Privacy vs. Pricing for Smart Grids

Stojan Z. Denic, Georgios Kalogridis, and Zhong Fan
The Telecommunications Research Laboratory
Toshiba Research Europe Limited, Bristol, UK, BS1 4ND
e-mails: {stojan.denic, george, zhong.fan}@toshiba-trel.com

***Abstract*—In this paper, problems of privacy protection and power pricing for a new generation of electric power networks are addressed simultaneously. For an adopted electric power cost function, effects of the application of a privacy algorithm are studied. It is illustrated that a privacy algorithm can affect the price of the electric power by modulating the consumer's demand. It turns out that the effect is more pronounced for the networks with high uncertainty and inefficiency in power production.**

***Keywords*-Smart grid privacy; pricing**

I. Introduction

The smart grid is a recent paradigm representing a large number of different technologies aiming at revitalizing the electric power network. One of the goals of the smart grid is to bring intelligence into the existing aging network to improve its efficiency and robustness such that it will be more capable to respond to new higher consumption demands. (It is expected that the electric power consumption will be tripled worldwide by 2050 [1].) One way to achieve this is to employ communication networks which will enable the scanning of the power network state and carrying out appropriate actions to provide its stability and functionality.

Other factors that necessitate this metamorphosis is the introduction of renewable resources and electric vehicles into the network. The power production based on the renewable resources, such as solar and wind energy, may experience rapid changes due to weather conditions. This may cause large voltage variations which is not desirable from the point of view of the network stability. On the other hand, the electric vehicles represent a considerable new load, but in the same time they can serve as storage units for energy.

The new nature of the electric power network in terms of the production uncertainty and digitalization will affect overall network design including two network features, privacy and electric power price. The focus of this paper is an interplay between the consumer privacy protection and pricing of the electric power subject to the previous conditions which characterize the new electric power networks.

A. Contributions

To study the effect of privacy algorithms on the pricing of the electric power, we adopt the pricing model found in [2]. This model relates the price with the power consumer demand, and in the same time reflects the efficiency (or equivalently, uncertainty) of the power production. We employ the algorithm found in [3], and compute the price of the electric power for a given demand. This price is compared with the price when the algorithm is not used.

The results and contributions of this paper are the following:

- We use a Markov chain (which has already been tested in [4] for a single user power consumption modeling) to model a consumer group demand.
- The privacy algorithm is applied for different number of users, different sizes of batteries and for different levels of the network efficiency.
- Empirical cumulative distribution functions for the electric power demand and electric power price are computed for different model parameters.
- Relative changes in the power price which compare the case when the privacy algorithm is used and not used are computed for different battery sizes and different power production efficiencies.
- The effect of the new network architecture on the privacy algorithms applications is discussed.

The paper is organized as follows. Section II contains background material on the smart grid privacy and the pricing of the electric power. Section III gives the privacy system model. Section IV describes how the consumers' demand can be modeled by Markov chains. Section V introduces the electric power price model. In Section VI, the simulation results are provided accompanied with the result discussion. Section VII gives concluding remarks.

II. Related Work

A. Consumer Privacy Protection

As mentioned above, the main assumption for the functioning of the smart grid is its ability to collect and store the information from the network continuously (such as power consumption) at even household level with increased granularity [5]. Although current policy regulations in the US and elsewhere are restrictive from the point of view of the collected data reuse [5], the storage of these data gives a possibility of their misemployment. If, in addition, the collected and stored data become available to other parties (besides utility companies) such as law enforcement agencies, marketing and malicious individuals, this could represent a privacy and security risk for consumers. A potential threat can be illustrated by the following example; the amount of information obtained from the household smart metering data may be demonstrated with the use of non-intrusive appliance load monitors (NALM), which analyze collected power consumption data to track appliance usage patterns [6], [7]. The

 ISBN: 978-1-61208-136-6

author of [8] argues that frequently collected metering data, e.g. at 15 minute intervals, may provide a window into the activities within homes, exposing a wealth of private activities to anyone with access to energy usage information.

To protect privacy, Kalogridis et al. [3] proposed a simple home power load management scheme. The power flow within a home may be controlled by running a portion of a consumption demand off a rechargeable battery, rather than directly off the grid. That is, smart metering data privacy can be protected by using a battery to mask power usage profiles.

B. Pricing of Electric Power and Privacy

As shown in [3], a consequence of the privacy algorithm usage is that it modifies the probability distribution of a power consumption (demand) as seen by the utility company. Because the electric power production cost depends on the demand [2], this means that the price of the electric power production can be different comparing to the case when the privacy algorithms are not used. Even more, in the smart grid, other factors to influence the probability distribution of the demand are the renewable resources and the battery storage implying that the privacy algorithms are only one part of this price equation.

That is why the goal of this paper is to explore to what extent the privacy protection can modulate the consumers' demand and the price of the electric power.

III. SMART GRID PRIVACY SYSTEM MODEL

A. Appliance load signature masking

In this section we give a brief overview of the privacy protection scheme introduced in [3]. The system assumes the existence of 1) An energy storage facility, such as Electric Vehicle (EV), and 2) An 'electrical power routing' mechanism, where this term is taken to mean the selective control and power mixing of a number of electricity sources to cover consumption demands [9]. The system may be implemented with a rechargeable battery and a bidirectional inverter to optimize the flow and storage of electricity. Optionally, the system may also control energy generated locally from photovoltaic (PV) panels or wind turbines.

An overview of the privacy system can be seen in Fig. 1, comprising the following sub-systems.

- *Metering mechanism*: is used to obtain a set of electricity measurements from the smart meter or from smart appliances.
- *Event detection*: analyzes metering data in order to detect an occurring, or predict an imminent, event that may contain 'privacy information'. For example, this may be a power trigger generated by a particular event, such as a change in power consumption (e.g. appliance switch-on/off event).
- *Privacy protection algorithm*: configures power routing to mask a detected consumption event. Different protection settings may be edited with the help of an *in-home display* (IHD).

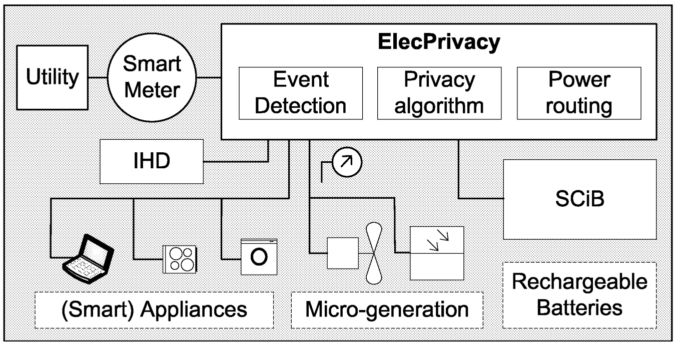

Fig. 1. Privacy protection system overview.

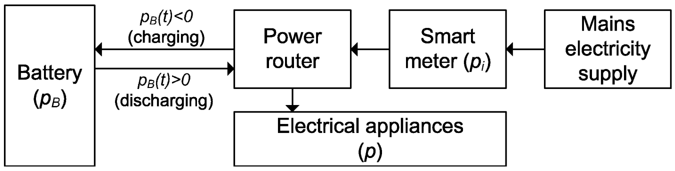

Fig. 2. Battery power mixing moderation model.

- *Power routing*: mixes a private (i.e. non-utility) energy resource (e.g. rechargeable battery) with utility energy to meet appliance demands.

The main objective is to 'detect a privacy threat' and respond by 'configuring power routing' in order to mask appliance load signatures. For simplicity, we assume that the system can perform such tasks in real-time.

B. Privacy protection water-filling algorithm

We consider the simple case where a battery is discharged or recharged with a $p_B(t)$ average power over a Δt metering interval in order to 'disguise' a given consumption load $p(t)$. With the use of battery power mixing, the home power trace becomes $p_i = p - p_B - p_L$, where $p_L(t)$ is the (average) battery power loss due to charging/discharging during $(t-\Delta t, t)$; this model is illustrated in Fig. 2. (In this paper the assumption is that a battery can fully discharge/recharge without any losses, i.e. $p_L = 0$.) We say that p_i is introduced by a transformation $\mathcal{G}$ on the (real-time) load demand p such that $p_i = \mathcal{G}p$. We then refer to $\mathcal{G}$ as privacy (protection) algorithm.

In our experiments we use the privacy algorithm in [3], which simulates water-filling [10], as outlined in Table I. Energy $e(t)$ denotes the (cumulative) energy consumed up to time t, with $e(0) = 0$, and $p(t) = \frac{e(t)-e(t-\Delta t)}{\Delta t}$.

Suppose that the battery has a finite capacity E_C, and a maximum discharge and recharge power of P_D and P_R, $-P_R \leq p_B(t) \leq P_D$, for all t. The proposed algorithm uses the battery in order to resist against power load changes. That is, the algorithm will force the battery to either discharge or recharge when the required load $p(t)$ is either larger or smaller (respectively) than the previously metered load $p_i(t - \Delta t)$. The power and duration of battery charging/discharging are configured to equal the power differences, unless battery bounds are reached.

 ISBN: 978-1-61208-136-6

TABLE I
BATTERY WATER-FILLING ALGORITHM.

Current battery charge level: $p_B(t) = e_i(t) - e(t - \Delta t) + p(t)\Delta t$
if $D(t) = p(t) - p_i(t - \Delta t) > 0$ (discharging case) **then**
  if There is enough battery energy/power to provide $D(t)$ for Δt **then**
    Mix in battery power so that $p_i(t) = p_i(t - \Delta t)$
  else
    Use maximum battery power while $B(t) > 0$
  end if
end if
if $C(t) = p_i(t - \Delta t) - p(t) > 0$ (charging case) **then**
  if Enough battery 'emptiness' to absorb $C(t)$ for Δt **then**
    Recharge battery so that $p_i(t) = p_i(t - \Delta t)$
  else
    Fully recharge battery
  end if
end if

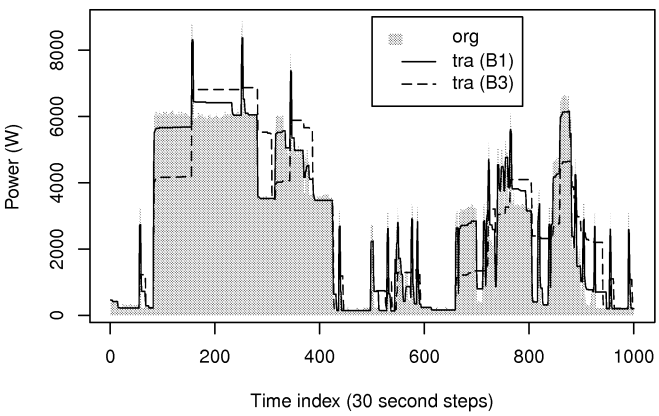

Fig. 3. Load signatures before and after the water-filling algorithm using different batteries: a) $B_1 = 500$W/1kWh and b) $B_3 = 2$kW/4kWh.

The effect of the water-filling algorithm can be seen in Fig. 3: the bigger the battery size, the more p is masked. In Fig. 3, it is assumed that $P_R = P_D$, and the battery is denoted by $B = P_D/E_C$.

IV. POWER CONSUMPTION MODELING

In [4], we demonstrated how a simple Markov chain model could be applied in representing the power consumption within a household. This representation relies on the clustering analysis of the measured data obtained from the measurement campaign performed during 30 days in several apartments [4]. Denote the Markov chain representation by the sequence of Markov chain states $X := \{X(k)\}_{k\geq 0}$, where the state $X(k) \in \{x_1, \dots, x_N\}$. The Markov chain X is completely defined by the transition probability matrix $\mathbf{A}(k)$ and the vector of state probabilities $\mathbf{P}(k) := [\Pr\{X(k) = x_1\}, \dots, \Pr\{X(k) = x_N\}]^T$, where T denotes the transpose of the vector. The transition probability matrix $\mathbf{A}$ contains conditional probabilities $a_{ij} := \Pr\{X(k+1) = x_i | X(k) = x_j\}$. Under the assumption that the power consumption can be described by a stationary process, the evolution of the state probability vector is given by

$$\mathbf{P}(k+1) = \mathbf{A}\mathbf{P}(k), \qquad (1)$$

when $\mathbf{P}(0)$ is known.

It is shown in [4] that an accurate prediction of the power consumption can be carried out via its Markov chain representation. The Markov model is used in Section VI to describe the electric power demand of large number of consumers.

V. ELECTRIC POWER PRICE MODEL

The price model adopted in this paper had already been used in the smart grid literature [11], [12], to adapt power consumption demand in order to optimize its utility function. Next, this model will be briefly described, and for more details, readers are referred to [2].

The price model assumes that there are N_p power producers, which use the same technology to produce the power. Between the power producers and the consumers, there are several retailing companies which buy the power from the producers and sell it to final consumers. Both, the producers and the retailers can sell the power at a current moment or in forward market (in future). When the physical production of the producers is equated to the total retailer demand (which depends on the consumer demand), profit-maximizing price of each producer is given by

$$P_W = a\Big(\frac{Q}{N_p}\Big)^{c-1}. \qquad (2)$$

Here, Q is the total retailer demand, a is a proportionality constant, and $c \geq 2$ is a constant which is related to the energy production efficiency. The expression given by (2) reflects a few important characteristics of the power production. First, the price is an increasing function of the demand Q, which captures the fact that the electric power comes from a variety of different sources such as hydro, nuclear, oil and coal plants each having a different cost of production. Second, when the power comes from inefficient resources, the constant c is chosen to be larger than 2 which implies an increasing price rate vs demand Q. In current systems, c can take value up to 5 [2].

VI. SIMULATION RESULTS ANALYSIS

To study the influence of the privacy algorithm on the price of the electrical power production, we assume that the number of homes (consumers) within one area is 300. According to Section IV, each consumer's power demand is modeled by a Markov chain with appropriately chosen transition probability matrix $\mathbf{A}$. Here, the consumers are considered to have a similar pattern of consumption, and the matrix $\mathbf{A}$ is taken from [4].

It is assumed that each house will apply the same algorithm and a battery of the same size to protect its privacy. The algorithm will be tested for three battery sizes, $B_1 = 500$W/1kWh $B_2 = 1$kW/2kWh and $B_3 = 2$kW/4kWh. It is interesting to note that charging rates for EVs could be from 7kW to 10kW leaving opportunity for usage of larger batteries if needed.

The results are generated in the following way. First, the power demands of all 300 consumers obtained when the privacy algorithm is not applied are summed up, generating the overall cumulative power demand for one area. Thereafter, the price of the electrical power production is obtained from (2) 'on an hourly' (OAH) basis; the time axis of 30 days is divided into the hour intervals, and the value of the cumulative energy demand for each hour interval is replaced in (2). The same procedure is repeated when the privacy algorithm is applied to modulate the demand of each of all 300 consumers. This OAH approach is in line with [2], since the most active electric power markets are for the next-hour and next-day delivery.

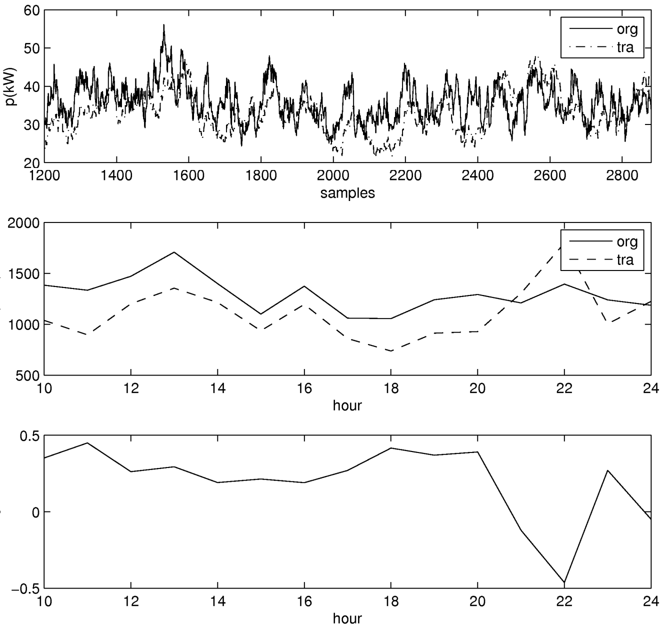

Fig. 4. From top to bottom: 1) The instantaneous power demand for 300 consumers, original and transformed ($p_{\text{org}}(t)$ and $p_{\text{tra}}(t)$), 2) Energy demand, original and transformed ($Q_{\text{org}}(t)$ and $Q_{\text{tra}}(t)$), computed on an hourly basis, 3) The OAH relative price difference between the original and transformed demand $\delta(t)$. The battery size is $B_2 =$ 1kW/2kWh.

Fig. 4 shows the instantaneous power demands ($p_{\text{org}}(t)$ and $p_{\text{tra}}(t)$), the energy demands ($Q_{\text{org}}(t)$ and $Q_{\text{tra}}(t)$), and the OAH relative price difference

$$\delta(t) = (P_{W,\text{org}}(t) - P_{W,\text{tra}}(t))/P_{W,\text{org}}(t) \tag{3}$$

for 300 users for a fraction of time measured (14 hours) out of 30 days. The battery size is $B_2 =$ 1kW/2kWh. The figure compares two cases, when the privacy algorithm is not used (original demand giving rise to the subscript 'org'), and when the privacy algorithm is used (transformed demand giving rise to the subscript 'tra'). It can be seen that due to the application of the privacy algorithm, the OAH price $P_{W,\text{tra}}(t)$ may vary by even 50% ($\delta(t) = \pm 0.5$) as compared to $P_{W,\text{org}}(t)$. Here, the parameter $c = 4$ implying high uncertainty of the electric power production. That the cumulative distribution (cdf) of the transformed demand $f_{Q,\text{tra}}$ is indeed changed as compared to the cdf of the original demand $f_{Q,\text{org}}$ is depicted in Fig. 5 and 6.

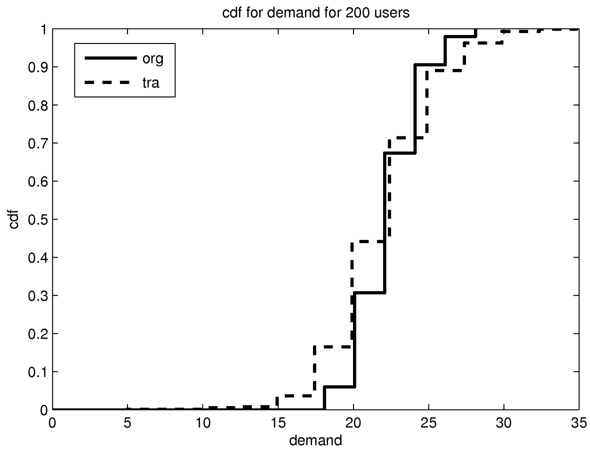

Fig. 5. The cdfs of the demand $f_{Q,\text{org}}$ and $f_{Q,\text{tra}}$ for the 200 consumers.

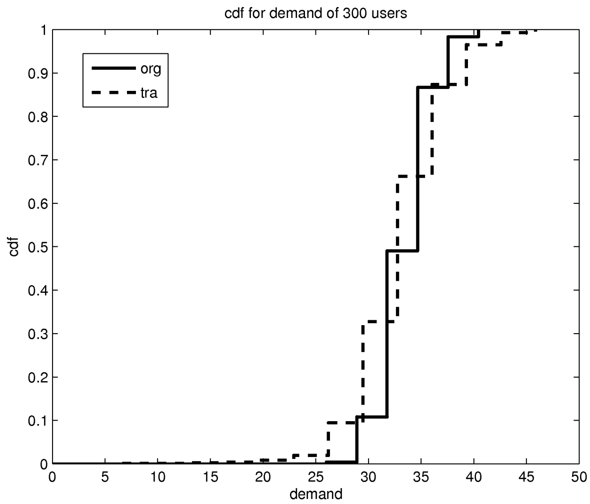

Fig. 6. The cdfs of the demand $f_{Q,\text{org}}$ and $f_{Q,\text{tra}}$ for the 300 consumers.

In addition, the cdfs of the prices $f_{P,\text{org}}$ and $f_{P,\text{tra}}$ are shown in Fig. 7 and 8. For a smaller value of c ($c = 2$ meaning smaller production uncertainty), the difference in the cdf of the original $f_{P,\text{org}}$ and transformed demand $f_{P,\text{tra}}$ is not so obvious. However, when $c = 4$ (meaning larger production uncertainty), the difference between cdfs is obvious as well as the difference between the cases of $c = 2$ and $c = 4$.

The tables II, III and IV contain the relative price differences

$$\delta_m = (P^m_{W,\text{org}} - P^m_{W,\text{tra}})/P^m_{W,\text{org}} \tag{4}$$

of cumulative (30 days) prices between the original and transformed demands for different numbers of the consumers and for 3 different battery sizes. $P^m_{W,\text{org}}$ and $P^m_{W,\text{tra}}$ are the cumulative 30 day prices of the original and transformed demand, respectively. The results suggest that: 1) For larger uncertainty in the electric power production ($c = 4$ or $c = 5$),

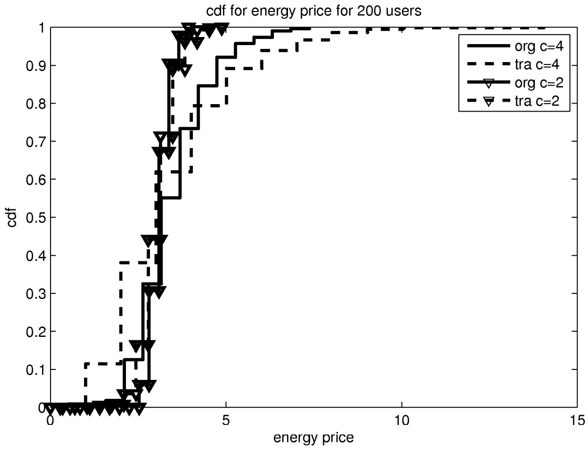

Fig. 7. The cdfs of the price $f_{P,\text{org}}$ and $f_{P,\text{tra}}$ for the 200 consumers.

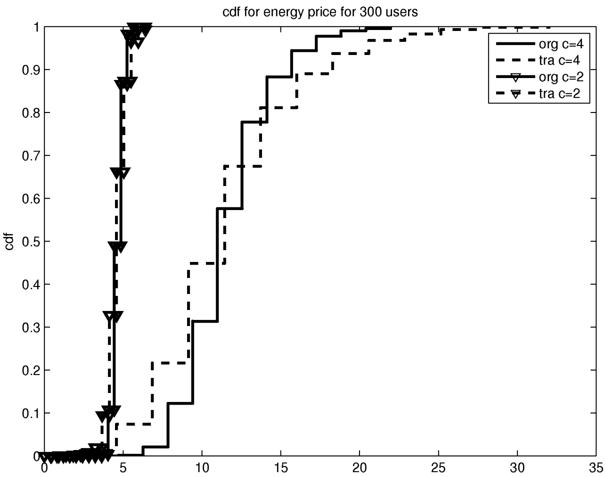

Fig. 8. The cdfs of the price $f_{P,\text{org}}$ and $f_{P,\text{tra}}$ for the 300 consumers.

the relative price difference is susceptible to the value of the consumer number, and it gets smaller as the number of consumers grows, 2) For smaller uncertainty in the production, the relative price difference is small, 3) At least for this example, the price of the transformed demand $P^m_{W,\text{tra}}$ is larger than the price of the original demand $P^m_{W,\text{org}}$ for larger uncertainty ($c = 4$ or $c = 5$) for all three batteries.

TABLE II
CUMULATIVE PRICE RELATIVE DIFFERENCE FOR $B_1 = 500$W/1KWH

Consumer #	100	150	200	250	300
$\delta_m(\%)$ for $c = 2$	0.24	0.26	0.24	0.24	0.23
$\delta_m(\%)$ for $c = 4$	-2.58	-1.65	-1.29	-0.84	-0.61
$\delta_m(\%)$ for $c = 5$	-5.42	-3.68	-2.96	-2.08	-1.62

Hence, we next discuss the influence of two parameters on the price, the number of consumers and the production uncertainty as described by c. The results suggest that if the same pricing model is applied for large number of consumers, the cumulative price for longer time period will be similar regardless of the application of the privacy algorithm. However, it is an open question if this will remain the same when dynamic pricing models (demand-response) are applied per consumer and not to one large group of consumers. From the point of view of the production uncertainty, it could be expected that, due to the presence of the electric vehicles and new sources of the electric power, the parameter c might be larger. Therefore, the effect of the application of privacy algorithms on pricing could be more pronounced.

TABLE III
CUMULATIVE PRICE RELATIVE DIFFERENCE FOR $B_2 = 1$KW/2KWH

Consumer #	100	150	200	250	300
$\delta_m(\%)$ for $c = 2$	0.56	0.62	0.62	0.6	0.6
$\delta_m(\%)$ for $c = 4$	-6.42	-3.82	-2.66	-1.87	-1.25
$\delta_m(\%)$ for $c = 5$	-14.06	-8.8	-6.46	-4.81	-3.54

TABLE IV
CUMULATIVE PRICE RELATIVE DIFFERENCE FOR $B_3 = 2$KW/4KWH

Consumer #	100	150	200	250	300
$\delta_m(\%)$ for $c = 2$	0.68	0.69	0.69	0.66	0.64
$\delta_m(\%)$ for $c = 4$	-3.7	-1.69	-1.05	-0.46	-0.29
$\delta_m(\%)$ for $c = 5$	-8.52	-4.5	-3.32	-2.07	-1.66

Although, the cumulative price relative difference δ_m is small for long time interval, it is interesting to notice that OAH relative price difference $\delta(t)$ can be large. For three different battery sizes discussed earlier and $c = 4$, $\delta(t) \in [-0.56, 0.89]$ for B_1, $\delta(t) \in [-1.35, 0.97]$ for B_2 and $\delta(t) \in [-1.48, 0.98]$ for B_3. Therefore, it seems that this interval size increases as the battery size increases. This instantaneous difference could be important for the electric power producers and retailers when they negotiate the deal between themselves.

VII. CONCLUSION

The smart grid should transform existing electric power network into very efficient, robust and flexible network which will use some of the latest achievements in the communication and control engineering and computational science. This paper considers the interaction between two important problems related to the design of the smart grid, privacy and pricing. We show by means of simulations that privacy algorithms affect the cdf of consumers' demand, and in that way can change the price of the electric power production. The level of influence depends on: 1) The size of the network, 2) The efficiency of the power production (through the parameter c) and 3) The length of the observation interval. This could be of interest to electrical power producers, retailers and designers.

ACKNOWLEDGMENT

The authors would like to thank the Directors of the Toshiba Telecommunications Research Laboratory for their support.

REFERENCES

[1] K. Kowalenko, "The smart grid: a primer," *IEEE The Institute Newsletter*, vol. 34, no. 4, page 5, Dec. 2010.

[2] H Bessembinder and M. Lemmon, "Equilibrium pricing and optimal hedging in electricity forward markets," *Journal of Finance,* pp. 1347–1382, Jun. 2002.

[3] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," *Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm10)*, Maryland, USA, Oct. 4-6 2010, pp. 232–237.

[4] G. Kalogridis, S. Z. Denic, T. Lewis, and R. Cepeda, "Privacy protection system and metrics for hiding electrical events," *Int. J. Security and Networks*, vol. 6, no. 1, 2011, in press.

[5] M. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security Privacy*, vol. 8, no. 1, pp. 11-20, Jan. 2010.

[6] C. Laughman, D. Lee, R. Cox, S. Shaw, S. B. Leeb, L. K. Norford, and P. Armstrong, "Advanced nonintrusive monitoring of electric loads," *IEEE Power Energy Mag.*, pp. 56-63, 2003.

[7] H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A novel method to construct taxonomy electrical appliances based on load signatures," *IEEE Trans. on Consum. Electron.*, vol. 53, no. 2, pp. 653-660, 2007.

[8] E. L. Quinn, "Privacy and the New Energy Infrastructure," Feb 2009. [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract\id=1370731

[9] N. V. Nedap, "The power router," Sep 2010. [Online]. Available: http://www.powerrouter.com

[10] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, Inc. New York, NY, USA, 2006.

[11] Z. Fan, "Distributed demand response and user adaptation in smart grids," to appear in the *12th IFIP/IEEE International Symposium on Integrated Network Management (IM'11)*, Dublin, Ireland, May 2011, in press.

[12] C. Wang and M. de Groot, "Managing end-user preferences in the smart grid," *Proceedings of the First International Conference on Energy-Efficient Computing and Networking (e-Energy10)*, 2010, pp. 105–114.