



Quantifying the Utility-Privacy Tradeoff in the Smart Grid

Roy Dong

Joint work with Lillian J. Ratliff, Henrik Ohlsson, S. Shankar Sastry



Privacy in the Smart Grid



The Post and Courier Search Article

[Home](#) [News](#) [Sports](#) [Business](#) [Multimedia](#) [Entertainment](#) [Features](#) [Special Sections](#)

[Home](#) > [News](#) > [Local/State News](#)

Marijuana bust shines light on utilities

Glenn Smith
Posted: [Sunday, January 29, 2012 12:01 a.m.](#), Updated: [Friday, March 23, 2012 6:08 p.m.](#)

Privacy in the Smart Grid

- * Privacy is a difficult problem because **the data is useful!**

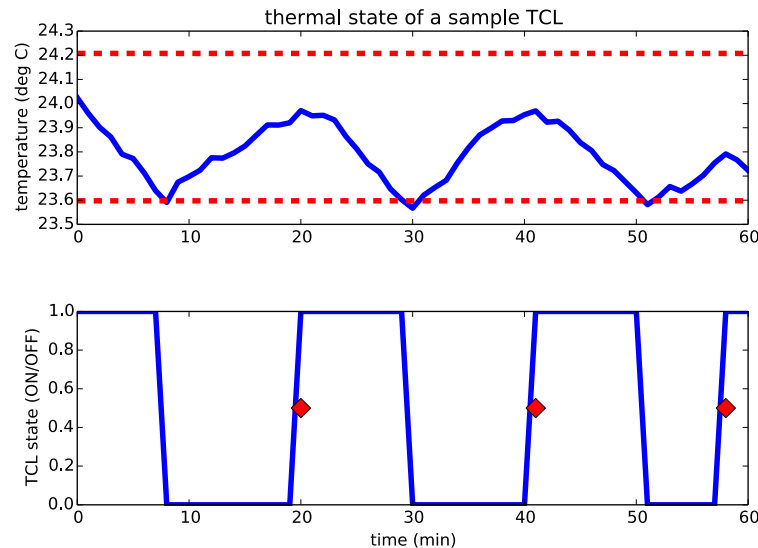
- * **Data minimization principle (NISTIR 7628)**

- * Limit the collection of data to only that necessary for Smart Grid operations, including planning and management, improving energy use and efficiency, account management, and billing.*

- * Quantify the trade-off between the amount of data and the performance of Smart Grid operations.
- * Analyze the amount of private information which can be inferred from data.

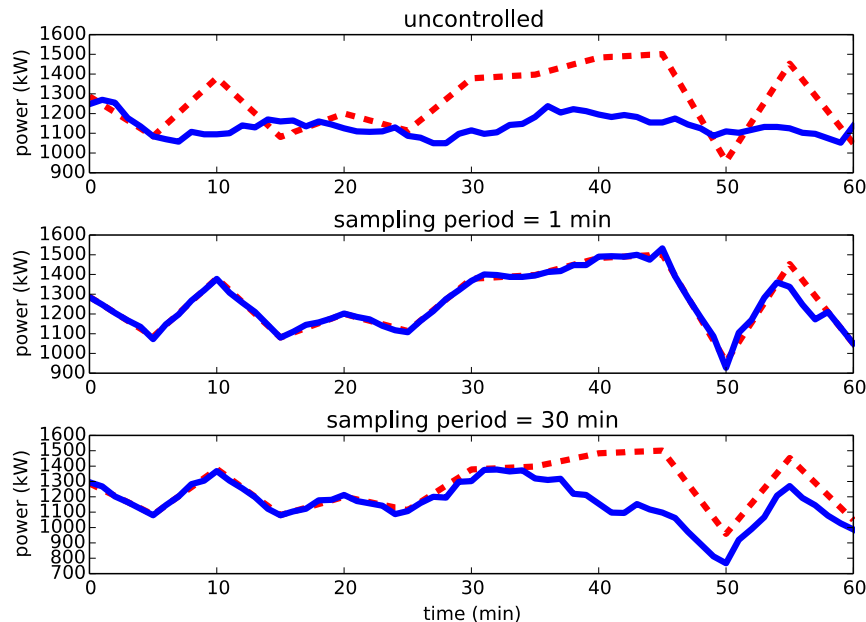
Smart Grid Operations

- * **Example:** Direct load control of thermostatically controlled loads (TCL) to correct load imbalances.
 - * Ruiz, Cobelo, Oyarzabal 2009. Callaway and Hiskens 2011. Mathieu, Koch, Callaway 2013. Moura, Bendtsen, and Ruiz 2013.
- * Tighten a hysteresis controller's deadband by issuing commands to TCLs to switch ON or OFF.



Smart Grid Operations

- * The aggregate of several TCLs can provide significant control over the total load.
- * However, the control efficacy will degrade as the direct load controller receives fewer measurements.



Privacy Metric

- * The power consumption signal is not private in and of itself. **It is what we can infer that is private.**
 - * Household occupancy.
 - * Behavioral patterns.
 - * Which devices are present in a household, and how they are used.
- * If an AMI measures only the aggregate power consumption, what can we infer?

Privacy Metric

- * This leads to our notion of privacy. In this model, our **adversary**:
 - * Observes the AMI signals.
 - * Has knowledge of what devices are in the house.
 - * Knows the dynamics and signatures of these devices.
- * The inferences this adversary can make are **bounded by the fundamental limits of nonintrusive load monitoring**.
 - * A continuation of our earlier work in energy disaggregation.

Utility-Privacy Tradeoff

- * Combining these two results, we can quantify the tradeoff between smart grid operations and privacy.

