Impact of Social Behavior on Energy Theft Detection and Smart Meter User Privacy

Jinyuan Stella Sun*†, Pan Li‡, Chien-fei Chen*† and Kevin Tomsovic*†
* University of Tennessee, Knoxville
† Center for Ultra-wide-area Resilient Electric Energy Transmission Networks (CURENT)
‡ Mississippi State University

I. Introduction

In the U.S., energy theft causes about six billion dollar losses to utility companies (UCs) every year. With the smart technologies being developed to modernize the electric power grid, energy theft is becoming an even more serious problem since the "smart meters" are vulnerable to more types of attacks compared to the traditional mechanical meters. Although a few schemes have been proposed for the UCs to detect energy theft in smart grids, they all require users to reveal their private information, e.g., load profiles or meter readings at certain times, to the UCs, which invades users' privacy and raises safety concerns. In a survey we conducted recently, the majority of users expressed privacy concerns towards using smart meters. If not addressed properly, these concerns will hinder the UCs promoting their cost-efficient smart technologies. An interesting and challenging question is raised regarding energy theft detection and smart meter user privacy. The former is of ultimate interest to the UCs while the latter is of most interest to the users. But they are conflicting goals! Implementing energy theft detection on smart meters is indispensable for UCs which needs users' smart meter data as input. If the data is not sufficiently protected and reveals user privacy, it is difficult for users to accept and purchase smart metering services. In this paper, we show the necessity and challenges in solving this problem, discuss our preliminary work, and point out future research direction and a promising solution incorporating the impact of social behavior.

II. State of The Art

Energy theft has been a notorious problem in electric power grids. In the U.S. and Canada, it is estimated that utility companies (UCs) lose billions of dollars in revenue every year [1] [2]. In developing countries, energy theft can amount to 50% of the total energy delivered [3]. In the last three years, Ireland's main energy supplier has seen a 50% increase in meter box tampering. In Hong Kong, a few months back police rounded up more than 90 people suspected in a meter-tampering scheme to help restaurants lower their utility bills, with a cost estimated at HK$ 30 million to power and gas utilities [4]. The whole world seems to be suffering from this problem. Energy theft also leads to excessive energy consumption which may cause equipment malfunction or damage [5], and often enables other criminal activities [2]. Besides, utility companies usually amortize energy theft losses by increasing energy rates on honest users.

Recently, smart technologies have been developed to modernize the electric power grids to efficiently deliver reliable, economic, and sustainable electricity services. One of the most salient features of smart grids is the replacement of conventional analog mechanical meters by digital meters, usually called "smart meters". In addition to recording users' energy usage, due to their communication capability, smart meters can provide a two-way communication path between UCs and energy users, which can facilitate efficient power system control and monitoring. However, compared to mechanical meters which can only be physically tampered with, smart meters are vulnerable to more types of attacks (e.g., network attack), which makes energy theft easier to commit and hence an even more serious problem in smart grids.

In existing research works on energy theft detection, e.g., [6]–[9], the UCs need to know users' detailed energy consumption data in order to detect energy theft. However, the disclosure of such information would violate users' privacy and raise concerns about safety. In particular, users' private information may be sold to interested third-parties. Insurance companies may buy load-profiles from the UCs to make premium adjustments on the users' policies. Marketing companies may also be interested in this data to identify potential customers. Moreover, criminals (e.g., burglars) may use such private information to commit crimes, by analyzing the energy consumption pattern of the potential victims to deduce their daily behavior or whether a robbery

alarm has been set at their target location [10], [18]. Many researchers, such as Quinn [11], have realized how high resolution electricity usage information can be used to reconstruct many intimate details of a user's daily life and invade his/her privacy, and thus call for state legislators and public utility commissions to address this new privacy threat [12].

It is imperative to develop effective and efficient energy theft detection solutions while preserving smart meter users' privacy. In our previous work [13], we made a first attempt towards this goal.

III. Future Research Direction

While current research mainly focuses on the information technological solutions, we have started looking at the social aspects to stress a user-centric approach to this problem, since privacy concerns and acceptance/adoption of a technology rely largely on social and psychological factors of users and their social communities.

We conducted a preliminary online survey through Amazons Mechanical Turk in August 2013 to test the social-psychological factors affecting public acceptance and adoption of smart meters. The Mechanical Turk web site is a forum that Amazon has established to let companies and researchers pay people a small amount of money in order to carry out research. Mechanical Turk has been gaining popularity in social scientists as a useful data collection tool. Among 820 residents surveyed in the U.S., 59.5% were males, 40.0% were females, and the rest preferred not to disclose their gender; the average age was 31.38 ranging from 18 to 76; 44.6% of the participants had an annual household income higher than $50,000. Based on the data, the majority of people expressed concerns about privacy issues of smart meters. As shown in Fig. 1, 69% of people disagreed that the risk of unauthorized third party accessing smart meter data is low. Using structural equation modeling, our study also analyzed several social-psychological factors including privacy concern, environmental concern, perceived usefulness, money consciousness, perceived usefulness, trust of utility companies, and support of smart meters. The results indicated that there was a negative relationship between privacy concern and public support of smart meters, i.e., the higher the privacy concern, the lower the public support.

The results of this survey further motivated us to address energy theft and user privacy by studying the impact of social behavior and community (family, friends, neighbors, professional groups, etc.). For example, how privacy concerns of others affect the concern of an individual and his/her adoption of smart meters, how

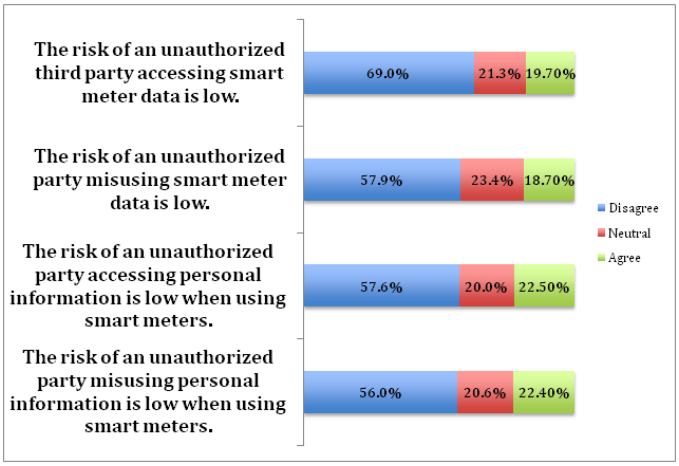

Fig. 1. Consumers' privacy concerns on smart meters.

energy theft detection can be conducted distributively and collaboratively in neighborhoods or social communities so that the violator will be shamed and educated by group members, how incentives (rewarding well-behaving neighborhoods or social communities and punishing misbehaving ones) can play a role in reducing energy theft and promoting smart meter adoption, etc. More importantly, in the end, we would like to see loss reduction in energy theft and increase in public adoption of smart metering technology, and be able to quantify such differences and compare with solutions that are not based on social behavior and interaction. The results of this study will be invaluable to both utility companies and consumers. Besides saving huge amount of money from energy theft, utility companies can identify users/groups to market smart meter services and gain insights in how to promote technology in general. Consumers can benefit from the power of their social communities and networks to understand the importance of protecting their privacy, overcome the fear for new technologies, and learn ways to improve the quality and convenience of living.

References

[1] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, May-June 2009.

[2] E. Journal, Pot growers stealing $100M worth of power: B.C. Hydro, 2010. [Online]. Available: http://www2.canada.com/edmontonjournal/news/story.html?id=0d0332f0-b8c8-42f1-a9a2-696728dbae57

[3] J. Smith, Smart Meters Take Bite Out of Electricity Theft, 2011. [Online]. Available: http://news.nationalgeographic.com/news/energy/2011/09/110913-smart-meters-for-electricity-theft/

[4] "Energy theft: From bad to worse," SmartGridNews.com, Jan 3, 2013.

[5] P. Kelly-Detwiler, Electricity Theft: A Bigger Issue Than You Think, 2013. [Online]. Available: http://www.forbes.com/sites/peterdetwiler/2013/04/23/electricity-theft-a-bigger-issue-than-you-think/

[6] A. Nizar, Z. Dong, and Y. Wang, "Power utility nontechnical loss analysis with extreme learning machine method," *IEEE Transactions on Power Systems*, vol. 23, no. 3, pp. 946–955, August 2008.

[7] J. Nagi, K. Yap, S. Tiong, S. Ahmed, and A. Mohammad, "Detection of abnormalities and electricity theft using genetic support vector machines," in *Proceedings of the IEEE Region 10 Conference*, Hyderabad, India, November 2008.

[8] S. Depuru, L. Wang, and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in *Proceedings of the Power Systems Conference and Exposition (PSCE)*, Phoenix, Arizona, USA, March 2011.

[9] C. Bandim, J. Alves, A. Pinto, F. Souza, M. Loureiro, C. Magalhges, and F. Galvez-Durand, "Identification of energy theft and tampered meters using a central observer meter: a mathematical approach," in *Proceedings of the Transmission and Distribution Conference and Exposition*, Dallas, Texas, USA, September 2003.

[10] A. Ruzzelli, C. Nicolas, A. Schoofs, and G. O'Hare, "Real-time recognition and profiling of appliances through a single electricity sensor," in *Proceedings of IEEE SECON*, Boston, Massachusetts, USA, June 2010.

[11] E. L. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network*, pp. 1995–2008, 2009. [Online]. Available: http://ssrn.com/paper=1370731

[12] "Privacy and the smart grid," NIST Guidelines for Smart Grid Cyber Security: Vol.2, August 2010. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf

[13] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids," in *Proceedings of the 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'12)*, Seoul, Korea, June 2012.

[14] M. Li, S. Salinas, A. Thapa, and P. Li, "n-cd: A geometric approach to preserving location privacy in location-based services," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'13)*, Turin, Italy, April 2013.

[15] M. Pan, H. Li, P. Li, and Y. Fang, "Dealing with the untrustworthy auctioneer in combinatorial spectrum auction," in *IEEE GLOBECOM*, Houston, TX, USA, December 2011.

[16] S. Depuru, L. Wang, and V. Devabhaktuni, "A conceptual design using harmonics to reduce pilfering of electricity," in *Proceedings of the Power and Energy Society General Meeting*, Minneapolis, Minnesota, USA, July 2010.

[17] M. LeMay and C. A. Gunter, "Cumulative attestation kernels for embedded systems," in *Proceedings of the 14th European conference on Research in computer security (ESORICS)*, Saint Malo, France, September 2009.

[18] A. Molina-Markham and P. Shenoy and K. Fu and E. Cecchet and D. Irwin, "Private Memoirs of a Smart Meter." in *BuildSys 2010*, Zurich, Switzerland, November 2010.