The Price of Privacy in Real-time Electricity Markets

Christos Dimitrakakis Maryam Kar

July 11, 2017

1 Introduction.

We consider the problem of privacy for households participating in smart grid system. From the point of view of the households, there are two distinct problems: firstly, how much privacy do they lose in general by participating in an online price mechanism? Secondly, given that they participate in the mechanism, how much privacy can they expect with respect to their household occupancy?

Here we analyse both a Cournot and a Bertrand pricing model for electricity markets from the point of view of achieving consumer privacy. This requires us to deviate slightly fro the equilibrium prices in order to protect sensitive information.

1.1 A Bertrand model for electricity demand pricing

Here we have an actual demand function $x(p)$ at a given price level p. We must differentiate between posted demand a_t and the actual demand x_t, as the price p_t is determined by the posted demand, and later households decide how much to actually consume based on the posted price. Finally, we define a utility function for the posted price level, in order to measure our loss due to deviation from equilibrium.

$$x_t = x(p_t, a_t) = a_t - \zeta p_t \qquad \text{(demand function)}$$
$$u(p_t) = (p_t - c)[x(p_t) + \beta_t] = (p_t - c)(a_t - \zeta p_t + \beta_t). \qquad \text{(utility)}$$

MK: who's utility function is this? Why the utility is not p_t times the actual demand? it seems to me demand should follow the price, not price following the demand! :)

CD: Replying in the actual text below:

Here, players post a planned demand $x_t = (x_t^i)_{i=1}^n$ corresponding to their type. Then the provider selects a price level p_t, taking into account the fact that the actual demand x_t of the players is going to depend on the price and their asked demand through the elasticity ζ. The provider's utility is simply the profit per unit of electricity sold, times the total demand of electricity, with c being the fixed unit cost of production.

MK: What is the interpretation of the "c" here?

[1] Within this model, the optimal price level is

$$p_t^* = \frac{1}{2}\left(\frac{a_t + \beta_t}{\zeta} + c\right),$$

which intuitively represents a price level halfway between the cost of the electricity production and the satisfiable demand with the given elasticity.

[1] Note that in the previous model, demand seemed to increase with price, but the causation is inverse, it's just that the intercept of the two lines moves in this way: when there is more demand there are more buyers willing to pay the higher price. In our setting, the market may not clear.

MK: Ok, but this is the same price function we had before..just relabeling of the constants.

CD: Yeah, we get the same linear price structure, but there is a separation between planned demand and actual demand. I guess that at equilibrium, the planned and actual demand are the same. However, but I think the Bertrand model gives a slightly different Nash equilibrium.

As the price signal is public, it is possible that the electricity provider leaks information about individual consumption. For that reason, we consider differentially private pricing mechanisms.

1.2 Privacy model.

Consider a mechanism like the above that, given the demanded consumption x_t^i of households i at times t, decides upon a price level p_t for that time period, which depends on x_t. As the mechanism's price level is public knowledge, it can leak private information about demand (or consumption). For that reason, we shall consider price-setting algorithms that have privacy guarantees.

Planned consumption privacy. If the mechanism for determining the price level is ϵ-differentially private for period t, the we must have

$$\left| \ln \frac{\mathbb{P}(p_t \mid a_t)}{\mathbb{P}(p_t \mid a_t')} \right| \leq \epsilon$$

where $a_t = (a_t^1, \ldots, a_t^n)$ is a vector of bids and/or consumptions of individual households for the t-th time period and a_t' is a vector where the data of one individual is added or missing. However this only protects us against one time period: for T periods, this only guarantees $T\epsilon$ differential privacy.

Demand privacy. If there is no public signal associated with demand, then we need not consider privacy. However, smart metering technology may involve storing consumption data locally. If the electricity provider has access to the detailed data, this can severely violate privacy. If the provider only has limited query access to the smart meter, then it is easier to control the privacy loss.

CD: How can we guarantee that the provider only has limited access?

MK: I remember we talked about this and you mentioned we can trust the provider but consider info leaking from price. it makes sense to me to start with this consideration.

2 Private mechanisms for planned consumption

Privacy can be achieved within each period through a differentially private mechanism. The simplest one to use is the exponential mechanism, which works with the utility of the decision maker. Alternative methods involve using a differentially private version of the total planned consumption, and selecting the optimal response for this.

2.1 The exponential mechanism.

This would mean that, at each step t, we choose a price p with probability

$$\mathbb{P}(p \mid a_t) \propto \exp(\epsilon(p-c)[x(p) + \beta_t]/\Delta), \tag{1}$$

where $\Delta = 1/\zeta - c$, is the sensitivity of the utility function with respect to one customer's data changing.

Lemma 1. *Under bounded consumption, with $a_t^i \in [0,1]$, prices bounded in $[0, 1/\zeta]$ but unbounded price, a mechanism selecting prices according to the exponential mechanism is ϵ-differentially private with respect to individual planned consumption at time t.*

Proof. A single customer will change a_t by at most 1. This will alter u by at most $(p_t - c)$. As prices must be bounded in $[0, 1/\zeta]$ and $\Delta = 1/\zeta - c$, the exponent is ϵ-Lipshitz. Hence sampling from this exponential distribution is ϵ-DP. □

Interpretation. In this setting, prices are a linear function of planned consumption. Even though prices and total consumption are necessarily bounded, the sensitivity of the utility to one person's change remains the same, no matter how many people are in the population.

2.2 The noisy sum mechanism.

We can use the idea of a noisy sum to calculate prices. This can be efficiently implemented in a distributed manner through a tree structure that also guarantees local differential privacy to each participant. In the simplest case, we can simply add noise to the total ask:

$$\hat{a}_t = a_t + \varepsilon_t, \qquad \varepsilon_t \sim \text{Laplace}(1/\epsilon). \tag{2}$$

Lemma 2. *With probability $1-\delta$, our realised utility is within $O(\epsilon \ln(1/\delta))$ of the non-private utility. In addition, our expected utility is identical to that of the non-private utility.*

Proof. The Laplace distribution has exponential tails and so $\mathbb{P}(|\varepsilon_t| > k) < \exp(-k/\epsilon)$. Hence, with probability at least $1 - \delta$, the error in our noisy ask is

$$k = \epsilon \ln(1/\delta).$$

Since the utility is a linear function of the total ask a_t and price, and the price is bounded, the first result follows. Finally, note that the expectation of Laplace noise is zero. Combined with linearity, the result follows as well. □

An advantage of the noisy sum mechanism is that it can also confer local privacy, by adding some noise to each individual's ask.

2.3 An illustration.

Here we compare the exponential and Laplace mechanisms for a fixed ask in the linear price model. The exponential mechanism needs the price and utility model as an input. The Laplace mechanism used here, simply adds noise to the total ask.

Figure 1 shows see the effect of price changes on the utility, as well as the effect of ϵ on the average price and utility. Higher values of ϵ definitely increase our utility, and bring the expected price level closer to the optimal. We can see that the two mechanisms produce comparable results.

A Deleted scenes

A.1 A Cournot model.

In Cournot-type models, price depends on the total demand.

This dependence can be any increasing function. The consumers submit their demand schedule, and the price structure is published. The question is whether a given can learn anything about others' consumptions or hidden variables (occupancy for example) based on observing the price.

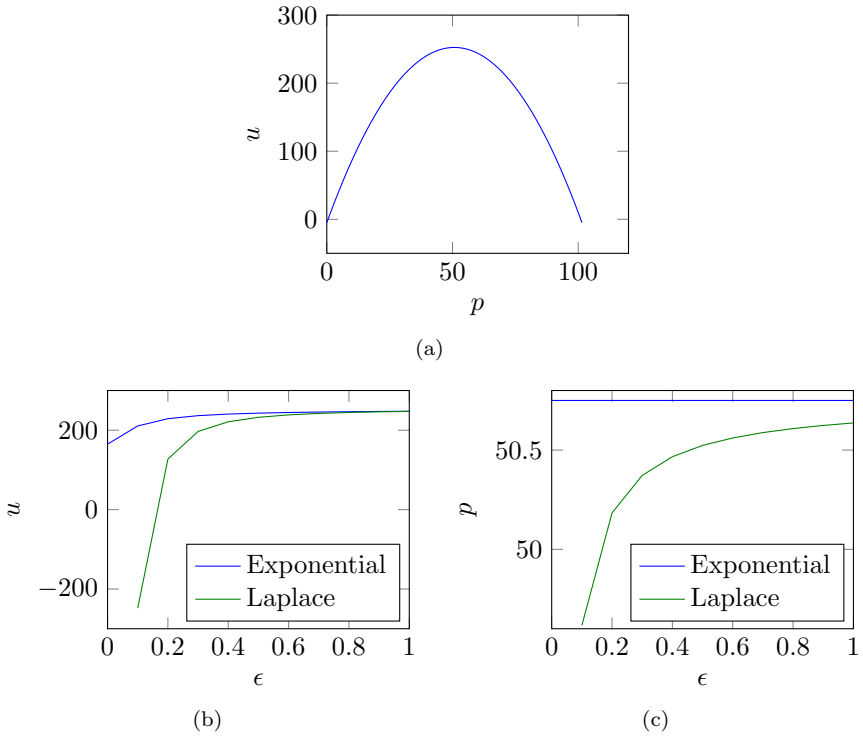

Figure 1: Figure1(a) shows the effect of prices on the expected utility of the provider. Figures 1(b) and 1(c) show the effect of the privacy parameter ϵ on the expected utility and price respectively, for the Exponential and Laplace mechanisms. All the results are for elasticity $\zeta = 0.1$, ask $a_t = 10$, cost $c = 0.5$, and baseline $b = 0.1$.

Let the central utility have a quadratic loss function based on total demand $x_t \triangleq \sum_i x_t^i$ of users $i = 1, \ldots, n$, at time t.

$$\ell_t(x) = c(x_t + \beta_t)^2/2, \tag{3}$$

where β_t is a fixed demand term, that must be met independently. Then, for a large number of players, the price

$$p_t = c(x_t + \beta_t), \tag{4}$$

ensures that at the Nash equilibrium minimises ℓ_t, and that the individual cost is

$$c_t^i = p_t x_t^i. \tag{5}$$

For the sake of the argument, I will assume that our utility function is going to be

$$u(x, p) = px - c(x + \beta)^2/2 \tag{6}$$