# Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures

Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, Tim A. Lewis and Rafael Cepeda
Toshiba Research Europe Limited, Telecommunications Research Laboratory, 32 Queen Square, Bristol, BS1 4ND, UK
Email: {george, costas, stojan.denic, timl, rafael}@toshiba-trel.com

***Abstract*—Smart grid privacy encompasses the privacy of information extracted by analysing smart metering data. In this paper, we suggest that home electrical power routing can be used to moderate the home's load signature in order to hide appliance usage information. In particular, 1) we introduce a power management model using a rechargeable battery, 2) we propose a power mixing algorithm, and 3) we evaluate its protection level by proposing three different privacy metrics: an information theoretic (relative entropy), a clustering classification, and a correlation/regression one; these are tested on different metering datasets. This paper sets the ground for further research on the subject of optimising home energy management with regards to hiding load signatures.**

## I. Introduction

Smart grids are an emerging engineering challenge to reform the world's electrical grids [1]. Their aim is to use advanced information control and communication technologies to save energy, reduce cost, and, ultimately, meet environmental goals such as the EU's 20-20-20 goals (20% increase in energy efficiency, 20% reduction of $CO_2$ emissions, and 20% renewables by 2020) [2]. This challenge will require significant efforts in technology development, standards, policy and regulatory activities because of its inherent complexity.

Smart grids differ from current (legacy) power grids in that they interconnect their components with a two-way communications network to support real-time optimisations such as load shedding/management, distributed energy storage (e.g. in electric vehicles), and distributed energy generation (e.g. from renewable resources)—this system is referred to as Advanced Metering Infrastructure (AMI). Smart meters have a pivotal role in AMI: they can measure energy consumption in much more detail than conventional meters, communicate collected information to authorised parties (e.g. utility providers), and facilitate power monitoring and control.

The security of AMI data is considered to be of prime importance, given the scale of potential threats. A classification of smart grid risks and vulnerabilities has been drafted by NIST [3]. In addition, a comprehensive specification of AMI security requirements has been published by OpenSG [4].

The problem of smart grid privacy has been widely discussed in the media [5]. In an elaborate review, Quinn [6] argues that AMI provides a window into the activities within homes, exposing once private activities to anyone with access to electricity usage information. This privacy threat goes beyond the exposition of private information to a common 'spy'; AMI can facilitate the collating and analysing of such personal data on an industrial scale.

In this paper we introduce a method to hide information contained in consumption data by moderating home load signatures, after mixing utility energy with energy provided by, or required by, a rechargeable battery (§III). Ideally (from a privacy viewpoint) we wish to hide or obscure load signatures so that appliance usage events cannot be detected. In practical scenarios, 'perfect privacy' cannot be achieved due to a number of physical limitations and cost, which gives rise to an energy mixing optimisation problem (§IV). We propose a privacy moderation algorithm and introduce three methods to evaluate different aspects of the offered privacy protection (§V): an information theoretic (relative entropy), a clustering classification, and a correlation/regression one. Results (§VI) and further discussion (§VII) suggest that the proposed algorithm can significantly improve privacy using feasible battery sizes.

## II. Related Work

The information gleaned through metered energy data processing can be demonstrated with the use of *non-intrusive appliance load monitors* (NALM), which can recognise and track appliance usage patterns [7], [8]. There is a rich and ongoing line of research in the construction and upkeep of NALM algorithms, providing means to identify appliance usage even when multiple household power signatures are aggregated [9], [10]. In the future (considering, for example, a metering data collection interval of 15 minutes) it has been discussed that it will be possible to pinpoint exactly how and when someone has operated certain home appliances [6].

The full extent of smart grid privacy concerns, and its ramifications, is not yet fully understood [3], [11]. NIST has discussed that "the major benefit provided by the Smart Grid, i.e. the ability to get richer data to and from customer meters and other electric devices, is also its 'Achilles' heel' from a privacy viewpoint" [12]. Current work is focusing on policy formulation and enforcement in domains (e.g. utility provider) that will be managing this data [3].

In Europe, data privacy is addressed by the European Union Data Protection Directive ('the Directive') [13], which requires that personal data should (among other things) "be collected for a specified purposes and not be further processed for other purposes". The Directive may protect smart-metered electricity consumers against inadvertent disclosure of the information

978-1-4244-6511-8/10/$26.00 ©2010 IEEE

to parties with nefarious intentions [13]. However, its scope is restricted to safeguard other interests such as a) national or public security; b) police investigations; c) important economic or financial interests; and d) monitoring, inspection or regulatory functions connected, even occasionally, with the exercise of official authority in previous cases. These exceptions (some of which are equivocal) weaken the Directive's protection. Generally, although policies and regulations are essential, the scope of the user data privacy protection they offer is usually constrained, and they cannot be easily enforced.

This paper focuses on solutions that protect smart metering privacy by preventing its exposure. Currently, not many technological solutions exist to protect smart grid privacy; the most relevant one suggests that metering data can be aggregated and encrypted so that an individual's information is anonymised to roughly the scale of a city block [6]. However, data aggregation may be reverse-engineered with the use of NALM, as discussed, and the privacy offered depends on trust relationships and data policies that govern aggregators.

Our proposed privacy protection method does not depend on specific smart grid architectures or trust relationships: we show how privacy can be protected by managing energy usage within the home, before (potentially sensitive) metering data are collected. Our solution can still co-exist with others discussed above, and constitute an additional layer of privacy: this can serve to increase the effectiveness of each solution.

## III. Concept And Overview

### A. Definitions

We define 'load signature' to be a series of time-stamped average power loads $p(t)$ derived from (cumulative) energy values $e(t)$ metered at intervals $\Delta t$, $p(t) = \frac{e(t)-e(t-\Delta t)}{\Delta t}$. A 'home load signature' is the sum of all home appliance loads.

From a privacy point of view, the information contained in a home load signature comprises individual consumption events identified within the (composite) home load signature. We define 'load signature moderation' as a load signature reshaping technique, with which the presence of appliance load signatures may be changed, hidden, smoothed, obfuscated or emulated. Adapting the definition of 'undetectability' from [14], we consider that privacy is protected when, given a home load signature, we cannot sufficiently distinguish whether an appliance load event exists or not.

### B. System Overview

An overview of a home power and communications network is illustrated in Fig. 1 comprising a) a smart meter; b) a utility provider; c) consumers: electrical devices or appliances; d) suppliers: alternative private sources of energy such as wind turbines, solar panels, or (electric vehicle) batteries; e) a power router; f) a 'Load Signature Moderator' (LSM): responsible for shaping load signatures via power routing; and g) Home Area Network (HAN): home communications network, for energy management or other purposes.

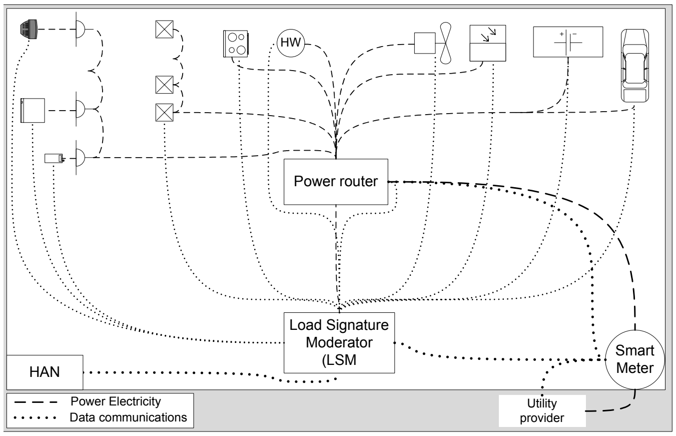

Fig. 1. System overview

In order to perform load signature moderation, we assume that future smart homes will contain a variety of energy storage and energy generation devices, and that 'electrical power routing' is feasible, where this term is taken to mean the selective control and power mixing of a number of electricity sources to 'route' electricity to a number of consumers [15]. An example would be a kettle drawing 2kW of power when switched on; the power router could be configured so that 1kW is supplied from a solar panel, 0.5kW from a battery, and 0.5kW from the mains electricity supply.

Note that the LSM, power router, and smart meter could all be either separate devices or integrated into one device, and they could be physically located near or within future 'smart' fuse boxes or distribution boards.

### C. Threat Detection And Response

The main role of LSM is to 'detect a privacy threat' and respond by 'configuring power routing'. The LSM may detect a threat after it identifies a power consumption event (within the home); this could be a power trigger generated by a consumer or supplier, such as a change in power consumption (e.g. appliance switch-on/off event).

Threats may, alternatively, be detected after processing information communicated within the HAN: smart appliances may notify the LSM of scheduled, desired, or predicted future events within the HAN. For example, the LSM and the washing machine may organise (or negotiate) an operational schedule (e.g. when a private supplier is speculated to sufficiently cover projected energy demands). In this case, the LSM needs to allocate resources optimally and prepare power routing configuration rules for expected power events.

Some basic privacy-driven LSM power mixing examples are given in Fig. 2, in which the private supplier is taken to be a rechargeable battery. In Fig. 2a, all appliance demand is supplied by the battery, which is later on slowly recharged; the resulting metered load signature hides (absorbs) the appliance consumption event. In Fig. 2b, the appliance demand is covered by a mix of battery and utility energy. The metered load signature is smoother than the appliance load signature, which in this manner masks the appliance consumption event. Finally, in Fig. 2c, we obfuscate the load signature by restoring the used battery energy in a series of recharging events; in

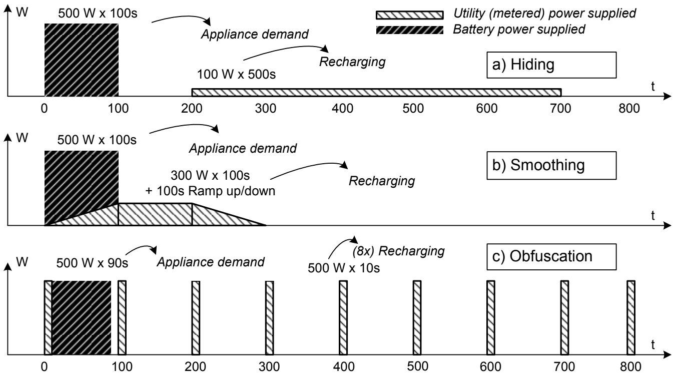

Fig. 2. Example load shaping strategies

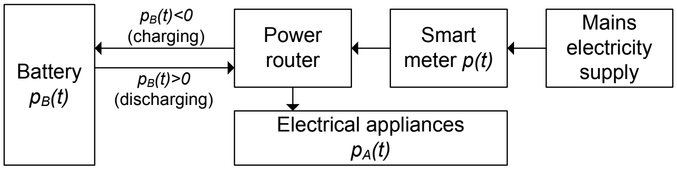

Fig. 3. Battery power mixing moderation model

this case the utility may not be able to determine which spike coincides with the appliance event.

An LSM power mixing (e.g. battery moderation) algorithm should be subject to diverse constraints such as power efficiency ones (e.g. pricing costs and *demand-side management*), available home energy resources, and user requirements. In §IV-B we propose a simple algorithm for real-time battery power mixing reconfiguration, in favour of privacy.

## IV. Problem Formulation

### A. The Rechargeable Battery Model

Suppose that there is a rechargeable battery that can be discharged or recharged within a metering interval $\Delta t$ with power $p_B(t)$, which is configured to 'disguise' a given consumption load $p_A(t)$ (e.g. home load, excluding the battery); this model is illustrated in Fig. 3. Also suppose (for simplicity) that this battery can fully discharge/recharge without any losses.

With the use of the battery, the metered home load becomes $p(t) = p_A(t) - p_B(t)$. The objective is to modify $p_B(t)$ in order to moderate $p(t)$ in a manner that makes $p_A(t)$ undetectable, i.e. $p_A(t)$ cannot be determined given $p(t)$. This modification is bounded by the physical battery capabilities:

1) The battery has a finite capacity $B_E$ (hence, it has to maintain its energy by recharging), i.e. $0 \leq \int_0^T p_B(t)dt \leq B_E$, for all $T \geq 0$ (assuming that for $t = 0$, the battery is fully charged).
2) The battery has a maximum discharge and recharge power of $B_P$, i.e. $|p_B(t)| \leq B_P$.

Intuitively, the level of privacy protection should approach a maximum when $p(t) = 0$, for $0 \leq t \leq T - \Delta t$ (the battery covers all the power demand), and $p(T) = C = \int_0^T p_A(t)dt$, for $T - \Delta t < t \leq T$ (battery fully recharges): privacy should be maximised when $T \to \infty$; however, this would require $B_E \to \infty$. Alternatively, it should be equally secure to have $p(t) = C/T$ for $0 \leq t \leq T$ (the load $p_A(t)$ is transformed to a constant value representing its average): this moderation should use the battery more efficiently but, on the downside, it requires knowledge of all future consumption events.

The problem is how to maximise privacy protection, given any set of loads $p_A(t)$, for any $0 \leq t \leq T$, battery capacity/power bounds ($B_E$, $B_P$), and no knowledge of the future. Suppose that a moderated home load $p(t)$ is introduced by a transformation $\mathcal{G}$ on the (real-time) appliance load demand $p_A(t)$ such that $p = \mathcal{G}p_A$. In order to design an optimal $\mathcal{G}$, it is necessary to measure the level of protection it offers.

To evaluate $\mathcal{G}$, we first define what needs to be protected. Given a load dataset $p_A(t)$, the difference between successive power measurements, $dp_A(t) = p_A(t) - p_A(t - \Delta t)$, represents a change (or not) of the state of some appliance as its power usage increases/decreases (or remains the same). We consider that any change (or no change) of appliance state, is 'private information'; hence, we wish to measure the degree to which $dp_A(t)$ is detectable, given $dp(t)$ after the application of $\mathcal{G}$.

### B. Bounded Moderation Algorithm

Given the battery bounds ($B_E$, $B_P$) we propose the following 'best-effort' privacy algorithm: the idea is to resist (to the degree possible) against power load changes, i.e. to maintain a constant metered load $p(t)$ as such. The algorithm will force the battery to either discharge or recharge when the required load $p_A(t)$ is either larger or smaller (respectively) than the previously metered load $p(t - \Delta t)$. The power and duration of battery charging/discharging is configured to equal the power differences, unless battery bounds are reached. The outline of this algorithm $\mathcal{G}$ is given in Table I.

TABLE I
'Best-Effort' Moderation Algorithm $\mathcal{G}$

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

We should note that this algorithm is by no means designed to be 'optimal', as discussed in §IV-A. However, it can be used for benchmarking the privacy different batteries offer.

## V. Measuring Privacy Protection

In cryptography, privacy protection is typically discussed in the context of anonymity: the property of hiding the identity of a user associated with a message (rather than hiding the message itself) [16]. Typically, anonymity protocols are analysed stochastically; thus, it is useful to quantify anonymity using information theoretic metrics, for which there is a line of active research [17], [18].

The 'undetectability' problem defined in this paper differs from the anonymity one, as we wish to hide $dp_A(t)$ rather than the user; yet it is similar in a sense, if 'user' is taken to be the signal $dp(t)$—this observation enables us to adapt known information theoretic metrics. Additionally, the nature of this privacy evaluation problem allows us to use other known stochastic and statistical techniques as discussed below.

### A. Privacy Levels Based on Relative Entropy

The *relative entropy* or *Kullback Leibler distance* [19] is a well known information theoretic quantity which can be used to compare two sources of information. To employ this metric in our privacy context, we will assume that $dp_A(t)$ and $dp(t)$ can be modelled as stochastic processes with probability measures $P$ and $Q$. If $f_P(x)$ and $f_Q(x)$ are the *probability density functions* (pdfs) of $P$ and $Q$, the relative entropy $D(P||Q)$ is defined [19]:

$$D(P||Q) = \int_{x_{min}}^{x_{max}} f_P(x) \log \frac{f_P(x)}{f_Q(x)} dx.$$

The importance of the relative entropy is that (although it is not a distance as defined in mathematical sense) it quantifies the relation between $P$ and $Q$. For example, the relative entropy is always positive, and for $P$ identical to $Q$, it is zero. Strictly speaking, the relative entropy is premetric. Accordingly, the level of protection offered by a mapping $\mathcal{G}$ can be measured by the relative entropy $D_{\mathcal{G}}(P||Q)$ such that the higher the level of protection offered by $\mathcal{G}$, the larger the relative entropy.

One can think of other information theoretic privacy metrics [20], such as the the *mutual entropy*, or *equivocance*, introduced in [21], but we leave this for further research.

### B. Similarity Based on Cluster Classification

As a second metric, we consider a simple method of trace analysis that aims to recover information about device power usage within $dp(t)$, and show how this approach yields less information when applied to $dp_A(t)$.

The motivation for clustering data values is based on the observation that power traces have fluctuations around a set of values that correspond to significant power levels of the underlying system. Provided that the fluctuations are small, these power levels can be extracted from the trace. In order to remove the subjective nature of spotting these levels and permit automation of the technique we can use one of the many cluster analysis techniques to locate the presence of these levels [22]. These techniques take a set of data with a distance metric and group them into $n$ clusters that minimise the distance between points. In this paper the distance metric is the difference between power consumption values.

In addition, we use the method of *silhouette maximisation* [23] to choose the best number $n$ of clusters for $dp_A(t)$. By averaging over all points in the dataset (constructing the *silhouette average*), we can extract a measure of how good a clustering is; this allows us to compare with other clusterings of different $n$ and select the *silhouette optimal* $n$. This is dependent on the particular clustering method used, and particular run of algorithm for the non-deterministic versions. We use the 'clara' method from [22] since it is deterministic and scales to the large datasets we use in this paper.

Finally, we use the following method to compute how close $dp(t)$ is to $dp_A(t)$, which is an indication of how well the power consumption transitions $dp_A(t)$ are hidden:

1) Find the silhouette optimal $n$ for $dp_A(t)$.
2) Classify $dp_A(t)$ into set of clusters $\mathcal{A} = \{a_1, \ldots, a_n\}$.
3) Classify $dp(t)$ into set of clusters $\mathcal{B} = \{b_1, \ldots, b_n\}$.
4) Ignore values from cluster $a_1$ and their corresponding values in $\mathcal{B}$ (we assume that $a_1$ corresponds to insignificant power change).
5) Compute the ratio ($\rho$) of 'correct' classifications in $\mathcal{B}$.

### C. Regression Analysis

As a third metric, we quantify privacy by combining *cross-correlation* and *regression* procedures. The idea is that the degree to which $dp$ 'predicts' $dp_A$ can be analysed by a) shifting (in time) $dp$ in order to align it with $dp_A$ at the point of their maximum cross-correlation, and b) comparing the two aligned signals using regression methods. In this paper we use a simple linear regression of the form $dp = \hat{\alpha} + \hat{\beta} dp_A + \epsilon$, in which we have a predicted value $\hat{dp} = \hat{\alpha} + \hat{\beta} dp_A$ affected by noise $\epsilon$, and defined by an *intersection point* $\hat{\alpha}$ and a *slope factor* $\hat{\beta}$. The factors $\hat{\alpha}$ and $\hat{\beta}$ can be estimated by using a least squares linear fit aiming to minimise the square of the distance between every data point and the line of best fit [24].

The overall solution minimises the sum of squared residuals, with a residual being the difference between an observed value $dp(t)$ and the value provided by the model $\hat{dp}(t)$. The validity of the fitting can be tested by using *goodness-of-fit* tests. In this work, we only consider the *coefficient of determination*, $R^2$, which indicates the proportion of variability in a dataset that is accounted for by the statistical model. To define $R^2$, we estimate the error sum of squares $SS_E = \sum_t (dp(t) - \hat{dp}(t))^2$ and the regression sum of squares $SS_R = \sum_t (\hat{dp}(t) - \bar{dp})$, in which $\bar{(\cdot)}$ represents the mean value. Then, it follows that:

$$R^2 = 1 - \frac{SS_E}{SS_R + SS_E}, \quad 0 \leq R^2 \leq 1.$$

$R^2 = 1$ indicates that predictions are fully explained by the model; whereas, $R^2 = 0$ indicates the opposite. In fact $R^2$ approaches zero when $SS_E \gg SS_R$ or when $SS_R \to 0$. The first case occurs when the noise $\epsilon$ increases, and the second occurs when $dp(t)$ do not change much with respect to $\bar{dp}$ ($\hat{\beta} \to 0$). In either case, we suggest that $R^2$ can be used as a privacy metric: the closer the $R^2$ to zero, the higher the privacy protection level.

## VI. Evaluation of Moderation Algorithm

In our evaluations we use three different datasets $p_A(t)$: one obtained from real-time measurements (*Real*) at an old *Georgian* apartment on a 'busy' 24h period, one reconstructed

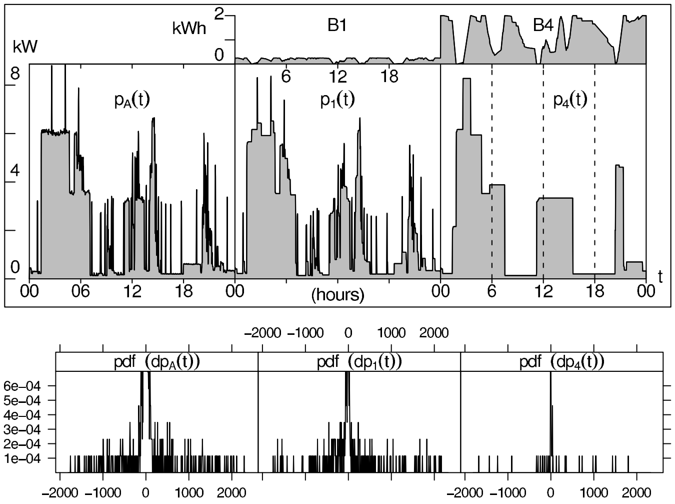

Fig. 4. B1, B4 battery charge levels, $p_A(t)$, $p_1(t)$, $p_4(t)$ load signatures and empirical pdfs for the *Real* dataset

from a signature profile in [6] (*Rec*), and a simulated one (*Sim*) that models a set of 60 home appliances as Markov chains; readings are taken every $\Delta t$ = 1min (this choice is further discussed in §VII).

For each dataset $p_A(t)$, we operate four transformations $\mathcal{G}$, by running our 'best-effort' battery algorithm for four batteries increasing in size: B1, 250W/500Wh; B2, 500W/1kWh; B3, 1KW/2kWh; and B4, 2KW/4kWh (these could be projected by stacking up SCiB$^{\text{TM}}$ batteries [25]). We denote the four moderated (transformed) loads $p_i(t)$, for $i = \{1, 2, 3, 4\}$.

Figure 4 shows the B1, B4 battery charge level fluctuations; the $p_A$, $p_1$, and $p_4$ load signatures; and the pdfs for respective delta loads, for the *Real* dataset. Note that the pdfs have been computed using a *bin width* of 6W, which equals the quantisation level of the smart meter used for data collection. It should be noticed how the batteries try to resist to changes by discharging/recharging when positive/negative $dp_A(t)$ occur. The larger the battery, the smoother the transformation, and the sparser the delta pdfs.

Figure 5 shows scatter plots for the normalised $(\dot{(\cdot)})$ and aligned $\dot{dp}_A$ vs. $\dot{dp}_i$, $i = 1, 4$, for the *Real* dataset. The $\dot{dp}_A$ vs. $\dot{dp}_A$ case yields a straight line: the norm of the residuals is zero and $R^2$ is one (which means that the model fully predicts the output, as expected). In the other two cases, the uncertainty in the prediction increases. In the case of B1, we notice that when $\dot{dp}_A < 0$ (power drop) the battery induces positive error, and when $\dot{dp}_A > 0$ (power increase) the battery induces negative error. In the case of B4, we can see that for several input values $(\dot{dp}_A)$ the output $(\dot{dp})$ is zero, which indicates that less information is available to predict the output.

The results of all three privacy metrics (§V) across all batteries and datasets, are summarised in Table II. Note that $\rho = R^2 = 0$ and $D(P||Q) \to \infty$ indicate best privacy, whereas $\rho = R^2 = 1$ and $D(P||Q) = 0$ indicate no privacy.

It should be observed that all three metrics indicate that privacy increases with the size of battery, which is a consistent result. The largest battery performs better for *Real*: cluster similarity and $R^2$ suggest that over 99% of the transitions are disguised—this is attributed to closely distanced events within the *Real* load signature allowing the battery to make good use of its charge level dynamic range. The first three batteries perform marginally better for *Rec*: this is due to *Rec* having a larger percentage of smaller power delta values. *Sim* is hard to protect: the batteries just aren't large enough to considerably modify the values and their pdf. However the cluster similarity suggests that batteries B3 and B4 are disguising 90% of the second cluster, which still is a positive result.

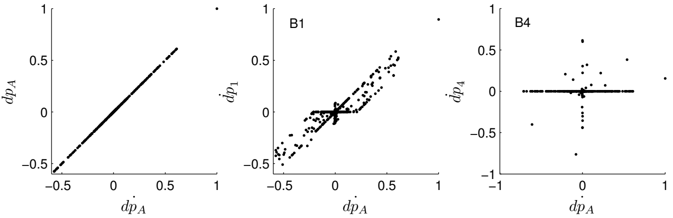

Fig. 5. Scatter plot of $\dot{dp}_A$ vs. $\dot{dp}_1$ and $\dot{dp}_4$

TABLE II

EVALUATIONS OF THREE PRIVACY METRICS (FOR DIFFERENT DATASETS)

| Dataset<br>$(dp_A)$ | Battery<br>$(dp_i)$ | Rel. Entropy<br>$D(P\|\|Q)$ | Cluster<br>sim/ty | Reg/sion<br>coeff. $R^2$ |
|---|---|---|---|---|
| <u>*Real*</u> | B1 | 1.455 | 0.468 | 0.871 |
| $dp_{A,max} = 4.5$kW | B2 | 1.638 | 0.320 | 0.645 |
| 1386 events | B3 | 1.921 | 0.135 | 0.182 |
| 4 clusters | B4 | 3.237 | 0.004 | 0.008 |
| <u>*Rec*</u> | B1 | 0.662 | 0.496 | 0.831 |
| $dp_{A,max} = 6.9$kW | B2 | 0.691 | 0.228 | 0.468 |
| 1864 events | B3 | 0.860 | 0.055 | 0.167 |
| 3 clusters | B4 | 1.059 | 0.016 | 0.074 |
| <u>*Sim*</u> | B1 | 1.106 | 0.854 | 0.992 |
| $dp_{A,max} = 38$kW | B2 | 1.301 | 0.812 | 0.982 |
| 12389 events | B3 | 1.531 | 0.104 | 0.955 |
| 2 clusters | B4 | 1.770 | 0.104 | 0.878 |

It should be noted that all three metrics evaluate different aspects of privacy: the relative entropy and cluster similarity assume that $dp_A(t)$ and $dp(t)$ are represented by the collection of independent and identically distributed random variables, whereas in regression timing is critical. For example, consider the case where two appliance events in $dp_A(t)$ are swapped; this will change (permute) the signal in time but not its pdf; hence, the regression coefficient yields improved level of privacy, whereas the relative entropy and cluster similarity yield no improvement. Still, there is value in all results: probabilistic measures become more suitable when we prefer to protect the information associated with the occurrence of an event (in case of relative entropy) or a group of similar events (in case of cluster classification), rather than the time of its occurrence; whereas regression becomes more suitable when the privacy of the 'timing information' is also important. It appears that our proposed battery moderation algorithm improves the privacy level in all these aspects.

## VII. DISCUSSION

Different levels of privacy-driven moderation may be required for different appliances at different times. For example, the user may wish to hide the use of a kettle, but not the use of a washing machine (whose large and prolonged energy usage may be difficult to hide). If we consider the load signature of the kettle (or any other appliance) to be 'interference' within the composite load signature, the objective would then be to mitigate this interference. Additionally, the battery may be recharged in a way that inserts fake appliance load signatures. For example, appliance operation (TV, lighting, etc) may be emulated to mask 'unusual' periods of inactivity. In this respect, our 'best-effort' battery could become 'smarter' and offer customised privacy. Further work is required to define and measure customised privacy information and protection level in a unified manner.

On another note, user privacy requirements may conflict with other requirements (such as cost-saving from energy pricing arbitrage). For example, if battery energy is used during a low tariff period, the lost battery energy may need to be restored during a higher tariff period, or, alternatively, an opportunity to store further energy at a low cost may be missed. Furthermore, energy will be lost within a battery. In general, the LSM should use the battery in a manner advantageous to both privacy and efficiency. We leave the evaluation and optimisation of such system economics (e.g. costs against security gains) for further research.

Finally, we comment on the choice of $\Delta t = 1\text{min}$, which assumes that consumption data is collected at intervals no less than that. This means that from the (real-time) detection of a power change (threat) the LSM has (on average) 30 seconds to moderate the next projected reading—the assumption here being that the LSM has access to more frequent internal measurements (e.g. every 10 seconds or less). An event occurring a few seconds before the next minute's reading may not allow enough time to react; still, the error, i.e. the difference between the target (desirable) reading $p(t_i)$ and the recorded reading $p'(t_i)$, should be relatively small (depending on the LSM reaction time and the consumer's demand).

## VIII. Conclusion

This paper introduces a load signature moderation system that protects smart metering data privacy without depending on or restricting smart grid functionalities. A model is discussed where the amount of utility energy required may (partially) hide the consumer's demand, by configuring a power router to determine the power provided or required by a rechargeable battery. Such a system allows users to control (to a certain degree) their energy usage and their home energy privacy.

A battery power mixing privacy algorithm and three metrics have been proposed to test different aspects of privacy protection: relative entropy and clustering evaluate the privacy offered on the probabilistic domain of the occurrence of electricity events, or clusters of events; whereas regression evaluates privacy in the time domain of sequenced events. Results show that different aspects of privacy are improved with increasing battery sizes. This sets the groundwork for future work where the proposed privacy metrics may be expanded (e.g. by combining them with NALM techniques); and, ultimately, 'smarter' battery privacy algorithms may be designed. For example, a detected (in real-time) or expected/predicted (future) event may be masked (with smoothing or dithering), rescheduled, or emulated (if applicable).

## Acknowledgment

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

## References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Magazine*, vol. 7, no. 2, pp. 52–62, 2009.

[2] Z. Fan, G. Kalogridis, C. Efthymiou, M. Sooriyabandara, M. Serizawa, and J. McGeehan, "The New Frontier of Communications Research: Smart Grid," in *Proceedings of the 2010 ACM e-Energy Conference*, Passau, Germany, Apr. 2010.

[3] A. Lee and T. Brewer, *Smart grid Cyber Security Strategy and Requirements*, Feb. 2010, NISTIR 7628, 2nd Draft.

[4] B. Brown, B. Singletary, B. Willke, C. Bennett, *et al.*, *AMI System Security Requirements*, Dec. 2008, AMI-SEC TF.

[5] http://voices.washingtonpost.com/securityfix/2009/11/experts_smart_grid_poses_priva.html.

[6] E. L. Quinn, "Privacy and the New Energy Infrastructure," Feb. 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731.

[7] G. W. Hart, "Nonintrusive Appliance Load Monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[8] C. Laughman, D. Lee, R. Cox, S. Shaw, *et al.*, "Power Signature Analysis," *IEEE Power and Energy Magazine*, pp. 56–63, 2003.

[9] H. Y. Lam, G. S. K. Fung, and W. K. Lee, "A Novel Method to Construct Taxonomy Electrical Appliances Based on Load Signatures," *IEEE Trans on Consumer Electronics*, vol. 53, no. 2, pp. 653–660, 2007.

[10] A. Prudenzi, "A Neuron Nets Based Procedure for Identifying Domestic Appliances Pattern-of-Use from Energy Recordings at Meter Panel," in *IEEE Power Engineering Society Winter Meeting*, 2002, pp. 941–941.

[11] R. Stallman, "Is digital inclusion a good thing? How can we make sure it is?" *IEEE Comms. Magazine*, vol. 48, no. 2, pp. 112–118, 2010.

[12] NIST, *Framework and Roadmap for Smart Grid Interoperability Standards*, Sep. 2009, Release 1.0 (Draft).

[13] D. J. Solove, M. Rotenberg, and P. M. Schwartz, *Information Privacy 900 (2006): Discussing the European Union Data Protection Directive of 1995*, directive 95/46/EC, http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

[14] A. Pfitzmann and M. Hansen, *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, 2010, v0.33, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.33.pdf.

[15] http://www.powerrouter.com.

[16] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[17] Y. Deng, J. Pang, and W. P., "Measuring Anonymity with Relative Entropy," in *Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust*. Springer, LNCS 4691, 2006, pp. 65–79.

[18] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Proceedings of the workshop on Privacy Enhancing Technologies*, R. Dingledine and P. F. Syverson, Eds. Springer, LNCS 2482, 2002, pp. 41–53.

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

[20] K. Chatzikokolakis, C. Palamidessi, and P. Panangaden, "Anonymity protocols as noisy channels," *Information and Computation*, vol. 206, no. 2-4, pp. 378–401, 2008.

[21] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[22] R Development Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2009, http://www.R-project.org.

[23] P. Rousseeuw, "Silhouettes: A graphical aid to the interpretation and validation of cluster analysis," *Journal of Computing and Applied Mathematics*, vol. 20, pp. 53–65, 1987.

[24] W. Hines, D. Montgomery, D. Goldsman, and C. Borror, *Probability and statistics in engineering*, 4th ed. New York: John Wiley, 2003.

[25] http://www.scib.jp/en/product/spec.htm.