

# Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures

Authors: Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, Tim A. Lewis and Rafael Cepeda

Presenter : Lin Lai

Submitted in Partial Fulfillment of the Course Requirements for  
ECEN 689: Cyber Security of the Smart Grid  
Instructor: Dr. Deepa Kundur

# Overview

- Introduction
- Related work
- System overview
- Moderation strategy
- Measuring privacy protection
- Assessment
- References

# Introduction

## Smart grid

Two-way communications within its components:

- Load management
  - Distributed energy storage (in electric vehicles)
  - Distributed energy generation (from renewable resources)
- AMI (Advanced Metering Infrastructure)

# Introduction

## Smart meter

- Measure the energy consumption in much more detail
- Communicate collected information to authorized parties

Provide a window into activities within homes, exposing one's private activities to anyone with access to electricity usage information.

# Related work

## 1. Policy level

Personal data should “be collected for specified purposes and not be further processed for other purposes” (European Union Data Protection Directive)

Exceptions:

- a) national or public security;
- b) police investigations;
- c) important economic or financial interests;
- d) monitoring, inspection or regulatory functions connected with the exercise of official authority in previous cases.

# Related work

## 2. Technology level

Metering data can be aggregated and encrypted so that an individual's information is anonymised.

NALM (Non-intrusive appliance load monitors)

NALM algorithms, providing means to identify appliance usage even when multiple household power signatures are aggregated

# Related work

## NALM

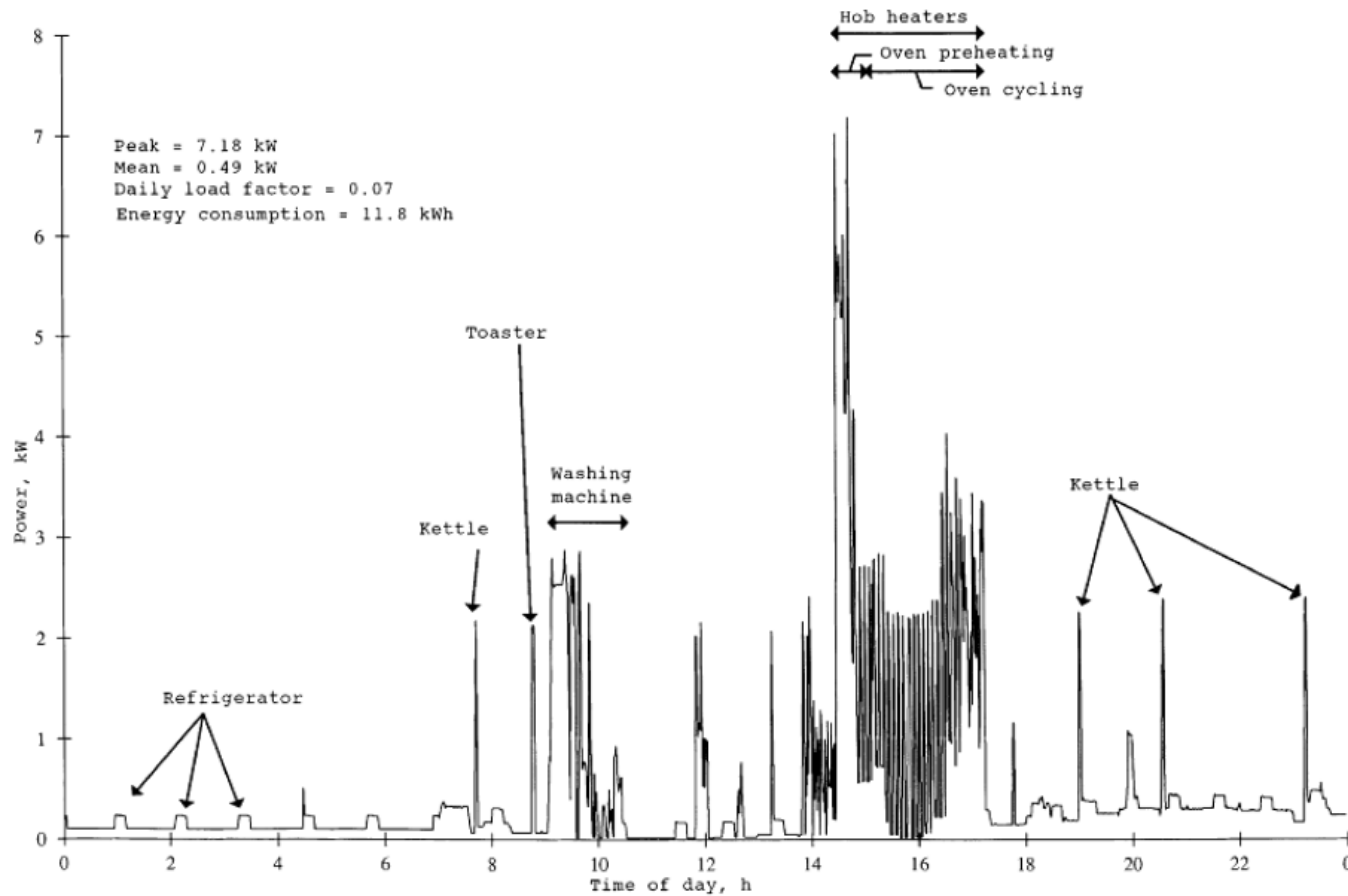


Fig. Household electricity demand profiled<sup>[2]</sup>

# Motivation

Protect the privacy by managing energy usage within the home, before metering data is collected.

Privacy is protected: given load signature of a house, we cannot sufficiently distinguished whether an appliance load event exists or not.



# System overview

- a) a smart meter;
- b) a utility provider;
- c) consumers: electrical devices or appliances;
- d) suppliers: alternative private sources of energy;
- e) a power router;
- f) a 'Load Signature Moderator' (LSM): responsible for shaping load signatures via power routing;
- g) Home Area Network (HAN): home communications network, for energy management or other purposes.

# System overview

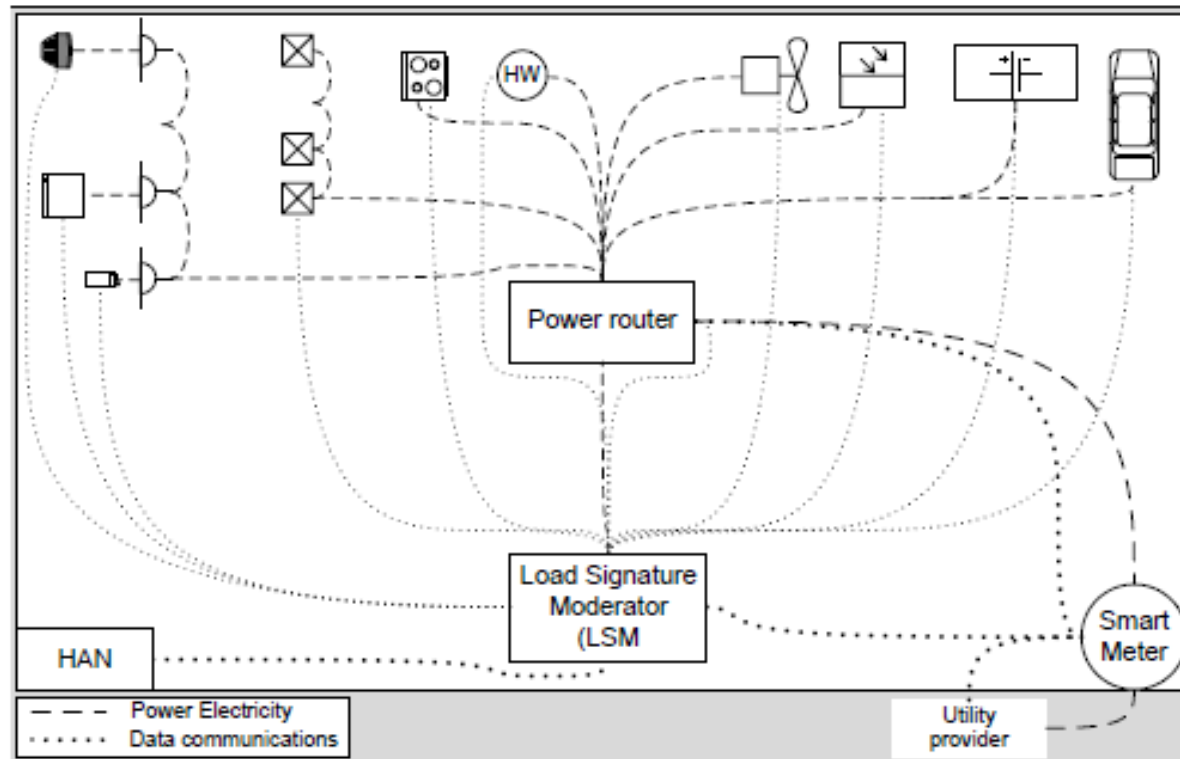


Fig. System overview<sup>[1]</sup>

# System overview

## Load signature moderation

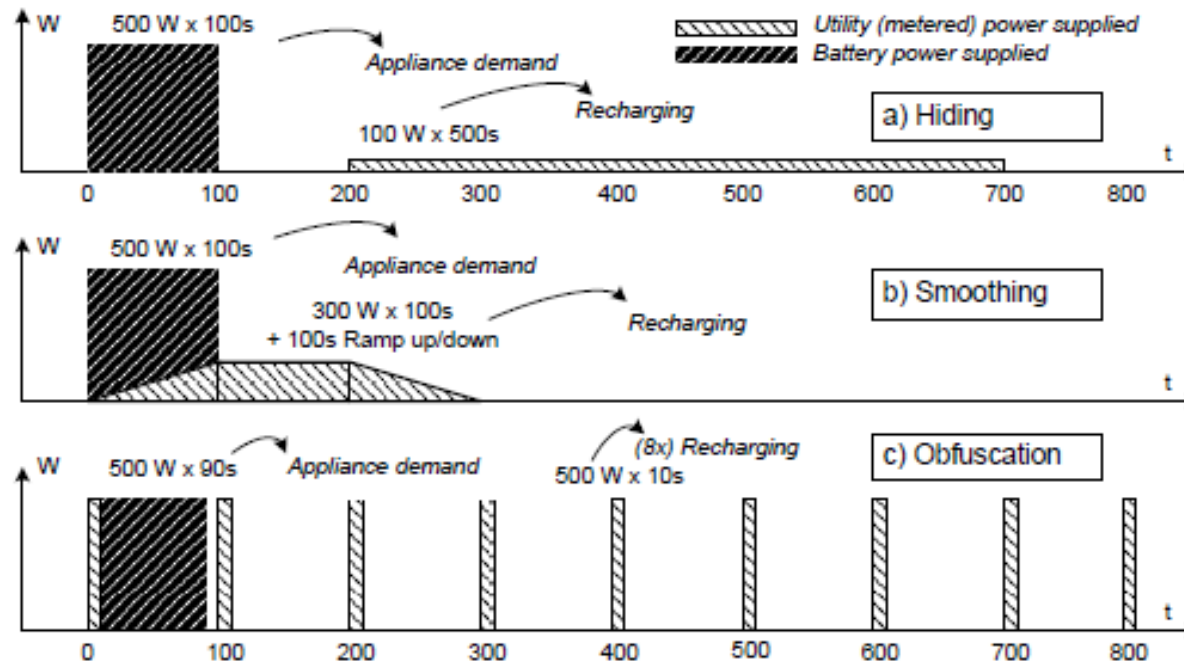
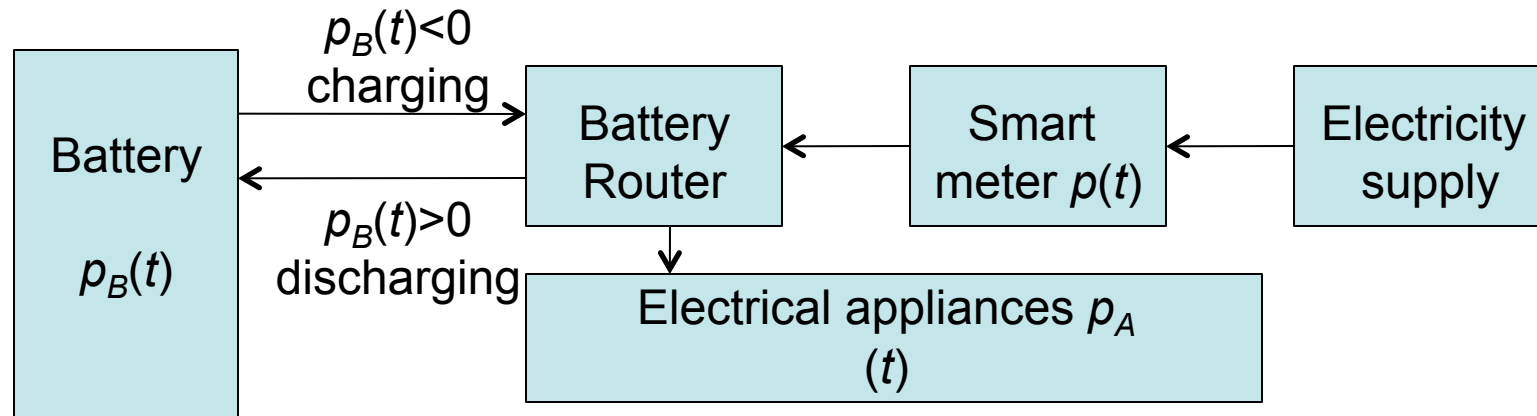


Fig. Example of load shaping strategy [1]

# Moderation Strategy



$$p(t) = p_A(t) - p_B(t)$$

- $p(t)$  – the metered home load
- $p_A(t)$  – given consumption load
- $p_B(t)$  – the battery charge and discharge power

# Moderation Strategy

Bounded moderation algorithm:

Resist against power load changes (to maintain a constant metered load  $p(t)$ ).

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  $p(t - \Delta t)$ .

# Moderation Strategy

## Bounded moderation algorithm:

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**

# Measuring privacy protection

Privacy levels based on relative entropy:

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

$dp_A(t)$  and  $dp(t)$  are modeled as probability measures  $P$  and  $Q$ ;

$f_P(x)$  and  $f_Q(x)$  are the probability density functions of  $P$  and  $Q$ ;

The higher the level of protection, the larger the relative entropy.

# Measuring privacy protection



## Evaluation

Datasets of  $p_A(t)$ :

obtained from real-time measurements at an old Georgian apartment on a 'busy' 24h period.

Reading takes every 1 min.

Four batteries: B1, 250W/500Wh; B2, 500W/1kWh; B3, 1KW/2kWh; and B4, 2KW/4kWh



# Measuring privacy protection

## Simulation result

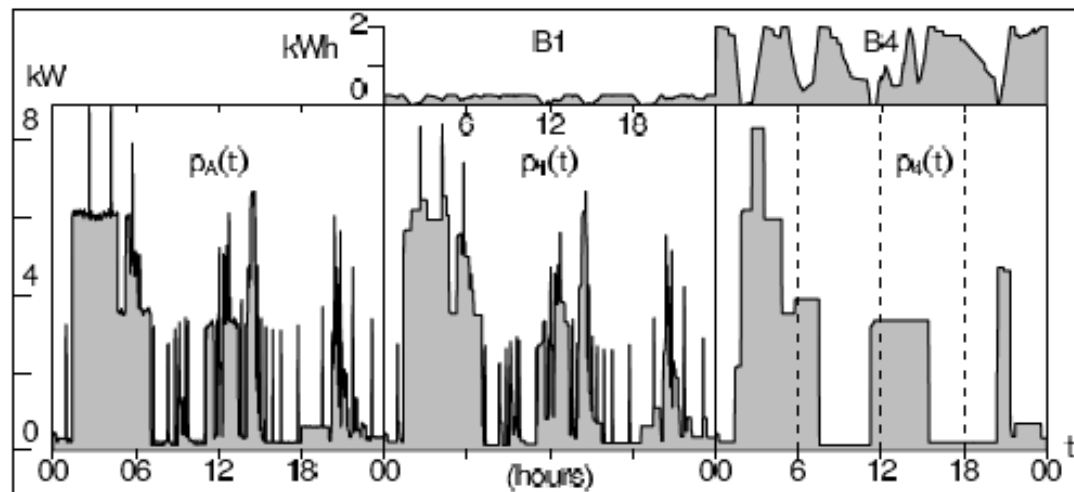


Fig. B1,B4 battery charge levels,  $p_A(t), p_1(t), p_4(t)$  load signature<sup>[1]</sup>

Dataset	Battery	D(P  Q)	Cluster	R <sup>2</sup>
Max=4.5kw 1386 events 4 clusters	B1	1.455	0.468	0.871
	B2	1.638	0.320	0.645
	B3	1.921	0.135	0.182
	B4	3.237	0.004	0.008

# Assessment

- The balance between the privacy and the efficiency;
- “Smarter” algorithm can be designed. Expected/ predicted event may be masked or rescheduled;
- Fake appliance load signature can be inserted by charging the battery.

# References

1. G. Kalogridis, C. Efthymiou, S.Z. Denic, T.A. Lewis, R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," *Proc. IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, October 2010. Related work
2. E. L. Quinn, "Privacy and the New Energy Infrastructure," Feb. 2009, <http://papers.ssrn.com/sol3/papers.cfm?abstract id=1370731>.
3. 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.
4. 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.