Privacy-Aware Sampling for Residential Demand Response Programs*

Alvaro A. Cárdenas
Fujitsu Laboratories of America
cardenas@fla.fujitsu.com

Saurabh Amin
Masachusetts Institute of Technology
amins@mit.edu

Galina Schwartz
University of California at Berkeley
schwartz@eecs.berkeley.edu

ABSTRACT

Deployment of Advanced Metering Infrastructures (AMIs) brings numerous new privacy concerns. The governments and standard organizations are responding to these concerns by developing guidelines and policies for AMIs. In USA, the June 2011 smart grid policy framework report examines privacy issues [11]. In accordance with the Federal Fair Information Practice (FIP) principles, the report recommends that State and Federal regulators consider methods which ensure the protection of consumers' detailed energy usage. Recent standardization guidelines (e.g., the NIST-IR 7628 [1]) and regulations by the state public utility commissions (e.g., California (Docket No. 08-12-009), Colorado (Docket No. 10R-799E)) refer to the key FIP principle of data minimization by stating that AMIs should only collect the data necessary for Smart Grid operations. Despite the fact the data minimization is acknowledged as a key requirement, the technical criteria on selection of sampling intervals in AMIs are notably absent. In this paper we approach the question of privacy-enabling design of smart meter sampling intervals for Demand-Response (DR) schemes as a Cyber-Physical System (CPS) problem. In particular, we introduce the problem of choosing the optimal sampling intervals in AMIs subject to the performance constraints of DR schemes. Our goal is to draw attention to the trade-offs between the privacy-aware sampling and the desired properties of DR schemes modeled as closed-loop systems.

1. INTRODUCTION

Smart grid refers to the modernization of the power grid infrastructure with new technologies to enable a more efficient networked control system, with the goal of improving the system reliability and providing more transparency and choices to electricity consumers. On the consumption side, Advanced Metering Infrastructures (AMIs) refer to the new electricity metering systems that are replacing old mechanical meters. The term "smart meters" denotes the new embedded devices that provide two-way communications between the utility and the consumer. These devices permit the utilities to avoid sending the personnel to read the meters on-site, and also provide several new capabilities: e.g., monitoring of network-wide and individual electricity consumption, faster remote diagnosis of outages, remote disconnect options, and automated power restoration. The AMIs also improve the consumers' access to their energy usage information (including the sources of electricity, renewables or otherwise) and promote the implementation of Demand Response (DR) schemes.

However, the AMIs also introduce new privacy threats to residential consumers because these devices permit large-scale data collection. This makes individual household data available at unprecedented levels of disaggregation. Monitoring energy consumption with high-granularity can allow the inference of detailed information about consumers' lives. This includes the times when consumers eat, watch TV, take a shower, and whether they tend to use microwave/stove for cooking, the types of appliances they own, and the periods that they are inside/outside their homes. Such information is highly valuable to advertising companies [7], law enforcement [16], and criminals [15].

In addition to the aforementioned technological capabilities, the current regulatory and judicial environments permit to reuse the household consumption data gathered by AMIs, which could lead to revelation and exploitation of consumers' personal identities [26]. While the utility companies do have the responsibility of protecting AMI records, this data can be shared with third parties by the consumers who are unaware of the exposure of their privacy, or by the utility companies themselves. For e.g., in Oklahoma [4] the utility company owns the meter data and it is "authorized to share customer data without customer consent with third parties who assist the utility in its business and services, as required by law, in emergency situations, or in a business transaction such as a merger".

Finally, the AMIs could be themselves subject to security attacks. Such attacks could be implemented by outsiders (e.g., computer hackers) capable of exploiting vulnerabilities of data transmission networks and storage devices, or rogue

*A. Cárdenas acknowledges the support of the Trusted Systems Innovation Group, Fujitsu Laboratories of America, Sunnyvale, CA. S. Amin was supported by the MIT faculty start-up grant. G. Schwartz was supported by NSF grant CNS-0910711 and by TRUST (Team for Research in Ubiquitous Secure Technology).

HiCoNS, April 17–18, 2012, Beijing, China.

insiders (e.g., disgruntled employees) working for the utility company.

In response to these concerns, governments and standard organizations are engaged in the development of privacy standards and policies to guide AMI deployments. In the United States, the June 2011 smart grid policy framework report by the Executive Office of the President has examined privacy issues [11]. The report recommends that as a starting point, the State and Federal regulators consider methods to ensure that consumers' detailed energy usage data is protected in a manner consistent with federal Fair Information Practice (FIP) Principles. The key principle of *data minimization* entails the notion of *privacy-by-design* [10].

The NIST-IR guidelines [1] for privacy protection in smart grid deployments state that utilities should "limit the collection of data to only that is necessary for Smart Grid operations". The same principle is worded differently in the rules and regulations to protect the privacy of consumers in California and Colorado who have smart meters in their homes. For example, the privacy rules of California Public Utility Commission (CPUC) [3] for smart meters state that utilities "shall collect, store, use and disclose only as much covered information as is reasonably necessary or as authorized by the commission to accomplish a specific primary purpose".

While these principles and regulations are clearly necessary, further technical criteria are needed to fully realize their benefits. At present, there are no clear guidelines on the selection of sampling intervals used in AMIs. To the best of our knowledge, the utilities routinely select metering frequencies based on rules-of-thumb without using sound analytical criteria. For e.g., in countries like Japan, China and USA, these frequencies range from 10-minute to 4-hour intervals.

Indeed, the optimal sampling intervals (or collection rates) may differ depending on the performance requirements. Thus, it is necessary to characterize the trade-off between data minimization and performance objectives. There are many legitimate reasons for utilities to gather fine-grained smart meter data–e.g., to inform customers about their consumption patterns, and for dispute resolution or fraud detection. Still, the primary reason for gathering fine-grained samples of residential consumers' energy usage is to enable residential DR schemes.

In this brief paper we approach the problem of privacy-aware sampling in AMIs by modeling the sampling rate as a design parameter. The sampling rate determines the privacy properties of the system and at the same time it affects the performance of DR schemes. We outline our approach of characterizing the trade-off between increased sampling rate (thus enhancing privacy) in AMIs and the closed-loop performance of DR systems.

2. RELATED WORK

We now review the recent efforts to address privacy related issues in AMI deployments. Firstly, privacy can be improved by using *selective load control and power mixing* of a number of electricity sources. A local source of power can be used to shape the electricity usage collected at the meter and prevent the inferences that can be made with Non-Intrusive Load Monitoring (NILM) [8, 17]. Future smart homes will contain a variety of energy storage and generation devices that can make this solution feasible. Kalogridis et.al. [21] have proposed the use of power routing to prevent attackers from using energy consumption data to infer the usage patterns of home appliances. In particular, the authors propose a load signature moderator as a way of shaping load signatures in a home. 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 main electricity supply. In this case, the attackers monitoring the metered data will be unable to identify the signatures of these devices. This work has been extended by McLaughlin et.al. [27], who analyzed the challenges of introducing a battery into a residential setting, providing better privacy guarantees, and simulating different scenarios with real-world data. The use of local generation to shape the electricity consumption signals is an intuitive idea. These papers have considered residential electricity consumption devices—such as TED [5] or Current Cost [2]–and not smart meters. Indeed, several challenges need to be addressed to facilitate large-scale penetration of local generation and storage devices, including additional operational costs, battery maintenance costs, etc.

Secondly, privacy can be improved via *data aggregation* [24, 34]. These papers suggest to store only the result of computations (e.g., sum of meter readings) while deleting individual meter readings. Aggregation can be done at a collection point (e.g., utility server) or in the network (i.e., in-network aggregation with smart meters). Aggregating at a collection point still has the vulnerability of a single point of failure where the adversary can attack to obtain the data before it is aggregated. But performing in-network aggregation is expensive for the resource-constrained meters, and this might require updating millions of meters that are already deployed. A related approach is differential privacy [6], which can also be used to share aggregated smart grid data with third parties while preventing the identification of the patterns of a single consumer. However, the latter approach still requires the utility to store the original database of user consumption patterns.

Thirdly, the privacy of smart meters can be improved by using *cryptographic techniques* [23, 30]. These methods can be used to prove the validity of monthly payments, while keeping electricity consumption private. A significant limitation of the protocols suggested by these papers is the requirement of zero-knowledge proofs which are computationally expensive for most smart meters. Thus, these approaches requires additional hardware deployed at the consumer locations. In addition, they mostly focus on the prevention of billing frauds, and do not directly address the issues in DR schemes, where the utility needs to obtain accurate electricity consumption readings (possibly from individual meters).

The aforementioned three approaches (mixing, aggregation, and the use of cryptographic techniques) are indeed promising, but suffer from the limitation of extra costs due to real-time computation and communication requirements. Moreover, they do not address the privacy-by-design principle of data minimization; i.e., what is the minimum data collection frequency that still allows the utilities to efficiently perform advanced smart grid operations, including load management and demand-response?

The closest work to the problem we consider in this paper is the research of Sankar et.al. [33], who studied the tradeoff between sharing data versus withholding data among Regional Transmission Organizations (RTOs). However, there

are fundamental differences with our work. First, Sankar et.al. address privacy by quantization, our approach considers sampling (not quantization) as a fundamental design parameter for preserving privacy. Second, Sankar et.al. study the problem of estimating the state of the power grid accuracy by aggregating information from multiple RTOs; in contrast, we use well-known results from control theory to identify optimal sampling intervals to preserve the desired closed-loop properties of DR schemes viewed as discrete-time control systems. Third, we focus on the end consumers at the distribution networks, and not on the information sharing between corporate RTOs in the bulk transmission systems.

In comparison to [33] which focuses on how privacy pertains to corporations (data sharing), we focus on individual privacy as in [32]. Individual privacy is the right of determining to what extent the individual's thoughts, sentiments, and emotions are communicated to others [37]. Historically, this right has been tied to uniquely human interests such as human flourishing (by helping individuals avoid embarrassment — which stunts social development and growth), human dignity, respect, autonomy, and helping individuals construct intimacy to others [22]. While corporations clearly have an interest in maintaining the confidentiality of certain information, it is debatable whether it is really identical to the concept of individual privacy; see e.g., [18]. When dealing with a corporation or organization's proprietary information, statutes typically use the term "confidentiality", as opposed to "privacy". For example, the Telecommunications Act of 1996 states that every telecommunication carrier has a duty to *protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers* (similar to the case study of Sankar et.al. where the RTOs have to protect confidential information from other RTOs). In the same act, the section on *privacy* relates to the protection of consumer's data.

3. DISCRETE-TIME CONTROL PROBLEM

The term *Demand Response (DR) program* stands for describing the schemes which aim to improve the reliability and efficiency of consumption side of the power grid. For example, some DR schemes use pricing to incentivize the consumers to reduce electricity consumption during peak hours. Currently, most DR programs are driven by the concerns for grid stability, and largely limited to large commercial consumers. The operation of these schemes is based on informal signals such as phone calls by the utility or a third-party DR scheme provider, who asks the consumer to lower or shift their energy consumption from peak demand periods to off-peak periods. In USA, companies such as EnerNOC manage DR services for large corporations and several government agencies. However, with widespread deployments of smart meters the DR schemes are also expected to include residential consumers. These new DR schemes will potentially utilize advanced capabilities of AMIs, and may permit significant improvements in energy efficiency while maintaining grid stability.

An important goal of AMIs is to make DR programs viable to a broader range of consumers [13]. By sending real-time pricing information (time-based rates) to smart meters, utilities can create incentives for consumers to distribute their load more evenly—e.g., consume more energy when there is high wind or solar energy in the grid, and reduce consumption during peak demand times. Consumers will have a choice to trade off between cost and convenience. This price-sensitive peak shaving can defer the need for grid expansion and reduce the investments on generators that are only used for short peak demands.

Many DR schemes (e.g., direct load control, emergency DR, Real-Time Pricing, etc.) have been suggested [12], and specific mathematical models have been developed for a few of them [31]. Still, it is unclear which of these schemes will find widespread adoption. In this Section, we propose to include the sampling interval of smart meters as a design parameter in the existing generic models of DR schemes. A DR scheme can be viewed as a dynamical system with the state $x(t)$ denoting the electricity load and the control signal $u(t)$ denoting an incentive such as real-time price) (See Figure 1).

It is standard to model the electricity consumption as a continuous-state dynamical system of the following form:

$$\dot{x}(t) = f(x(t), u(t)), \quad y(t) = g(x(t), u(t)).$$

The AMIs can only send consumption information back to the utilities in discrete time intervals. Let h denote the corresponding sampling interval. We assume that the DR incentive (control) signal reconstruction is based on zero-order hold. This enables the utilities to provide piecewise constant incentive signals (e.g., price of electricity), with a time interval h^0. The resulting discrete-time control system is sketched in Figure 2.

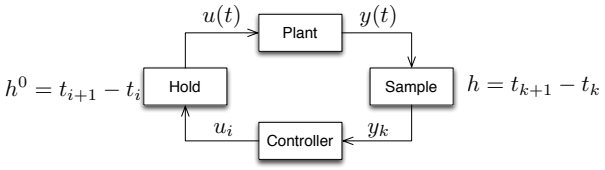

Figure 2: Demand-response viewed as discrete-time control loop

A similar DR model was introduced in [31], where the authors note that presenting the wholesale market price of electricity to retail consumers may result in market instabilities. To mitigate this problem, they propose new retail-market price signals $u(t)$ to stabilize the system. In fact, price most retail-utilities pay for electricity based on critical peak pricing. Therefore, the utilities have the incentives to reduce the peak consumption in order to reduce the costs of electricity provision. However, this research does not directly address the problem of choosing h and h^0 for DR schemes viewed as closed-loop control system.

We argue that the smart-metering sampling interval h and the zero-order hold interval h_0 will affect the closed-loop system properties. To simplify, we consider h^0 as fixed and focus on choosing h to balance the goal of minimizing the collection of user data while still permitting to maintain the DR schemes' performance. Specifically, we formulate the following problem: Given a closed-loop property $\mathcal{P}(x(t))$ of the system (e.g., safety, stability, properties of the transient response, etc.), we would like to find the largest sampling interval h such that $\mathcal{P}(x(t))$ remains within the set of desirable

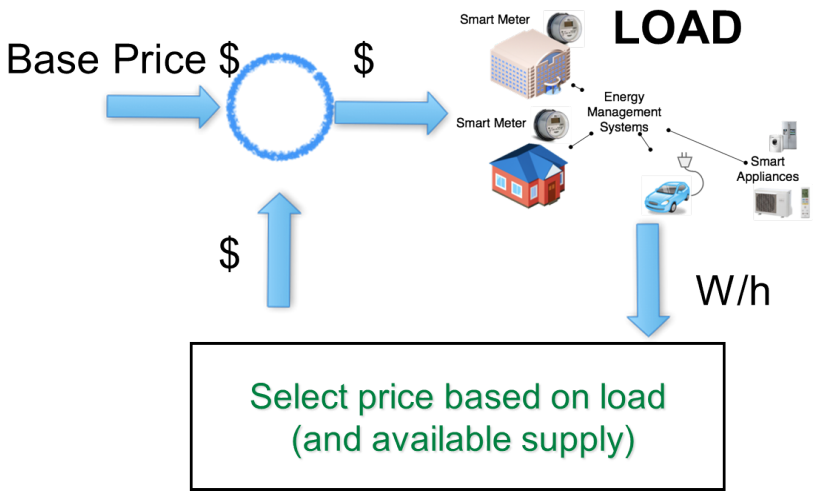

Figure 1: Control-loop of demand response systems

performance goals, denoted by $\mathcal{S}$, i.e.,

$$\begin{aligned} &\text{maximize} \quad h \\ &\text{subject to:} \quad \mathcal{P}(x(t)) \in \mathcal{S} \quad \forall t. \end{aligned}$$

For e.g., if a utility wants to maintain system safety by regulating the peak load, the overall load needs to be less than a pre-specified upper bound at all times.

3.1 Linear System Example

Let us consider a linear system as a starting point for understanding the problem:

$$\dot{x} = Fx + Gu, \quad y = Cx.$$

Consider the case when smart-meter reading interval and the duration of the zero-order hold of the control signal are the same, i.e., $h = h^0$. The resulting discrete-time linear system is

$$x_{k+1} = Ax_k + Bu_k, \quad y_k = Cx_k \tag{1}$$

where $A = e^{Fh}$ and $B = \int_0^h e^{F(h-\tau)}Gd\tau$ are functions of the sampling interval h.[1]

It is well-known that for open-loop unstable continuous-time system, large sampling times can lead to unstable dynamics of the closed-loop discrete-time system. The problem of identifying the maximum sampling interval that keeps the system stable (with a given stability margin) has been studied in standard control theory texts; see e.g., [29]. A fundamental result is the sampling theorem, which states that the sampling angular frequency w_h must be at least twice the closed-loop bandwidth of control system w. In other words, $h < \frac{\pi}{w}$. In practice, however, the sampling time-interval needs to be at least an order of magnitude smaller than the upper bound described by the sampling theorem. This becomes necessary to ensure smaller transient response-times, low sensitivity to parameter variations, and robustness to random disturbances [14].

[1]Past results on multi-rate sampling for linear systems also include the case when the plant sampling rate h is different from the control-update rate h^0 [35].

Recent research in networked control systems (NCS) has also studied the problem of selecting sampling intervals [19] when plant-controller communications are subject to network induced unreliabilities. One of the early results for NCS was the introduction of the Maximum Allowable Transfer Interval (MATI) to bound the sampling time h required to maintain NCS stability [36]. These bounds were limited to linear systems and were overly conservative; however, there is ongoing research generalizing and tightening the sampling bounds [20].

There are also exact results for the sampling time interval. Assuming $u = y$ and defining $\Phi(h) = e^{Fh} + \Gamma(h)BC$, where $\Gamma(h) = \int_0^h e^{Fz}Gdz$, it is known that the system in Eq. (1) is exponentially stable if and only if $\Phi(h)$ is Schur (i.e., all its eigenvalues have magnitude strictly less than one) [9]. A similar result was obtained in a system where the control signal u uses a model-based control [28] (without a zero-order hold). This result also shows that the state evolution matrix of the new system is exponentially stable if and only if the given matrix is Schur. It is interesting to note that by introducing a model-based controller, a load-forecasting system similar to the one described in [31] can be obtained. An interesting research question is whether the forecasting systems can allow utilities to increase the sampling intervals, and if these results can be generalized to include a zero-order hold for the control signals.

The theory of NCS also has many other stability results which consider transmission delays, packet drops and variable sampling (as opposed to periodic sampling). For example, in the case of variable delays τ_i, the closed-loop system can be written as a switched system (for each possible delay–assuming a finite and discrete number of possible delays). For each switched system, the stability defined in [9] still applies. Lin et.al. [25] further extend these notion assuming that for small delays, the $\Phi(h, \tau_i)$ matrix is Schur stable, and for large delays it is not. They use average dwell time properties to provide stability guaranties. The currently implemented in AMI systems have sample times that range from 15 minutes to several hours. On the other hand, a typical AMI network delay τ is in the order milliseconds to a few seconds (and may have negligible effect on the design

of DR sampling intervals). Thus, the specific application of NCS stability results to the problem of DR in AMI systems remains to be investigated.

Another interesting issue that has not been investigated so far is variable sampling for AMIs. The communication of smart meter measurements based on non-periodic sampling schemes might introduce new privacy concerns. Currently, all AMI systems encrypt communications to prevent eavesdroppers from learning the values that are being transmitted. Indeed, periodic transmission prevents an attacker to exploit the transmission times and patterns. However, if the meter-readings are based on some consumption events (e.g., large changes in power consumption), an eavesdropper can attempt to use traffic analysis to infer information from the encrypted transmissions. Finally, the variable sampling schemes may be subject to additional barriers due to human factors, such as consumer preferences for information about their own energy usage. Specifically, it is not clear if the consumers would be satisfied when they are able to learn their energy consumption sampled only at irregular intervals (e.g., via a web-portal provided by the utility).

4. CONCLUSIONS

In this brief paper we have advocated the importance of designing optimal smart meter sampling intervals. We suggest that the privacy-aware design of AMI sampling intervals must address the trade-offs between the gains in improving the specified closed-loop properties of DR scheme and the losses in customer privacy due to faster sampling intervals (that are desirable for improving the efficiency of DR schemes). In our future work, we will perform a detailed study of DR schemes and their closed-loop properties as a function of smart meter sampling intervals.

Our line of research is complementary to the existing research directions in privacy-aware AMIs. The three approaches reviewed in Section 2 (mixing, aggregation, and the use of cryptographic techniques) are indeed promising, despite their common limitation of extra costs due to real-time computation and communication overheads. An important advantage of our approach is its feature of no extra real-time operational costs. While in isolation our approach of optimizing smart meter sampling intervals may be insufficient to provide effective privacy guarantees, its combination with the existing approaches should permit improved privacy guarantees in AMIs. Our approach of identifying optimal smart meter sampling intervals has the potential of developing rigorous and concrete best-practices for smart-meter data collection. We hope that our efforts will be useful in assisting the standard organizations and regulatory authorities to define model-based privacy requirements.

References

[1] Guidelines for smart grid cyber security: Vol 2., privacy and the smart grid. NIST IR 7628, Aug. 2010.

[2] Current Cost. http://www.currentcost.com, 12 2011.

[3] Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, July 2011.

[4] House bill 1079, 59 leg., 1st sess. Oklahoma., 2011.

[5] The Energy Detective (TED). http://www.theenergydetective.com, 12 2011.

[6] G. Acs and C. Castelluccia. I have a DREAM! DiffeRentially privatE smArt Metering. In *Proceedings of the Information Hiding Conference*, 2011.

[7] R. Anderson and S. Fuloria. On the security economics of electricity metering. In *Workshop on the Economics of Information Security 2010*, June 2010.

[8] D. Bergman, D. Jin, J. Juen, N. Tanaka, C. Gunter, and A. Wright. Distributed non-intrusive load monitoring. In *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, pages 1 –8, jan. 2011.

[9] M. Branicky, S. Phillips, and W. Zhang. Stability of networked control systems: explicit analysis of delay. In *American Control Conference, 2000. Proceedings of the 2000*, volume 4, pages 2352 –2357 vol.4, 2000.

[10] A. Cavoukian, J. Polonetsky, and C. Wolf. Smart privacy for the smart grid: embedding privacy into the design of electricity conservation. *Identity in the Information Society*, 3:275–294, 2010.

[11] Executive Office of the President. A policy framework for the 21st century grid: Enabling our secure energy future, June 2011.

[12] Federal Energy Regulatory Commission. 2010 assessment of demand response and advanced metering, February 2011.

[13] Federal Energy Regulatory Commission. 2011 assessment of demand response and advanced metering, November 2011.

[14] G. Franklin, J. Powell, and M. Workman. *Digital control of dynamic systems*. Addison-Wesley world student series. Addison-Wesley, 1998.

[15] Government Accountability Office. Electricity grid modernization. progress being made on cybersecurity guidelines, but key challenges remain to be addressed, January 2011.

[16] R. Guest. Austin TX police have access to austin energy customer accounts. http://seesdifferent.wordpress.com/2007/11/07/austin-tx-police-have\-access-to-austin-energy-customer-accounts/, November 2007.

[17] G. W. Hart. Nonintrusive appliance load monitoring. *Proceedings of the IEEE*, 80(12):1870–1891, 1992.

[18] S. Hartman. Privacy, personhood and the courts: Foia exemption 7(c) in context. In *Yale L.J.*, pages 379–388, 2010.

[19] J. Hespanha, P. Naghshtabrizi, and Y. Xu. A survey of recent results in networked control systems. *Proceedings of the IEEE*, 95(1):138 –162, jan. 2007.

[20] A. Jentzen, F. Leber, D. Schneisgen, A. Berger, and S. Siegmund. An improved maximum allowable transfer interval for L^p-stability of networked control systems. *Automatic Control, IEEE Transactions on*, 55(1):179 –184, jan. 2010.

[21] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda. Privacy for smart meters: Towards undetectable appliance load signatures. In *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[22] J. Kang. Information privacy in cyberspace transactions. In *Stan. L. Rev.*, pages 1212–16, 1998.

[23] K. Kursawe, G. Danezis, and M. Kohlweiss. Privacy-friendly aggregation for the smart-grid. In *Privacy Enhancing Technologies - 11th International Symposium, PETS*, July 2011.

[24] F. Li, B. Luo, and P. Liu. Secure Information Aggregation for Smart Grids Using Homomorphic Encryption. In *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[25] H. Lin, G. Zhai, and P. Antsaklis. Robust stability and disturbance attenuation analysis of a class of networked control systems. In *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*, volume 2, pages 1182 – 1187 Vol.2, dec. 2003.

[26] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker. Inferring personal information from demand-response systems. *IEEE Security & Privacy Magazine*, 8(1):11–20, January/February 2010.

[27] S. E. McLaughlin, P. McDaniel, and W. Aiello. Protecting consumer privacy from electric load monitoring. In *ACM Conference on Computer and Communications Security*, pages 87–98, 2011.

[28] L. A. Montestruque and P. Antsaklis. Model-based networked control systems: Necessary and sufficient conditions for stability. In *10th Mediterranean Contr. Conf. and Auto.*, Lisbon, Portugal., 2002.

[29] K. Ogata. *Discrete-time control systems*. Prentice-Hall, Englewoods Cliffs, NJ, 2nd. edition, 1995.

[30] A. Rial and G. Danezis. Privacy-preserving smart metering. In *Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society, WPES*, October 2011.

[31] M. Roozbehani, M. Dahleh, and S. Mitter. Dynamic Pricing and Stabilization of Supply and Demand in Modern Electric Power Grids. In *First IEEE Smart Grid Commnunications Conference (SmartGridComm)*, October 2010.

[32] M. Rotenberg, J. Verdi, and A. Stepanovich. Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Legal Scholars And Technical Experts in Support of the Petitioners., November 16 2010.

[33] L. Sankar, S. Kar, R. Tandon, and V. Poor. Competitive privacy in the smart grid: An information-theoretic approach. In *Proceedings of the IEEE Conference on Smart Grid Communications*, Brussels, Belgium, October 2011.

[34] G. Taban and V. D. Gligor. Privacy-preserving integrity-assured data aggregation in sensor networks. In *The 2009 International Symposium on Secure Computing (SecureCom) 2009*, pages 168–175, 2009.

[35] J. Tornero, Y. Gu, and M. Tomizuka. Analysis of multirate discrete equivalent of continuous controller. In *American Control Conference, 1999. Proceedings of the 1999*, volume 4, pages 2759 –2763 vol.4, 1999.

[36] G. Walsh and H. Ye. Scheduling of networked control systems. *Control Systems, IEEE*, 21(1):57 –65, feb 2001.

[37] S. Warren and L. Brandeis. The right to privacy. In *Harv. L. Rev.*, 1890.