Generating Power Footprints without Appliance Interaction: an Enabler for Privacy Intrusion

A. Sintoni[†], A. Schoofs[†], A. Doherty[*], A.F. Smeaton[*], G.M.P. O'Hare[†], A.G. Ruzzelli[†]
CLARITY: Centre for Sensor Web Technologies
[†]University College Dublin
[*]Dublin City University
Dublin, Ireland

***Abstract*—Appliance load monitoring (ALM) systems are systems capable of monitoring appliances' operation within a building using a single metering point. As such, they uncover information on occupants' activities of daily living and subsequently an exploitable privacy leak. Related work has shown monitoring accuracies higher than 90 % achieved by ALM systems, yet requiring interaction with appliances for system calibration. In the context of external privacy intrusion, ALM systems have the following obstacles for system calibration: (1) type and model of appliances inside the monitored building are entirely unknown; (2) appliances cannot be operated to record power footprints; and (3) ground truth data is not available to fine-tune algorithms. Within this work, we focus on monitoring those appliances from which we can infer occupants' activities. Without appliance interaction, appliances' profiling is realised via automated capture and analysis of shapes, steady-state durations, and occurrence patterns of power loads. Such automated processes produce unique power footprints, and naming is realised manually using heuristics and known characteristics of typical home equipment. Data recorded within a kitchen area and one home illustrates the various processing steps, from data acquisition to power footprint naming.**

I. Introduction

A. Fine-Grained Electricity Monitoring

Electricity represents 41% of the total energy used in the Unites States [1], and about one third of it is wasted [2]. Recent efforts for a modernised electrical grid—*smart grid*—are primary triggers to counterbalance and reduce electricity consumption [3]. Smart meters are being introduced within homes for providing real-time access to power readings remotely, facilitating utilities' global control and management of electricity consumption and generation, respectively.

As a short-term alternative to longer-term smart meter widespread deployment, commercial electricity monitors reduced to mere electricity reading and local reporting are also being made available. Such devices measure a rich cocktail of electrical parameters and provide real-time power consumption feedback to electricity consumers.

This work will demonstrate that access to electricity readings via the introduction of smart meters and electricity monitors enables illicit monitoring of private activities of daily living.

B. Enabler for privacy intrusion

Activities of Daily Living (ADLs) include, but are not limited to cooking, showering, washing, and sleeping; they therefore involve interactions with electrical equipment. Appliance load monitoring (ALM) systems are systems capable of monitoring appliances' operation within a building using a single metering point. As such, they uncover information on occupants' interactions with electrical equipment and subsequently an exploitable ADL privacy leak. The privacy of ADLs is a matter well-discussed elsewhere [4], [5], [9]. For instance, such privacy intrusion may be inappropriately used to infer medical conditions [6] or to simply inquire a person's presence for a potential burglary [9]. Related work has shown monitoring accuracies higher than 90 % achieved by ALM systems, yet requiring interaction with appliances for system calibration. In the context of external privacy intrusion, ALM systems have the following obstacles for system calibration: (1) type and model of appliances inside the monitored building are entirely unknown; (2) appliances cannot be operated to record power footprints; and (3) ground truth data is not available to fine-tune algorithms.

Within this work, we focus on monitoring those appliances from which we can infer occupants' activities. Without appliance interaction, appliances' profiling is realised via automated capture and analysis of shapes, steady-state durations, and occurrence patterns of power loads. Such automated processes produce unique power footprints, and naming is realised manually using heuristics and known characteristics of typical home equipment.

II. Related work

The potential abuse of ALM systems for surveillance purpose has been discussed abundantly [9]. Power-based surveillance for monitoring the activities of suspected criminals or political opposition; identifying the movements of occupants to time a break-in; advertising consumers lacking consumer appliances; taxing bad electricity users turning on their air-conditioning system in restricted hours are exemplars. Privacy intruders may range from single individuals to enterprises and utilities themselves.

Appliance load monitoring systems are designed to achieve a building's power decomposition, down to equipment level.

Appliance *signatures* are measurable parameters of the total load that give information about the nature or operating state of individual appliances in the load [12]. They are therefore the patterns that ALM systems try to extract from a congregated building power signal. Knowing appliances' signatures, complex pattern recognition techniques return the list of appliances which combination of signatures provides the best match with the measured signal, e.g. [7], [12].

Mature research in the area of appliance load monitoring has as yet not been transferred to actual commercial integration. Indeed, most ALM systems require complex calibration and verification to be carried out by a trained technician or an auxiliary system [8] before it can be used in a domestic or commercial environment. Hart *et al.* proposed an automatic set-up nonintrusive appliance load monitoring system (AS-NALM), setting the basic steps for an automated capture and naming of appliance signatures. Since then, a number of calibration-free systems have been proposed. Molina-Markham *et al.* [10] utilise statistical methods to derive complex appliances' usage patterns from electricity readings, claiming no prior knowledge of household activities and no training phase. They however relate to power activity journals annotated by home occupants and used to map opaque labels to real-life events. Unless occupants agree to be monitored and provide such brief logs, those cannot be assumed for configuring appliance load monitoring systems. Lisovich *et al.* [11] provide a technical study showing how activity information can be extrapolated from power-consumption data. They assume that the adversary has a list of appliances present inside, as well as their turn-on/turn-off profiles.

Although automated calibration and risks of privacy issues are well-discussed, few systems have been implemented and evaluated for exploiting effectively such privacy leaks in a real-world scenario where pre-calibration is impossible. This work proposes an initial experimental evaluation of such system in an ADL privacy case study. We argue that identifying the monitoring objective prior to operation is essential to achieving high accuracy, focusing monitoring on the subset of appliances of interest and discarding uninteresting power activity.

III. Monitoring Activities of Daily Living using a Single Electricity Monitor

Primary challenges in deriving activity patterns of a building occupant from a single electricity monitor are threefold. First, the intruder needs to have access to the building power flow. Second, the attacker requires an appliance load monitoring system that can disaggregate a power load without prior knowledge of the building appliances' signatures. Finally, appliance activities need to be matched to ADLs.

We investigate the case of power flow captured at the live wire, via illicit clamping of an electricity monitor, see Figure 1. Electric meters may be located in the power pylon serving the property; in a meter-box external to the house; in a public space such as a building's corridor or an office open distribution board; or inside the premises. Once the electricity monitor is clamped, raw electricity consumption of the building under surveillance is reported wirelessly to the intruder's PC-class machine.

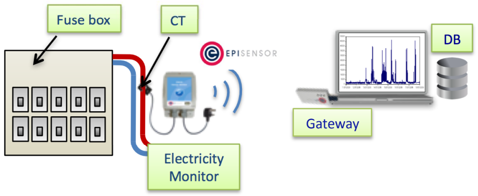


Fig. 1. Illicit clamping of an electricity monitor returns a building's electricity readings to the intruder's machine.

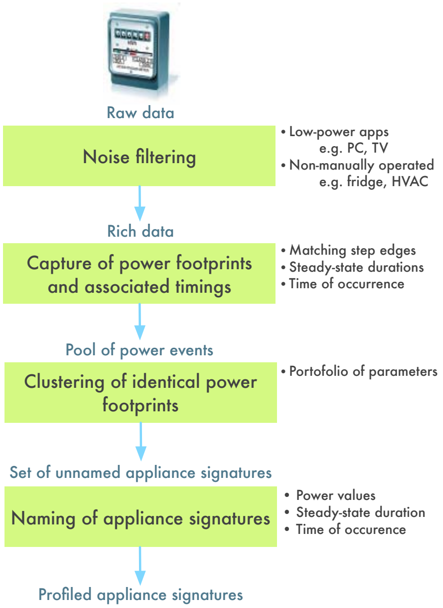

Raw data
Noise filtering
• Low-power apps e.g. PC, TV
• Non-manually operated e.g. fridge, HVAC
Rich data
Capture of power footprints and associated timings
• Matching step edges
• Steady-state durations
• Time of occurrence
Pool of power events
Clustering of identical power footprints
• Portofolio of parameters
Set of unnamed appliance signatures
Naming of appliance signatures
• Power values
• Steady-state duration
• Time of occurence
Profiled appliance signatures

Fig. 2. Four-step processing of the raw electricity data captured at the electric meter to profile appliance signatures passively.

A. Profile-free Appliance Load Monitoring System

In order to disaggregate a building's power flow without access to the premises, the appliance load monitoring system used by the intruder needs to be free of any human supervised calibration procedure.

The technique we propose takes advantage of the attacker's prior knowledge of the kind of appliances and patterns that he wishes to recognise. In an ADL intrusion context, appliances that will indicate an occupant activity are the ones that are instrumented during an ADL, reducing the monitoring objectives to their detection. For instance, detecting the activity of a fridge compressor has no intrinsic value as it is not linked to any user activity, and is either filtered out or kept unnamed.

The proposed technique follows a four-step processing on the raw power flow, as shown in Figure 2. The following describes in greater details the four steps using experimental data to illustrate.

1) Noise filtering and capture of power signatures: These two initial processing steps consist of detecting and recording

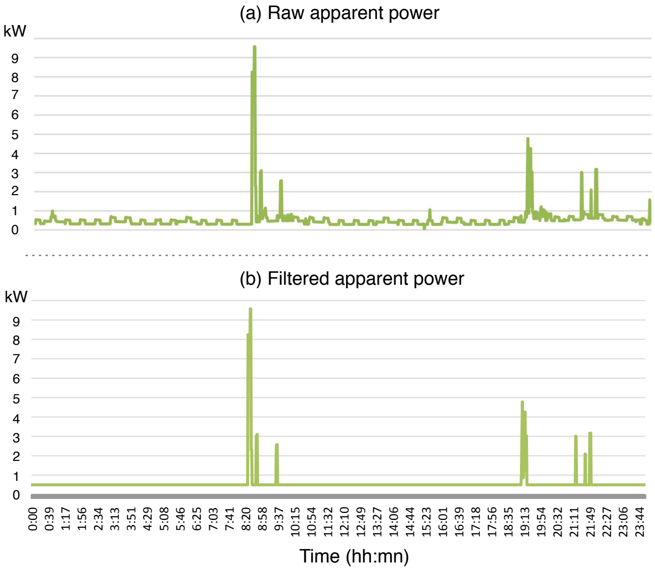


Fig. 3. (a) Capture of power flow over one day illustrating appliance activity, and (b) Filtered power flow over one day revealing only the significant appliance activity.

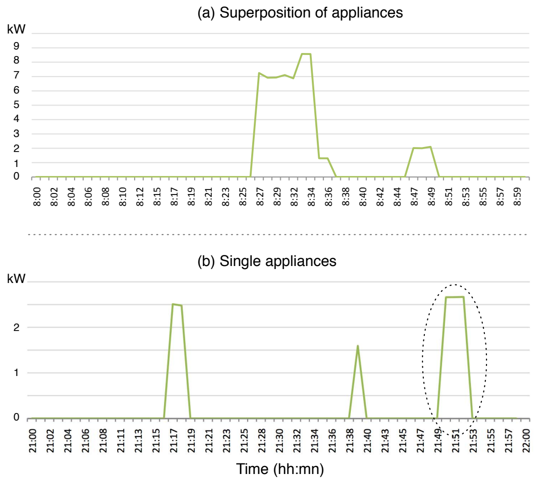


Fig. 4. (a) Zoom to the 8am-9am time slot indicates superposition of appliance signatures, and (b) Zoom to the 9pm-10pm time slot indicates single appliance signatures.

any power steps on the electricity reading that may be useful for the attacker. At this point, the attacker does not know anything about the appliances, habits and patterns of the occupant being tracked. Figure 3(a) shows the apparent power of a one-person household, captured by the electricity monitor over a period of one day. Activity is visible in the morning between 8 and 9am, and in the evening between 7 and 10pm.

In an ADL intrusion context, noise is considered as being the power associated to always-on appliances and appliances with periodic patterns, such as the periodic power step visible on Figure 3(a). They indeed cannot be used to uncover manual actuation. A first processing step is therefore to cancel out the noise via filtering with thresholds and using pattern recognition techniques. The output of Figure 3(a) after filtering is given in Figure 3(b).

Resulting peaks will often be a superposition of multiple appliances signatures, when several appliances are used concurrently—see zoom to the 8-9am time slot on Figure 4(a). However, as Figure 4(b) shows via a zoom on the 9-10pm apparent power data, single appliance signatures often appear on a power reading, facilitating their capture. The range of electrical parameters as well as a timestamp are recorded for each of the unique power footprints that are detected after filtering. The objective of this second processing step is to aggregate a pool of power footprints to later cluster them type and time wise, in order to facilitate their naming.

2) Clustering of identical power signatures: The third processing step is to cluster identical power footprints, and analyse the times at which they appear. The goal is to derive a distribution of occurrences for each power footprint that will be used for understanding the nature of the appliances.

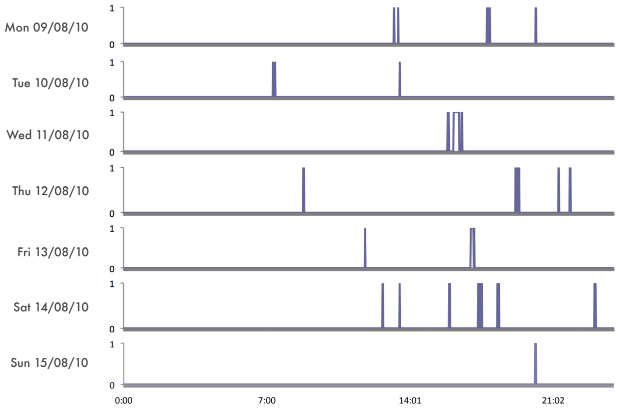


Fig. 5. Distribution of occurrences of the power footprint shown at the right of Figure 4(b) over a period of 7 days. Vertical lines indicate when the power footprint has been detected.

Figure 5 shows as an example the distribution of occurrences of the power footprint that appears at the very right of Figure 4(b). This clustering was produced from one week of data captured at the electricity monitor over a different period. At this point, the attacker has in his hands the power characteristics of a given appliance, such as an apparent power of 2.6 kW in that case, and the times at which such signature has appeared.

3) Naming of appliances signatures: Naming is facilitated by the fact that the attacker knows the typical shape and power characteristics of the appliances signatures he is interested in. Figure 6 recalls generic power footprints for three appliances that can be used for detecting ADLs. They are signatures of an hair-dryer, a toaster, and an oven, used for monitoring cleaning duties, eating, and cooking respectively. These signatures are not the footprints of appliances present within the building, but are footprints of similar appliances procured by the intruder beforehand. Ideally, the intruder will possess a library of signatures which footprints captured within the building can be compared to.

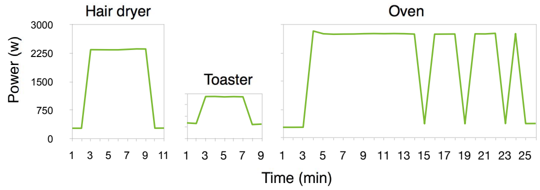


Fig. 6. Generic power signatures of an hair dryer, a toaster, and an oven.

Naming of the building's appliances' signatures is realised by comparing the power characteristics of power footprints detected from the electricity readings with typical appliances' signatures, and reasoning on the produced time distributions of occurrences.

Morning-only distribution of occurrences would be helpful for characterising breakfast-type of machines such as toaster and coffee machines. Power footprints appearing several times per day would as well rule out appliances such as hair dryers, washing machines, and similar appliances that are used at maximum a few times per day. In this example, Figure 5 provides the following hints: (1) the appliance is not a breakfast-type or a cooking-type of equipment (used at random times during the day), (2) the appliance is not a long-activity type of equipment (used over short periods), and (3) the appliance has a repetitive activity pattern (used consecutively over short periods). Such observations point to a kettle. Once names are given to each power footprint, the appliance load recognition system is ready to disaggregate in real-time the power flow. The last step of the ADL monitoring consists of bridging appliances' activities to ADLs.

TABLE I
ADLs THAT MAY BE ASSOCIATED WITH APPLIANCES.

	Eating	Toileting	Moving
Dish-washer	x		
Electric heater		x	
Electric shower		x	
Fitness equipment			x
Hair-dryer		x	
Induction cookers	x		
Kettle	x		
Microwave	x		
Oven	x		
Toaster	x		

B. *Matching appliances' activities to ADLs*

There exist a number of basic ADLs including eating, dressing, washing, and transferring (moving). Such ADLs can be inferred when interaction with appliances exists. For instance, detecting that the microwave is on is a good indication of eating activity. Table I categorises the set of ADLs and associated home appliances that may be used by an attacker in the context of an health condition privacy intrusion. Health condition relates importantly to the ability of a person to eat, wash and move independently. As shown in Table I, there are only few direct activity relationships between appliances and ADLs. Yet, more reasoning may provide extra information not visible in Table I. For instance, observing appliances being switched on consecutively in supposed different rooms, say the oven and the hair dryer, may indicate an occupant's mobility.

IV. Implementation

We developed RECAP-*free*, a calibration-free appliance load monitoring (ALM) system, based on RECAP, an ALM system capable of recognising appliance activities in real-time using a neural network machine learning technique and prior appliance profiling [7]. RECAP-*free* reuses the recognition components from RECAP, but handles discovery and naming of power footprints without equipment interaction.

RECAP-*free* has been implemented in Java. The four conceptual processing steps described in Section III-A have been integrated to provide more efficient coding and have been automated to minimise human supervision. Noise filtering is realised as soon as electricity readings are read to only conserve useful power variations. Power variations are individually analysed and clustered with similar power footprints when existing. At the end of the process, RECAP-*free* profiling engine provides clusters of unique power footprints and timestamps at which they occurred. At this stage, naming of power signatures is the only step done manually.

V. Experimentation

We have initially restricted our tests to a kitchen area, in order to fine-tune our system in a controlled environment with a limited set of appliances. After validation, we ran our algorithms within a real domestic environment for a period of one week.

A. *Fine-tuning the system*

A kitchen area has been equipped with an Episensor electricity monitor [13]. The monitoring setup is similar to that presented in Figure 1. The PC-class unit stores data readings transmitted by the electricity monitor at a granularity of one sample every 5 seconds and runs RECAP-*free*.

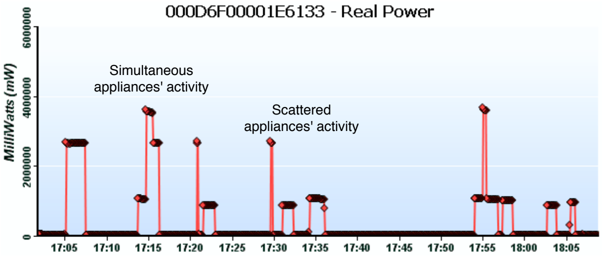
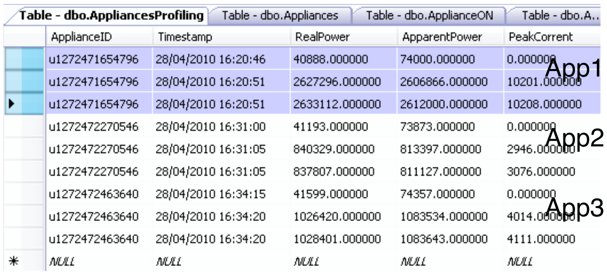


Fig. 7. Data retrieved in the kitchen area over a period of one hour.

Figure 7 represents one hour of data captured by the electricity monitor, showing both single and combined activity



	ApplianceID	Timestamp	RealPower	ApparentPower	PeakCorrent
	u1272471654796	28/04/2010 16:20:46	40888.000000	74000.000000	0.000000
	u1272471654796	28/04/2010 16:20:51	2627296.000000	2606866.000000	10201.000000
▶	u1272471654796	28/04/2010 16:20:51	2633112.000000	2612000.000000	10208.000000
	u1272472270546	28/04/2010 16:31:00	41193.000000	73873.000000	0.000000
	u1272472270546	28/04/2010 16:31:05	840329.000000	813397.000000	2946.000000
	u1272472270546	28/04/2010 16:31:05	837807.000000	811127.000000	3076.000000
	u1272472463640	28/04/2010 16:34:15	41599.000000	74357.000000	0.000000
	u1272472463640	28/04/2010 16:34:20	1026420.000000	1083534.000000	4014.000000
	u1272472463640	28/04/2010 16:34:20	1028401.000000	1083643.000000	4111.000000
*	*NULL*	*NULL*	*NULL*	*NULL*	*NULL*

Fig. 8. Power footprints generated by RECAP-*free* from the kitchen area data capture.

of various appliances. Figure 8 shows that 3 unique power footprints have been discovered and registered by RECAP-*free*. Power footprint registration with RECAP-*free* is also timestamped, but discrepancies in software configuration generate a one-hour time difference between table timetamps and graph timing.

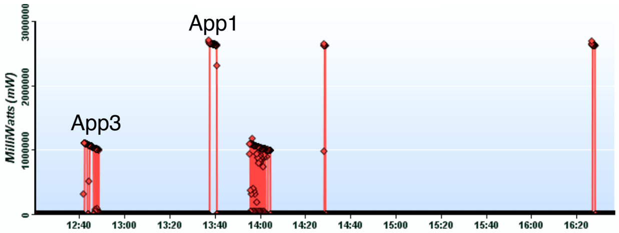


Fig. 9. Data retrieved in the kitchen area during working hours exhibiting the random use of the kettle and the use of the microwave at lunch time.

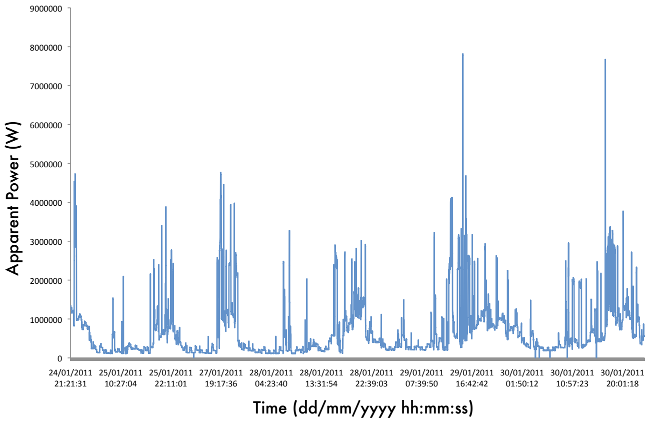
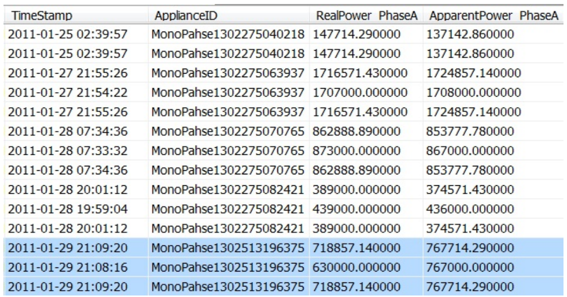


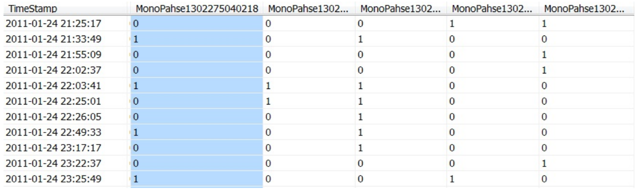
Fig. 10. Power measurement within a family home over a period of 7 days.

Figure 9 shows a data capture made during afternoon working hours, exhibiting numerous repetitions of one power signature at lunch time, and random appearance of another power signature throughout the day. Such usage pattern information is vital to associate names to the discovered footprints. Based on this timing as well as power characteristics, the *App1* signature captured is named as *kettle*, and the *App3* signature as *microwave*. More data will however be necessary to name confidently the second power footprint. This example has shown that naming can be straightforward when few appliances are instrumented with visible usage patterns.



TimeStamp	ApplianceID	RealPower PhaseA	ApparentPower PhaseA
2011-01-25 02:39:57	MonoPahse1302275040218	147714.290000	137142.860000
2011-01-25 02:39:57	MonoPahse1302275040218	147714.290000	137142.860000
2011-01-27 21:55:26	MonoPahse1302275063937	1716571.430000	1724857.140000
2011-01-27 21:54:22	MonoPahse1302275063937	1707000.000000	1708000.000000
2011-01-27 21:55:26	MonoPahse1302275063937	1716571.430000	1724857.140000
2011-01-28 07:34:36	MonoPahse1302275070765	862888.890000	853777.780000
2011-01-28 07:33:32	MonoPahse1302275070765	873000.000000	867000.000000
2011-01-28 07:34:36	MonoPahse1302275070765	862888.890000	853777.780000
2011-01-28 20:01:12	MonoPahse1302275082421	389000.000000	374571.430000
2011-01-28 19:59:04	MonoPahse1302275082421	439000.000000	436000.000000
2011-01-28 20:01:12	MonoPahse1302275082421	389000.000000	374571.430000
2011-01-29 21:09:20	MonoPahse1302513196375	718857.140000	767714.290000
2011-01-29 21:08:16	MonoPahse1302513196375	630000.000000	767000.000000
2011-01-29 21:09:20	MonoPahse1302513196375	718857.140000	767714.290000

Fig. 11. Power footprints discovered by RECAP-*net*.



TimeStamp	MonoPahse1302275040218	MonoPahse1302...	MonoPahse1302...	MonoPahse1302...	MonoPahse1302...
2011-01-24 21:25:17	0	0	0	1	1
2011-01-24 21:33:49	1	0	1	0	0
2011-01-24 21:55:09	0	0	0	0	1
2011-01-24 22:02:37	0	0	0	0	1
2011-01-24 22:03:41	1	1	1	0	0
2011-01-24 22:25:01	0	1	1	0	0
2011-01-24 22:26:05	0	0	1	0	0
2011-01-24 22:49:33	1	0	1	0	0
2011-01-24 23:17:17	0	0	1	0	0
2011-01-24 23:22:37	0	0	0	0	1
2011-01-24 23:25:49	1	0	0	1	0

Fig. 12. Appliances' power states generated by RECAP-*net*.

B. Real world testing

One home with multiple occupants has been equipped with an Episensor electricity monitor [13] for a period of 7 days. In that deployment, data readings are sampled every minute.

Figure 10 shows the apparent power measurement over the 7-day period. Immediately, one can see the difficulty at hand with real world experimentation; noise and number of appliances are increased. We ran RECAP-*free* over that data and Figure 11 shows that 5 primary power footprints have been discovered and initialised with a non-meaningful ApplianceID.

RECAP-*free* generated as well a table of activities, shown in Figure 12, containing the times at which each footprint has appeared.

The naming process is approached the same as for the kitchen experiment, focusing on Jan 28, 2011, see Figure 13. We can see that the power measurement is composed of a baseline power, as well as a recurrent power block pattern, and power peaks. When filtering out such data set, the apparent power variation is calculated for each data entry, subtracting the value of the new entry with the previous one. Variations under a the defined threshold are discarded and important variations generate a new power footprint record within the system. Figure 14 shows the data as considered by RECAP-*free*; successive power variations are seen as power peaks of various amplitude. As highlighted with symbols, similar power steps appear over time; new occurrences of an existing footprint are stored by RECAP-*free* in activity tables, see Figure 12.

At this stage, RECAP-*free* automatically provides the number of unique footprints and their time of occurrence. Manually naming however appears to be the bottleneck and requires

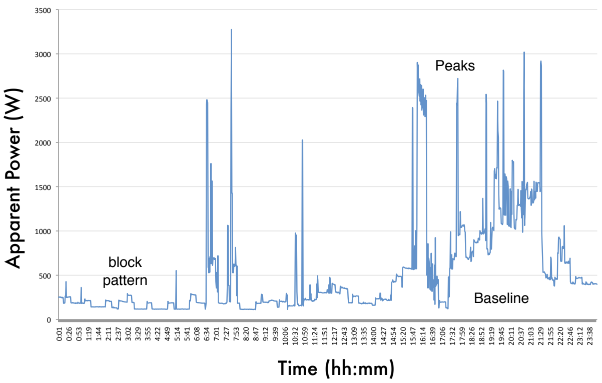


Fig. 13. Power measurement within a family home over a period of one day.

computational assistance. The home being occupied by multiple occupants, appliances are instrumented with no clear usage patterns and larger data sets needs to be analysed. Libraries of known power footprints will also be essential for automated comparison.

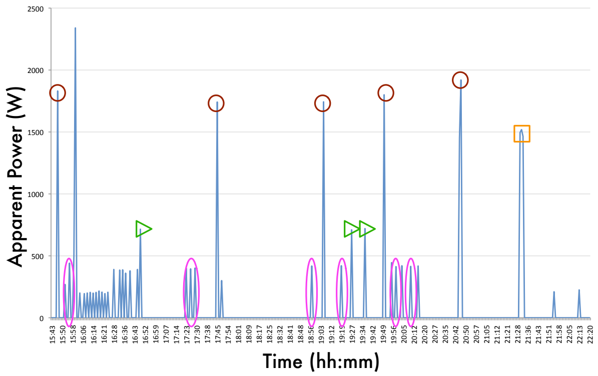


Fig. 14. Successive power variations are processed as power steps of various amplitude. Symbols highlight similar power steps.

VI. Conclusions

This work has presented the implementation and experimentation of a system facilitating the generation of power footprints without appliance interaction, for use with appliance load monitoring systems. With such capability, it becomes possible to learn about occupants' activity within a building without their knowing it. Results have put forward the capability of the system to automate the capture of unique power footprints. Naming of generated power footprints was shown to be feasible in environments with limited number of appliances and clear usage patterns, e.g. an elderly person living alone at home, but has highlighted the difficulty of naming footprints without computational assistance in real-world scenarii. Future work will investigate naming automation using libraries of known power footprints and intelligent algorithms.

Acknowledgment

This work is supported by Science Foundation Ireland under grant 07/CE/I1147. Author AD is supported by the Irish Health Research Board under grant number MCPD/2010/12.

References

[1] US Energy Information Administration, *Use of Energy in the United States Explained*, 2009

[2] US Energy Information Administration, *Commercial buildings energy consumption survey*, 2003

[3] US Department of Energy, *President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid*, 2009

[4] Elias Leake Quinn, *Smart Metering and Privacy: Existing Law and Competing Policies—A Report for the Colorado Public Utilities Commission*, 2009

[5] National Institute of Standards and Technology (NIST), *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, August 2010

[6] K. E. Covinsky, R. M. Palmer, R. H. Fortinsky, S. R. Counsell, A. L. Stewart, D. Kresevic, C. J. Burant, C. S. Landefeld, *Loss of Independence in Activities of Daily Living in Older Adults Hospitalized with Medical Illnesses: Increased Vulnerability with Age*, Journal of the American Geriatrics Society, Vol.51, Nb.4, pg.451-458, 2003

[7] A.G. Ruzzelli, G.M.P. O'Hare, A. Schoofs, C. Nicolas, *Real-Time Recognition and Profiling of Appliances through A Single Electricity Sensor*, In IEEE SECON'10, 2010

[8] A. Schoofs, A. Guerrieri, D.T. Delaney, G.M.P. OHare, A.G. Ruzzelli, *Annot: Automated Electricity Data Annotation Using Wireless Sensor Networks*, In IEEE SECON'10, 2010

[9] G.W. Hart, *Residential energy monitoring and computerized surveillance via utility power flows*, IEEE Technology and Society Magazine, 1989

[10] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, *Private Memoirs of a Smart Meter*, In 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys 2010), Zurich, Switzerland, November 2010

[11] M. A. Lisovich, D. K. Mulligan, S. B. Wicker, *Inferring Personal Information from Demand-Response Systems*, In IEEE Security & Privacy, vol.8, no.1, pp.11-20, January–February 2010

[12] G.W. Hart, *Non-intrusive Appliance Load Monitoring*, in IEEE, vol. 80, No 12, 1870–1891, 1992

[13] Episensor ZEM-30 Electricity monitor, http://www.episensor.com/products/wireless-nodes/zem-30/