Smart meter privacy by suppression of low power frequency components

Srđan Đorđević and Marko Dimitrijević
Faculty of Electronic Engineering
University of Niš
Niš, Serbia
{srdjan.djordjevic, marko.dimitrijevic}@elfak.ni.ac.rs

Slobodan Bojanić
Escuela Tecnica Superior de Ing. de Telecomunicacion
Universidad Politecnica de Madrid
Madrid, Spain
slobodan@die.upm.es

Abstract—**This paper focuses on the problems associated with privacy protection in smart grid. We will give an overview of a possible realization of a privacy-preserving approach that encompasses privacy-utility tradeoff into a single model. This approach proposes suppression of low power frequency components as a solution to reduce the amount of information leakage from smart meter readings. We will consider the applicability of the procedure to hide the appliance usage with respect to the type of home devices.**

Keywords- load monitoring, privacy protection, smart metering

I. INTRODUCTION

The increased interest in modern power systems or smart grid is a consequence of the fact that the traditional power system is not able to meet growing energy demands. Smart grid characterizes the two-way flow of electricity and information, which allows more effectively monitoring and control of energy use. Smart meter periodically and automatically transmits readings to the utility which enables efficient load balancing. However, collecting and transmitting measuring data also poses a serious privacy threat since an unauthorized third party is able to intercept data in transmission. They could process power consumption data to extract appliance usage and observe some events. This information together with demographic data provide an opportunity to model a typical human behavior [1].

Any privacy preserving technique makes a tradeoff between privacy and data collection requirements. The first attempt to develop a general theoretical framework for privacy-utility tradeoff was proposed by Sankar et al. [2]. Such theoretical framework enables us to make a compromise between the lost of privacy and the precision of aggregated measurements. The second benefit of a theoretical abstraction is a possibility to create procedures which are technology-independent. It is shown that an optimal compromise between privacy preserving and utility can be achieved by filtering out low power frequency components.

This paper focuses on the technological defenses against unwanted and unauthorized monitoring. The following section is related to the Non-Intrusive Load Monitoring (NILM). In the third section we investigate realization of a privacy-preserving approach that encompasses privacy-utility tradeoff into a single model. The fourth section considers the applicability of the proposed technique to hide the appliance usage with respect to the type of home devices.

II. NON-INTRUSIVE LOAD MONITORING

The metering data which smart meter transmits to the utility provide an opportunity to observe the daily activities of a person remotely. If an attacker intercepts data in transmission he is able to determine individual appliance operation schedules by using NILM algorithm. Therefore the smart grid privacy solutions must carefully examine how NILM algorithm can be used to extract personal information and develop more effective means of protection from it.

In order to save energy and use energy resource efficiently it is necessary to implement the load identification of appliances in individual households. The traditional load monitoring system which is based on Supervisory Control and Data Acquisition (SCADA) requires sensors attached to each appliance in the house and a home area network. The implementation of this system is very complex. In addition, it is unreliable and not scalable as a consequence of the large number of sensors.

The second method used to detect the operation state of individual electric appliances is NILM, proposed by Schweppe and Hart [3]. This method uses the nonintrusive monitoring concept by which individual loads need not be instrumented. An NILM system uses only aggregate power consumption signals from a sensor at the power service entrance. This load monitoring method is widely accepted because of the simple hardware installation.

The appliance signature represents a specific characteristic that makes a load unique. There are two main classes of nonintrusive signatures:

- Steady-state
- Transient

The steady-state signature (SS) represents the set of parameters that are derived under steady-state operation of the appliances. The NILM methods which use this kind of signature identify devices based on the steady state change of real and reactive power. The behavior of some appliances can be tracked from positive and negative real power variations. According to the method proposed by Hart step changes of the power consumption are grouped into clusters in order to extract

individual appliance usage. The important advantages of the steady state approach are: minimal hardware requirements, low sampling frequency and additivity of the SS signatures.

Any load identification algorithm needs to employ a library of load models during pattern recognition stage. In order to build a signature library, it is necessary to make a classification of electric home appliances.

A. Electric appliance classification

The electric equipments can be classified into following six categories depending on the electrical characteristics [4]: resistive appliances, motor driven appliances, pump operated appliances, electronically-fed appliances, electronic power control appliances and fluorescent lighting.

The classification is performed based on the: duration and shape of the current transients, current harmonics and the other parameters of the voltage or current signal. Resistive appliances draw current that is in phase with the voltage. Therefore, there is the only real power present on the electrical network. The current signal drawn by resistive appliances does not contain higher harmonics.

The second category of electric equipments contains an electric motor. The current signal drawn by motor driven appliances characterize a long transient and presence of odd-numbered harmonics. The appliances which contain a pump operated by an electric motor are often classified separately from other motor driven appliances, because the differences in switching-on transients. Common household appliances that belong to this category include refrigerators, freezers, washing machines etc.

Electronically-fed appliances are low power loads which use Switch Mode Power Supply (SMPS). The fundamental characteristic of any SMPS is high power efficiency and controllability. The SMPS current has a significant amount of triplen harmonics (3^{rd}, 9^{th}, 15^{th}, etc.) and high THD.

Electronic power control appliances are loads which characteristic significantly depend on power level at which they operate. Appliances such as halogen lights, some vacuum cleaners and cookers belong to this group.

Fluorescent light sources belong to the inductive loads which characterize a substantial phase shift between current and voltage and a long two-step switching on transient. They posses current spectrum dominated by third harmonic.

III. PRIVACY-PRESERVING TECHNIQUE BASED ON PRIVACY-UTILITY TRADEOFF

There are two approaches in the privacy preserving techniques proposed so far, non-cryptographic approaches and cryptographic approaches. Cryptographic techniques allow operation of the utility without access to meter readings. The main drawback of this approach is demand to implement protocols, and software on each smart meter.

The privacy-preserving techniques can be centralized or distributed. The more common approach uses data aggregation, which performs gathering and computing data in a gateway. The second approach is to use security techniques on the side of the smart meter which communicate directly to the utility.

The technique which ensures household privacy without utility cooperation is masking and obfuscation of metering data. One such solution named, Battery-based Load Hiding (BLH) [5, 6], uses controllable batteries which are charged and discharged at strategic times to hide the load demand. The BLH algorithm tries to prevent NILM by keeping metered load constant.

The theoretical framework proposed by Sankar et al. [2] shows that optimal privacy preserving solution requires suppression of low power frequency components. Low power frequency components are typically caused by short-lived fluctuations in energy consumption and reveal a great amount of information about human behavior. In contrast, frequency components that have high power are caused by continuously running appliances and contain much less information. A privacy-preserving technique which is based on utility-privacy preserving model must realize two functions, which are as follows [7]:

- Estimation of harmonic components in power system
- Removing certain frequency components from measuring data signal

Traditionally, harmonic analysis of current or voltage signal is performed by using FFT algorithm or bandpass filtering. The FFT algorithm can be implemented only if the number of samples per period is an exponentiation of 2. Therefore, one must determine the period of the fundamental frequency and adjust sampling frequency.

The key part of the proposed privacy preserving technique is to determine active power harmonics that can be suppressed. Removing the frequency components must be done adaptively from the power consumption spectrum.

The complex power can be expressed in terms of the active and reactive power harmonics in the following way:

$$S = P + jQ = \sum_{k=1}^{N} S_k = \sum_{k=1}^{N} P_k + j\sum_{k=1}^{N} Q_k \tag{1}$$

The proposed procedure of removing low power frequency components from measuring data signal results in the approximated active and reactive power, as follows:

$$P' = P - \sum_{k \in M} P_k \qquad Q' = Q - \sum_{k \in M} Q_k \tag{2}$$

where: **M** is the set of harmonics which are suppressed.

The approximation is acceptable if the active power relative error does not exceed the upper limit, δ_p.

$$\frac{P'-P}{P} < \delta_P \tag{3}$$

All other power quality measurements are performed without any approximation since they do not reveal privacy information.

IV. MEASUREMENTS

A. Measurement conditions and setup

Measurements and data analysis are performed using a real-time system for polyphase nonlinear loads analysis, described in [8]. The system is based on virtual instrument paradigm, using National Instruments NI9225 and NI9227 acquisition modules and PXI controller running real-time operating system (RTOS). In these measurements, we used 50 kSa/s sampling rate and 24bit accuracy. The current and voltage ranges are $\pm 5A_{RMS}$ and $\pm 300V_{RMS}$, respectively. All measurements are conducted using one acquisition channel, i.e. one phase.

The current spectra and waveforms are shown on Fig. 1 to 5. Fig.1 presents a current spectrum and waveform in case of pure linear resistive load, 100 W nominal power incandescent lamp. This measurement is given as reference. The waveform is almost sinusoidal, and one can observe small magnitude of 3rd, 5th and 7th harmonics. These harmonics exist due to power grid supply voltage, which is not pure sinusoide, having some harmonic pollution.

B. Results

Fig. 2 and 3 depicts measured results for Compact Fluorescent Lights (CFL) lamps with 15W and 20W nominal power, respectively. The waveforms are almost identical, and both spectra have the same harmonic structure, with odd harmonics. The envelope of spectra is approximately exponentially decaying function, with a small drop in 5th harmonic. The only observable difference between two spectra is different magnitudes of same order harmonics.

The measured data related to the CRT monitor are shown in Fig. 4. The waveform resembles the sine function. The spectrum contains low frequency components, i.e. 5th–9th harmonics, with small magnitude. This is an example of well compensated SMPS.

Finally, Fig. 5 represents spectrum and waveform obtained by measuring portable PC supply current. This is an example of time non-invariant electronic appliance. The power consumption, as well as spectrum structure of such nonlinear load varies in time, depending on working conditions (i.e. battery status) and activities within a PC, causing different CPU, GPU and I/O load [9]. This information can be also used for eavesdropping the computer activity, as shown in [10].

The measurements shown in Fig. 5 are performed with fully charged battery, when PC is in idle state – only OS and core services running. The AC/DC power converter draws current from the grid in bursts, causing heavily distorted waveform. The corresponding spectrum contains odd harmonics, with sinc function as envelope.

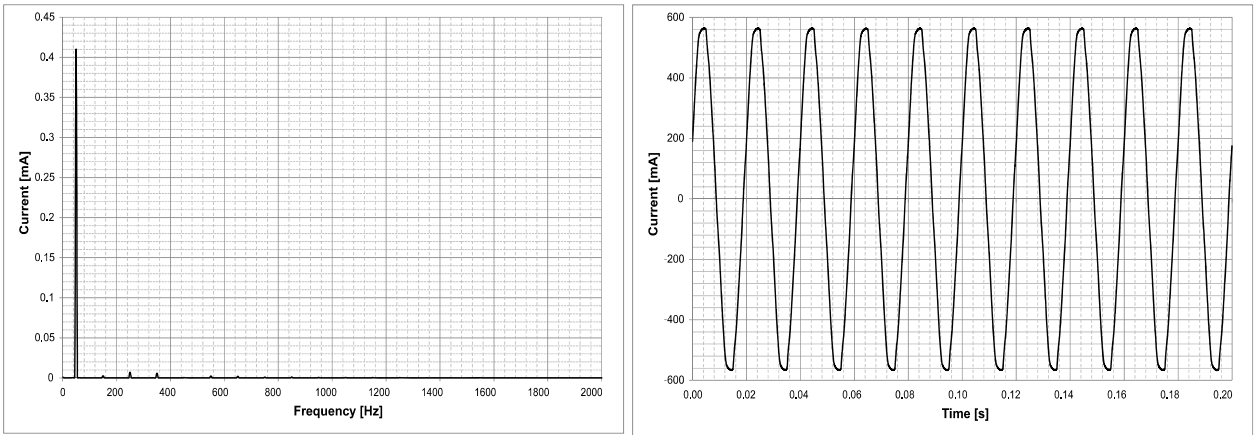

Figure 1. Incandescent lamp, 100W nominal power – spectrum (left) and waveform (right)

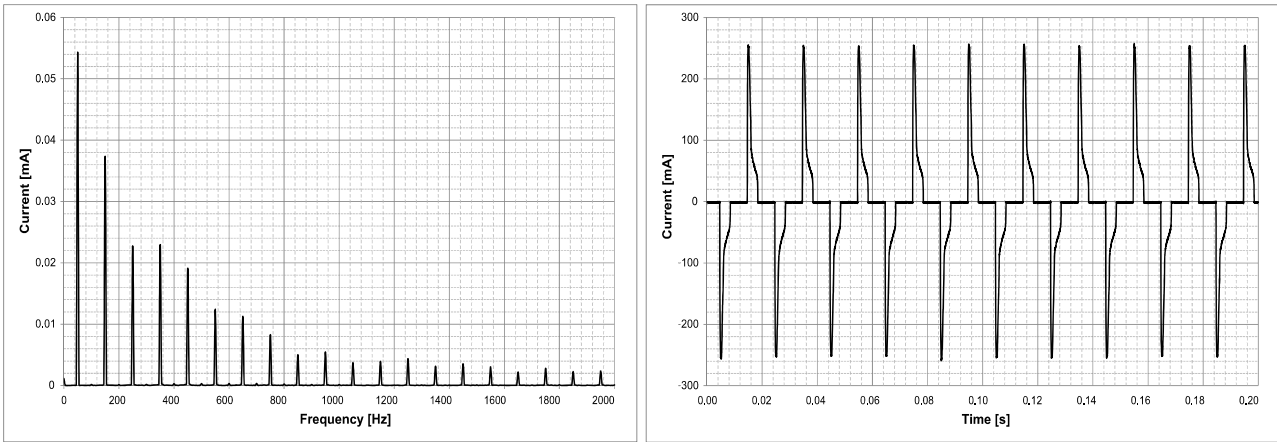

Figure 2. 15W nominal power CFL – spectrum (left) and waveform (right)

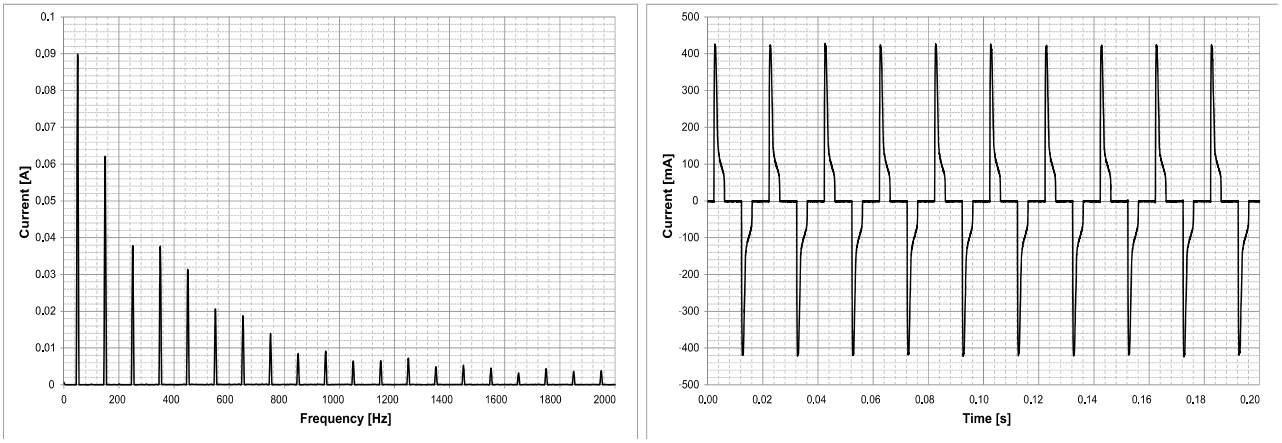

Figure 3. 20W nominal power CFL – spectrum (left) and waveform (right)

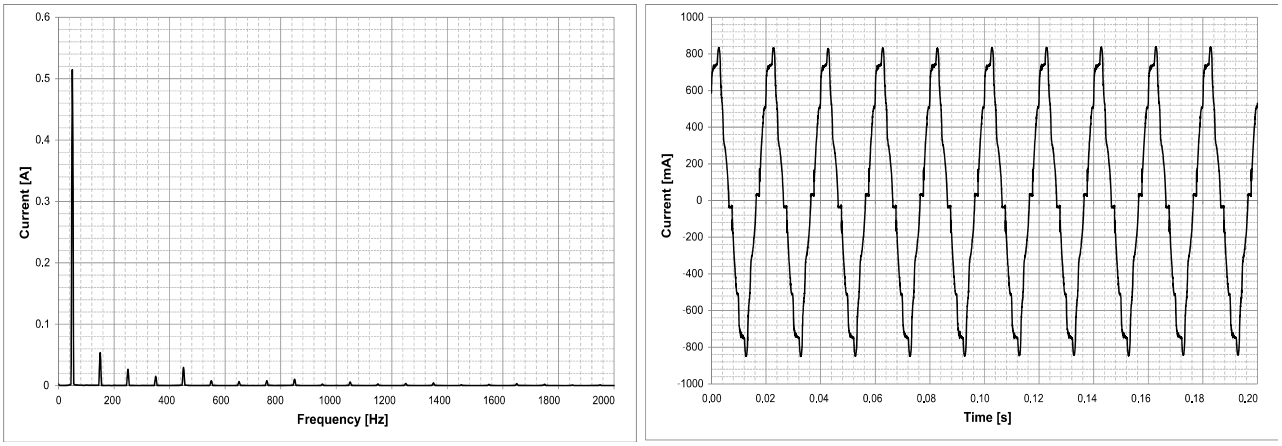

Figure 4. CRT monitor – spectrum (left) and waveform (right)

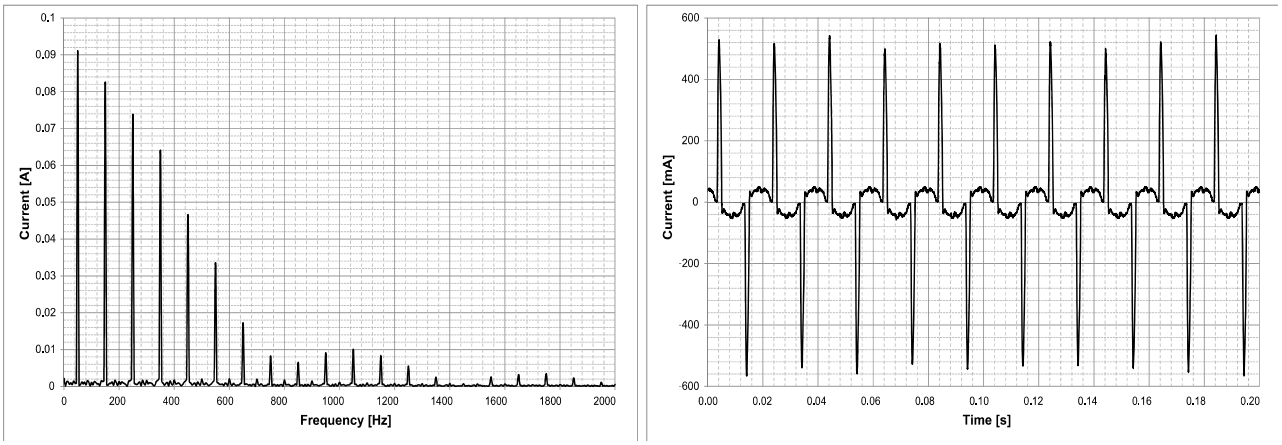

Figure 5. Portable PC – spectrum (left) and waveform (right)

V. CONCLUSION

By observing measured results, especially related spectra, one can conclude that each electronic appliance has unique harmonic signature, which can be used for identification. Identifying single appliance connected into power grid requires complex pattern based algorithms.

In this proceeding, we only take in consideration harmonic magnitudes. Harmonic phases can also be measured with described system, providing more information needed for appliance identification.

The proposed privacy-preserving technique is applicable to appliances with a current spectrum having relatively strong higher harmonics. Hence, the suppression of low-power frequency components is not effective on resistive appliances. According to the measurement results, the usage of electronically-fed and electronic power control appliances can be effectively hidden. This group of appliances encompasses

household appliances such as IT equipment (mainly computers), television sets, energy-efficient lighting (LED and CFL) which are becoming nowadays more prevalent in households.

ACKNOWLEDGMENT

This research was partly funded by The Ministry of Education and Science of Republic of Serbia under contract No.TR32004.

REFERENCES

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

[2] L. Sankar, S. Rajagopalan, S. Mohajer, H. Vincent Poor, "Smart Meter Privacy: A Theoretical Framework," *smart grid*, *IEEE transactions on*, vol. 4, no. 2, pp. 837-846, Jun 2013.

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

[4] F. Sultanem, "Using appliance signatures for monitoring residential loads at meter panel level," IEEE Transactions on Power Delivery, vol. 6, no. 4, pp. 1380–1385, 1991.

[5] S. McLaughlin, P. McDaniel, W. Aiello, "Protecting consumer privacy from electric load monitoring," In Proceedings of the 2011 ACM CCS: 87-98.

[6] W. Yang, N. Li, Y. Qi, et al. "Minimizing private data disclosures in the smart grid," In Proceedings of the 2012 ACM CCS: 415-427.

[7] S. Đorđević, S. Bojanić, "Tehničko rešenje za zaštitu privatnosti u novim elektroenergetskim mrežama zasnovano a optimalnom balansu između privatnosti i funkcionalnosti," Proc. of the LVIII Conf. of ETRAN, 2013, Vrnjačka Banja pp. EL1.1.

[8] M. Dimitrijević: "Electronic System for Polyphase Nonlinear Load Analysis," in serbian, PhD thesis, December 2012.

[9] O. Nieto-Tialdriz, M. Dimitrijević, D. Stevanović, D. Mirković "Energy Profile of a Personal Computer," Proc. of the LVI Conf. of ETRAN, 2012, Zlatibor pp. EL3.3-1-4.

[10] M. Andrejević Stošović, M. Dimitrijević, V. Litovski, "Computer Security Vulnerability Seen From the Electricity Distribution Grid Side," Applied Artificial Intelligence, Taylor & Francis Ltd., vol. 4, no. 28, pp. 323-336, London, 2014.