Preserving Privacy in Cyberphysical Systems

The operation of emerging large-scale monitoring and control systems, such as intelligent transportation systems or smart grids, relies on information continuously provided by and about their users. The result can be an undesirable loss of privacy for the participants, which could delay or compromise adoption of these new technologies, thereby putting their promised benefits at risk.

Disclosure limitation has long been recognized as an important issue in the analysis of statistical databases. More recently, the need has arisen for new theories and tools that can protect the individuals around whom sensor networks and other smart information sources are being built for purposes of collecting dynamic data.

The systems in question produce public aggregate signals from their users' data—for example, the average velocity on a road segment. The main challenge then is to ensure that individual information cannot be inferred from the released signals. Systems and control science provides fundamental insights into such problems, most crucially on how to rigorously establish tradeoffs between achievable system performance and privacy.

Can Smart Grid know too much?

Hydro meter info a boon for thieves, marketers, and must be protected, privacy czar says

Toronto Star, May 12, 2010

Tanya Talaga

THEY KNOW WHEN YOU ARE SLEEPING ...

What time you sleep,cook, shower, turn on the tv, or set the alarm system can be tracked by the province's emerging smart grid hydro system, possibly tipping off thieves to a household's habits. "This thing has to be protected like Fort Knox," says Ontario's privacy commissioner Ann Cavoukian.

THEY KNOW WHEN YOU ARE AWAKE ...

THEY KNOW WHEN YOU ARE IN THE SHOWER ...

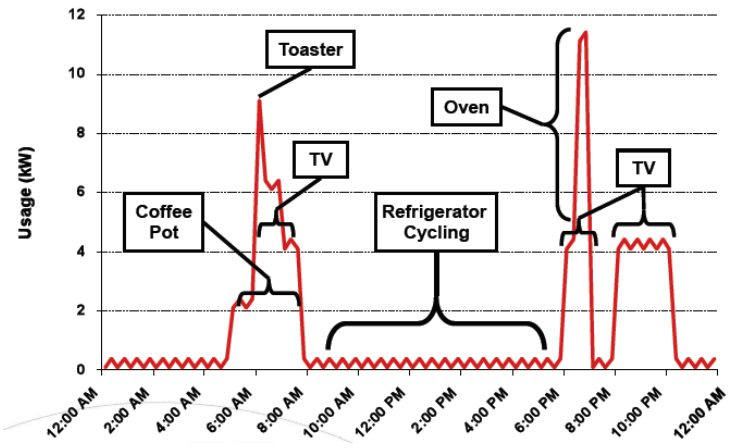
The time you jump into the shower in the morning, the time you finally flick off that to keep the information secret. Personal privacy must remain paramount as the "smart As the grid collects information on power usage and smart meters are installed in Ontario

Source: Toronto Star, May 2010

Definitions of Privacy

Defining a quantitative notion of privacy is a delicate question but is a necessary first step in providing rigorous guarantees. Privacy breaches generally arise from the possibility of linking the information released about a group of people with some additional publicly available information. Hence, simply anonymizing a dataset is usually far from enough to guarantee privacy.

Several formal definitions of privacy have been proposed for studying the tradeoff between the accuracy of the information released and the degree of privacy a given system provides. Information-theoretic definitions have a rigorous foundation but require statistical modeling of the available public information, a difficult task. A popular notion of privacy is k-anonymity, which requires that, from a released output, one cannot distinguish the information of an individual from that of k-1 others. A strong notion of privacy that has also become popular in recent years is differential privacy, a term characterizing certain algorithms releasing randomized outputs whose probability distribution is centered around the desired answer while being insensitive to the presence of any particular individual in the dataset.

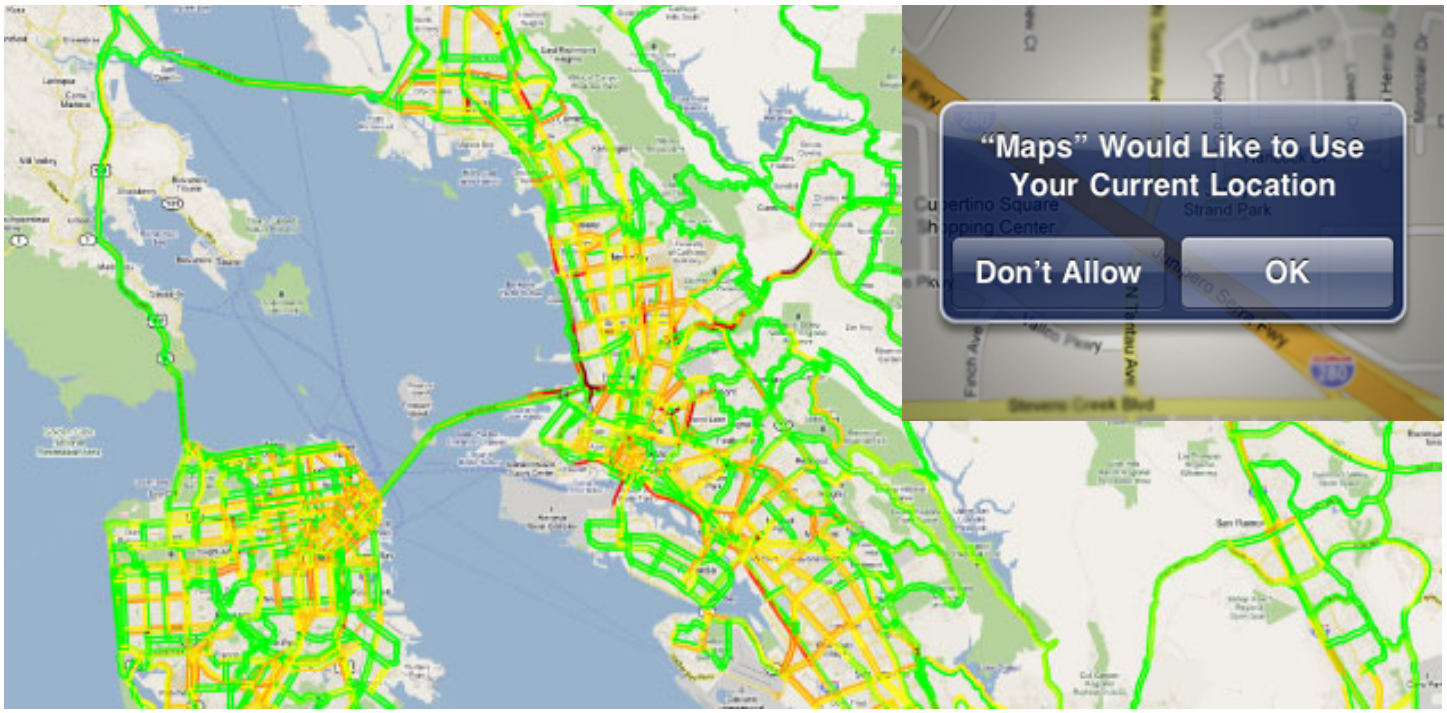


Source: M.J. Hertzler, Xcel Energy

The Smart Grid and Privacy

Privacy concerns related to cyberphysical systems (CPSs) have been targeted in particular at smart meters, halting their installation in some areas. In the 1980s, researchers noted that the appliances being turned on and off in a home can be identified by simply observing the sharp changes in total power consumption recorded by the meter, a technique called nonintrusive appliance load monitoring (see figure above). The danger is that by transmitting this data at frequent intervals, smart meters could be used to monitor the activity of a household. In fact, this data is already being broadcast every 30 seconds by certain automatic meter reading systems currently installed in millions of homes.

Contributors: Jerome Le Ny, Polytechnique Montreal, Canada, and George J. Pappas, University of Pennsylvania, USA



Source: Mobile Millennium, University of California, Berkeley

Privacy Issues in Intelligent Transportation Systems

Emerging traffic monitoring systems fuse data from a variety of sources, including feeds from GPS-enabled smartphones. Anonymity is not enough to guarantee privacy of the traces because most people can be identified just from knowing their two or three most frequently visited places (home, work, etc.). Schemes based on k-anonymity have been proposed to make the user tracking problem more difficult. Similar privacy issues arise with the smartcards used today in many public transportation systems.

Why Is Systems and Control Relevant?

Popular notions of privacy such as k-anonymity require modification before they can be effective in the context of dynamic, real-time systems. Control theory (e.g., optimal estimation) provides important tools for integrating privacy constraints into these systems without sacrificing too much performance. Intuitively, privacy is related to the system-theoretic notion of observability. Moreover, the sensitivity of an output to the data of specific individuals, which is a crucial object of study in the design of differentially private mechanisms, is also related to the standard notion of system gain.

These examples show that control scientists are well equipped to make fundamental contributions to the design of rigorous privacy schemes that can be integrated to the core of many cyberphysical systems. These user protection mechanisms will increase trust and thereby encourage the adoption of these systems, thus indirectly, and perhaps paradoxically, also contributing to improving their efficiency and performance.

For more information: I. Rouf et al., Neighborhood watch: Security and privacy analysis of automatic meter reading systems, Proc. 2012 ACM Conference on Computer and Communication Security; B. Hoh et al., Enhancing privacy and accuracy in probe vehicle based traffic monitoring via virtual trip lines, IEEE Transactions on Mobile Computing, 2012; J. Le Ny and G. J. Pappas, Differentially private filtering, to appear in IEEE Transactions on Automatic Control.