# A Privacy-Friendly Game-Theoretic Distributed Scheduling System for Domestic Appliances

Cristina Rottondi, Antimo Barbato, and Giacomo Verticale
Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Piazza Leonardo da Vinci, 32, Milano, Italy
{giacomo.verticale, cristinaemma.rottondi, antimo.barbato}@polimi.it

***Abstract*—Game-theoretic Demand Side Management (DSM) systems have been investigated as a decentralized approach for the collaborative scheduling of the usage of domestic electrical appliances within a set of households. Such systems allow for the shifting of the starting time of deferrable devices according to the current energy price or power grid condition, in order to reduce the individual monthly bill or to adjust the power load experienced by the grid while meeting the users' preferences about the time of use. The drawback of DSM distributed protocols is that they require each user to communicate his/her own energy consumption patterns to the other users, which may leak sensitive information regarding private habits.**

**This paper proposes a distributed Privacy-Friendly DSM system which preserves users' privacy by integrating data aggregation and perturbation techniques: users decide their schedule according to aggregated consumption measurements perturbed by means of Additive White Gaussian Noise (AWGN). We evaluate the noise power and the size of the set of users required to achieve a given privacy level, quantified by means of the Kullback-Leibler divergence. The performance of our proposed DSM system are compared to the ones obtained by a benchmark system which does not support privacy preservation in terms of social cost, peak demand and convergence time. Results show that privacy can be preserved at the cost of increasing the peak demand and the number of game iterations, whereas social cost is only marginally incremented.**

***Index Terms*—Smart Grid; Demand Side Management; Privacy-Friendly Load Scheduling.**

## I. Introduction

In the past few years, Demand-Side Management (DSM) has garnered increasing interest because of its potential impact in the sustainable development of power grids. DSM is a proactive approach aimed at managing the load demand of users based on the needs of both customers and power grid. [1]. Nowadays, the power demand is largely uncontrollable and is mainly driven by habits of users, who are unaware of the grid requirements. By properly redistributing loads, it would be possible to increase the efficiency of the whole power system. Specifically, DSM can have several benefits, among which increasing the amount of Renewable Energy Sources (RESs) that can be connected to the grid [2] by mitigating issues related to demand-supply balancing, power quality and unintentional islanding [3], preventing power outages and curtailing the grid capacity and investment [4].

The residential sector represents a promising area to apply DSM solutions [5], since it accounts for approximately 30% of the total electricity demand [6]. Residential users can be incentivized to properly optimize their demand through the adoption of dynamic pricing. In this case, the electricity price may exhibit hourly changes and reflects the costs incurred by the system to satisfy the users' demand (e.g., higher price during peak hours and lower price in off-peak hours). Consequently, tariffs evolve based on the conditions of the power system and the efficiency of the grid can be improved through minimization of the users' bills [7]. Game Theory is a key analytical tool to design decentralized DSM systems based on dynamic pricing, since it can model complex interactions among the independent rational players of the power grid [8].

The drawback of traditional game-theoretic DSM approaches is that they require users to communicate their own energy consumption patterns to the other players: even if aggregated over multiple appliances and on hourly basis, such data can still reveal the type of electrical devices in use [9], [10], which in turn leaks sensitive information regarding the private habits of the dwellers. Spatial aggregation over multiple households and data perturbation by means of noise injection are two countermeasures which have been already combined with the aim of enhancing privacy in the context of smart metering data collection (see, e.g., [11]).

In this paper, we formalize the notion of $\gamma$-**privacy** as a measure of the privacy of the users participating in a distributed game-theoretical privacy-friendly DSM system aimed at reducing their daily electricity bill. We define a communication protocol which allows for game interactions while integrating both data aggregation and perturbation techniques. We also analyze the impact of the size of the player set and the statistical characterization of the noise to be added to the individual consumption patterns in order to guarantee a given privacy threshold, evaluated by means of the Kullback-Leibler divergence. Moreover, we evaluate the degradation of the protocol performance caused by the alteration of the players' data due to noise injection by comparing it to a benchmark system which does not support privacy preservation.

The remainder of the paper is structured as follows: Section II provides a short overview of the related literature, whereas Section III describes the privacy-preserving scheduling framework. The attacker model is discussed in Section IV. The security analysis and the performance assessment of our

The work in this paper has been partially funded by the Italian Ministry of Education, University and Reserach (MIUR) project SHELL and by Regione Lombardia under grant no. 40545387 Smart Campus as Urban Open LAbs (SCUOLA).

proposed infrastructure are provided in Section V. Conclusions are drawn in the final Section.

## II. Related Work

Game-theoretic methods for DSM have been widely studied in the recent literature, since they can properly represent the interactions among the rational players of the power grid [8]. Specifically, game theory has been used to design distributed demand-management frameworks, where decisions are made locally by users. The goal of these solutions is to improve the efficiency of the whole power grid by reducing the peak of the aggregated demand [12] and the users' bills [13], as well as by increasing the amount of RESs connected to the grid [14]. Despite the effort in designing DSM systems based on game theory, only a few of them have specifically addressed the privacy preservation of the data exchanged within the participants. Moreover, the security assumptions modeling the adversarial entities which attempt to access users' data are quite various and most often too loose with respect to realistic attack scenarios. Paper [15] proposes a distributed architecture in which multiple Home Energy Management (HEM) units collaborate with each other in order to keep the demand and supply balanced in their neighbourhood by solving a multi-stage stochastic optimization problem. The proposed system hides the users' individual information to any external entity (e.g., energy provider or grid manager) but requires the customers to communicate their power schedules to their neighbours. Conversely, paper [16] avoids data exchange among households, but assumes a trusted energy utility to collect the individual power consumption curves and to broadcast price information which are updated at every game iteration. Our solution is completely decentralized and does not involve additional nodes besides the local HEM systems, thus, in our scenario, the adversarial entities are represented by the game players themselves.

Papers [17], [13] assume that exchanging aggregated power consumption data at household level (e.g., on hourly basis) is sufficient to hide the usage patterns of single electric appliances to untrustworthy neighbours. However, several studies on Non-Intrusive Load Monitoring (see, e.g., [18], [19]) prove that the power consumption patterns of individual appliances can easily be inferred from house-aggregated measurements. Data perturbation is an approach which is widely employed in combination to data aggregation in order to counteract such kind of attacks: the authors of [20] propose a secure game-theoretical framework for distributed appliance scheduling, which provides integrity and accountability to the messages exchanged among the players. The protocol also includes a multi-party computation scheme which allows a single player to obtain the aggregate consumption curve of all the remaining players by exposing a noisy version of his individual power consumption data, obtained by adding a random amount (either positive or negative) to the actual consumption. However, no discussion on the statistical characterization of the added noise is proposed, whereas in our study we evaluate the dependency of the privacy level on the power of the injected noise. The same paper discusses how to prevent dishonest nodes from cheating by declaring increased electric energy usages. Though our paper assumes that players behave according to an honest-but-curious adversary model, such countermeasures can be easily integrated in our framework.

Data perturbation in the context of energy management systems is achieved in [21] by relying on batteries installed at the customers' premises, which can be configured to disguise the actual appliance electricity consumption. That paper also defines three similarity metrics computed over the load consumption curves to evaluate the trade-off between energy cost minimization and information privacy leakages. Our scenario does not assume the usage of batteries and quantifies the achieved privacy level by means of the Kullback-Leibler divergence, which is computed from the probability density function of the stochastic process modeling the energy consumption curve, and not from the realizations of the process.

## III. The Privacy-Friendly Loads Scheduling Framework

In this paper, we consider a generic smart grid model in which a group of residential users, $\mathcal{U}$, has to efficiently allocate its power demand over a 24-hour time period divided into a set, $\mathcal{T}$, of time slots. We assume that each end-user $u \in \mathcal{U}$ has a set of non-preemptive electric appliances, $\mathcal{A}_u$, that must be executed only once during the day. Each appliance $a \in \mathcal{A}_u$ is characterized by a load profile having a duration of $N_a$ time slots. The power consumption of $a$ in the $n$th time slot of its load profile (with $n \in \mathcal{N}_a = \{1, 2.., N_a\}$), $l_{an}$, is constant within the time slot. Each user $u$ has to decide the starting time slot of each appliance $a$ within a time window delimited by a minimum starting-time slot, $ST_{au}$, and a maximum ending-time slot, $ET_{au}$. The price of electricity at time $t \in \mathcal{T}$, $c_t$, is modelled as an increasing function of the total power demand, $y_t$, of the group of users $\mathcal{U}$ at time $t$. The objective of each user is to minimize his daily bill by means of optimally scheduling the usage of his/her appliances.

### A. Load Scheduling Game

The load scheduling problem is modelled as a game $\mathbf{G} = \{\mathbf{U}, \{\mathbf{I_u}\}_{u\in\mathcal{U}}, \{\mathbf{P_u}\}_{u\in\mathcal{U}}\}$, defined by: the *players* representing the users in the set $\mathcal{U}$, the *strategy* of each player $u$, $\mathbf{I_u}$, corresponding to his/her loads scheduling, and the *utility function* of each user $u$, $\mathbf{P_u}$, which coincides with his/her daily electricity bill. Specifically, the strategy of the player $u$ is $\mathbf{I_u} \triangleq \{x_{at}\}_{a\in\mathcal{A}_u}$, where $x_{at}$ are binary variables defined for each appliance $a \in \mathcal{A}_u$ and for each time slot $t \in \mathcal{T}$. These variables are equal to 1 if the appliance $a$ starts in the time slot $t$, 0 otherwise. The utility function of each player, $\mathbf{P_u}$, is defined as a function of $\mathbf{I} \triangleq \{\mathbf{I_u}\}_{u\in\mathcal{U}}$ as follows:

$$\mathbf{P_u}(\mathbf{I}) = \sum_{t\in\mathcal{T}} y_{ut} \cdot c_t(y_t) \tag{1}$$

where $y_{ut}$ represents the amount of electricity bought by user $u$ at time $t$ and is a function of $x_{at}$, whereas $c_t$ is a function of $y_t = \sum_{u \in \mathcal{U}} y_{ut}$, which represents the total power demand of the players at time $t$ .

Let $\mathbf{P}$ be the total price paid by all the players to the electricity retailer. One can prove that $\mathbf{G}$ is a potential game if $c_t(y_t)$ is convex with respect to $y_t$, with $\mathbf{P}(\mathbf{I})$ being the potential function. Potential games have several properties, such as the existence of at least one pure Nash equilibrium. Furthermore, such games have the Finite Improvement Property (FIP): any sequence of asynchronous improvement steps is finite and converges to a pure equilibrium. Particularly, the sequence of best response update converges to a pure equilibrium.
In this paper, we assume that $c_t(y_t)$ is linear with respect to $y_t$, thus the load scheduling game is a potential game. As a consequence, best response dynamics always converge to a Nash equilibrium. Moreover, we consider a simple implementation of the best response dynamics: each player, in an iterative fashion, defines his optimal loads scheduling strategy based on electricity tariffs (calculated according to the strategies of the other players) and communicates his energy plan (i.e., his daily power demand profile) to the next user of the set $\mathcal{U}$[1]. At every iteration $j \in \mathcal{J}$ of the best response dynamics, energy prices are updated and, as a consequence, other users can decide to modify their schedules. In the $j$th iteration, the optimal schedule of the user $u$ is obtained by solving the following Mixed Integer Non-linear Programming (MINLP) model:

$$\min \sum_{t \in \mathcal{T}} \left( c_t^j \cdot y_{ut}^j \right) \tag{2}$$

$$s.t. \sum_{t=ST_{au}}^{ET_{au}-N_a+1} x_{at}^j = 1 \qquad \forall a \in \mathcal{A}_u \tag{3}$$

$$y_{ut}^j = \sum_{a \in \mathcal{A}_u} \sum_{\substack{n \in \mathcal{N}_a: \\ n \leq t}} l_{an} x_{a(t-n+1)}^j \qquad \forall t \in \mathcal{T} \tag{4}$$

$$y_{ut}^j \leq \pi \qquad \forall t \in \mathcal{T} \tag{5}$$

$$c_t^j = c^{MIN} + s(y_{ut}^j + p_{ut}^j) \qquad \forall t \in \mathcal{T} \tag{6}$$

The objective function (2) minimizes the daily bill of the user $u$. Constraints (3) guarantee that each appliance $a \in \mathcal{A}_u$ starts in exactly one time slot and is carried out in the required interval $[ST_{au}, ET_{au}]$. Constraints (4) determine the overall consumption of the appliances in each time slot at iteration $j$, which depends on the scheduling strategy. Constraints (5) limit the amount of purchasable power, according to the capacity of electricity meters, $\pi$. Finally, constraints (6) guarantee that the electricity price $c_t^j$ at iteration $j$ in each time slot $t \in \mathcal{T}$ is a linear increasing function of the total demand of the group of users $\mathcal{U}$. Specifically, in constraints (6), $p_{ut}^j$ is the total demand of the other players of the set $\mathcal{U}$ received by user $u$ at game iteration $j$, whereas $c^{MIN}$ is the minimum electricity price and $s$ is the slope of the cost function.

The iterative process is repeated until convergence is reached. Note that the number of iterations required to reach convergence (i.e., $|\mathcal{J}|$) may vary for different instances of the game.

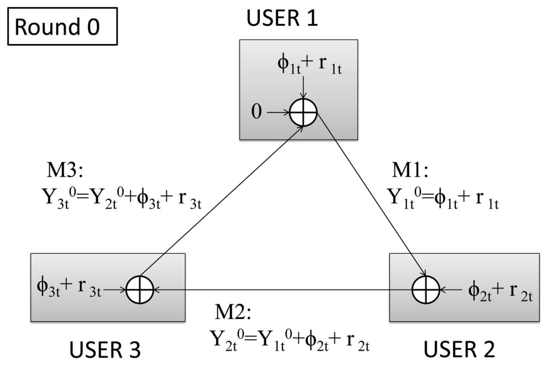
Round 0
USER 1
$\phi_{1t}$+ r $_{1t}$
0
M3:
$Y_{3t}{}^0$=$Y_{2t}{}^0$+$\phi_{3t}$+ r $_{3t}$
M1:
$Y_{1t}{}^0$=$\phi_{1t}$+ r $_{1t}$
$\phi_{3t}$+ r $_{3t}$
$\phi_{2t}$+ r $_{2t}$
M2:
$Y_{2t}{}^0$=$Y_{1t}{}^0$+$\phi_{2t}$+ r $_{2t}$
USER 3
USER 2

Fig. 1: The privacy-friendly communication protocol: initialization round

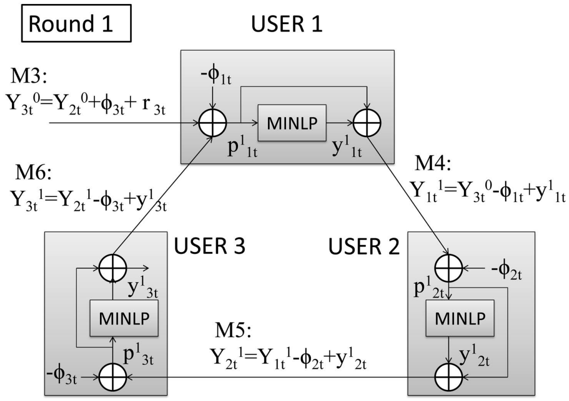
Round 1
USER 1
M3:
$Y_{3t}{}^0$=$Y_{2t}{}^0$+$\phi_{3t}$+ r $_{3t}$
-$\phi_{1t}$
MINLP
$p^1{}_{1t}$
$y^1{}_{1t}$
M6:
$Y_{3t}{}^1$=$Y_{2t}{}^1$-$\phi_{3t}$+$y^1{}_{3t}$
M4:
$Y_{1t}{}^1$=$Y_{3t}{}^0$-$\phi_{1t}$+$y^1{}_{1t}$
USER 3
USER 2
$y^1{}_{3t}$
MINLP
$p^1{}_{3t}$
-$\phi_{3t}$
-$\phi_{2t}$
$p^1{}_{2t}$
MINLP
$y^1{}_{2t}$
M5:
$Y_{2t}{}^1$=$Y_{1t}{}^1$-$\phi_{2t}$+$y^1{}_{2t}$

Fig. 2: The privacy-friendly communication protocol: first round

### B. The Privacy-Friendly Scheduling Protocol

We now detail the communication protocol run during the execution of the load scheduling game presented in Section III-A. During an initialization round (numbered as 0), each player $u$ generates two sequences $\phi_{ut}, r_{ut}$ $\forall t \in \mathcal{T}$, where $r_{ut} \sim N(0, \sigma^2)$ is a random variable representing AWGN noise with zero mean and variance $\sigma^2$ and the sequence $\phi_{ut}$ for $t = 1, \ldots, \mathcal{T}$ is an arbitrary partition of the quantity $\sum_{a \in \mathcal{A}_u, n \in \mathcal{N}_a} l_{an}$, i.e.:

$$\sum_{t \in \mathcal{T}} \phi_{ut} = \sum_{a \in \mathcal{A}_u, n \in \mathcal{N}_a} l_{an} \tag{7}$$

Then, the first player (user 1) initializes a sequence $\mathcal{Y}_u^j = [Y_{u1}^j, \ldots, Y_{u|\mathcal{T}|}^j]$ as $Y_{1t}^0 = \phi_{1t} + r_{1t}$ $\forall t \in \mathcal{T}$ and forwards it to the second player (user 2), who updates it by adding to each variable $Y_{1t}^0$ the corresponding quantity $r_{2t} + \phi_{2t}$ (see Fig. 1). The procedure is repeated for all the players, until user 1 obtains the final aggregated sequence of elements $Y_{|\mathcal{U}|t}^0 = \sum_{u \in \mathcal{U}} \phi_{ut} + r_{ut}$. Note that, since $\phi_{ut}$ are arbitrarily chosen and $r_{ut}$ are random variables, the quantity $r_{ut} + \phi_{ut}$ does not leak any information about the preferential usage periods $[ST_{au}, ET_{au}]$ of each appliance $a \in \mathcal{A}_u$. Constraint

[1] We assume that the order in which the players execute the protocol within a single game iteration is predefined and fixed for the whole duration of the game, which provides higher fairness w.r.t random ordering.

(7) imposes that the overall declared electricity usage is consistent with the actual cumulative power consumption of the appliances to be scheduled. Once the initialization round is completed, user 1 begins the first game round and calculates the parameters $p_{1t}^1$ as:

$$p_{1t}^1 = Y_{|\mathcal{U}|t}^0 - \phi_{1t} \qquad \forall t \in \mathcal{T} \tag{8}$$

and solves the MINLP problem described in Section III-A. Then, it computes:

$$Y_{1t}^1 = p_{1t}^1 + y_{1t}^1 \qquad \forall t \in \mathcal{T} \tag{9}$$

where $y_{1t}^1$ is outputted by the MINLP solver, and forwards it to the next player (see Fig. 2). This way, user $u$ replaces the partition $\phi_t \forall t \in \mathcal{T}$ with his/her own energy consumption curve, aggregated over all the appliances he/she owns and computed according to optimal solution of the MINLP problem. This procedure is repeated by all the users until completion of the first round of the game. In the following $j$th iterations (where $j \geq 2$), each user $u$ behaves analogously, by replacing Formula (8) with:

$$p_{ut}^j = Y_{(u-1)t}^j - y_{ut}^{j-1} \qquad \forall t \in \mathcal{T}$$

where $y_{ut}^{j-1}$ is the overall energy consumption pattern of user $u$ computed according to the most recent schedule (i.e., the schedule obtained at the $(j-1)$th iteration), and by applying Formula (9) as follows:

$$Y_{ut}^j = p_{ut}^j + y_{ut}^j \qquad \forall t \in \mathcal{T}$$

It results that, at the $j$th round, $p_{ut}^j$ is the sum of the current total energy consumption pattern (aggregated over the whole set of users) and of the AWGN noise injected by each of the users during the initialization round.

## IV. Attacker Model

We assume a scenario where the players behave according to the *honest-but-curious* attacker model: they honestly execute the protocol but try to infer the preferred time of use of the owners of active electrical appliances (i.e., the time windows $[ST_{au}, ET_{au}]$ of each appliance $a$ used by every user $u$)[2].

For the sake of easiness, we assume that each player runs a single appliance, i.e. $|\mathcal{A}_u| = 1 \forall u \in \mathcal{U}$ and that all the appliances are of the same type, i.e. they have the same energy consumption profile, which is public and known to all the players. Moreover, we assume that the duration of the time interval $[ST_{au}, ET_{au}]$ is set to $D$ time slots, i.e. $ET_{au} = ST_a + D \ \forall u \in \mathcal{U}, a \in \mathcal{A}_u$ and that $ST_{au}$ is a random variable with uniform distribution in $[1, \mathcal{T} - D]$.

**Definition** Consider a randomly chosen malicious player $u_m \in \mathcal{U}$ and a target player $u_o$ within the set $\mathcal{U} \setminus \{u_m\}$. Let $\mathcal{G}_0, \mathcal{G}_1$ be two instances of the scheduling problem: the former includes the time windows $[ST_{au}, ET_{au}]$ of the appliance $a$ used by every player $u \in \mathcal{U}$, the latter includes the time preferences expressed by all the players $u \in \mathcal{U} \setminus \{u_o\}$ and an additional user owning one appliance with time window $[ST', ET']$, where $ST'$ has the same statistical characterization of the uniform random variables $ST_{au}$. This way, the target user $u_o$ is substituted by a random user belonging to the same population of the users in $\mathcal{U}$. It follows that the two instances $\mathcal{G}_0, \mathcal{G}_1$ differ by exactly one time window ($[ST_{au_o}, ET_{au_o}]$ in $\mathcal{G}_0$ is replaced by $[ST', ET']$ in $\mathcal{G}_1$). Let $\mathbf{v_0}, \mathbf{v_1}$ be two $k$-dimensional multivariate random variables, where $k = |\mathcal{T}| \cdot J$ and $J = \max(|\mathcal{J}_0|, |\mathcal{J}_1|)$, defined as $\mathbf{v_b} = [p_{u_m 1}^{1\mathcal{G}_b}, \cdots, p_{u_m |\mathcal{T}|}^{1\mathcal{G}_b}, \cdots, p_{u_m 1}^{J\mathcal{G}_b}, \cdots, p_{u_m |\mathcal{T}|}^{J\mathcal{G}_b}]$, where $p_{u_m t}^{j\mathcal{G}_b}$ are $J$ sequences of $|\mathcal{T}|$ aggregated energy consumption measurements received by $u_m$ at each iteration of the load scheduling game performed over instance $\mathcal{G}_b$ with $b \in \{0, 1\}$ following the privacy-preserving protocol described in Section III-B (in case $|\mathcal{J}_b| < J$, we set $p_{u_m t}^{j\mathcal{G}_b} = p_{u_m t}^{|\mathcal{J}_b|\mathcal{G}_b} \ \forall t \in \mathcal{T}, j\colon |\mathcal{J}_b| < j \leq J$). We now define the function $f(\mathcal{G}_0, \mathcal{G}_1, u_m, u_o)$ as follows:

$$f(\mathcal{G}_0, \mathcal{G}_1, u_m, u_o) = D_{KL}(Q_0, Q_1)$$

where $Q_0, Q_1$ are the probability density functions of the multivariate variables $\mathbf{v_0}, \mathbf{v_1}$ and $D_{KL}$ indicates the Kullback-Leibler divergence operator. The architecture provides $\gamma$-**privacy** to the user $u_o$ if, for a given $u_m$, it holds that:

$$f(\mathcal{G}_0, \mathcal{G}_1, u_m, u_o) \leq \gamma \qquad \forall \mathcal{G}_0, \mathcal{G}_1 \tag{10}$$

Intuitively, the lower is the divergence between the two density function, the harder it is to discriminate among them. Therefore, a low divergence makes it hard to detect whether user $u_o$ belongs to the set of players. Thus, the lower is the value of $\gamma$ computed by means of Formula 10, the higher is the privacy provided to the user.

In the next Section, we will numerically evaluate the privacy level achieved by our proposed privacy-friendly DSM system, depending on the cardinality of the set of users and on the standard deviation $\sigma$ of the injected noise.

## V. Numerical Assessment

In this section, we first describe the methodology used in our tests, then we present the numerical results and the security analysis obtained by applying Privacy-Friendly DSM method on realistic instances defined according the Italian power grid parameters and standard consumer profiles [22], [23].

### A. Tests Methodology

In our tests, the 24-hour time horizon is represented by a set $\mathcal{T}$ of 24 time slots of 1 hour each. Each user, connected to the grid with a power limit, $\pi$, of 3 kW, has 1 appliance (i.e., washing machine) whose load profile, $l_{an}$, and activity duration, $N_a$ are the same for all players $\mathcal{U}$. The starting-time slot of the appliances, $ST_{au}$, is randomly selected for each user to represent a population of heterogeneous consumers. On the other hand, the ending-time slot, $ET_{au}$, is defined as $ST_{au} + N_a + 6$ thus guaranteeing 8 different possible schedules for each device. As for the size of the group of users, three different cases are investigated (i.e., 100, 300 and 500 consumers).

The electricity tariff used in our tests is defined according to

[2] For the sake of conciseness, the analysis of the effects of collusions of multiple honest-but-curious users is left for future work.

the dynamic pricing tariff currently used in Italy. Actually, this pricing approach is not (yet) applied to residential users, but only to large industrial consumers. For this reason, in order to realistically define this tariff, the dynamic pricing is computed by adding to the day-ahead market clearing prices, the costs of ancillary services (e.g., electricity transport, distribution and dispatching, frequency regulation, power balance). Specifically, we fix the minimum electricity price $c^{MIN} = 5 \times 10^{-5}$ € and the slope of the pricing function $s = 23 \times 10^{-11}$ €/kWh.

The AWGN used in the Privacy-Friendly load scheduling game, $r_{ut}$, is generated randomly for each user. In order to assess the performance of the Privacy-Friendly solution as the noise increases, four different cases are considered for its standard deviation, $\sigma$: 0, 100, 200 and 300 W.

For each scenario defined in our simulations, 50 different instances are generated (for a total of 600 instances). In Subsection V-B, we only report the average results obtained for each test case.

In order to evaluate the performance of the proposed Privacy-Friendly DSM game, we measure the following metrics:

- *Social cost*: is the electricity bill of the group of houses, $P(\mathcal{I})$.
- *Peak demand*: is the peak of the aggregated power demand of the group of users $\mathcal{U}$ and is defined as $\max_t y_t$.
- *Convergence time*: represents the number of iterations of the best response dynamics required to converge to the Nash Equilibrium.

### B. Performance Evaluation

Figures 3 and 4 illustrate, respectively, the social cost and the peak demand obtained by using our proposed DSM privacy-friendly mechanism, as a function of the standard deviation, $\sigma$, of the AWGN noise $r_{ut}$. Specifically, for each size of the group of consumers, we report the results normalized with respect to the benchmark scenario in which no noise is injected (i.e., $\sigma^2 = 0$), in order to show the net effect of the privacy-friendly protocol on the performance of the DSM.

As it can be observed in Figure 3, the injection of AWGN noise affects the performance of the demand-side management system just slightly, in terms of social cost: in all the considered cases, the gap between the overall consumers' electricity bills with respect to the benchmark scenario is always lower than $1\%$. Moreover, this gap decreases as the number of the users grows.

The privacy-friendly protocol has worse performance when considering the peak demand of the consumers. Specifically, as shown in Figure 4, the peak of the aggregated power demand of users increases up to $68\%$ when adding noise to the real power demand of the players. However, when applying the proposed method to large group of users, this effect is considerably decreased: as previously observed for the social cost, the degradation of the DSM game performance caused by the privacy-friendly protocol diminishes as the number of consumers grows.

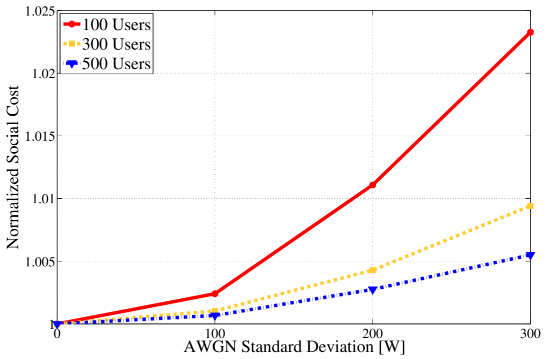

Fig. 3: Normalized social cost of the DSM game equilibrium as a function of the standard deviation of the AWGN noise, for different cardinalities of $\mathcal{U}$.

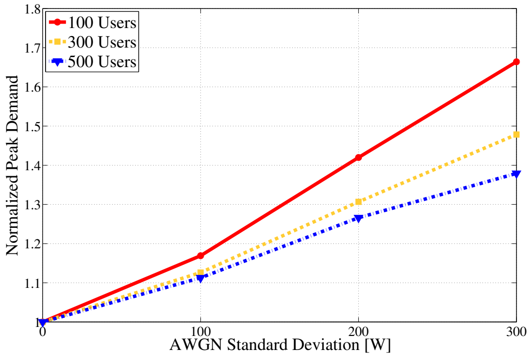

Fig. 4: Normalized peak demand of the DSM game equilibrium as a function of the standard deviation of the AWGN noise, for different cardinalities of $\mathcal{U}$.

In Figure 5 we show the number of iterations required by the loads scheduling mechanism to reach the equilibrium as a function of the standard deviation of the AWGN noise. As expected, the convergence time grows as the standard deviation, $\sigma$, increases. This inherent limitation of the privacy-friendly protocol appears to require a compromise between the opposing needs of fast convergence rate and good privacy level. However, a decrease of the convergence speed is actually acceptable since no tight real-time constraint is imposed in day-ahead load scheduling problems such as the one considered in this work.

### C. Security Analysis

The privacy level achieved by our framework have been evaluated by selecting one malicious user and one target player for each instance and by computing the Kullback-Leibler divergence as in the definition provided in Section IV. Results reported in Figure 6 show that increasing the standard deviation of the AWGN noise causes a consistent decrease in the Kullback-Leibler divergence, thus providing a lower $\gamma$ and a higher user privacy. We also observe that the higher is the cardinality of the set of users, the higher is the noise standard deviation required to achieve a given privacy threshold (e.g., setting $\gamma = 1000$ requires a standard deviation of 100 W in

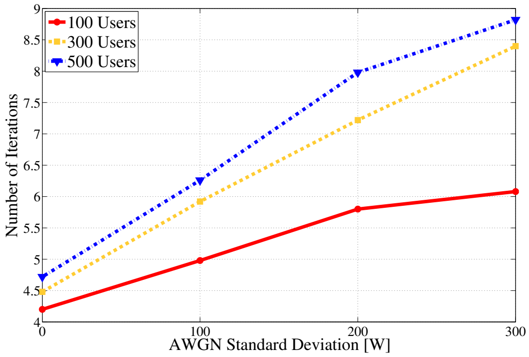

Fig. 5: Number of iterations required to converge to the equilibrium of the DSM game as a function of the AWGN noise standard deviation, for various sizes of $\mathcal{U}$.

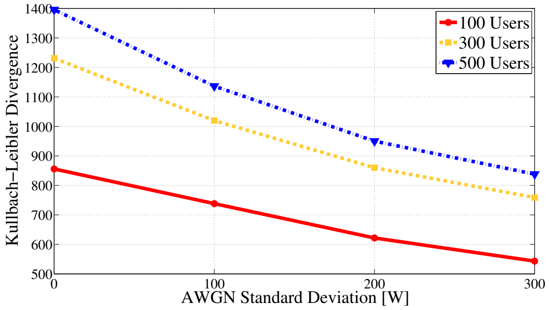

Fig. 6: Kullback-Leibler divergence as a function of the AWGN noise standard deviation, for various sizes of $\mathcal{U}$.

case of 300 users, whereas for 500 users the required noise standard deviation is approximately 175 W).

## VI. Conclusions

This paper proposes a privacy-preserving distributed demand side management system for the scheduling of power consumption requests generated by electrical appliances in a Smart Grid scenario. The interactions among the appliances owners are modelled by means of a load scheduling game which operates by relying exclusively on aggregated and noisy energy consumption data, which is perturbed by injecting additive white Gaussian noise. We show that the performance of the proposed system are only marginally affected by the data perturbation mechanism, and we evaluate the number of players and the noise power required to achieve a given privacy level, which is computed by means of the Kullback-Leibler divergence.

## VII. Acknowledgments

This work has been partially funded by Regione Lombardia project "Smart Campus as Urban Open LAbs (SCUOLA)".

## References

[1] C. W. Gellings and J. H. Chamberlin, "Demand-side management: concepts and methods," 1987.

[2] P. Finn, C. Fitzpatrick, D. Connolly, M. Leahy, and L. Relihan, "Facilitation of renewable electricity using price based appliance control in irelands electricity market," *Energy*, vol. 36, no. 5, pp. 2952–2960, 2011.

[3] M. Delfanti, D. Falabretti, M. Merlo, G. Monfredini, and V. Olivieri, "Dispersed generation in mv networks: performance of anti-islanding protections," in *Harmonics and Quality of Power (ICHQP), 2010 14th International Conference on*. IEEE, 2010, pp. 1–6.

[4] G. Strbac, "Demand side management: Benefits and challenges," *Energy Policy*, vol. 36, no. 12, pp. 4419–4426, 2008.

[5] N. Zhang, L. F. Ochoa, and D. S. Kirschen, "Investigating the impact of demand side management on residential customers," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*. IEEE, 2011, pp. 1–6.

[6] U. DoE, "Buildings energy data book," *Energy Efficiency & Renewable Energy Department*, 2011.

[7] A. Faruqui and S. Sergici, "Household response to dynamic pricing of electricity: a survey of 15 experiments," *Journal of Regulatory Economics*, vol. 38, no. 2, pp. 193–225, 2010.

[8] W. Saad, Z. Han, H. V. Poor, and T. Basar, "Game-theoretic methods for the smart grid: an overview of microgrid systems, demand-side management, and smart grid communications," *Signal Processing Magazine, IEEE*, vol. 29, no. 5, pp. 86–105, 2012.

[9] G. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870 –1891, dec 1992.

[10] C. Laughman, K. Lee, and R. e. a. Cox, "Power signature analysis," *Power and Energy Magazine, IEEE*, vol. 1, no. 2, pp. 56 – 63, 2003.

[11] C. Rottondi, M. Savi, D. Polenghi, G. Verticale, and C. Krau, "A decisional attack to privacy-friendly data aggregation in smart grids," in *IEEE Globecom 2013 - Symposium on Selected Areas in Communications - GC13 SAC Green Communication Systems and Networks*. IEEE, Dec. 2013.

[12] C. Ibars, M. Navarro, and L. Giupponi, "Distributed demand management in smart grid with a congestion game," in *IEEE, SmartGridComm '10*, Gaithersburg, USA, oct 2010, pp. 495–500.

[13] A.-H. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *Smart Grid, IEEE Transactions on*, vol. 1, no. 3, pp. 320–331, Dec 2010.

[14] L. Chen, N. Li, S. H. Low, and J. C. Doyle, "Two market models for demand response in power networks," *IEEE SmartGridComm*, vol. 10, pp. 397–402, 2010.

[15] T.-H. Chang, M. Alizadeh, and A. Scaglione, "Real-time power balancing via decentralized coordinated home energy scheduling," *Smart Grid, IEEE Transactions on*, vol. 4, no. 3, pp. 1490–1504, Sept 2013.

[16] P. Chavali, P. Yang, and A. Nehorai, "A distributed algorithm of appliance scheduling for home energy management system," *Smart Grid, IEEE Transactions on*, vol. 5, no. 1, pp. 282–290, Jan 2014.

[17] C. Chen, K. Nagananda, G. Xiong, S. Kishore, and L. Snyder, "A communication-based appliance scheduling scheme for consumer-premise energy management systems," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 56–65, March 2013.

[18] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, 2011.

[19] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications, 2010 First IEEE International Conference on*, oct. 2010, pp. 238 –243.

[20] M. Rahman, L. Bai, M. Shehab, and E. Al-Shaer, "Secure distributed solution for optimal energy consumption scheduling in smart grid," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, June 2012, pp. 279–286.

[21] Z. Chen and L. Wu, "Residential appliance dr energy management with electric privacy protection by online stochastic optimization," *Smart Grid, IEEE Transactions on*, vol. 4, no. 4, pp. 1861–1869, Dec 2013.

[22] ECORET Project, Official web site (ITA), http://www.rse-web.it/progetti.page?RSE_originalURI=/progetti/progetto/documento/178/312827&objId=178&typeDesc=Rapporto&RSE_manipulatePath=yes&docIdType=1&country=ita, apr 2014.

[23] MICENE Project,Official web site (ITA), http://www.eerg.it/index.php?p=Progetti_-_MICENE, apr 2014.

[24] R. Jain, *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. Wiley - Interscience, 1991.