Privacy on Hypothesis Testing in Smart Grids

Zuxing Li and Tobias J. Oechtering
School of Electrical Engineering and the ACCESS Linnaeus Centre
KTH Royal Institute of Technology, Stockholm, Sweden

***Abstract*—In this paper, we study the problem of privacy information leakage in a smart grid. The privacy risk is assumed to be caused by an unauthorized binary hypothesis testing of the consumer's behaviour based on the smart meter readings of energy supplies from the energy provider. Another energy supplies are produced by an alternative energy source. A controller equipped with an energy storage device manages the energy inflows to satisfy the energy demand of the consumer. We study the optimal energy control strategy which minimizes the asymptotic exponential decay rate of the minimum Type II error probability in the unauthorized hypothesis testing to suppress the privacy risk. Our study shows that the cardinality of the energy supplies from the energy provider for the optimal control strategy is no more than two. This result implies a simple objective of the optimal energy control strategy. When additional side information is available for the adversary, the optimal control strategy and privacy risk are compared with the case of leaking smart meter readings to the adversary only.**

I. Introduction

A smart grid is an energy network which manages the energy generation and distribution more efficiently following the real-time consumer's energy demand through control and communication technologies [1]. Benefited from the smart grid, the energy efficiency can be improved; the reliability and robustness can be enhanced; and the costs of the energy provider and consumer can be reduced. However, these benefits come with privacy challenges in the smart grid [2], [3]. In a smart grid, the smart meter provides real-time information of energy supplies from the energy provider on the demands of the consumer, which can be utilized for unauthorized purposes, e.g., to infer on the private information of the consumer. Regarding the smart meter privacy problem, different privacy-preserving schemes are developed. An encryption method was proposed in [4] to protect the privacy of individuals through the neighbor-level data aggregation in smart grids. In [5], a method was devised to schedule the usage of delay-tolerable appliances to hide the energy consumption characteristics of other appliances. Some works have been done from the information theoretic perspective to measure the privacy risk by the mutual information rate between the energy supplies and demands [1], [6]–[8]. In [6], the authors proposed to use a rechargeable battery to hide the private information by distorting the smart meter readings. A similar method studied in [7] was to exploit an alternative energy source. In [1], the smart meter privacy was protected in the presence of both energy harvesting and storage devices. In [8], a new framework abstracting both the privacy and utility was presented by using the information theoretic tools and a hidden Markov model. Another smart meter privacy-preserving idea was proposed in [9] to flatten the smart meter readings by utilizing a battery to minimize the variance of energy supplies from the energy provider.

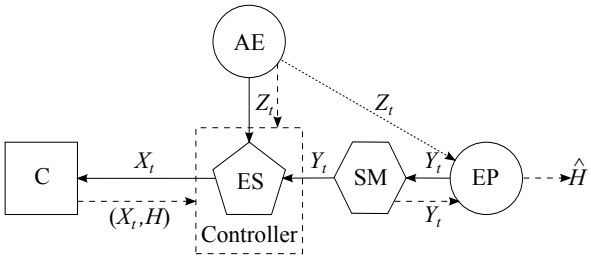

Fig. 1. In the smart grid model, we denote the energy flows by solid arrows and information flows by dashed arrows. The energy demands X^T of the consumer (C) are asymptotically satisfied by the energy supplies Y^T from the energy provider (EP) and Z^T from the alternative energy (AE) source. The energy storage (ES) device works as an agent between the energy inflows and demands. The energy controller determines the energy supply Y_t from the energy provider based on the information of energy demand x_t, behaviour of the consumer h, and alternative energy inflow z_t. The smart meter (SM) readings of energy supplies from the energy provider Y^T are assumed to be utilized by an adversary to infer on the behaviour of the consumer by making a guess $\hat{H}$. The dot arrow represents the side information flow of Z_t to the adversary in the later discussion.

In this paper, we consider a smart grid model in the presence of an alternative energy source and an energy controller equipped with an energy storage device. The smart meter privacy leakage is modelled as an unauthorized Neyman-Pearson hypothesis testing on a private behaviour of the consumer. Some works have been done to relate the hypothesis testing and privacy risk [10]–[12]. Here, the privacy risk is measured by the asymptotic exponential decay rate of the minimum Type II error probability of the adversary. We study and characterize the optimal energy control strategy which satisfies energy demands and suppresses the privacy risk to the lowest.

The remaining of this paper is organized as follows: The studied smart grid model is introduced in Section II; the control strategy against the unauthorized hypothesis testing is studied in Section III; and the conclusion is given in Section IV.

In the following, we will denote a random variable by a capital letter, its realization by the lower-case letter, and its definition domain by the corresponding calligraphic letter. Let X^T stand for a random vector $(X_1, \ldots, X_T)$ and x^T stand for a vector of realizations $(x_1, \ldots, x_T)$.

II. Smart Grid Model

In this paper, we consider the smart grid model shown in Figure 1 where the accumulated energy demands and supplies are discretized and reported at discrete times. For the consumer (C), let H defined on the domain $\mathcal{H} = \{h_0, h_1\}$ denote the binary behaviour hypothesis. Given each hypothesis realization h, we assume the energy demand X_t of the consumer in the time interval t is defined on the domain $\mathcal{X}$ and i.i.d. generated according to the pmf $p_{X|H}(\cdot|h)$. In the time interval t, we assume that the energy supply Z_t from an alternative energy (AE) source is defined on the domain $\mathcal{Z}$ and i.i.d. generated according to the pmf $p_Z(\cdot)$. The random energy supply Z_t is assumed to be independent of the energy demand X_t and hypothesis H. Given x_t, z_t, and h, the controller requests an energy supply Y_t defined on the domain $\mathcal{Y}$ from the energy provider (EP) in the time interval t according to the energy control strategy

$$Y_t = \Gamma(x_t, z_t, h)$$

which is characterized by the pmf $p_{Y|X,Z,H}(\cdot|x_t, z_t, h)$. The energy inflows y_t and z_t are stored in an energy storage (ES) device which meets the energy demand x_t of the consumer.

We consider a privacy leakage problem that the smart meter (SM) readings of energy supplies from the energy provider Y^T are utilized by an adversary, which might be the energy provider itself, to infer on the behaviour of the consumer, i.e., to make a guess $\hat{H}$ defined on the domain $\mathcal{H}$.

In this study, we make the following idealistic assumptions on the model:

1) The energy storage device can always satisfy the energy demand x_t.
2) In any case of hypothesis h,

$$\lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T} y_t + z_t = \lim_{T\to\infty} \frac{1}{T}\sum_{t=1}^{T} x_t.$$

3) $\mathbb{E}(X|h) \geq \mathbb{E}(Z), \forall h \in \mathcal{H}$.

The first assumption corresponds to having a *powerful* energy storage device which itself stores a sufficiently large amount of energy and has a sufficiently large capacity. When the energy inflows y_t and z_t are not enough, the energy storage device can compensate the energy deficit by its large amount of energy storage. On the contrary, the energy storage device can store the extra energy when the inflows are more than the demand.

The second assumption shows that the energy inflows and the energy demands are asymptotically balanced given any hypothesis h. Due to the law of large number, the second assumption implies

$$\mathbb{E}(Y + Z|h) = \mathbb{E}(X|h), \forall h \in \mathcal{H}. \tag{1}$$

The equation (1) reduces to the constraints on the average energy supply from the energy provider:

$$\begin{aligned} \mathbb{E}(Y|h_0) &= \mathbb{E}(X|h_0) - \mathbb{E}(Z) = f_0, \\ \mathbb{E}(Y|h_1) &= \mathbb{E}(X|h_1) - \mathbb{E}(Z) = f_1. \end{aligned} \tag{2}$$

The third assumption implies that the energy demand cannot be satisfied by the alternative energy source only. Further, we have $f_0, f_1 \geq 0$ in (2).

In the next section, we will first formulate the privacy problem and study the optimal control strategy based on the above settings. Later, we will briefly discuss the optimal control strategy when the adversary has side information.

III. Energy Control against Hypothesis Testing

A. Privacy Risk of Unauthorized Hypothesis Testing

We consider that an adversary has access to the smart meter readings Y^T of the energy supplies from the energy provider. In addition, the adversary is informed about the smart grid, i.e., he has the knowledge of the pmfs $p_{X|H}$, p_Z, and $p_{Y|X,Z,H}$. Based on the intercepted smart meter readings and the knowledge about the smart grid, the adversary infers on the behaviour of the consumer by making a guess $\hat{H}$. There are two types of errors associated with the adversary's unauthorized binary hypothesis testing:

- Type I error: Make a decision h_1 when h_0 is true;
- Type II error: Make a decision h_0 when h_1 is true.

In this paper, we assume that the adversary will use the Neyman-Pearson detection approach to minimize the Type II error probability $p_{\text{II}} = p_{\hat{H}|H}(h_0|h_1)$ subject to a constraint on the Type I error probability $p_{\text{I}} = p_{\hat{H}|H}(h_1|h_0) < \lambda$. According to Neyman-Pearson Theorem [13], the optimal decision strategy for the adversary is a likelihood-ratio test, i.e., he will make a guess h_0 when observing y^T in the decision region $\mathcal{U}_{h_0}$

$$\mathcal{U}_{h_0} = \left\{ y^T : \log \frac{p_{Y^T|H}(y^T|h_0)}{p_{Y^T|H}(y^T|h_1)} \geq T\psi \right\},$$

where the threshold ψ is determined by the constraint

$$p_{\text{I}} = \sum_{y^T \in \mathcal{U}_{h_0}^c} p_{Y^T|H}(y^T|h_0) < \lambda,$$

and the objective to minimize

$$p_{\text{II}} = \sum_{y^T \in \mathcal{U}_{h_0}} p_{Y^T|H}(y^T|h_1).$$

The minimum Type II error probability $p_{\text{II}}^{\min}$ was introduced in [14] as the privacy metric in the single-observation Neyman-Pearson detection. Here, the adversary uses T observations for its hypothesis testing and $p_{\text{II}}^{\min} \to 0$ as $T \to \infty$. According to Chernoff-Stein Lemma [15], the Kullback-Leibler (KL) distance $\mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1))$ characterizes the asymptotic exponential decay rate of $p_{\text{II}}^{\min}$:

$$\lim_{T\to\infty} -\frac{\log p_{\text{II}}^{\min}}{T} = \mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1)).$$

It implies that the adversary needs more smart meter readings (a larger T) in order to achieve a certain $p_{\text{II}}^{\min}$ when the KL distance $\mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1))$ is smaller. Denote the asymptotic exponential decay rate of $p_{\text{II}}^{\min}$ by r_{II} as

$$r_{\text{II}} = \mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1)).$$

To suppress the privacy risk to the lowest, our objective is to minimize the KL distance $\mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1))$ so that the adversary needs the maximum number of observations to achieve a certain $p_{\text{II}}^{\min}$ in the unauthorized Neyman-Pearson hypothesis testing.

B. Optimal Control Strategy

An energy control strategy Γ is characterized by a conditional pmf $p_{Y|X,Z,H}$. Due to the constraints on the average energy supply from the energy provider in (2), we only discuss $p_{Y|X,Z,H}$ in the feasible region $\mathcal{P}_{Y|X,Z,H} = \{p_{Y|X,Z,H} : \mathbb{E}(Y|h_0) = f_0, \mathbb{E}(Y|h_1) = f_1\}$. The optimal energy control strategy Γ^* with $p^*_{Y|X,Z,H} \in \mathcal{P}_{Y|X,Z,H}$ achieves the minimum KL distance and r_{II}^* to suppress the privacy risk to the lowest. Note that both the objective KL distance and average energy supply constraints depend on the conditional pmf $p_{Y|H}$ and we can always achieve a conditional pmf $p_{Y|H}$ by a control strategy which satisfies the Markov chain $Y - H - (X, Z)$. Therefore, the optimal control strategy Γ^* and its pmf $p^*_{Y|X,Z,H}$ achieve the optimal argument $p^*_{Y|H}$ of the following problem.

$$\min_{p_{Y|H} \in \mathcal{P}_{Y|H}} \mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1)), \tag{3}$$

where

$$\mathcal{P}_{Y|H} = \{p_{Y|H} : \mathbb{E}(Y|h_0) = f_0, \mathbb{E}(Y|h_1) = f_1\}.$$

In the privacy-preserving operational sense, we impose the following condition on the optimal energy control strategy Γ^*:

$$p^*_{Y|H}(y|h_0) = 0 \Leftrightarrow p^*_{Y|H}(y|h_1) = 0, \forall y \in \mathcal{Y}. \tag{4}$$

If Γ^* does not satisfy the condition in (4), the hypothesis realization can be exactly inferred by the adversary when he observes that an energy supply y_t from the energy provider is not in the intersection of support sets of pmfs $p^*_{Y|H}(\cdot|h_0)$ and $p^*_{Y|H}(\cdot|h_1)$. That is because such an energy supply can be requested in the case of only one hypothesis realization.

For the optimal control strategy Γ^*, define its output set $\mathcal{Y}^* \subseteq \mathcal{Y}$ as

$$\mathcal{Y}^* = \left\{ y : y \in \mathcal{Y}, p^*_{Y|H}(y|h_0) \neq 0, p^*_{Y|H}(y|h_1) \neq 0 \right\}.$$

Theorem 1. *For the optimal control strategy Γ^*, the cardinality of its output satisfies $|\mathcal{Y}^*| \leq 2$.*

Proof: The problem (3) is a convex optimization since its feasible region $\mathcal{P}_{Y|H}$ is a convex set restricted by linear constraints and its objective KL distance is a convex function of $p_{Y|H}$. The optimal solution $p^*_{Y|H}$ has to satisfy the following necessary KKT conditions (5)-(9).

$$\begin{aligned} \sum_{y \in \mathcal{Y}} y p^*_{Y|H}(y|h_0) &= f_0, \\ \sum_{y \in \mathcal{Y}} y p^*_{Y|H}(y|h_1) &= f_1. \end{aligned} \tag{5}$$

$$\begin{aligned} p^*_{Y|H}(y|h_0) &\geq 0, \forall y \in \mathcal{Y}, \\ p^*_{Y|H}(y|h_1) &\geq 0, \forall y \in \mathcal{Y}. \end{aligned} \tag{6}$$

$$\begin{aligned} \sum_{y \in \mathcal{Y}} p^*_{Y|H}(y|h_0) &= 1, \\ \sum_{y \in \mathcal{Y}} p^*_{Y|H}(y|h_1) &= 1. \end{aligned} \tag{7}$$

By introducing Lagrange multipliers λ, w, non-negative $\{\gamma_{y0}\}_{y \in \mathcal{Y}}$, non-negative $\{\gamma_{y1}\}_{y \in \mathcal{Y}}$, v_0, and v_1, the Lagrange function $\mathbb{L}$ is formulated as

$$\begin{aligned} \mathbb{L} =& \mathbb{D}(p_{Y|H}(\cdot|h_0)||p_{Y|H}(\cdot|h_1)) \\ &+ \lambda(\mathbb{E}(Y|h_0) - f_0) + w(\mathbb{E}(Y|h_1) - f_1) \\ &- \sum_{y \in \mathcal{Y}} \gamma_{y0} p_{Y|H}(y|h_0) - \sum_{y \in \mathcal{Y}} \gamma_{y1} p_{Y|H}(y|h_1) \\ &+ v_0(\sum_{y \in \mathcal{Y}} p_{Y|H}(y|h_0) - 1) + v_1(\sum_{y \in \mathcal{Y}} p_{Y|H}(y|h_1) - 1). \end{aligned}$$

For any $y \in \mathcal{Y}^*$, the conditions of stationarity and complementary slackness result in

$$\log \frac{p^*_{Y|H}(y|h_0)}{p^*_{Y|H}(y|h_1)} = -\lambda^* y - 1 - v_0^*, \tag{8}$$

and

$$\frac{p^*_{Y|H}(y|h_0)}{p^*_{Y|H}(y|h_1)} = w^* y + v_1^*. \tag{9}$$

From the necessary KKT conditions (8) and (9), it follows that any $y \in \mathcal{Y}^*$ has to satisfy the following equation

$$\exp(-\lambda^* y - 1 - v_0^*) = w^* y + v_1^*. \tag{10}$$

Denote the solution set of (10) by $\mathcal{Y}_{\text{s}}$. Then, the cardinality of the output set $\mathcal{Y}^*$ can be upper bounded as $|\mathcal{Y}^*| \leq |\mathcal{Y}_{\text{s}}|$.

1) If $\lambda^* \neq 0$ and $w^* \neq 0$, the equation
$$\exp(-\lambda^* y - 1 - v_0^*) = w^* y + v_1^*$$
has at most two solutions of y, i.e., $|\mathcal{Y}^*| \leq |\mathcal{Y}_{\text{s}}| \leq 2$.
2) If $\lambda^* = 0$ and $w^* \neq 0$, the equation
$$\exp(-1 - v_0^*) = w^* y + v_1^*$$
has only one solution of y, i.e., $|\mathcal{Y}^*| \leq |\mathcal{Y}_{\text{s}}| \leq 1$.
3) If $\lambda^* \neq 0$ and $w^* = 0$, the equation
$$\exp(-\lambda^* y - 1 - v_0^*) = v_1^*$$
has only one solution of y, i.e., $|\mathcal{Y}^*| \leq |\mathcal{Y}_{\text{s}}| \leq 1$.
4) If $\lambda^* = 0$ and $w^* = 0$, from (9) and (7), it follows that
$$\begin{aligned} p^*_{Y|H}(y|h_0) &= v_1^* p^*_{Y|H}(y|h_1), \forall y \in \mathcal{Y}^*, \\ 1 = \sum_{y \in \mathcal{Y}^*} p^*_{Y|H}(y|h_0) &= v_1^* \sum_{y \in \mathcal{Y}^*} p^*_{Y|H}(y|h_1) = v_1^*. \end{aligned}$$
Therefore, we have $v_1^* = 1$ which further implies that
$$\begin{aligned} p^*_{Y|H}(y|h_0) &= p^*_{Y|H}(y|h_1), \forall y \in \mathcal{Y}^*, \\ y p^*_{Y|H}(y|h_0) &= y p^*_{Y|H}(y|h_1), \forall y \in \mathcal{Y}^*, \\ \sum_{y \in \mathcal{Y}^*} y p^*_{Y|H}(y|h_0) &= \sum_{y \in \mathcal{Y}^*} y p^*_{Y|H}(y|h_1). \end{aligned}$$
According to the conditions in (5), this case corresponds to having equal constraints as $f_0 = \mathbb{E}(Y|h_0) = f =$

$\mathbb{E}(Y|h_1) = f_1$ in the optimization problem. We can achieve any feasible equal constraints by using equal pmfs $p^*_{Y|H}(y|h_0) = p^*_{Y|H}(y|h_1) > 0$ for any $y \in \mathcal{Y}^* = \{y_i^*, y_j^*\} \subseteq \mathcal{Y}$ where $y_i^* \leq f$ and $y_j^* \geq f$. Therefore, it is sufficient to consider $\mathcal{Y}^*$ with $|\mathcal{Y}^*| \leq 2$ in this case.

Finally, we can conclude that the cardinality of the energy supply from the energy provider for the optimal control strategy satisfies $|\mathcal{Y}^*| \leq 2$. ■

Based on Theorem 1, we can discuss the optimal control strategy Γ^* in two cases.

Corollary 1. *When $|\mathcal{Y}^*| = 1$, it corresponds to having equal constraints on $\mathbb{E}(Y|h_0)$ and $\mathbb{E}(Y|h_1)$ as $f_0 = f_1 = f \in \mathcal{Y}$. The minimum KL distance in this case is $r^*_{\text{II}} = 0$. $\mathcal{Y}^* = \{f\}$. The optimal control strategy Γ^* has $p^*_{Y|X,Z,H}(f|x,z,h) = 1$, $\forall \{x,z,h\} \in \mathcal{X} \times \mathcal{Z} \times \mathcal{H}$.*

Theorem 2. *When $|\mathcal{Y}^*| = 2$, $\mathcal{Y}^* = \{\min \mathcal{Y}, \max \mathcal{Y}\}$ and the minimum KL distance in this case is*

$$r^*_{\text{II}} = \frac{f_0 - \min \mathcal{Y}}{\max \mathcal{Y} - \min \mathcal{Y}} \log \frac{f_0 - \min \mathcal{Y}}{f_1 - \min \mathcal{Y}} + \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - \min \mathcal{Y}} \log \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - f_1}.$$

Proof: When $|\mathcal{Y}^*| = 2$, we only need to consider candidate sets with two elements as $\{y_i, y_j\} \subseteq \mathcal{Y}$. Suppose that $y_i < y_j$. To satisfy the constraints in (5), it follows that $y_i \leq \min\{f_0, f_1\} \leq \max\{f_0, f_1\} \leq y_j$ for a candidate set.

Given such a candidate set $\{y_i, y_j\}$, the constraints in (5) and (7) lead to $p_{Y|H}(y_i|h_0)$, $p_{Y|H}(y_i|h_1)$, $p_{Y|H}(y_j|h_0)$, and $p_{Y|H}(y_j|h_1)$ expressed in terms of y_i, y_j, f_0, and f_1 as

$$\begin{aligned} p_{Y|H}(y_i|h_0) &= \frac{y_j - f_0}{y_j - y_i}, \quad p_{Y|H}(y_j|h_0) = \frac{f_0 - y_i}{y_j - y_i}, \\ p_{Y|H}(y_i|h_1) &= \frac{y_j - f_1}{y_j - y_i}, \quad p_{Y|H}(y_j|h_1) = \frac{f_1 - y_i}{y_j - y_i}. \end{aligned} \tag{11}$$

Substitute the obtained pmfs into the objective KL distance. The problem (3) then reduces to the following optimization with $\mathcal{Y}^* = \{y_i^*, y_j^*\}$ as its solution.

$$\min_{\substack{\{y_i, y_j\} \subseteq \mathcal{Y} \\ y_i \leq \min\{f_0, f_1\} \\ y_j \geq \max\{f_0, f_1\}}} \frac{f_0 - y_i}{y_j - y_i} \log \frac{f_0 - y_i}{f_1 - y_i} + \frac{y_j - f_0}{y_j - y_i} \log \frac{y_j - f_0}{y_j - f_1}. \tag{12}$$

Although y_i and y_j in (12) are discrete variables, we can first treat them as continuous. The objective function is differentiable for each of y_i and y_j. It can be shown that the partial derivative $\frac{\partial r_{\text{II}}}{\partial y_i}$ is always non-negative when $y_i \leq \min\{f_0, f_1\}$ and the partial derivative $\frac{\partial r_{\text{II}}}{\partial y_j}$ is always non-positive when $y_j \geq \max\{f_0, f_1\}$. Therefore, in order to minimize the objective, we need to make y_i as small as possible and y_j as large as possible. Then, it can be concluded that $y_i^* = \min \mathcal{Y}$ and $y_j^* = \max \mathcal{Y}$.

Further, the minimum KL distance is $r^*_{\text{II}} = \frac{f_0 - \min \mathcal{Y}}{\max \mathcal{Y} - \min \mathcal{Y}} \log \frac{f_0 - \min \mathcal{Y}}{f_1 - \min \mathcal{Y}} + \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - \min \mathcal{Y}} \log \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - f_1}$. Plugging $y_i^* = \min \mathcal{Y}$ and $y_j^* = \max \mathcal{Y}$ in (11) leads to $p^*_{Y|H}$ achieved by the optimal control strategy Γ^* as $p^*_{Y|H}(\min \mathcal{Y}|h_0) = \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - \min \mathcal{Y}}$, $p^*_{Y|H}(\min \mathcal{Y}|h_1) = \frac{\max \mathcal{Y} - f_1}{\max \mathcal{Y} - \min \mathcal{Y}}$, $p^*_{Y|H}(\max \mathcal{Y}|h_0) = \frac{f_0 - \min \mathcal{Y}}{\max \mathcal{Y} - \min \mathcal{Y}}$, and $p^*_{Y|H}(\max \mathcal{Y}|h_1) = \frac{f_1 - \min \mathcal{Y}}{\max \mathcal{Y} - \min \mathcal{Y}}$. ■

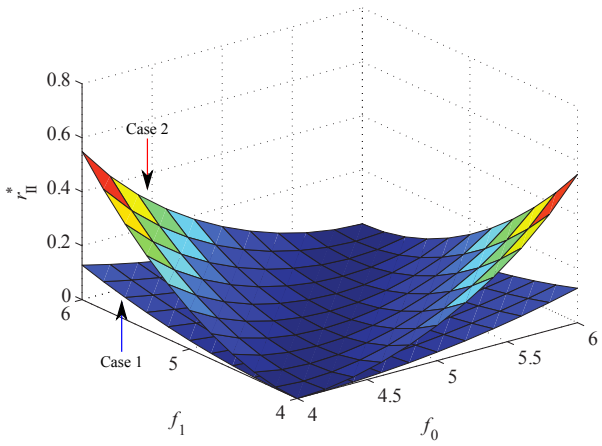

Fig. 2. The minimum KL distance r^*_{II} of the optimal control strategy Γ^* against the constraints on the average energy supply from the energy provider (f_0, f_1) with $f_0, f_1 \in [4, 6]$ for different cases (Case 1: $\min \mathcal{Y} = 1$ and $\max \mathcal{Y} = 9$, Case 2: $\min \mathcal{Y} = 3$ and $\max \mathcal{Y} = 7$). The numerical example shows two ways to enhance the smart meter privacy: increasing the difference $\max \mathcal{Y} - \min \mathcal{Y}$ and decreasing the difference $|f_0 - f_1|$.

Corollary 1 and Theorem 2 reveal how the minimum KL distance r^*_{II} of the optimal control strategy relates with the constraints on the average energy supply from the energy provider (f_0, f_1). This relation is illustrated in Figure 2 through a numerical example.

C. Unauthorized Hypothesis Testing with Side Information

In the previous discussion, the adversary makes the binary hypothesis testing only based on the intercepted smart meter readings of energy supplies from the energy provider. In practice, side information can be available to the adversary. For example, the alternative energy source in the smart grid can be a solar panel and the adversary can have an estimation or the exact information of the solar energy supply Z_t based on the current weather or his own measurement. Here, we consider another privacy problem where all previous settings of the smart grid model still hold and the adversary has additional side information of Z^T.

When the side information Z^T is available, the adversary makes the unauthorized hypothesis testing based on his observations (Y^T, Z^T). The asymptotic exponential decay rate r^{s}_{II} of $p^{\min}_{\text{II}}$ in the Neyman-Pearson detection can be characterized by a KL distance as

$$r^{\text{s}}_{\text{II}} = \mathbb{D}(p_{Y,Z|H}(\cdot|h_0)||p_{Y,Z|H}(\cdot|h_1)).$$

The optimal energy control strategy Γ^* and its conditional pmf $p^*_{Y|X,Z,H} \in \mathcal{P}_{Y|X,Z,H}$ are the solutions of the following problem to minimize the objective KL distance.

$$\min_{p_{Y|X,Z,H} \in \mathcal{P}_{Y|X,Z,H}} \mathbb{D}(p_{Y,Z|H}(\cdot|h_0)||p_{Y,Z|H}(\cdot|h_1)). \tag{13}$$

Similar as the condition (4), we impose the following condition on the optimal energy control strategy Γ^* of the problem (13):

$$p^*_{Y,Z|H}(y,z|h_0)=0 \Leftrightarrow p^*_{Y,Z|H}(y,z|h_1)=0, \forall\{y,z\}\in\mathcal{Y}\times\mathcal{Z}. \tag{14}$$

Compared with the optimal control strategy of the problem (3), Γ^* of the problem (13) has similar properties which can be proved by using similar arguments.

When the alternative energy supply is $z_t=z\in\mathcal{Z}$, for the optimal control strategy Γ^*, define the output set $\mathcal{Y}^*_z\subseteq\mathcal{Y}$ as

$$\mathcal{Y}^*_z=\left\{y: y\in\mathcal{Y}, p^*_{Y,Z|H}(y,z|h_0)\neq 0, p^*_{Y,Z|H}(y,z|h_1)\neq 0\right\}.$$

Theorem 3. *For the optimal control strategy Γ^*, the cardinality of the output set $\mathcal{Y}^*_z$ satisfies $|\mathcal{Y}^*_z|\leq 2$ for any $z\in\mathcal{Z}$.*

This property can be proved by studying the KKT conditions of the problem (13) and using similar arguments in the proof of Theorem 1.

Theorem 4. *When the adversary has the side information Z^T, the minimum KL distance of the problem (13) is*

$$\begin{aligned} r^{\text{s}*}_{\text{II}} =&\frac{f_0-\min\mathcal{Y}}{\max\mathcal{Y}-\min\mathcal{Y}}\log\frac{f_0-\min\mathcal{Y}}{f_1-\min\mathcal{Y}}\\ &+\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-\min\mathcal{Y}}\log\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-f_1}. \end{aligned} \tag{15}$$

Proof: Since the adversary has additional side information Z^T, the privacy risk of information leakage is not lower than the case of having the smart meter readings Y^T only. Therefore, the minimum KL distance can be lower bounded as

$$\begin{aligned} r^{\text{s}*}_{\text{II}}\geq r^{*}_{\text{II}} =&\frac{f_0-\min\mathcal{Y}}{\max\mathcal{Y}-\min\mathcal{Y}}\log\frac{f_0-\min\mathcal{Y}}{f_1-\min\mathcal{Y}}\\ &+\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-\min\mathcal{Y}}\log\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-f_1}. \end{aligned} \tag{16}$$

Given a conditional pmf $p^{\Delta}_{Y|X,Z,H}\in\mathcal{P}_{Y|X,Z,H}$ with

$$\begin{aligned} p^{\Delta}_{Y|X,Z,H}(\min\mathcal{Y}|x,z,h_0)&=\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-\min\mathcal{Y}},\forall x,z,\\ p^{\Delta}_{Y|X,Z,H}(\min\mathcal{Y}|x,z,h_1)&=\frac{\max\mathcal{Y}-f_1}{\max\mathcal{Y}-\min\mathcal{Y}},\forall x,z,\\ p^{\Delta}_{Y|X,Z,H}(\max\mathcal{Y}|x,z,h_0)&=\frac{f_0-\min\mathcal{Y}}{\max\mathcal{Y}-\min\mathcal{Y}},\forall x,z,\\ p^{\Delta}_{Y|X,Z,H}(\max\mathcal{Y}|x,z,h_1)&=\frac{f_1-\min\mathcal{Y}}{\max\mathcal{Y}-\min\mathcal{Y}},\forall x,z, \end{aligned}$$

the minimum KL distance can be upper bounded as

$$\begin{aligned} r^{\text{s}*}_{\text{II}}\leq r^{\text{s}\Delta}_{\text{II}} =&\frac{f_0-\min\mathcal{Y}}{\max\mathcal{Y}-\min\mathcal{Y}}\log\frac{f_0-\min\mathcal{Y}}{f_1-\min\mathcal{Y}}\\ &+\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-\min\mathcal{Y}}\log\frac{\max\mathcal{Y}-f_0}{\max\mathcal{Y}-f_1}. \end{aligned} \tag{17}$$

Combining the bounds in (16) and (17), we can obtain the result in Theorem 4. ■

Theorem 4 shows that the side information Z^T does not help the adversary to increase the privacy risk. Therefore, any degraded knowledge of Z^T cannot help the adversary as well. An intuitive explanation of this result is that the side information Z^T is independent of the hypothesis H.

IV. Conclusion

In this paper, we study the smart meter privacy problem from the Neyman-Pearson hypothesis testing perspective. The optimal energy control strategy manages the energy inflows to satisfy the energy demands and also to suppress the privacy risk by minimizing the asymptotic exponential decay rate of the adversary's minimum Type II error probability. If the constraints on the average energy supply from the energy provider do not differ with the consumer's behaviour, then a constant energy supply from the energy provider is optimal for privacy preserve. When there are different constraints on the average energy supply from the energy provider, it is interesting to note that the privacy is preserved most if the energy is supplied from the energy provider by using the maximum and minimum levels. Moreover, it is shown in our setup that the knowledge about the alternative energy supply does not help the adversary.

References

[1] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 7, pp. 1331–1341, 2013.

[2] E. L. Quinn, "Privacy and the new energy infrastructure," *SSRN*, 2009.

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

[4] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Proceedings of SmartGridComm 2010*, 2010, pp. 327–332.

[5] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proceedings of SmartGridComm 2010*, 2010, pp. 232–237.

[6] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proceedings of ICASSP 2011*, 2011, pp. 1932–1935.

[7] D. Gunduz and J. Gomez-Vilardebo, "Smart meter privacy in the presence of an alternative energy source," in *Proceedings of ICC 2013*, 2013, pp. 2027–2031.

[8] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 837–846, 2013.

[9] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *Smart Grid, IEEE Transactions on*, vol. 6, no. 1, pp. 486–495, 2015.

[10] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Proceedings of FOCS 2013*, 2013, pp. 429–438.

[11] R. F. Barber and J. Duchi, "Privacy: A few definitional aspects and consequences for minimax mean-squared error," in *Proceedings of CDC 2014*, 2014, pp. 1365–1369.

[12] P. Kairouz, S. Oh, and P. Viswanath, "Extremal mechanisms for local differential privacy," eprint arXiv:1407.1338.

[13] R. E. Blahut, *Principles and Practice of Information Theory*. Addison-Wesley, 1987.

[14] Z. Li, T. J. Oechtering, and J. Jaldén, "Parallel distributed Neyman-Pearson detection with privacy constraints," in *Proceedings of ICC 2014 Workshop*, 2014, pp. 765–770.

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