53rd IEEE Conference on Decision and Control
December 15-17, 2014. Los Angeles, California, USA

Privacy and Customer Segmentation in the Smart Grid

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

Abstract— **In the electricity grid, networked sensors which record and transmit increasingly high-granularity data are being deployed. In such a setting, privacy concerns are a natural consideration. In order to obtain the consumer's valuation of privacy, we design a screening mechanism consisting of a menu of contracts offered to the energy consumer with varying guarantees of privacy. The screening process is a means to segment customers. Finally, we design insurance contracts using the probability of a privacy breach to be offered by third-party insurance companies.**

I. Introduction

Increasingly advanced metering infrastructure (AMI) is replacing older technology in the electricity grid. Smart meters send detailed information about consumer electricity usage to the utility company every half-hour, quarter-hour, or in some cases, every five minutes. This high-granularity data is needed to support energy efficiency efforts as well as demand-side management. However, improper handling of this information can also lead to unprecedented invasions of consumer privacy [1], [2].

Given that smart grid operations inherently have privacy and security risks [2], the utility company can benefit by answering the following questions: How do consumers in the population value privacy? How can we quantify privacy? How do privacy-aware policies impact smart grid operations? In this paper we address these questions as well as expose new directions for future research on privacy and customer segmentation in the smart grid.

Using our results on the fundamental limits of non-intrusive load monitoring [3], we use probabilities for the success of an attack by an adversarial agent independent of the algorithm. Then using these probabilities we design a screening mechanism consisting of a menu of contracts to be offered to consumers. One set of contracts to be offered by the utility company assess how the consumer values privacy thereby revealing his preferences. Based on their valuation of privacy as a good, consumers can select the quality of the service contract with the utility company. Essentially, electricity service is offered as a product line differentiated according to privacy where consumers can select the level of privacy that fits their needs and wallet. The screening process is a way to do customer segmentation the result of which can lead to targeting.

L. J. Ratliff, R. Dong, H. Ohlsson, and S. S. Sastry are with Faculty of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, 94707, USA {ratliffl, roydong, ohlsson, sastry}@eecs.berkeley.edu

A. A. Cárdenas is with the Department of Computer Science, University of Texas, Dallas, Dallas, TX 75080, USA alvaro.cardenas@utdallas.edu

In particular, using knowledge of consumer preferences, the utility company can incentivize consumers based on their preferences to choose a low privacy setting which helps increase the granularity of data for use by the utility company for programs like demand response, direct load control, etc. In addition, third-party insurance companies can design insurance contracts. Insurance allows the consumer to protect themselves in the event of a privacy breach, i.e. they will be compensated for any experienced loss.

The paper is organized as follows. In Section II we review notions of privacy metrics and quantification of the utility-privacy tradeoff on the demand-side of the smart grid with the goal of showing that there are methods of determining the likelihood of a privacy breach. This likelihood of a loss occurring can in turn be used in the design of insurance and privacy-based contracts. Further, we summarize existing literature on the quantification of utility-privacy tradeoff when privacy-aware data collection policies are in place thereby motivating the study of privacy-based contracts in demand-side operations. In Section III we use the notion of a privacy metric to design a screening mechanism that consists of privacy contracts between the consumer and the utility company. Similarly, in Section IV we use the privacy metric to design insurance contracts. Finally, in Section V we summarize the results and discuss future research directions.

II. Privacy Metrics

Increasing availability of large amounts of data has motivated research in privacy with a variety of different applications.

One of the common theoretical definitions for a privacy metric is the notion of differential privacy [4], [5]. While differential privacy has many attractive properties, it is most useful when we want to share data via a trusted third party aggregator, or by injecting noise in the original messages sent to a third party; however, for many practical, regulatory, dispute resolution, performance, or business reasons, there will always be several cases where we need to get access to the raw data, and in these cases differential privacy will not help us identify a good security mechanism to prevent raw data from being compromised.

In contrast, we formulated a dynamical system to model the aggregate power consumption of a household as a function of the device usage patterns [6]. We suppose the user has a set of possible inputs, and he wishes to keep the true input private. An example of a privacy breach in this setting might be whether or not an adversary knows if the user is doing dishes in the dishwasher, watching TV, or exercising on a treadmill in the evening. This notion of equivocation is

related to recent work in privacy who measures privacy not with differential privacy but with equivocation metrics [7]. We consider an adversary who is able to observe the AMI signals, knows a superset of the devices present in the house, and knows the dynamics and power consumption signatures of all these devices. For any definition of a privacy breach, we can use results from detection theory to place an upper bound on the probability the adversary is able to infer the private data, independent of the algorithm used by the adversary. The upper bound on the adversary being able to infer private data acts as a worst-case metric for privacy.

Authors in [8] have used tools from information theory such as mutual information for form a metric for privacy. The authors in [9] propose three different notions of privacy metrics: relative entropy, clustering classification, and correlation/regression. In all cases such privacy metrics can be used to determine the likelihood of privacy breach — creating a loss for the invaded party.

A. Utility-Privacy Tradeoff

In other works, researchers have made efforts to quantify the utility-privacy tradeoff in data collection policies.

Intuitively, lowering the sampling rate of advanced metering infrastructure (AMI) data will increase the privacy of smart grid users. However, the performance of smart grid operations naturally degrade as measurements become less frequent.

In our recent work, we quantified both of these tradeoffs [10]. For smart grid operations, we consider a direct load control scheme to track load imbalances. The scheme we consider uses thermostatically controlled loads. We were able to quantify the cost incurred by independent system operators for different sampling rates of user data. For privacy, we used our notion of privacy metric introduced in [3]. A more detailed treatment of this topic is available in [10].

Others have taken an information theoretic approach to quantifying the utility-privacy tradeoff [11]. In all cases, the result of adding privacy-aware data collection policies results in some reduction in the fidelity of the data and hence, in the operations that depend on such data. This motivates the need for privacy-based contracts. Due to the utility-privacy tradeoff, utility companies have a need to incentivize consumers having a high valuation of privacy to allow for higher-fidelity data to be collected as needed by smart grid operations.

III. Privacy Contracts

In this section, we discuss the design of privacy-based contracts to be offered to the consumer by the utility company where the utility company faces a consumer with unknown type.

We consider a model in which there are only two types and we utilize standard results from the theory of screening (see, e.g., [12]) to develop a framework for designing privacy contracts. In general, the fundamental characteristics of the two-type problem extend to the any number of types including a continuum of types. We remark that as a result of the screening process, the utility company will know how each consumer values privacy and can leverage that in the design of incentives aimed at inducing the consumer to select a privacy setting more desirable from the perspective of the utility company. In addition, the screening process can be thought of as customer segmentation since it will extract each consumer's type which can be used for segmentation.

A. Two Types: High-Privacy and Low-Privacy Settings

We model privacy-settings on smart meters as a good. The *quality* of the good is either a high-privacy setting x_H or a low-privacy setting x_L. The consumer can choose either a high privacy setting or a low privacy setting, i.e. the consumer selects $x \in \mathcal{X} = \{x_H, x_L\} \subset \mathbb{R}$ where $-\infty < x_L < x_H < \infty$. The consumer's valuation of privacy is his *type* which takes values $\theta \in \{\theta_L, \theta_H\} \subset \mathbb{R}$ where θ represents how much the consumer values high-privacy over low-privacy and $\theta_L < \theta_H$. We assume that type θ is distinct from the private information itself; by this we mean that how much the consumer values privacy is not also private information. We note here that these types implicitly make use of the metrics for privacy presented in Section II.

The consumer's type θ is related to his willingness to pay in the following way: if the utility company announces a price t for choosing x, the type-dependent consumer's utility is equal to zero if he does not select a privacy setting x, and it is

$$U(x,\theta) - t \geq 0 \tag{1}$$

if he does select a privacy setting. The case in which the consumer does not select a privacy setting is considered the *opt-out* case in which consumer exercises his right to not participate. The inequality in (1) is often called the *individual rationality* constraint. The function $U : \mathbb{R} \times \Theta \to \mathbb{R}$ is assumed to be strictly increasing in (x,θ), concave in x, and represents the consumer's preferences.

Since we have only two types, the contracts offered will be indexed by the privacy settings x_L and x_H. Further, as we mentioned before, the consumer can opt-out by not selecting a privacy option at all. Hence, we need to constrain the mechanism design problem by enforcing the inequality given in Equation (1) for each value of $\theta \in \{\theta_L, \theta_H\}$. In addition, we need to enforce *incentive-compatibility* constraints

$$U(x_H,\theta_H) - t_H \geq U(x_L,\theta_H) - t_L \tag{2}$$

and

$$U(x_L,\theta_L) - t_L \geq U(x_H,\theta_L) - t_H \tag{3}$$

where the first inequality says that given the price t_H a consumer of type θ_H should prefer the high-privacy setting x_H and the second inequality says that given the price t_L a consumer of type θ_L should prefer the low-privacy setting x_L.

The utility company has unit utility

$$v(x,t) = -g(x) + t \tag{4}$$

where we assume that the function $g : \mathcal{X} \to \mathbb{R}$ is the unit cost to the utility company for the privacy setting x. We assume

that it is a strictly increasing, continuous function which is reasonable because, as we have mentioned in Section II, a low-privacy setting x_L provides the utility company with the high-granularity data it needs to efficiently operate and maintain the smart grid.

The screening problem is to design the contracts, i.e. $\{(t_L,x_L),(t_H,x_H)\}$ where $t_L,t_H \in \mathbb{R}$, so that the utility company's expected profit is maximized. The expected profit is given by

$$\Pi(t_L,x_L,t_H,x_H) = (1-p)v(x_L,t_L) + pv(x_H,t_H) \tag{5}$$

where $p = \mathrm{P}(\theta = \theta_H) = 1 - \mathrm{P}(\theta = \theta_L) \in (0,1)$ where $\mathrm{P}(\cdot)$ denotes probability.

In particular, to find the optimal pair of contracts, we solve the following optimization problem:

$$\max_{\{(t_L,x_L),(t_H,x_H)\}} \Pi(t_L,x_L,t_H,x_H) \tag{P-1}$$

$$\begin{aligned}
\text{s.t.} \quad & U(x_H,\theta_H) - t_H \geq U(x_L,\theta_H) - t_L && \text{(IC-1)}\\
& U(x_L,\theta_L) - t_L \geq U(x_H,\theta_L) - t_H && \text{(IC-2)}\\
& U(x_L,\theta_L) - t_L \geq 0 && \text{(IR-1)}\\
& U(x_H,\theta_H) - t_H \geq 0 && \text{(IR-2)}\\
& x_L \leq x_H.
\end{aligned}$$

Depending on the form of $U(x,\theta)$ and $g(x)$, problem (P-1) can be difficult to solve. Hence, we reduce the problem using characteristics of the functions and constraints.

First, we show that (IR-1) is active. Indeed, suppose not. Then, $U(x_L,\theta_L) - t_L > 0$ so that, from the first incentive compatibility constraint (IC-1), we have

$$U(x_H,\theta_H) - t_H \geq U(x_L,\theta_H) - t_L \geq U(x_L,\theta_L) - t_L > 0 \tag{6}$$

where the second to last inequality holds since $U(x,\theta)$ is increasing in θ by assumption. As a consequence, the utility company could increase the price for both types since neither incentive compatibility constraint would be active. This would lead to an increase in the utility company's payoff, i.e. a contradiction.

Now, since $U(x_L,\theta_L) = t_L$, the last inequality in (6) is equal to zero. This implies that (IR-2) is redundant. Further, this argument implies that the constraint (IC-1) is active. Indeed, again suppose not. Then,

$$U(x_H,\theta_H) - t_H > U(x_L,\theta_H) - t_L \geq U(x_L,\theta_L) - t_L = 0 \tag{7}$$

so that it would be possible for the utility company to decrease the incentive t_H without violating (IR-2).

Now, let us assume that the marginal gain from raising the value of the privacy setting x is greater for type θ_H, i.e. $U(x,\theta_H) - U(x,\theta_L)$ is increasing in x. Then, since (IC-1) is active, we have

$$t_H - t_L = U(x_H,\theta_H) - U(x_L,\theta_H) \geq U(x_H,\theta_L) - U(x_L,\theta_L). \tag{8}$$

This inequality implies that we can ignore (IC-2). Further, since U is increasing in (x,θ) and we have assumed that $\theta_H > \theta_L$, we can remove the constraint $x_L \leq x_H$. We have reduced the constraint set to

$$t_H - t_L = U(x_H,\theta_H) - U(x_L,\theta_H) \tag{9}$$

$$t_L = U(x_L,\theta_L). \tag{10}$$

Thus the optimization problem (P-1) reduces to two independent optimization problems:

$$\max_{x_L} \{U(x_L,\theta_L) - (1-p)g(x_L) - pU(x_L,\theta_H)\} \tag{P-3a}$$

$$\max_{x_H} \{U(x_H,\theta_H) - g(x_H)\}. \tag{P-3b}$$

B. Direct Load Control Example

Recall that the unit gain the utility company gets out of the privacy setting x is a function $g : \mathcal{X} \to \mathbb{R}$. In this section, we discuss a particular example in which g is a metric for how access to high-granularity data affects direct load control (DLC).

In [10] we show that the DLC or thermostatically controlled loads (TCLs) degrade in a quadratic way as the duration between samples increases. Hence, this motivates a choice for g such that $g(x_L) > g(x_H)$ and decreases in a linear way. Hence, for this example, let

$$g(x) = \frac{1}{2}\zeta x^2 \tag{11}$$

where $0 < \zeta < \infty$ and $x \in [0,1]$ so that the privacy setting is normalized to live on the zero-one interval. Note that a decreased sampling rate corresponds to a higher privacy setting. The function g as defined is increasing in x so that $g(x_L) > g(x_H)$.

Assume that the consumer's utility is given by

$$U(x,\theta) = x\theta \tag{12}$$

so that the utility of the consumer is proportional to both the privacy setting and its type.

Suppose that the utility company knows the types of the agents. Then, the solution — which we call the *first-best* solution — is characterized by

$$(x_L^\dagger, x_H^\dagger) = \left(\frac{\theta_H}{\zeta}, \frac{\theta_L}{\zeta}\right). \tag{13}$$

Now, let p be the probability that the utility company faces the high-type in the population, i.e. $p = \mathrm{P}(\theta = \theta_H)$. Then, the optimal solutions to the screening problem are

$$(x_H^*, x_L^*) = \left(\frac{\theta_H}{\zeta}, \frac{1}{\zeta}\left[\theta_L - \frac{p}{1-p}(\theta_H - \theta_L)\right]_+\right) \tag{14}$$

where $[\cdot]_+ = \max\{0,\cdot\}$, i.e. $x_L^* = 0$ when $p \geq p^* = \theta_H/\theta_L$. The optimal prices t_H^*, t_L^* can be found by plugging (x_H^*, x_L^*) into (9) and (10).

In Figure 1, we show that as the probability of the high-type being drawn from the population increases, x_L^* decreases away from the firs-best solution $x_L^\dagger$ until $p = p^* = \theta_L/\theta_H$ — the critical probability — after which $x_L^* = 0$.

We can calculate the utility company's expected profit

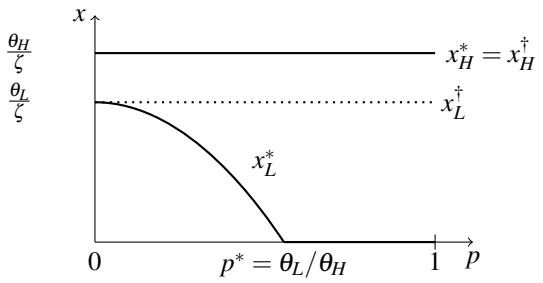

Fig. 1. Comparison between full information and asymmetric information solutions as a function of p the probability of the high-type in the population.

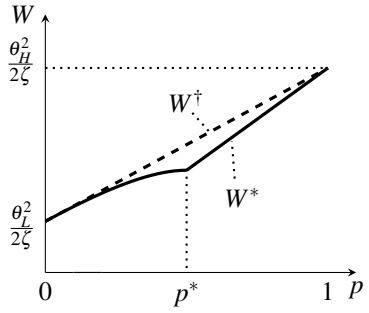

Fig. 2. Social welfare as a function of p. Notice that the social welfare at the first-best solution, $W^\dagger$, is greater than the social welfare under the optimal screening mechanism, W^*. However, this does not imply that individuals are all better off under the first-best solution.

under the optimal screening mechanisms;

$$\Pi(t_L^*, x_L^*, t_H^*, x_H^*) = \begin{cases} \frac{\theta_L^2 + p\theta_H^2 - 2p\theta_L\theta_H}{2\zeta(1-p)}, & p \le p^* \\ \frac{p\theta_H^2}{2\zeta}, & p > p^*. \end{cases} \tag{15}$$

The social welfare is defined to be sum of the pay-off to the utility company and to the consumer and is given by

$$W^*(p) = \Pi(t_L^*, x_L^*, t_H^*, x_H^*) + p(U(x_H^*, \theta_H) - t_H^*); \tag{16}$$

$U(x_L^*, \theta_L) = t_L^*$. In Figure 2, we show the plot of the social welfare for the first-best solution and the optimal screening mechanism. The social welfare reaches a critical point at p^* beyond which the utility company will exclude the low-type from the market and only provide privacy contracts to the high-type. This is called the *shutdown solution*. It is reasonable that as soon as the probability of the utility company facing a consumer of high-type reaches a critical point, they will focus all their efforts on this type of consumer since a high-type desires a higher privacy setting which results in a degradation of the DLC scheme.

We remark that people who value high privacy more need greater compensation to participate in the smart grid. If there are two contracts, then even consumers who do not value privacy much will have an incentive to lie. The screening mechanism induces the consumer to report his type truthfully.

IV. Privacy Insurance Contracts

In this section, we will design an insurance contract, to be offered by a third-party company to the consumer, that uses the probability $1-\eta$ that an adversary will successfully infer private information about the consumer where η can be constructed in practice from any of the privacy metrics mentioned in Section II. In the previous section we designed contracts to get consumers to allow for lower privacy settings; in this section we design insurance contracts that allow consumers to purchase protection against attacks given they know the probability of a successful attack occurring. The analysis that follows is well known in the economics literature (see, e.g., [13], [14], [15]). Our contribution is to show the impact on insurance for privacy in the smart grid.

A. Analysis of Consumer's Decision

Let us suppose that the consumer is *risk-averse*, which means that the consumer, who makes a decision under uncertainty, will try to minimize the impact of the uncertainty on her decision. The function $V : \mathbb{R} \to \mathbb{R}$ is used to model the consumer's risk-aversion and is assumed increasing, twice differentiable, strictly concave and for the sake of analysis we assume $V(0) = 0$. In addition, suppose the consumer has initial wealth y, runs the risk of loss $\ell > 0$ with probability $1-\eta$. In the context of our problem, wealth represents *private information* that can be gained through analysis of consumer energy consumption data, and loss represents exposure of this private information.

Let the cost of one unit of insurance be c and suppose that the insurer pays the consumer β in the event that an adversary attacks them resulting in an exposure of private information where β is the amount of insurance the consumer agrees to buy. The consumer then solves the following optimization problem:

$$\max_{\beta \ge 0} \{\eta V(y - \beta c) + (1-\eta) V(y + (1-c)\beta - \ell)\}. \tag{P-4}$$

We characterize the consumer's decision in the following two propositions. First, suppose that $\beta^* \ge 0$ is a local optimum, then there exists a Lagrange multiplier $\lambda \ge 0$ such that

$$\begin{cases} 0 = -\lambda - \eta c V'(y - \beta^* c) \\ \qquad\quad + (1-\eta)(1-c)V'(y + (1-c)\beta^* - \ell) \\ 0 = \lambda \beta^*. \end{cases} \tag{17}$$

These conditions are the Karush-Khun-Tucker (KKT) necessary conditions. Since $\lambda \ge 0$, from the first condition we get

$$0 \ge -\eta c V'(y - \beta^* c) + (1-\eta)(1-c)V'(y + (1-c)\beta^* - \ell). \tag{18}$$

Proposition 1: Suppose that the consumer is offered privacy insurance at the rate $c = 1-\eta$, i.e. at a rate equal to the probability of a successful attack. Then the consumer will choose to purchase an amount of insurance equal to the loss, i.e. $\beta^* = \ell$.

Proof: Since $c = 1-\eta$ and $(1-\eta)\eta \ge 0$, (18) reduces

to

$$0 \geq V'(y+\eta\beta^*-\ell)-V'(y-\beta^*(1-\eta)). \tag{19}$$

Since V is strictly concave, its derivative V' is decreasing. Hence, for $\ell > 0$,

$$V'(z) < V'(z-\ell). \tag{20}$$

Thus (19) and (20) imply $\beta^* > 0$. Now, we claim that $\beta^* = \ell$. Indeed, suppose that $0 < \beta^* < \ell$, then from (19) we have

$$V'(y+\eta\beta^*-\ell) \leq V'(y+\eta\beta^*-\beta^*) \tag{21}$$

which violates (20). On the other hand, suppose that $0 \leq \ell \leq \beta^*$, then from (20) we have

$$V'(y+\eta\beta^*-\beta^*) > V'(y+\eta\beta^*-\ell), \tag{22}$$

but this violates the KKT inequality (19). Hence, $\beta^* = \ell$. ■

Proposition 2: Suppose that the consumer is offered insurance at the rate $c > 1-\eta$, i.e. at a rate higher than the probability of a successful attack. Then the consumer will not purchase the full insurance, i.e. $\beta^* < \ell$.

Proof: Suppose that the consumer is offered privacy insurance at a rate $c > 1-\eta$ and that the optimal choice for the consumer is $\beta^* = \ell \geq 0$. Then, first-order optimality conditions imply that

$$-\eta V'(y-\ell c)c + (1-\eta)V'(y-\ell c)(1-c) = 0. \tag{23}$$

However, since $c > 1-\eta$ and V is increasing, from (18) we have

$$(-\eta c + (1-\eta)(1-c))V'(y-\ell c) < 0 \tag{24}$$

so that, in fact, the optimal β has to be less than the loss experienced, i.e. $\beta^* < \ell$. ■

We remark that what is interesting about the characterization of the consumer's decision is that whether or not they will fully insure depends on the relationship between the unit cost of insurance and the likelihood of a successful attack which, in turn, depends on the privacy metric and the privacy-aware data collection policies. This warrants further investigation into the exact relationship between the privacy metric and the data collection policy as it greatly impacts both the contracting and the insurance problems. We leave this for future work.

B. Analysis of the Insurer's Decision

We consider a scenario in which the insurer faces two types: a high-risk consumer θ_r and low-risk consumer θ_s. That is to say we are assuming that there is a portion of the population that is more likely to be attacked, i.e. the risky consumers, possibly because they engage in high-risk behavior, e.g. selecting a low-privacy setting contract with the utility company. With probability $1-\eta_j$ the consumer faces a breach of privacy resulting in a loss $\ell > 0$ where $j = r,s$ indicates the consumer's type. We assume that $1-\eta_s < 1-\eta_r$ — this is reasonable since we expect a high-risk consumer will have a higher likelihood of attack. Again, η_j is the probability of a successful attack and in practice can be constructed via a privacy metric. The insurer has a prior over the distribution of types characterized by $p = P(\theta = \theta_r)$ and $1-p = P(\theta = \theta_s)$.

Consider a consumer of type i. An insurance contract (α_a^i, α_n^i) is defined such that α_a^i is the compensation given that a successful attack occurred and α_n^i is the neutral case (no attack). Let X^i be a random variable representing the consumer's wealth such that with probability $1-\eta_i$ it takes value $y-\ell+\alpha_a^i$ and with probability η_i it takes value $y-\alpha_n^i$. Then the consumer's expected utility is

$$E[V(X^i)] = (1-\eta_i)V(y-\ell+\alpha_a^i) + \eta_i V(y-\alpha_n^i) \tag{25}$$

Note that in the previous subsection we analyzed the consumer's decision given a insurance contract of the form

$$(\alpha_a^i, \alpha_n^i) = ((1-c)\beta, \beta c). \tag{26}$$

The insurer solves a screening problem subject to incentive compatibility and individual rationality constraints:

$$\begin{aligned}
\max_{\{(\alpha_a^j,\alpha_n^j)\}_{j=r,s}} \quad & \Pi(\alpha_a^h, \alpha_n^h, \alpha_a^l, \alpha_n^l) && \text{(P-5)}\\
\text{s.t.} \quad & (1-\eta_i)V(y-\ell+\alpha_a^i) + \eta_i V(y-\alpha_n^i) \\
& \geq (1-\eta_i)V(y-\ell+\alpha_a^j) + \eta_i V(y-\alpha_n^j), \\
& \quad i,j \in \{r,s\},\ i \neq j && \text{(IC-i)}\\
& (1-\eta_i)V(y-\ell+\alpha_a^i) + \eta_i V(y-\alpha_n^i) \\
& \geq (1-\eta_i)V(y-\ell) + \eta_i V(y),\ i \in \{r,s\} && \text{(IR-i)}
\end{aligned}$$

where

$$\begin{aligned}
\Pi(\alpha_a^r, \alpha_n^r, \alpha_a^s, \alpha_n^s) = & p\left(-(1-\eta_r)\alpha_a^r + \eta_r\alpha_n^r\right) \\
& + (1-p)\left(-(1-\eta_s)\alpha_a^s + \eta_s\alpha_n^s\right).
\end{aligned} \tag{27}$$

Since $1-\eta_s < 1-\eta_r$, as in Section III-A, the incentive compatibility condition for the high-risk type and the individual rationality constraint for the low-type are active:

$$\begin{aligned}
& (1-\eta_r)V(y-\ell+\alpha_a^r) + \eta_r V(y-\alpha_n^r) \\
& \quad = (1-\eta_r)V(y-\ell+\alpha_a^s) + \eta_r V(y-\alpha_n^s) && \text{(IC-r)}\\
& (1-\eta_s)V(y-\ell+\alpha_a^s) + \eta_s V(y-\alpha_n^s) \\
& \quad = (1-\eta_s)V(y-\ell) + \eta_s V(y). && \text{(IR-s)}
\end{aligned}$$

Since we have assumed that V is strictly concave, increasing and twice differentiable, let W be its inverse where $W' > 0$ and $W'' > 0$. Further, let $V_a^i = V(y-\ell+\alpha_a^i)$ and $V_n^i = V(y-\alpha_n^i)$. The transformed utility is

$$\begin{aligned}
\widetilde{\Pi}(V_a^r, V_n^r, V_a^s, V_n^s) = & p\big(-\eta_r W(V_n^r) - (1-\eta_r)W(V_a^r) \\
& + x - (1-\eta_r)\ell\big) + (1-p)\big(-\eta_l W(V_n^s) \\
& - (1-\eta_s)W(V_a^s) + x - (1-\eta_s)\ell\big).
\end{aligned} \tag{28}$$

Then problem (P-5) becomes

$$\begin{aligned}
\max_{\{(V_a^i,V_n^i)\}_{i=r,s}} \quad & \widetilde{\Pi}(V_a^r, V_n^r, V_a^s, V_n^s) && \text{(P-6)}\\
\text{s.t.} \quad & (1-\eta_r)V_a^r + \eta_r V_n^r = (1-\eta_r)V_a^s + \eta_r V_n^s \\
& (1-\eta_s)V_a^s + \eta_s V_n^s = (1-\eta_s)V(y-\ell) + \eta_s V(y).
\end{aligned}$$

The Lagrangian of the optimization problem is

$$\begin{aligned} L(V_a^r, V_n^r, V_a^s, V_n^s, \lambda_1, \lambda_2) &= \widetilde{\Pi}(V_a^r, V_n^r, V_a^s, V_n^s) \\ &+ \lambda_1((1-\eta_r)V_a^r + \eta_r V_n^r - (1-\eta_r)V_a^s - \eta_r V_n^s) \\ &+ \lambda_2((1-\eta_s)V_a^s + \eta_s V_n^s - (1-\eta_s)V(y-\ell)). \end{aligned} \quad (29)$$

Proposition 3: Given the probabilities $1-\eta_j$, $j = r,s$ that the consumer of type j will experience a privacy breach, if the insurer solves the optimization problem (P-6), then the high-risk consumer will be fully insured and the low-risk consumer will not be fully insured.

Proof: We first show that the risky type will be fully insured. Taking the derivative of the Lagrangian with respect to V_a^r and V_n^s we get the following two equations:

$$0 = -p(1-\eta_r)W'(V_a^r) + \lambda_1(1-\eta_r) \quad (30)$$

$$0 = -p\eta_r W'(V_n^r) + \lambda_1 \eta_r \quad (31)$$

which together imply that $V_a^r = V_n^r$ so that $\ell - \alpha_a^r = \alpha_n^r$, i.e. the amount the high-risk type pays for insurance is equal to the compensation minus the loss in the event of a privacy breach. Thus, the high-risk type will be fully insured.

Now, we claim that the low-risk type will not be fully insured. Taking the derivative of the Lagrangian with respect to V_a^s and V_n^s, we get

$$0 = (1-\eta_s)(1-p)W'(V_a^s) + \lambda_1(1-\eta_r) - \lambda_2(1-\eta_s) \quad (32)$$

$$0 = -(1-p)\eta_s W'(V_n^s) - \lambda_1\eta_r + \lambda_2\eta_s. \quad (33)$$

From (30), we have $\lambda_1 = pW'(V_a^r)$ so that (32) and (33) give us

$$\begin{aligned} 0 =& W'(V_a^r)p\left(-\eta_r + \eta_s\frac{1-\eta_r}{1-\eta_s}\right) \\ &+ \eta_s(1-p)(W'(V_a^s) - W'(V_n^s)). \end{aligned} \quad (34)$$

Since $\eta_s > \eta_r$ and W' is increasing by assumption, the above equation implies that $V_n^s - V_a^s > 0$ and hence, the low-risk type does not fully insure. ∎

The above proposition tells us that in order to keep the high-risk type from masking as a low-risk type, the insurer must make the contract for the low-risk type unappealing to the high-risk type.

We remark that the analysis in this section can be applied to the case where the utility company is purchasing insurance as well. In particular, if the utility company has not invested in a lot of security or they are not following the best practices recommendations, e.g. NIST-IR 7628 [16], then they are engaging in *risky* behavior. The insurance company will not know a priori whether or not the utility company is high-risk type. Through the design of insurance contracts, the insurance company can asses the utility's type while offering contracts that maximize their own utilty.

V. Conclusion

Using privacy metrics along with the upper bound on the probability for a successful privacy breach, we design a screening mechanism for the problem of obtaining the consumer's type when there is asymmetric information. Further, we design insurance contracts using the probability of successful privacy breach given that in the population of consumers there is both high-risk and low-risk consumers.

This work opens up a number of questions in the area of privacy metrics as well as customer segmentation and targeting. In particular, deriving η from the existent privacy metrics and studying their effect on the performance of the contracts is an interesting avenue for investigation and is practically relevant. In addition, we considered that the utility would offer a contract solely based on privacy settings whereas in reality the contract would normally contain additional items such as maximum power consumption, rate, etc. Consumers in the population may value these goods differently. In this setting, the screening problem would be come multi-dimensional [17]. We are exploring this in the context of privacy-aware incentive design for behavior modification.

References

[1] E. L. Quinn, "Smart metering and privacy: Existing laws and competing policies," Colorado Public Utilities Commission, Tech. Rep., 2009.

[2] M. Salehie, L. Pasquale, I. Omoronyia, and B. Nuseibeh, "Adaptive security and privacy in smart grids: A software engineering vision," in *International Workshop on Software Engineering for the Smart Grid*, June 2012, pp. 46–49.

[3] R. Dong, L. Ratliff, H. Ohlsson, and S. S. Sastry, "Fundamental limits of nonintrusive load monitoring," *Proceedings of the 3rd ACM International Conference on High Confidence Networked Systems*, 2013.

[4] C. Dwork, "Differential privacy," in *Proceedings of the International Colloquium on Automata, Languages and Programming*. Springer, 2006, pp. 1–12.

[5] J. Le Ny and G. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[6] R. Dong, L. J. Ratliff, H. Ohlsson, and S. Sastry, "Energy disaggregation via adaptive filtering," in *Proceedings of the 51st Annual Allerton Conference on Communication, Control, and Computing*, Oct 2013, pp. 173–180.

[7] R. Shokri, G. Theodorakopoulos, J. Le Boudec, and J. Hubaux, "Quantifying location privacy," in *IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 247–262.

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

[9] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *First IEEE International Conference on Smart Grid Communications*, 2010, pp. 232–237.

[10] R. Dong, A. A. Cárdenas, L. J. Ratliff, H. Ohlsson, and S. S. Sastry, "Quantifying the utility-privacy tradeoff in the smart grid," *arxiv*, no. 1406.2568v1, 2014.

[11] S. Rajagopalan, L. Sankar, S. Mohajer, and H. Poor, "Smart meter privacy: A utility-privacy framework," in *IEEE International Conference on Smart Grid Communications*, 2011, pp. 190–195.

[12] T. A. Weber, "Optimal control theory with applications in economics," *MIT Press Books*, vol. 1, 2011.

[13] M. Rothschile and J. Stiglitz, "Equilibrium in competitive insurance markets: An essay on the economics of imperfect information," *The Quarterly Journal of Economics*, vol. 90, no. 4, pp. 629–6459, 1976.

[14] G. D. Jaynes, "Equilibria in monopolistically competitive insurance markets," *Journal of Economic Theory*, vol. 19, no. 2, pp. 394 – 422, 1978.

[15] M. Mussa and S. Rosen, "Monopoly and product quality," *Journal of Economic Theory*, vol. 18, no. 2, pp. 301 – 317, 1978.

[16] Smart Grid Interoperability Panel Cyber Security Working Group and others, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," NIST, Tech. Rep., 2010.

[17] S. Basov, "Multidimensional screening," in *Studies in Economic Theory*. Springer, 2005, vol. 22.