \sum_{i \in \mathbb{Z}} \hat{m}_i(k) \). If \( \left( \sum_{i \in \mathbb{Z}} \hat{m}_i(k) \right) P > P_{\text{des}}(k) \), then too many TCLs are on and our controller will issue a command to switch from ON to OFF for some TCLs. It will try to turn off \( \left[ P_{\text{des}}(k)/P \right] - \sum_{i \in \mathbb{Z}} \hat{m}_i(k) \) TCLs.

To do so, it will issue a probability to each bin, based on how many TCLs are estimated to be in each bin. Since we prefer to switch TCLs that are likely to switch to an OFF state soon, we start by turning off items in bin \( (1, \text{ON}) \). If there are more than enough TCLs in bin \( (1, \text{ON}) \), we issue a fraction based on how many TCLs we wish to turn off and the estimated number in a bin. If there are not enough, we command every TCL in the bin to turn off, and move on to the next bin \( (2, \text{ON}) \). The algorithm is described in more detail in Algorithm \[ 1 \].

An analogous process takes place if \( \left( \sum_{i \in \mathbb{Z}} \hat{m}_i(k) \right) P < P_{\text{des}}(k) \) and the controller must turn TCLs on. This algorithm would be the same, only the variable \( b \) in Algorithm \[ 1 \] would be initialized with \( N_{\text{bin}}/2 \) and would decrement across iterations, and ON would be replaced with OFF.

\(^4\)Here, for a proposition \( p \), \( 1\{p\} = 1 \) if \( p \) is true, and \( 1\{p\} = 0 \) otherwise.
Algorithm 1 DLC operator’s algorithm at time $k$ for issuing commands to bins to reduce power consumption.

```
Initialize the number of TCLs to switch, $N$, and the bin number $b$.
$N \leftarrow \lfloor P_{\text{des}}(k)/P \rfloor - \sum_{i \in \mathcal{I}} \hat{m}_i(k)$
$b \leftarrow 1$

while $N > 0$ and $b \leq N_{\text{bin}}/2$
  Calculate the estimated number of TCLs in bin $(b, \text{ON})$.
  $n \leftarrow \sum_{i \in \mathcal{I}} 1\{\psi_i(\hat{\theta}_i(k)) = b \text{ and } \hat{m}_i(k) = \text{ON}\}$
  if $n \geq N$ then
    There are enough TCLs. Switch as many as are needed.
    $c \leftarrow N/n$
    $N \leftarrow 0$
  else
    There are not enough TCLs. Switch all of them.
    $c \leftarrow 1$
    $N \leftarrow N - n$
  end if
  issueCommand$(c, (b, \text{ON}))$
  $b \leftarrow b + 1$
end while
```

At the level of an individual TCL, the TCL can calculate which bin it is in, based on its true state $(\theta_i(k), m_i(k))$ and its deadband. When its been receives a command $c$, it will switch states with probability $c$. Using a probability allows the centralized controller to issue commands without broadcasting individual TCL identities, and without explicit knowledge of which TCLs will switch. Additionally, a TCL can decide whether or not to switch entirely on its own, without coordination or communication with other members of its bin. An example of this control algorithm is depicted in Figure 1 with an explanation in the caption.

E. Direct load control simulations

We summarize how simulations were generated for the framework just outlined. We considered a DLC operator in control of 1000 TCLs, each which consume $P_i = 2.5$ kW when on. Parameters for each TCL $i$ are drawn independently from the following distributions:

\begin{align*}
R &\sim U(1.5, 2.5) \, ^{\circ}\text{C/kW}  \\
C &\sim U(1.5, 2.5) \, \text{kWh/}^\circ\text{C}  \\
\theta_{\text{set}} &\sim U(15, 25) \, ^{\circ}\text{C}  \\
\delta &\sim U(0.25, 1) \, ^{\circ}\text{C}  \\
P_{\text{trans}} &\sim U(10, 18) \, \text{kW}  \\
m(0) &\sim B(0.5)
\end{align*}

Then, $\theta_i(0)$ is drawn uniformly from within the deadband $(\theta_{\text{set},i} - \delta/2, \theta_{\text{set},i} + \delta/2)$ for each TCL $i \in \mathcal{I}$. These parameters are inspired by recent studies of a 250 m$^2$ home [22], [18]. The time step $h$ was chosen to be $h = 1$ minute, and the number of bins $N_{\text{bin}} = 10$.

\footnote{Here, $U(a, b)$ denotes the uniform distribution on the interval $(a, b)$, $B(p)$ denotes a coin flip with probability $p$ of success, and $N(\mu, \sigma^2)$ denotes a normal distribution with mean $\mu$ and variance $\sigma^2$.}

The ambient temperature $\theta_a = 32^\circ\text{C}$ for all TCLs, and the noise process $\epsilon_i(k)$ is independent across $k$ and distributed according to a $N(0, 0.0005)$ distribution for each $k$.

In normal operation, assuming the uniform distribution across the deadband and the Bernoulli distribution across ON/OFF states, the expected number of TCLs in the ON state is $1000/2 = 500$. Since each device consumes 2.5 kW when on, that means the expected power consumption at any time $k$ is $500 \cdot 2.5 = 1250$. kW.

California Independent System Operator (CAISO) market signals are given in 5 minute intervals [22], [26], so for
Simulations, the signal \( P_{\text{des}} \) is independently drawn from a \( U(1.25 \text{ MW·3/4}, 1.25 \text{ MW·5/4}) \) distribution. That is, \( P_{\text{des}}(k) \) is uniformly drawn for \( k \in \{0, 5, 10, \ldots \} \). For other values of \( k \), we take the linear interpolation.

One simulation of the aggregate power consumption of all the TCLs is shown in Figure 2. Comparing the top plot with the middle and bottom plots, we can see that a DLC policy can reduce the load imbalance even when the controller does not always receive measurements. However, small unforeseen temperature deviations can cause the controller’s performance to degrade if enough measurements are not provided, as seen by comparing the middle and bottom plots.

Additionally, the thermal state of one TCL is shown in Figure 3 for when \( h = 1 \) minute. We can see that the temperature inside the TCL remains inside the deadband, resulting in no loss of comfort to the consumer.

In Figure 4, we plot the load imbalance for each sampling rate. First, we randomly drew a \( P_{\text{des}} \) signal and TCL parameters. Then, for this fixed \( P_{\text{des}} \) signal and TCL parameters, we ran 500 trials for each sampling period \( h \), and we consider the empirical distribution of the difference between the actual power consumed by all the TCLs and the desired power signal:

\[
\sum_{i \in I} P_i m_i - P_{\text{des}}
\]

We used the \( \ell_1 \) norm on the error signal, so, if we assume a fixed price for spot market electricity purchases/sales throughout the hour interval, this is directly proportional to the cost the utility company must pay.

**III. Privacy Metric**

In Section II, we consider how a larger sampling period affects the performance of a DLC program. Whereas it is intuitive that receiving fewer samples will increase a consumer’s privacy, we can leverage results from nonintrusive load monitoring (NILM) to give guarantees of privacy to a user. In this section, we introduce our metric for privacy.

**A. Privacy problem**

First, we note that the aggregate power consumption signal is not private in and of itself; rather, it is the information about the consumer that can be inferred from this signal. Thus, suppose we have some private variable \( u \). For example, \( u \) could be a binary variable representing whether or not a user is home, or whether or not a high-power grow lamp is being used inside the building. \( u \) could be an \( n \)-ary variable as well, or a variable taking values in \( \mathbb{R} \). We note that the extension to the \( n \)-ary case is simple, and the continuum case can be reduced to the \( n \)-ary case by partitioning \( \mathbb{R} \) into a finite number of sets. Thus, for the scope of this paper, we focus on the binary case where either \( \{u = 0\} \) or \( \{u = 1\} \).
Now, suppose an adversary is observing the aggregate power consumption signal as it is being transmitted by an AMI. This signal will live in $R^T$, where $T$ is the number of measurements sent in the time horizon. Let $\nu$ denote a probability kernel such that $\nu(v, \cdot)$ denotes the distribution of the aggregate power consumption across $R^T$ given that the private variable takes value $v$. Let $u^*$ be the true value of $u$, and $y \sim \nu(u^*, \cdot)$ be the random variable representing the power consumption signal. The goal of the adversary is to recover $u^*$ given $y$.

We note here that this particular inference problem is a growing topic of research, known either as nonintrusive load monitoring or energy disaggregation [27], [28], [29], [30], [31]. People are actively working on recovering device usage from an aggregate power consumption signal, and the privacy issue of inferring consumption patterns fromAMI signals is a real threat.

B. Adversary model and guarantees of privacy

Now, we outline the capabilities of our adversary. We assume a powerful adversary that has a prior on $u$ in the population, and that knows the probability distributions $\nu(0, \cdot)$ and $\nu(1, \cdot)$. We assume the adversary is able to observe the aggregate power consumption signal whenever it is being transmitted across the AMI, but is not able to observe the device-level signals for a building. Additionally, we assume this adversary has an arbitrary amount of computational power.

Adversary model and guarantees of privacy

This framework allows us to phrase the adversary’s inference problem as a hypothesis testing problem. More formally, suppose that $\nu(0, \cdot)$ and $\nu(1, \cdot)$ both admit a probability density function (pdf). Denote these pdfs as $f_0$ and $f_1$ respectively. Also, let $p(\cdot)$ denote the adversary’s prior.

The adversary wishes to maximize the probability he successfully estimates $u^*$ given $y$. That is, he wishes to solve the following optimization problem for functions $\hat{u}: R^T \rightarrow \{0, 1\}$:

$$\max_{\hat{u}} \Pr(\hat{u}(y) = u^*) \tag{13}$$

We will refer to solutions to Equation (13) as optimal estimators of $u^*$ given $y$. Results from detection theory give us one such solution.

Proposition 1. An optimal estimator of $u^*$, the true value of $u$, given $y$, is the maximum a posteriori (MAP) estimator, given by:

$$u_{MAP}(y) = \begin{cases} 1 & \text{if } f_1(y) \geq p(u=0) \frac{p(u=1)}{p(u=1)} \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

A quick consequence of this statement can give a guarantee of privacy.

Proposition 2. For any estimator $\hat{u}: R^T \rightarrow \{0, 1\}$, the adversary’s probability of correctly identifying $u^*$ given $y$ is bounded by the probability of correctly identifying $u^*$ with the MAP estimate.

$$\Pr(\hat{u}(y) = u^*) \leq \Pr(u_{MAP}(y) = u^*) \tag{15}$$

These are established results in hypothesis testing [32], but the implications are powerful. Regardless of the algorithm the adversary uses, we can bound the probability he will successfully breach a consumer’s privacy. Furthermore, this formula allows us to vary different parameters of the AMI, such as how often data is collected and transmitted. We will examine this on a concrete example in Section [II-D].

C. Connections to differential privacy

Recently, differential privacy has been a popular metric for measuring the privacy of users in a system [35], [36]. Differential privacy is a very attractive theoretical notion, as it is a broad definition which abstracts away the problem of defining an adversary model or privacy breach to provide a privacy guarantee independent of the adversary or definition of a privacy breach.

However, the concept of differential privacy often relies on additive noise of some form to give the privacy guarantees. In electrical grid applications, there are many cases where the original raw data is required, for practical, regulatory, performance, or economic reasons. To the best of our knowledge, there is no straightforward way to apply concepts of differential privacy to different sampling policies.

In contrast to differential privacy, our metric for privacy fixes a definition of privacy breach, i.e. whether $\{u = 0\}$ or $\{u = 1\}$. Our definition is closer to the concept of equivocation metrics, e.g. [17], than differential privacy.

D. Privacy metric example

We instantiate our privacy metric on a concrete example here. In practice, many algorithms that attempt to solve the inference problem in Equation (13) assume Gaussian distributions [29], [30], [31]. In the case that $f_0$ and $f_1$ are both pdfs of a Gaussian random variable with a shared covariance matrix $\Sigma$, the MAP estimate in Proposition 2 can be calculated explicitly.

Proposition 3. If $\nu(0, \cdot)$ is Gaussian with mean $\mu_0$ and covariance $\Sigma$, and $\nu(1, \cdot)$ is Gaussian with mean $\mu_1$ and covariance $\Sigma$, then an optimal estimator of $u^*$, the true value of $u$, given $y$, is the maximum a posteriori (MAP) estimator, given by:

$$u_{MAP}(y) = \begin{cases} 1 & \text{if } a^T y + b \leq 0 \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

where:

$$a^T = (\mu_0 - \mu_1)^\top \Sigma^{-1} \tag{17}$$

$$b = \frac{1}{2} \left(\mu_1^\top \Sigma^{-1} \mu_1 - \mu_0^\top \Sigma^{-1} \mu_0\right) \tag{18}$$

In this case, if the $\{u = 0\}$ and $\{u = 1\}$ are equally likely, it is possible to integrate the pdf of the resulting Gaussian and derive the following upper bound.
Proposition 4. Suppose \( \nu(0, \cdot), \nu(1, \cdot), a, \) and \( b \) are defined as in Proposition 3 and \( \Pr(u = 0) = \Pr(u = 1) = 1/2. \) Then, for any estimator \( \hat{u} \), the following bound holds:

\[
\Pr(\hat{u}(y) = u) \leq \frac{1}{2} \left( 1 + \text{erf} \left( \frac{1}{\sqrt{2\sigma^2}} (a^\top \mu_0 + b) \right) \right)
\]

where \( \text{erf} \) is the Gauss error function and:

\[
\sigma^2 = \frac{1}{\|a\|_2^2} a^\top \Sigma a = \frac{1}{\|a\|_2^2} \sum k = 1 \sum_{a} (\mu_0 - \mu_1)^\top \Sigma^{-1} (\mu_0 - \mu_1)
\]

Consider the following scenario. The private variable is whether or not a consumer uses the microwave on a particular day. Suppose the adversary knows that there is a 1/2 probability the consumer will turn on the microwave at some point in time to microwave a 5 minute frozen dinner, and, given that the microwave turns on, the turn-on time is uniformly distributed between 6pm and 7pm. Thus, we are fixing our definition of a privacy breach.

For data, we use the Reference Energy Disaggregation Dataset (REDD) [37]. Using the low frequency data, collected at roughly 1/3 Hz, we take the power consumption signal of a microwave to form a microwave model\(^3\). We note that the power consumption of a microwave is roughly constant when it is on. However, the magnitude when it turns on varies across uses. When it is on, the power consumption has empirical mean 1.96 kW. Thus, for a microwave model, we assume the microwave consumes 1.96 kW when it is on, and consumes 0 when it is off.

Additionally, when the microwave is on, the power consumption has standard error 0.9 kW. We assume this number is representative of the uncertainty the adversary has in the power consumption of devices in the household.

Now suppose our adversary knows the usage of the other devices in the house. That is, suppose the power consumption of the other devices in the house follow a \( N(\mu_k, 0.9^2) \) distribution at time \( k \), independent across \( k \), where \( \mu_k \) is some constant that is available to the adversary. Thus, supposing the microwave’s power consumption is \( q(k) \) at time \( k \), the hypothesis testing problem with \( T \) measurements is to distinguish between the distributions \( N(\mu, 0.9^2 I_{T \times T}) \) and \( N(\mu + q, 0.9^2 I_{T \times T}) \). Since we assume the adversary knows \( \mu \), an equivalent problem is the separation problem between distributions \( N(0, 0.9^2 I_{T \times T}) \) and \( N(q, 0.9^2 I_{T \times T}) \). This is depicted in Figure 5.

We note that, in our model, the two distributions above are conditional distributions given \( q \), which can be a random variable. For example, in the scenario described here, \( q \) is a sampled signal of a continuous random process which draws a time \( t \) uniformly between 6pm and 7pm, and equals 1.96 kW on the interval \( [t, t + 5 \text{ min}] \), and 0 otherwise.

Finally, we can now consider different sampling schemes, which will affect the dimension \( T \) and the distribution of \( q \). Suppose that the microwave is used between 6pm and 7pm. Recall that we assumed the microwave will be used for 5 minutes. Then, if the sampling period \( h = 1 \) minute, then with probability 1, the adversary will have 4 observations where the microwave is ON, i.e. there exists 4 values of \( k \) such that \( q(k) \neq 0 \). If the sampling period is \( h = 60 \) minutes, then with probability (5 min/60 min), the adversary will have 1 observation where the microwave is ON, and will otherwise not have any observations of the microwave.

We can similarly reason about other sampling periods in between. If \( h = 2 \) minutes, then with probability 1/2, the adversary will have 2 observations and with probability 1/2, the adversary will have 3 observations. This follows from the uniform distribution across turn-on times for the microwave.

Proposition 4 gives us a bound on the optimal estimator if the adversary knows \( t \), the time at which the microwave turns on. Thus, if we give the adversary side information \( t \), that will give us a conservative upper bound on the probability of successfully identifying the microwave. Thus, using the above analysis in conjunction with Proposition 4, we can plot the upper bound on the probability of a successful privacy breach, as a function of the sampling period \( h \). The results are shown in Figure 6. Although we focus on a particular example here, this analysis can be applied to any other definition of a privacy breach. For instance, the same reasoning can be applied when considering whether or not a household contains a high-power grow lamp.

IV. Conclusion

We consider a direct load control model which uses thermostatically controlled loads, and analyze how its performance degrades as it receives samples less and less frequently. Similar analysis techniques can be applied to many proposed smart grid operations, to quantify how much data should be collected

\(^3\)The REDD collects data from several channels for several houses. The aggregate data was taken by summing Channels 1 and 2 from House 1, and the microwave signal was taken from Channel 11 in House 1.

\(^4\)Here, we treat \( \mu \) and \( q \) as vectors in \( \mathbb{R}^T \), where the \( k \)th entry of \( \mu \) is \( \mu_k \), and \( I_{T \times T} \) is the \( T \)-dimensional identity matrix.
for a certain level of system performance. We introduce a new metric of privacy, based on a strong adversarial model. For a fixed definition of a privacy breach, this privacy metric allows us to give guarantees for when the adversary can enact a privacy breach, regardless of the computational power and method used by the adversary. Combining these two results allows us to quantify the tradeoff between the data collected for smart grid operations and the privacy risk to consumers.

REFERENCES

[1] M. Lisovich, D. Mulligan, and S. Wicker, “Inferring personal information from demand-response systems,” IEEE Security Privacy, vol. 8, no. 1, pp. 11–20, Jan 2010.

[2] R. Anderson and S. Fuloria, “On the security economics of electricity metering,” Ninth Workshop on the Economics of Information, 2010.

[3] G. Smith, “Marijuana bust shines light on utilities,” Post and Courier, Jan 2012.

[4] Government Accountability Office, “Electricity grid modernization: Progress being made on cybersecurity guidelines, but key challenges remain to be addressed,” Jan 2011.

[5] K. Kursawe, G. Danezis, and M. Kohlweiss, “Privacy-friendly aggregation for the smart-grid,” in Proceedings of the 11th International Conference on Privacy Enhancing Technologies, ser. PET’s’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 175–191.

[6] A. Rial and G. Danezis, “Privacy-preserving smart metering,” in Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, ser. WPES ’11. New York, NY, USA: ACM, 2011, pp. 49–60.

[7] G. Taban and V. Gligor, “Privacy-preserving integrity-assured data aggregation in sensor networks,” in International Conference on Computational Science and Engineering, 2009. CSE ’09, vol. 3, Aug 2009, pp. 168–175.

[8] F. Li, B. Luo, and P. Liu, “Secure information aggregation for smart grids using homomorphic encryption,” in 2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm), Oct 2010, pp. 327–332.

[9] G. Acs and C. Castelluccia, “I have a DREAM! (Differentially private smArt Metering),” in Information Hiding, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, vol. 6958, pp. 118–132.

[10] The Smart Grid Interoperability Panel - Cyber Security Working Group, “NISTIR7628 – Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid.”

[11] North American Energy Standards Board, “NAESB privacy policy.”

[12] Department of Energy, “Data access and privacy issues related to smart grid technologies.”

[13] Public Utility Commission of Texas, “Electric Substantive Rules – Chapter 25.”

[14] California Public Utilities Commission, “Decision adopting rules to protect the privacy and security of the electricity usage data of the customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company.”

[15] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. S. Sastry, “A game theory model for electricity theft detection and privacy-aware control in AMI systems,” in Proceedings of the 50th Allerton Conference on Communication, Control, and Computing, 2012, pp. 1830–1837.

[16] L. Sankar, S. Kar, R. Tandon, and H. Poor, “Competitive privacy in the smart grid: An information-theoretic approach,” in 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Oct 2011, pp. 220–225.

[17] L. Sankar, S. Rajagopalan, and H. Poor, “Utility-privacy tradeoffs in databases: An information-theoretic approach,” Information Forensics and Security, IEEE Transactions on, vol. 8, no. 6, pp. 838–852, June 2013.

[18] D. S. Callaway, “Tapping the energy storage potential in electric loads to deliver load following and regulation, with application to wind energy,” Energy Conversion and Management, vol. 50, no. 5, pp. 1389 – 1400, 2009.

[19] C. Perfumo, E. Kofman, J. H. Bruslavsky, and J. K. Ward, “Load management: Model-based control of aggregate power for populations of thermostatically controlled loads,” Energy Conversion and Management, vol. 55, pp. 36 – 48, 2012.

[20] M. Alexander, K. Agnew, and M. Goldberg, “New approaches to residential direct load control in california,” in 2008 ACEEE Summer Study on Energy Efficiency in Buildings, 2008.

[21] California Energy Commission, “Docket No. 13-IEP-1F: Increasing demand response capabilities in California,” 2013.

[22] J. Mathieu, S. Koch, and D. Callaway, “State estimation and control of electric loads to manage real-time energy imbalance,” IEEE Transactions on Power Systems, vol. 28, no. 1, pp. 430–440, 2013.

[23] N. Ruiz, I. Cobelo, and J. Oyarzabal, “A direct load control model for virtual power plant management,” IEEE Transactions on Power Systems, vol. 24, no. 2, pp. 959–966, May 2009.

[24] S. Gupta, M. S. Reynolds, and S. N. Patel, “Electrisense: single-point sensing using EMI for electrical event detection and classification in the home,” in Proceedings of the 12th ACM international conference on Ubiquitous computing, ser. Ubicomp ’10. New York, NY, USA: ACM, 2010, pp. 139–148.

[25] J. Z. Kolter and T. Jaakkola, “Approximate inference in additive factorial HMMs with application to energy disaggregation,” in Proceedings of the International Conference on Artificial Intelligence and Statistics, 2012.

[26] O. Parson, S. Ghosh, M. Weal, and A. Rogers, “Nonintrusive load monitoring using prior models of general appliance types,” in Proceedings of the 26th AAAI Conference on Artificial Intelligence, 2012.

[27] R. Dong, L. J. Ratliff, H. Ohlsson, and S. S. Sastry, “Energy disaggregation via adaptive filtering,” in 2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton), Oct 2013, pp. 173–180.

[28] T. M. Cover and J. A. Thomas, Elements of Information Theory. Wiley-Interscience, 1991.

[29] R. Dong, L. Ratliff, H. Ohlsson, and S. S. Sastry, “Fundamental limits of nonintrusive load monitoring,” in Conference on High Confidence Data Mining Applications in Sustainability, 2011.