Enabling Privacy in a Distributed Game-Theoretical Scheduling System for Domestic Appliances

Cristina Rottondi*, Antimo Barbato*, Lin Chen† and Giacomo Verticale*

* Department of Electronics, Information and Bioengineering
Politecnico di Milano
{giacomo.verticale, cristinaemma.rottondi, antimo.barbato}@polimi.it

† Laboratoire de Recherche en Informatique
Paris-Sud University
{lin.chen}@lri.fr

***Abstract*—Demand Side Management (DSM) makes it possible to adjust the load experienced by the power grid while reducing the consumers' bill. Game-theoretic DSM is an appealing decentralized approach for collaboratively scheduling the usage of domestic electrical appliances within a set of households while meeting the users' preferences about the usage time. The drawback of distributed DSM protocols is that they require each user to communicate his/her own energy consumption patterns, which may leak sensitive information regarding private habits. This paper proposes a distributed Privacy-Friendly DSM system that 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 number of users required to achieve a given privacy level, quantified by means of the increase of the information entropy of the aggregated energy consumption pattern. The performance of our proposed DSM system is compared to the one of a benchmark system that does not support privacy preservation in terms of total bill, peak demand and convergence time. Results show that privacy can be improved at the cost of increasing the peak demand and the number of game iterations, whereas the total bill is only marginally incremented.**

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

I. Introduction

Demand Side Management (DSM) is a proactive approach aimed at managing the electricity demand of users based on the needs of both customers and power grid [1]. By properly redistributing loads through the local control of the electric resources of residential users [2] it is possible to achieve several benefits, among which preventing power outages and curtailing the grid capacity and investments by shifting the users' demand from peak to off-peak periods [3]. Moreover, DSM can increase the amount of Renewable Energy Sources (RESs) that can be connected to the grid [4] by mitigating issues related to demand-supply balancing, power quality and unintentional islanding [5].

Users can be incentivized to properly shift their demand through the adoption of convenient pricing schemes. Among the energy tariffs already proposed in the literature, Real-Time Pricing (RTP) is generally advocated as the most efficient solution to incetivize customers to conveniently shift their loads [6]. 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 prices during peak hours and lower prices 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]. However, the uncoordinated shifting of customers' loads may cause large peaks of demand (e.g., during low-cost periods) and, possibly, service interruptions. To contain these unwanted side-effects and achieve relevant results from a system-wide perspective, DSM must be applied to groups of users (e.g., a neighborhood or micro-grids). Two different types of strategies are proposed in the literature to design these systems: centralized and distributed ones. In the first case, consumers are considered unselfish and cooperate in managing their resources. Centralized DSM frameworks are typically based on optimization methods and aim to maximize a shared utility function [8]. On the other hand, in case of distributed systems, consumers are considered selfish and their goal is to maximize their individual utility function. In this case, each consumer locally defines his/her energy plan. In order to design distributed frameworks, game theory is widely applied since it naturally captures the strategic interactions in such distributed decision making scenarios and helps to study and predict the effects of consumers' selfishness [9]. Moreover, game theoretic DSM methods can be used to identify policies that lead to socially optimal outcomes which improve the efficiency of the whole power grid by means of reducing the peak of the aggregated demand [10] and the users' bills [11], as well as by increasing the amount of RESs connected to the grid [12].

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 an hourly basis, such data can still reveal the type of electrical devices in use [13], [14], 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 that have been already combined with the aim of enhancing privacy in the context of smart metering data collection (see, e.g., [15]).

In this paper, we formalize the notion of γ**-privacy** as a

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). A preliminary version appeared in C. Rottondi, A. Barbato, and G. Verticale, "A Privacy-Friendly Game-Theoretic Distributed Scheduling System for Domestic Appliances" *SmartGridComm, IEEE International Conference on Smart Grid Communications*, Venice, Italy, Nov. 2014.

measure of the privacy of the users participating in a distributed game-theoretical privacy-friendly DSM system aimed at reducing their daily electricity bill. In this game, the players are the end-users, the set of strategies is their possible load schedules and the utility function is their daily electricity bill. Each customer has to schedule the time of use of his/her shiftable electric appliances within a predefined time window chosen according to his/her preferences, with the final goal of minimizing the daily bill. A dynamic pricing approach is used to determine the electricity tariff. For this game, we define a communication protocol that integrates both data aggregation and perturbation techniques: each user provides to the other players a noisy version of his/her scheduled power demand profile in order to obtain a cheap schedule of the appliances' starting times without revealing his/her preferred time windows. However, the noise is not added to the measurements collected by the meters, thus maintaining the real energy consumption unvaried.

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

II. Related Work

Data perturbation and aggregation are the two main privacy-preserving approaches originally applied in data mining which have been leveraged to avoid the inference of sensitive information from individual metering data in smart grid scenarios. Counteracting attacks based on Non-Intrusive Load Monitoring (NILM) of energy usage traces has been addressed by a consistent body of literature (see [16] for a survey). Typical solutions rely on battery-based load hiding [17], [18], on noise injection (e.g. according to the framework of differential privacy [19]) or on multi-party computation cryptographic techniques [20], [21]. However, in game-theoretic DSM frameworks the data communicated by the users are not real energy consumption measurements but forecasted patterns which are defined based on the current schedule of the starting time of their appliances. Such data are circulated during the execution of the game at the beginning of the optimization horizon.

Despite the substantial body of work on the design of DSM systems based on game theory, only a few studies specifically addressed the privacy preservation of the data exchanged among the participants. Moreover, the security assumptions modeling the adversarial entities that attempt to access users' data are most often too loose with respect to realistic attack scenarios: some frameworks [22], [11] assume that exchanging aggregated power consumption data at the household level (e.g., on hourly basis) is sufficient to hide the usage patterns of single electric appliances to untrustworthy neighbours. However, various studies on NILM [23], [24] prove that sensitive data can be easily inferred from house-aggregated measurements. Other proposals assume the presence of at least one trusted entity that is in charge of managing energy consumption data: paper [25] avoids data exchange among households, but includes a trusted energy utility that collects the individual power consumption curves and broadcasts price information which are updated at every game iteration, whereas the DSM system discussed in [26] 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 neighbors, who are assumed to be trusted. Conversely, our proposed framework is completely decentralized and does not involve additional nodes besides the local energy management systems. Therefore, in our scenario the adversarial entities are represented by the game players themselves, who behave according to the honest-but-curious attacker model.

The impact of a dishonest intrusive attacker manipulating energy prices to achieve both economical losses and physical damages is investigated in [27] in the framework of Stackelberg game within multiple energy utilities and consumers, aimed at maximizing the revenue of each utility company and the payoff of each user. Conversely in our framework the aim of the adversary is inferring the energy usage preferences of the users, and not achieving unfair economical advantages.

A communication protocol for a DSM game-theoretical framework in which each user receives only the overall energy consumption pattern aggregated over the whole set of the remaining players has been proposed in [28]. However, spatial aggregation over multiple users cannot completely avoid information leakages (think e.g. to the degenerate case in which all the users but one declare zero consumption for the whole scheduling horizon). A solution combining data aggregation and perturbation that provides integrity and accountability to the messages exchanged among the players is proposed in [29]. The proposed multi-party computation scheme allows a single player to obtain the aggregate consumption curve of the other players by exposing a noisy version of his/her 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. In this study, we leverage the same combination of data perturbation and aggregation techniques to evaluate the dependency of the privacy level on the power of the perturbation noise. The same paper proves that a dishonest player has no economic incentives in declaring false electric energy usages, as long as the declared energy usage remains equal to the actual amount. Our paper assumes the same adversarial model, and leverages on the proof therein provided to propose a protocol enhancement aimed at preventing players from cheating.

Our proposed protocol leverages some building blocks firstly appeared in our previous study [30]. With respect to that work, however, we introduce a novel privacy notion, which quantifies the privacy level provided to a single user by means of the information entropy of the aggregated consumption data learned by an honest-but-curious adversarial player during the game iterations. Similar information-theoretic definitions based on conditional entropy and mutual information have already been applied to other smart-grid related contexts such as distributed state estimation [31], [32] and battery-based load hiding [18], [33], since they quantify the inherent information available for exploitation by an adversary independently of the specific algorithm implemented by the attacker. In [33], extensive validations show that entropy-based metrics significantly outperform privacy measures based on mutual information in capturing data correlation exhibited by long time-series.

TABLE I
TABLE OF SYMBOLS

Notation	Description
$\mathcal{U}, \mathcal{T}$	set of users and set of time slots within the optimization horizon
$\mathcal{A}_u = \mathcal{A}_u^F \cup \mathcal{A}_u^S$	set of appliances of user $u \in \mathcal{U}$, including non-shiftable ($\mathcal{A}_u^F$) and shiftable appliances ($\mathcal{A}_u^S$)
$\mathcal{I} = \{\mathcal{I}_u\}_{u \in \mathcal{U}}$	set of strategies $\mathcal{I}_u$ of users $u \in \mathcal{U}$
$\mathcal{P} = \{P_u\}_{u \in \mathcal{U}}$	set of utility functions P_u of users $u \in \mathcal{U}$
$\mathcal{J}_{\mathcal{U}}$	set of iterations of the load scheduling game played by the users in $\mathcal{U}$
$P = \sum_{u \in \mathcal{U}} P_u$	total utility function of users $u \in \mathcal{U}$
N_{au}, ST_{au}, ET_{au}	load profile duration, window starting slot, and window ending slot of appliance $a \in \mathcal{A}_u$ owned by user $u \in \mathcal{U}$
l_{an}^u	power consumption of appliance $a \in \mathcal{A}_u$ owned by user $u \in \mathcal{U}$ during slot $n \in \{1, 2, \ldots, N_{au}\}$
s, c^{Anc}	slope of the energy cost function and cost of ancillary services
T	duration of a time slot
π	maximum user energy consumption per slot
y_{ut}^j	energy consumption of user $u \in \mathcal{U}$ during slot $t \in \mathcal{T}$ at game iteration $j \in \mathcal{J}_{\mathcal{U}}$
p_{ut}^j	aggregated energy consumption of users in $\mathcal{U} \backslash \{u\}$ during slot $t \in \mathcal{T}$ at game iteration $j \in \mathcal{J}_{\mathcal{U}}$
x_{at}^j	binary variable set to 1 if the start time of appliance a of user u is scheduled at time $t \in \mathcal{T}$ at game iteration $j \in \mathcal{J}_{\mathcal{U}}$, 0 otherwise
r_{ut}	random noise added by user $u \in \mathcal{U}$ to his/her energy consumption at slot $t \in \mathcal{T}$
ϕ_{ut}	energy consumption of user $u \in \mathcal{U}$ at slot $t \in \mathcal{T}$ declared during the initialization round

III. The Privacy-Friendly Loads Scheduling Framework

We consider a generic smart grid model in which a set 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 of duration T (the list of symbols used in the remainder of the paper are reported in Table I). We assume that each user $u \in \mathcal{U}$ owns 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_{au} time slots. The power consumption of appliance a in the nth time slot of its load profile (with $n \in \mathcal{N}_{au} = \{1, 2.., N_{au}\}$), l_{an}^u, is assumed to be constant within the time slot and varies according to the appliance type and usage (e.g. the specific washing cycle of the dishwasher selected by the user). The starting time slot of each appliance $a \in \mathcal{A}_u$ must fall within a time window delimited by a minimum starting-time slot, ST_{au}, and a maximum ending-time slot, ET_{au}, which have been decided by the user beforehand. These two parameters represent the user's preferences in scheduling each electric appliance.

Each user $u \in \mathcal{U}$ can have two different kinds of appliances:

- Fixed appliances (e.g., light, TV), represented by the subset $\mathcal{A}_u^F \subseteq \mathcal{A}_u$, are non-manageable devices whose starting time is fixed. In case of such appliances, their parameters ST_{au} and ET_{au} must satisfy the following equation $ET_{au} - ST_{au} = N_{au} - 1$ ("-1" is used as a consequence of the adoption of a discretized-time model), which guarantees that fixed devices have only one possible starting time and that the system is forced to start them at time ST_{au}.
- *Shiftable* appliances (e.g., washing machine, dishwasher), represented by the subset $\mathcal{A}_u^S \subseteq \mathcal{A}_u$, are manageable devices whose starting time is a variable of our model. In case of such appliances, their parameters ST_{au} and ET_{au} must satisfy the following equation $ET_{au} - ST_{au} > N_{au} - 1$ which guarantee that each shiftable device has more than one possible starting time.

In order to run these appliances, each end-user must buy electric energy from the retailer and his/her goal is to minimize his/her daily bill by means of optimally scheduling the usage of his/her appliances. Since the higher the demand of electricity, the larger the capacity of grid generation and distribution to install, we model the price of electricity at time $t \in \mathcal{T}$, $c_t(\cdot)$ as an increasing function of the total power demand, y_t, of the group of users $\mathcal{U}$ at time t [11].

Since the electricity price is defined as a function of the total demand of the whole group of users, the load scheduling problem cannot be solved with a centralized model because of the conflict between users' goals. For this reason, a distributed approach based on a game-theoretic approach is used, since game theory naturally models interactions in distributed decision making processes. The starting time of each shiftable appliance will be therefore provided as output of the load scheduling game described in the next subsection.

A. Load Scheduling Game

The load scheduling problem is modeled as a game $\mathcal{G} = \{\mathcal{U}, \mathcal{I}, \mathcal{P}\}$, defined by: the *players* representing the users in the set $\mathcal{U}$, the *strategy* set $\mathcal{I} \triangleq \prod_{u \in \mathcal{U}} \mathcal{I}_u$, where $\mathcal{I}_u$ is the strategy set of player u corresponding to his/her possible load schedules, and the *payoff function* set $\mathcal{P} \triangleq \{P_u\}_{u \in \mathcal{U}}$, where P_u is the payoff function of user u, which coincides with his/her daily electricity bill. Specifically, the strategy of the player u is $\mathcal{I}_u \triangleq \{x_{at}\}_{a \in \mathcal{A}_u}$, 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 payoff function of each player, P_u, is defined as a function of $\mathcal{I}$ as follows:

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

where y_{ut} is the power demand of user u at time t and is a function of x_{at}, T is the time slot duration and is used to convert power in energy demand, and $c_t(y_t)$ is the price of electricity at time t and 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. In this paper, we focus on a specific class of energy tariffs named regular pricing functions, which are defined as follows.

Definition 1 (Regular Pricing Function)**.** *The pricing function* $\{c_t(y_t)\}_{t\in\mathcal{T}}$ *is a regular pricing function if for any two time intervals* $[t^1, t^2]$, $[t^3, t^4]$, *power demand in these intervals* $\{y_t\}_{t\in[t^1,t^2]}$, $\{y_t\}_{t\in[t^3,t^4]}$ *and deviation* $\delta_y \geq 0$, *it holds that:*

$$\sum_{t=t^1}^{t^2} c_t(y_t) > \sum_{t=t^3}^{t^4} c_t(y_t) \Longrightarrow \sum_{t=t^1}^{t^2} y_t c_t(y_t) - \sum_{t=t^3}^{t^4} y_t c_t(y_t) \geq$$
$$\geq \sum_{t=t^1}^{t^2} (y_t - \delta_y) c_t(y_t - \delta_y) - \sum_{t=t^3}^{t^4} (y_t - \delta_y) c_t(y_t - \delta_y) \tag{2}$$

Notice that when deviation δ_y is infinitesimally small and $c_t(y_t)$ is derivable, the assumption (2) becomes:

$$\sum_{t=t^1}^{t^2} c_t(y_t) > \sum_{t=t^3}^{t^4} c_t(y_t) \Longrightarrow \sum_{t=t^1}^{t^2} [y_t c_t(y_t)]' > \sum_{t=t^3}^{t^4} [y_t c_t(y_t)]' \tag{3}$$

Let $\mathcal{I}_{-u} \triangleq \prod_{i\in\mathcal{U}\setminus u} \mathcal{I}_i$ and $P(\mathcal{I})$ be the total cost paid by all players to the electricity retailer:

$$P(\mathcal{I}) = \sum_{u\in\mathcal{U}} P_u(\mathcal{I}) = T \sum_{u\in\mathcal{U}} \sum_{t\in\mathcal{T}} y_{ut} c_t(y_t) \tag{4}$$

Then the following Lemma can be proved [34]:

Lemma 1. *If* $\{c_t(y_t)\}_{t\in\mathcal{T}}$ *is a regular pricing function, then for any player* $u \in \mathcal{U}$, *for any two strategies* $i'_u, i''_u \in \mathcal{I}_u$ *and for any strategy* $i_{-u} \in \mathcal{I}_{-u}$, *it holds that:*

$$P_u(i'_u, i_{-u}) > P_u(i''_u, i_{-u}) \Longrightarrow P(i'_u, i_{-u}) > P(i''_u, i_{-u}) \tag{5}$$

Based on Lemma 1 and on the definition reported hereafter of generalized ordinal potential games [35], Theorem 1 can be immediately obtained.

Definition 2 (Generalized Ordinal Potential Game)**.** *Given a finite strategic game* $\Gamma \triangleq \{\mathcal{U}, \{I_u\}_{u\in\mathcal{U}}, \{P_u\}_{u\in\mathcal{U}}\}$, Γ *is a generalized ordinal potential game if there exists a function (called potential function)* $\Phi : I \to \mathbb{R}$ *such that for every player* $u \in \mathcal{U}$ *and every* $i_{-u} \in I_{-u}$ *and* $i'_u, i''_u \in I_u$, *it holds that:*

$$P_u(i'_u, i_{-u}) > P_u(i''_u, i_{-u}) \Longrightarrow \Phi(i'_u, i_{-u}) > \Phi(i''_u, i_{-u}) \tag{6}$$

Theorem 1. *Under the condition that* $\{c_t(y_t)\}_{t\in\mathcal{T}}$ *is a regular pricing function, the load scheduling game* $\mathcal{G}$ *is a generalized ordinal potential game, with* $P(\mathcal{I})$ *defined in Eq. 4 being the potential function.*

Proof. To prove the theorem, it suffices to show that for every player $u \in \mathcal{U}$ and every $i_{-u} \in I_{-u}$ and $i'_u, i''_u \in I_u$, it holds that:

$$P_u(i'_u, i_{-u}) > P_u(i''_u, i_{-u}) \Longrightarrow P(i'_u, i_{-u}) > P(i''_u, i_{-u}) \tag{7}$$

For the sake of simplicity, assume that each player u has only one home appliance (the proof of Theorem 1 in case of players with multiple appliances can be derived from the demonstration hereafter presented). Moreover, assume that in the strategy i'_u (i''_u, respectively), player u starts his appliance in time interval $[t^1, t^2]$ ($[t^3, t^4]$). Let y'_t denote the total power demand of players at time t under strategy profile (i'_u, i_{-u}). The difference between the strategy profiles (i'_u, i_{-u}) and (i''_u, i_{-u}) is that player u migrates his power demand, denoted by p_u, from time interval $[t^1, t^2]$ to $[t^3, t^4]$. As a consequence, one can derive that:

$$P_u(i'_u, i_{-u}) - P_u(i''_u, i_{-u}) = \sum_{t=t^1}^{t^2} p_u c_t(y'_t) - \sum_{t=t^3}^{t^4} p_u c_t(y'_t + p_u) =$$
$$= p_u \left(\sum_{t=t^1}^{t^2} c_t(y'_t) - \sum_{t=t^3}^{t^4} c_t(y'_t + p_u) \right) \tag{8}$$

The difference between $P(i'_u, i_{-u})$ and $P(i''_u, i_{-u})$ can also be derived as follows:

$$P(i'_u, i_{-u}) - P(i''_u, i_{-u}) = \sum_{t=t^1}^{t^2} y'_t c_t(y'_t) + \sum_{t=t^3}^{t^4} y'_t c_t(y'_t) +$$
$$- \sum_{t=t^1}^{t^2} (y'_t - p_u) c_t(y'_t - p_u) - \sum_{t=t^3}^{t^4} (y'_t + p_u) c_t(y'_t + p_u) =$$
$$= \sum_{t=t^1}^{t^2} y'_t c_t(y'_t) - \sum_{t=t^3}^{t^4} (y'_t + p_u) c_t(y'_t + p_u) +$$
$$- \left[\sum_{t=t^1}^{t^2} (y'_t - p_u) c_t(y'_t - p_u) - \sum_{t=t^3}^{t^4} y'_t c_t(y'_t) \right] \tag{9}$$

Recalling the definition of regular pricing functions, it then holds that:

$$P_u(i'_u, i_{-u}) > P_u(i''_u, i_{-u}) \Longrightarrow \sum_{t=t^1}^{t^2} c_t(y'_t) > \sum_{t=t^3}^{t^4} c_t(y'_t + p_u) \Longrightarrow$$
$$\Longrightarrow \sum_{t=t^1}^{t^2} y'_t c_t(y'_t) - \sum_{t=t^3}^{t^4} (y'_t + p_u) c_t(y'_t + p_u) >$$
$$> \sum_{t=t^1}^{t^2} (y'_t - p_u) c_t(y'_t - p_u) - \sum_{t=t^3}^{t^4} y'_t c_t(y'_t) \Longrightarrow$$
$$\Longrightarrow P(i'_u, i_{-u}) > P(i''_u, i_{-u}) \tag{10}$$

The proof is thus completed. □

Potential games have several properties, such as the existence of at least one pure Nash Equilibrium (NE). Moreover, such games have the same pure NE when payoffs are replaced by the potential function, hence the original problem is equivalent to a distributed optimization model in which the objective function is the potential function. Solving the global problem directly may be prohibitively complex due to the high dimension of the problem in case of real use-cases. Moreover, it would require the users to provide a wide set of sensitive information to the solver. For this reason, distributing the computation of smaller problems to each users based on distributed techniques is, in general, much more efficient both in terms of computational complexity and privacy. To this end, one can use the Finite Improvement Property (FIP) of potential games to solve this problem: any sequence of asynchronous improvement steps is finite and converges to a pure equilibrium. Particularly, the sequence of best response updates converges to a pure equilibrium [36].

In this paper, we assume that $c_t(y_t)$ is linear with respect to y_t, thus satisfying the regular pricing function conditions. As a consequence, $\mathcal{G}$ is a generalized ordinal potential game and best response dynamics can be applied to converge to a NE. In this work, we consider a simple implementation of the best response dynamics: each player, in an iterative fashion, defines his/her optimal load scheduling strategy based on electricity tariffs (calculated according to the strategies of the other players) and communicates his/her energy plan (i.e., his/her daily power demand profile) to the next user of the set $\mathcal{U}$. 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. It also results in the best privacy level for a given noise power. At every iteration $j \in \mathcal{J}_{\mathcal{U}}$ of the best response dynamics, energy prices are updated and, as a consequence, other users can decide to modify their schedules. In the jth iteration, the optimal schedule of the user u is obtained by solving the following Mixed Integer Non-linear Programming (MINLP) model:

$$\min \sum_{t \in \mathcal{T}} \left(y_{ut}^{j} \cdot T \right) c_t^{j} \tag{11}$$

s.t.

$$\sum_{t=ST_{au}}^{ET_{au}-N_{au}+1} x_{at}^{j} = 1 \qquad \forall a \in \mathcal{A}_u \tag{12}$$

$$y_{ut}^{j} = \sum_{a \in \mathcal{A}_u} \sum_{\substack{n \in \mathcal{N}_{au}: \\ n \leq t}} l_{an}^{u} \cdot x_{a(t-n+1)}^{j} \qquad \forall t \in \mathcal{T} \tag{13}$$

$$y_{ut}^{j} \leq \pi \qquad \forall t \in \mathcal{T} \tag{14}$$

$$c_t^{j} = c^{Anc} + s \cdot (y_{ut}^{j} \cdot T + p_{ut}^{j} \cdot T) \qquad \forall t \in \mathcal{T} \tag{15}$$

The objective function (11) minimizes the daily bill of the user u. Note that the decision variables x_{at}^{j} appear in the objective function through the equality constraints (13) and (15).

Constraints (12) guarantee that each appliance $a \in \mathcal{A}_u$ is executed only once in the time window $[ST_{au}, ET_{au}]$. Notice that in order to be executed within time ET_{au}, appliance a must be started within the interval $[ST_{au}, ET_{au} - N_{au} + 1]$. Constraints (13) determine the overall consumption of the appliances in each time slot at iteration j, which depends on the scheduling strategy: the power required by each device a in each time slot t, y_{ut}^{j}, is equal to power consumption indicated by the n-th sample (with $n \in \mathcal{N}_{au} = \{1, 2.., N_{au}\}$) of the load profile, l_{an}^{u}, executed at time t. Note that the power amount indicated by the n-th sample of the appliance load profile is consumed during slot t if and only if the appliance started at time $t - n + 1$, thus if $x_{a(t-n+1)}^{j} = 1$. Constraints (14) bound the amount of purchasable power in order not to exceed the contractual limit, π. Finally, constraints (15) 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 (15), 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^{Anc} is the cost of ancillary services (e.g., electricity transport, distribution and dispatching, frequency regulation, power balance) and s is the slope of the cost function.

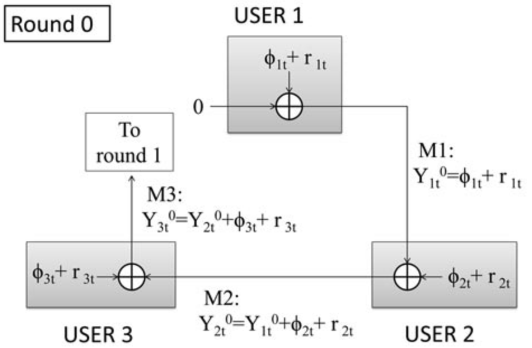

Fig. 1. The privacy-friendly communication protocol: initialization round

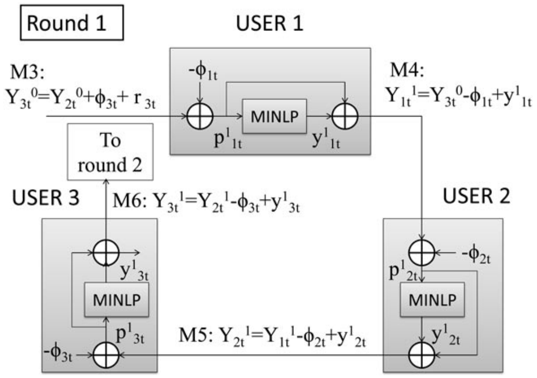

Fig. 2. The privacy-friendly communication protocol: first round

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

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. The protocol is executed over an Internet Protocol-based network, comprising both the user nodes as endpoints and other intermediate nodes such as routers. In addition we also assume that point-to-point communication among any pair of users is confidential and authenticated by means of a standard secure protocol such as IPSec or TLS. As a results, the logical topology seen by the protocol is a full mesh network including only the user nodes. Under such assumptions, any random sequence that includes each user exactly once can be chosen for running the algorithm. During an initialization round (numbered as 0), each player u generates two sequences

ϕ_{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 σ^2 and the sequence ϕ_{ut} for $t = 1, \ldots, \mathcal{T}$ is an arbitrary partition of the quantity $\sum_{a \in \mathcal{A}_u, n \in \mathcal{N}_a} l_{an}^u$, i.e.:

$$\sum_{t \in \mathcal{T}} \phi_{ut} = \sum_{a \in \mathcal{A}_u, n \in \mathcal{N}_a} l_{an}^u \tag{16}$$

Note that the value of σ^2 is defined in order to provide a target privacy level to a group of $|\mathcal{U}|$ users (see Sections IV and V). 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 ϕ_{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 (16) 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, calculating the parameters p_{1t}^1 as:

$$p_{1t}^1 = Y_{|\mathcal{U}|t}^0 - \phi_{1t} \qquad \forall t \in \mathcal{T} \tag{17}$$

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

$$Y_{1t}^1 = p_{1t}^1 + y_{1t}^1 \qquad \forall t \in \mathcal{T} \tag{18}$$

where y_{1t}^1 is output by the MINLP solver, and forwards it to the next player (see Fig. 2). This way, user u replaces the partition ϕ_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 jth iterations (where $j \geq 2$), each user u behaves analogously, by replacing Formula (17) 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 (18) as follows:

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

It results that, at the jth 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. Note that, during the initialization round, the u-th player receives the partial aggregate of the sequences generated by users $1, \ldots, u-1$ (i.e., fewer than $|\mathcal{U}|$), thus the variance of the added noise is not sufficient to provide the target privacy level. Therefore, it is necessary that the sequences ϕ_{ut} transmitted during the first iteration do not provide any sensitive information. Once the first round is completed, the aggregate contains $|\mathcal{U}|$ random sequences ϕ_{ut} and $|\mathcal{U}|$ noise sequences r_{ut}, which provide the desired privacy level. Then, at the beginning of round 1, the random sequences are gradually substituted with the real user schedules.

Also notice that the privacy-friendly technique here proposed does not strictly depend on the setup of the game and may therefore be applied also to other DSM frameworks in which the convergence to the equilibrium is reached in a similar manner to the one considered in our work (e.g. [11]).

In addition, it is worth noting that our framework only requires additive noise and independency of the noise from the data. We choose to focus on AWGN since it has the above properties and it is well known and easy to generate. If additional assumptions are made on the user preferences, it is possible that other noise spectra and noise distributions result in better privacy levels for the same noise power. For the sake of simplicity we do not discuss these issues in this paper.

Finally, we observe that Theorem 1 also applies to the privacy-preserving algorithm. To prove this, one can think at the whole aggregate additive noise as the consumption profile of an additional player $\overline{u}$ who owns a single fixed appliance, i.e. $\mathcal{A}_{\overline{u}}^S = \emptyset$ and $\mathcal{A}_{\overline{u}}^F = \{\overline{a}\}$. Its consumption profile spans the entire optimization horizon (i.e., $\mathcal{N}_{\overline{a}\overline{u}} = \mathcal{T}$) and its energy consumption profile satisfies the following equality:

$$\begin{aligned} l_{\overline{a}t}^{\overline{u}} &= \sum_{u \in \mathcal{U}} r_{ut} && \forall t \in \mathcal{T} \\ r_{\overline{u}t} &= 0 && \forall t \in \mathcal{T} \end{aligned}$$

There is a single strategy in the set $\mathcal{I}_{\overline{u}}$ of player $\overline{u}$, namely starting appliance $\overline{a}$ at the beginning of the optimization horizon. Consequently, from round 1 on, player $\overline{u}$ always outputs the above response.

By virtue of Theorem 1, the privacy-preserving game is an ordinal potential game and thus the algorithm converges in a finite amount of steps. The resulting schedule, however, does not necessarily achieve the minimum electricity bill. In the following Sections we will discuss the tradeoff between the increase in the electricity bill and the achieved privacy.

IV. Attacker Model

A. Security Definitions

We assume a scenario with a fixed set of users $\mathcal{U}$. The set contains one attacker, denoted as u_m, who behaves according to an honest-but-curious model: he/she correctly executes the protocol but tries to infer the preferred time windows $[ST_{au}, ET_{au}]$ of the appliances $a \in \mathcal{A}_u$ of all the users $u \in \mathcal{U}$. Let Ψ be the multivariate random variable that describes the probability of each possible combination of users' preferences. Let $\mathbf{v} = [p_{u_m 1}^{|J_\mathcal{U}|}, \ldots, p_{u_m |\mathcal{T}|}^{|J_\mathcal{U}|}]$ be the aggregated energy consumption schedule received by attacker u_m in the last iteration of the privacy-preserving protocol described in Section III-B. Since $\mathbf{v}$ depends on the users' preferences and on the random noise chosen by the users, it can be modeled as an instance of the $|\mathcal{T}|$-dimensional multivariate random variable $\mathbf{V}$. Clearly, the knowledge of $\mathbf{v}$ improves the attacker's knowledge about the time windows chosen by the users before the execution of the DSM privacy-preserving protocol. Therefore, analogously to the definitions provided in [37], [38], we quantify the privacy provided by our proposed DSM framework as follows:

Definition 3. *The architecture provides γ-**privacy** if it holds that:*

$$\gamma = H(\Psi) - H(\Psi|\mathbf{V}) \tag{19}$$

where $H(\cdot)$ indicates the random variable's information entropy defined as:

$$H(X) = E[-\log_2(P(X))] \tag{20}$$

being $E[\cdot]$ the expected value operator and $P(X)$ the probability mass function of the generic random variable X. Note that, by applying the Bayes' rule, the following equality holds:

$$H(\Psi|\mathbf{V}) = H(\mathbf{V}|\Psi) + H(\Psi) - H(\mathbf{V}) \tag{21}$$

Therefore, by substitution, it results that:

$$\gamma = H(\Psi) - H(\mathbf{V}|\Psi) - H(\Psi) + H(\mathbf{V}) = H(\mathbf{V}) - H(\mathbf{V}|\Psi) \tag{22}$$

The goal of the attacker is to gain information about the users' preferences given the knowledge of the aggregated scheduled consumption. As an extreme case, when $\gamma = 0$ the attacker learns nothing. In a general case, the attacker's knowledge improves by γ bits, meaning that the attacker is capable of answering at most γ yes/no questions about the user preferences.

The relation between the added noise and the privacy level is discussed in the next Section, in which we numerically evaluate the privacy level achieved by our proposed privacy-friendly DSM system versus the added noise power, for various sizes of the user set. We will show that, as the noise increases, γ quickly decreases, providing a tradeoff between privacy and accuracy of the data. Since data accuracy has an impact on peak demand, we will show that a tradeoff must be found between privacy expectations and the total bill.

B. Countermeasures against Semi-honest Adversaries

Users may also behave semi-honestly and declare false or inconsistent consumption patterns during the game iterations while still adhering to the protocol rules, e.g. in order to increase the energy cost in some specific slots. In turn, this may induce other players to alter their schedules accordingly and the cheaters may take advantage of such alterations.

It has been proved in [29] that a semi-honest player has no economic incentives in declaring false electric energy usages during the scheduling definition phase, as long as the declared aggregated daily consumption remains equal to the actual amount. This result is still applicable to our privacy-preserving algorithm as long as as the player cannot simply choose his/her own noise, but must generate noise independently of the users preferences. This assumption makes it possible to consider the privacy-preserving game as a non-privacy-preserving game in which the added noise is an additional honest player. Thus, according to [29, Theorem 1], providing false energy consumption patterns with the same aggregated value of the true schedule would not lead to any economic benefit. In such scenario, the cheater may only lie about his/her own scheduled appliance starting times but cannot modify the aggregated value of his/her overall energy consumption over the day.

To ensure that the hypotheses of the proof are satisfied it is necessary either to implement the noise addition and communication protocol in a tamper-proof device, or to implement cheat detection mechanisms.

The privacy-preserving protocol can be easily enhanced by including a Controller, which is not directly involved in the scheduling protocol, but is in charge of performing security checks aimed at the detection of cheaters. The Controller is supposed to have full knowledge of the actual energy consumption of each user, aggregated on daily basis (e.g., it is directly informed by the energy utility, which is responsible for the billing and thus has access to individual energy usage measurements).

To ensure that users do not declare a false demand, the Controller performs the following checks: at the beginning of the game, every user communicates the quantities $r_u = \sum_{t\in\mathcal{T}} r_{ut}$ and $\Phi_u = \sum_{a\in\mathcal{A}_u, n\in\mathcal{N}_a} l_{an}$ to the Controller. At the end of each scheduling period, for each user the Controller compares Φ_u to his/her actual energy consumption. In case of significant differences, the user is considered as a cheater. Moreover, once the initialization round of the protocol is concluded, the Controller is provided with the sequence $\mathcal{Y}_u^1$ and verifies whether the equality $\sum_{t\in\mathcal{T}} Y_{ut}^1 = \sum_{u\in\mathcal{U}}(R_u + \Phi_u)$ holds. This way it is possible to detect whether R_u and Φ_u provided by the users to the Controller correspond to the amounts of energy consumption and noise declared by the user during the execution of the protocol. In case the equality is not satisfied, the game is immediately stopped. Finally, in order to prevent cheaters from changing their declared daily energy consumption throughout the game rounds, at each round j every user verifies whether the equality $\sum_{t\in\mathcal{T}} Y_{ut}^j = \sum_{t\in\mathcal{T}} Y_{ut}^{j-1}$ holds: in fact, if all the users behave honestly, the overall daily aggregate must remain unchanged. In case the equality is not satisfied, the user reports an alarm message to the Controller and the game is stopped. The above cheat detection mechanism can be extended to test for whiteness of the noise and, thus, independence of the scheduling preferences.

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 the Privacy-Friendly DSM method on instances defined according the Italian power grid parameters and standard consumer profiles.

A. Test Methodology

In our tests, the 24-hour time horizon is represented by a set $\mathcal{T}$ of 24 time slots of 1 hour each. The parameters of the electricity tariff, c_t, are defined based on the real-time pricing currently used in Italy for large consumers. Specifically, $c^{Anc} = 0.05\,€/\mathrm{MWh}$ and $s = 2.3 \times 10^{-4}\,€/\mathrm{MWh}^2$.

In order to evaluate the performance of the privacy-friendly protocol as the size of the group of users $\mathcal{U}$ grows, three different cases are investigated: 5, 10 and 50 consumers.

Each of these users u is connected to the grid with a power limit, π, of $3\,\mathrm{kW}$ and can have up to 4 shiftable appliances (i.e., $\mathcal{A}_u^S = \{$ washing machine, dishwasher, boiler, vacuum cleaner $\}$) and 7 fixed ones (i.e., $\mathcal{A}_u^F = \{$ refrigerator, purifier, lights, microwave oven, oven, TV and iron$\}$). The energy consumption patterns of each appliance have been extracted from a real dataset [39]. For the sake of easiness, the duration of the time intervals $[ST_{au}, ET_{au}]$ are all set to D time slots, i.e. $ET_{au} = ST_{au} + D - 1\ \forall u \in \mathcal{U}, a \in \mathcal{A}_u$. Further, ST_{au} is a random variable with uniform distribution in $[1, |\mathcal{T}| - (D-1)]$. As for the starting-time slot ST_{au} and ending-time slot ET_{au} of the appliances, 10 different instances are generated by randomly defining these parameters. Specifically, the starting-time slot of each appliance, 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 $ST_{au} + N_{au} + 6$ in the case of shiftable appliances $\mathcal{A}_u^S$, guaranteeing therefore 8 different possible schedules for each device, and as $ST_{au} + N_{au} - 1$ in the case of fixed appliances $\mathcal{A}_u^F$, so as to force the system to start each of these devices at time ST_{au}.

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, six different cases are considered for its standard deviation, σ: 1, 100, 200, 300, 400 and $500\,\mathrm{W}$. Moreover, for each of these cases, 100 different instances of the AWGN are created. In Subsection V-B, only the average results obtained for each test case (i.e., number of users and AWGN standard deviation) are reported.

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

- *Total bill*: 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.

In Section V-B and V-C, we evaluate the performance of the privacy-friendly protocol. Specifically, in Section V-B, we report the results obtained when each user has only one appliance (i.e., washing machine). This case is indeed the least computationally burdensome one and, therefore, we used it to extensively test the privacy-friendly protocol, even in large-scale scenarios. At a latter stage, in Section V-C, we discuss the numerical results obtained with a higher number of appliances, but only in case of smaller scenarios (i.e., 5 end-users).

B. Performance Evaluation: Test Case A

In this test case, each user $u \in \mathcal{U}$ owns a single shiftable appliance (i.e., a washing machine). Figures 3 and 4 illustrate, respectively, the total bill and the peak demand obtained by using our proposed DSM privacy-friendly mechanism, as a function of the standard deviation, σ, of the AWGN noise r_{ut}. Specifically, for each size of the group of consumers, we report the results normalized with respect to a benchmark scenario in which $\sigma = 1$ W (i.e. the standard deviation is so low that the addition of noise to the scheduled consumption profiles leads to negligible alterations and intuitively provides no privacy preservation), in order to show the net effect of the privacy-friendly protocol on the performance of the DSM. Notice that the comparison between the performance of the proposed load scheduling game and the benchmark case without demand-side management has already been presented and discussed in [34], where it is shown that the electricity bill and the peak demand decrease by as much as 55% with respect to the case without DSM and that this gain is influenced by the appliances flexibility and householders preferences.

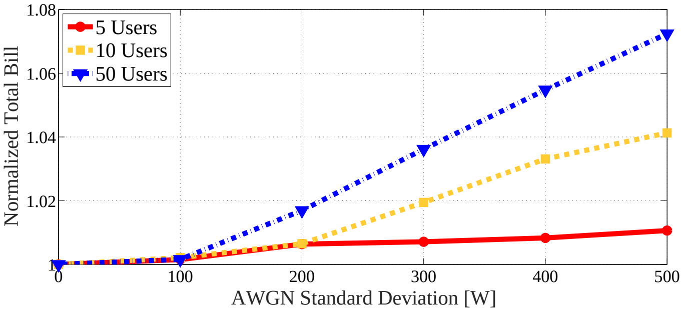

Fig. 3. Normalized total bill of the DSM game equilibrium as a function of the standard deviation of the AWGN noise, for different cardinalities of $\mathcal{U}$ and one appliance per user.

As it can be observed in Figure 3, the injection of AWGN noise may affect the performance of the demand-side management system in terms of the total bill. The maximum gap between the overall consumers' electricity bills with respect to the benchmark scenario is around 7%. Moreover, as expected, this gap increases as the number of users grows, since the greater is the size of the group of players, the greater is the overall noise added by the users.

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 by up to 110% when adding noise to the real power demand of the players. Nevertheless, it is worth noting that in our tests the peak demand obtained when applying the proposed DSM system has always been lower than that experienced without any demand-management framework, independently of the standard deviation of the AWGN noise.

The convergence time of the load scheduling mechanism is another important metric to be considered in assessing the applicability of the proposed solution to real use-case scenarios. In Figure 5 we show the number of iterations required 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, σ, 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

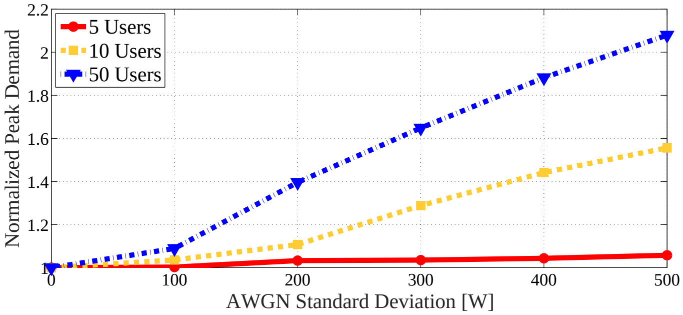

Fig. 4. Normalized peak demand of the DSM game equilibrium as a function of the standard deviation of the AWGN noise, for different cardinalities of $\mathcal{U}$ and one appliance per user.

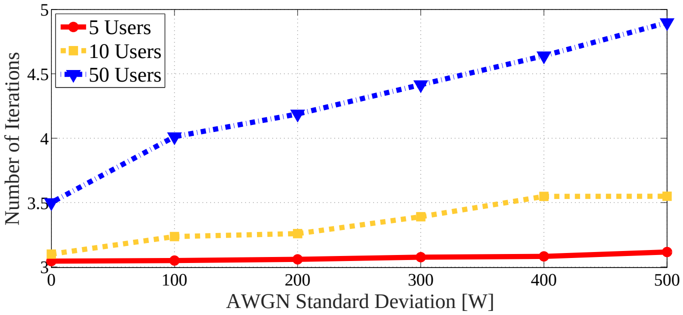

Fig. 5. Number of iterations required to converge to the equilibrium of the DSM game as a function of the AWGN noise standard deviation, for different cardinalities of $\mathcal{U}$ and one appliance per user.

of the convergence speed is acceptable since no tight real-time constraint is imposed in day-ahead load scheduling problems such as the one considered in this work.

The privacy level achieved by our framework is evaluated by computing γ according to Eq. 22. Results reported in Figure 6 show that increasing the standard deviation of the AWGN noise causes a consistent decrease in the entropy difference, thus providing a lower γ 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 $\gamma = 2$ requires a standard deviation of 50 W in case of 5 users, whereas for 10 users the required noise standard deviation is approximately 210 W).

C. Performance Evaluation: Test Case B

In this test case, each user $u \in \mathcal{U}$ has multiple appliances. Specifically, we have investigated three different scenarios:

1) Each user has 5 appliances, 2 of which are shiftable ($\mathcal{A}_u^S = \{$washing machine and dishwasher$\}$) and 3 are fixed ($\mathcal{A}_u^F = \{$refrigerator, lights and oven$\}$).
2) Each user has 8 appliances, 3 of which are shiftable ($\mathcal{A}_u^S = \{$washing machine, dishwasher and boiler$\}$) and 5 are fixed ($\mathcal{A}_u^F = \{$refrigerator, lights, oven, TV and iron$\}$).
3) Each user has 11 appliances, 4 of which are shiftable ($\mathcal{A}_u^S = \{$washing machine, dishwasher, boiler and vacuum cleaner$\}$) and 7 are fixed ($\mathcal{A}_u^F = \{$refrigerator, lights, oven, TV, iron, purifier and microwave oven$\}$).

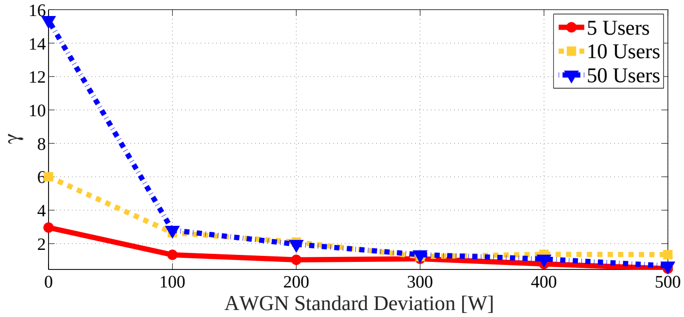

Fig. 6. Privacy level as a function of the AWGN noise standard deviation, for various sizes of $\mathcal{U}$.

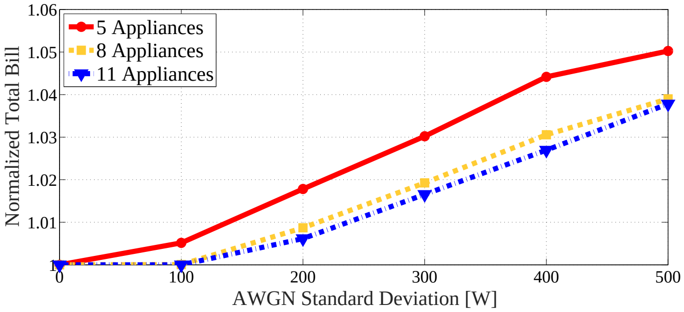

Fig. 7. Normalized total bill of the DSM game equilibrium as a function of the AWGN noise standard deviation, for $\mathcal{U} = 5$ and various numbers of appliances per user.

Figure 7 illustrates the total bill obtained by applying our proposed DSM privacy-friendly mechanism to a group of 5 consumers, as a function of the standard deviation, σ, of the AWGN noise r_{ut}. Specifically, for each size of the set of the consumers' appliances, we report the results normalized with respect to the benchmark scenario in which almost no noise is injected (i.e., $\sigma = 1$ W). As it can be observed, also in this test case the gap between the overall consumers' electricity bills and the benchmark scenario increases as the AWGN standard deviation increases. However, the effect of the AWGN noise on the performance of the DSM system becomes less and less significant as the number of appliances per user grows. Indeed, the greater is the number of appliances, the smaller is the ratio between the energy of the noise injected by users and their overall energy demand. For this reason, the greater is the number of appliances, the less energy prices (and consequently users' decisions) are influenced by the noise. Notice that in our tests the same effect has also been observed in reference to the peak demand of users. However, for the sake of brevity, we do not report here these results.

Finally, Figure 8 depicts the trend of the privacy level γ versus the standard deviation of the injected noise. With respect to the single-appliance case, γ decreases more smoothly as σ increases. For example, this a standard deviation of 300 W is necessary to achieve $\gamma < 2$. Therefore, the higher the number of deferrable appliances in the system, the higher the noise to be injected to guarantee a given privacy level.

Based on the above discussed results, we conclude that high values of σ (e.g. 500 W) lead to very moderate increments of the daily bill (at most 7% w.r.t. the benchmark case for

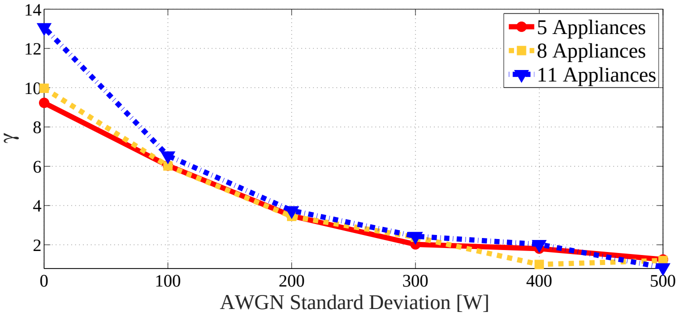

Fig. 8. Privacy level as a function of the AWGN noise standard deviation, for $\mathcal{U} = 5$ and various numbers of appliances per user.

a scenario with 50 users) but provide a high privacy level, since for such values γ approaches 0. Therefore, privacy can be achieved at the price of a slight increase in the electricity cost and of an acceptable growth of the number of iterations required for the game convergence, provided that the electricity grid is correctly dimensioned to cope with the increase of the peak demand due to noise injection.

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 appliance owners are modeled by means of a load scheduling game which operates by exclusively relying on aggregated and noisy energy consumption data, perturbed by 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 evaluated by means of the information entropy of the aggregated energy consumption patterns.

References

[1] C. W. Gellings and J. H. Chamberlin, *Demand-side management: concepts and methods*. The Fairmont Press Inc., Lilburn, GA, 1987.

[2] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Optimal residential load control with price prediction in real-time electricity pricing environments," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 120–133, 2010.

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

[4] 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.

[5] 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.

[6] E. Bloustein, "Assessment of customer response to real time pricing," *Rutgers-The State University of New Jersey, Tech. Rep*, 2005.

[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] A. Barbato and A. Capone, "Optimization models and methods for demand-side management of residential users: A survey," *Energies*, vol. 7, no. 9, pp. 5787–5824, 2014.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: Review and outlook," *IEEE Transactions on Consumer Electronics*, pp. 76–84, 2011.

[17] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 504–512.

[18] 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.

[19] G. Acs and C. Castelluccia, "I have a DREAM!(differentially private smart metering)," in *The 13th Information Hiding Conference (IH)*, 2011.

[20] F. G. Marmol, C. Sorge, O. Ugus, and G. M. Pérez, "Do not snoop my habits: preserving privacy in the smart grid," *Communications Magazine, IEEE*, vol. 50, no. 5, pp. 166–172, 2012.

[21] M. Badra and S. Zeadally, "Design and performance analysis of a virtual ring architecture for smart grid privacy," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 2, pp. 321–329, 2014.

[22] 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.

[23] Z. Wang and G. Zheng, "Residential appliances identification and monitoring by a nonintrusive method," *Smart Grid, IEEE Transactions on*, vol. 3, no. 1, pp. 80–92, March 2012.

[24] 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.

[25] 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.

[26] 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.

[27] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A stackelberg game approach," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 120–132, March 2013.

[28] Z. Baharlouei and M. Hashemi, "Efficiency-fairness trade-off in privacy-preserving autonomous demand side management," *Smart Grid, IEEE Transactions on*, vol. 5, no. 2, pp. 799–808, March 2014.

[29] 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.

[30] C. Rottondi, A. Barbato, and G. Verticale, "A privacy-friendly game-theoretic distributed scheduling system for domestic appliances," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, Nov 2014, pp. 860–865.

[31] L. Sankar, S. Kar, R. Tandon, and H. Poor, "Competitive privacy in the smart grid: An information-theoretic approach," in *Smart Grid Commu-*

nications (SmartGridComm), 2011 IEEE International Conference on, Oct 2011, pp. 220–225.

[32] E. Belmega, L. Sankar, and H. Poor, “Repeated games for privacy-aware distributed state estimation in interconnected networks,” in *Network Games, Control and Optimization (NetGCooP), 2012 6th International Conference on*, Nov 2012, pp. 64–68.

[33] C. Y. Ma and D. K. Yau, “On information-theoretic measures for quantifying privacy protection of time-series data,” in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS ’15. New York, NY, USA: ACM, 2015, pp. 427–438.

[34] A. Barbato, A. Capone, L. Chen, F. Martignon, and S. Paris, “A distributed demand-side management framework for the smart grid,” *Computer Communications*, vol. 57, pp. 13–24, 2015.

[35] D. Monderer and L. S. Shapley, “Potential games,” *Games and economic behavior*, vol. 14, no. 1, pp. 124–143, 1996.

[36] N. S. Kukushkin, “Best response dynamics in finite games with additive aggregation,” *Games and Economic Behavior*, vol. 48, no. 1, pp. 94–110, 2004.

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

[38] E. Bertino, D. Lin, and W. Jiang, “A survey of quantification of privacy preserving data mining algorithms,” in *Privacy-Preserving Data Mining*, ser. Advances in Database Systems, C. Aggarwal and P. Yu, Eds. Springer US, 2008, vol. 34, pp. 183–205.

[39] MICENE Project,Official web site (ITA), http://www.eerg.it/index.php?p=Progetti_-_MICENE, feb 2015.

Cristina Rottondi received both Master and Ph.D. Degrees cum laude in Telecommunications Engineering from Politecnico di Milano in 2010 and 2014 respectively. She is currently postdoctoral researcher in the Department of Electronics, Information, and Bioengineering (DEIB) of Politecnico di Milano. Her research interests include communication security in the metering infrastructure of smart grids, energy management in smart buildings, and optical networks planning.

Antimo Barbato Antimo Barbato is a postdoctoral researcher in the Department of Electronics, Information, and Bio-engineering (DEIB) at Politecnico di Milano, Italy. He received the Bachelor degree in Telecommunications Engineering from the University of Naples Federico II, Italy, and the Master of Science degree in Telecommunications Engineering from Politecnico di Milano. In 2013, he received his PhD in Information and Communication Technologies from Politecnico di Milano. His research interests include optimal systems operation, communication technologies and data science for Smart Grids.

Lin Chen (S07-M10) received his B.E. degree in Radio Engineering from Southeast University, China in 2002 and the Engineer Diploma from Telecom ParisTech, Paris in 2005. He also holds a M.S. degree of Networking from the University of Paris 6. He currently works as associate professor in the department of computer science of the University of Paris-Sud. He serves as Chair of IEEE Special Interest Group on Green and Sustainable Networking and Computing with Cognition and Cooperation, IEEE Technical Committee on Green Communications and Computing. His main research interests include modeling and control for wireless networks, distributed algorithm design and game theory.

Giacomo Verticale is Researcher at Politecnico di Milano, Italy. He is co-head of the Broadband Optical Networks, Security and Advanced Internet (BONSAI) Laboratory in the Department of Electronics, Information, and Bioengineering (DEIB). Before joining Politecnico di Milano, he was with the CEFRIEL research center. He graduated in 2003 at Politecnico di Milano defending a thesis on the performance of packet transmission in 3G mobile networks. His research interests are in network security and in performance evaluation of network protocols.