Securing the Smart Grid Marketplace: General Trends and Overnight Scheduling Electric Vehicle Demand[1]

J. Rowe*, J. Bushnell*, G. Kesidis†, K. Levitt*, D.J. Miller†, D.S. Rapson*, A. Scaglione*

*Univ. California at Davis {rowe,levitt}@cs.ucdavis.edu
† The Pennsylvania State Univ. {gik2,djm25}@psu.edu

Abstract

We give an overview of data security issues for the smart electrical grid. In the recent past, the electrical power system has experienced unexpected, large-scale, cascading failures initiated by relatively small failures (which may be deliberately caused in the future), and market manipulation (a well-known example of which is Enron's manipulation of the California ISO marketplace). The hope is that such problems will be addressed by the onset of the Smart Grid. Finally, we describe the future problem of automated, overnight scheduling of electric vehicle demand, wherein the consumers may selfishly misrepresent their needs to a demand aggregator.

Keywords: smart electrical grids, security, scheduling, economics

1. Introduction

For nearly 40 years, the United States has faced a critical problem: increasing demand for energy has outstripped the ability of the systems and markets that have evolved to supply past demand. Today, a variety of promising new technologies offer a partial solution to this problem. Clean, renewable power generation, such as solar and wind, are increasingly available. Hybrid and plug-in electric vehicles are currently on the market, offering greater energy efficiency in transportation, the largest single consumer of fossil fuel. The power grid that manages the generation, transmission and distribution of electric power, however, was designed and constructed in the 1960s and is ill-suited for integration with these emerging energy technologies. Electrical grid state estimation and prediction that includes generation assets with

random availability, like solar and wind, requires new sensing and control algorithms [16]. Widespread use of plug-in electric or hybrid-electric vehicles (PEV/PHEV) will not only require far greater power capacity than is currently available, but will also radically change the peak usage profile, with large evening demand that cannot be shifted [25] (but which may be well suited to exploit renewable wind energy, a significant portion of which is generated at night [9]).

To address this problem, and to generally improve robustness, our current power grid must be upgraded with a control system that uses the full power of modern sensor and computing technology to increase efficiency. This new power grid, with an integrated, modern IT control plane is commonly referred to as the Smart Grid [7].

In the future grid, individual power customers themselves will be integrated as grid control components. PEVs/PHEVs, Heating Ventilation and Air Conditioning (HVAC), and new sustainable energy devices (solar, wind, battery storage, *etc.*) will be optimally scheduled in coordination with the grid operators using price as an incentive. Households will use SmartMeter gateways running automated power scheduling programs, just as the current grid wide energy operator-to-operator transactions are software automated.

This paper is organized as follows. In Section 2, we give a brief overview of significant problems with the electrical power system/grid in the recent past: cascading failures and market manipulation. In Section 3, we describe the Smart Grid framework and its security challenges. The specific future problem of automated, overnight scheduling of PEV/PHEV demand is described in Section 4. We conclude in Section 5 with a summary of the challenges facing the Smart Grid.

2. Problems from the recent past

2.1. Cascading failures: physical power system and its internal sensing and communication system

On several occasions in the recent past, a relatively small failure in an interconnected power system (*e.g.*, the failure of a power relay, or an overloaded line) has quickly and unexpectedly caused, in cascading fashion, a broader system failure leading to a significant blackout, *e.g.*, [6]. The conclusion of a survey of such events identified the main causes as (naturally) increasing failure rate of aging equipment (so part of a more general problem

of inadequate system maintenance and upgrading), and a lack of reliable operational telemetry (power system state) communicated to automated and coordinated controls capable of responding with remedial action in real time (to prevent cascading failures) [3]. Considering the apparently unexpected nature of these events, prior risk/sensitivity analysis of these systems was poorly reckoned and/or subjected to peculiar cost/threat trade-off decisions.

Though these examples are not ones of malicious intent, the potential is there to deliberately precipitate such events given knowledge of the vulnerabilities to cascading failures, and an avenue for an outside-attacker would be via public Internet interfaces to the grids Supervisory Control and Data Acquisition (SCADA) system. Risk analysis typically includes deliberate attack scenarios, and optimal remedial response may need be based in part on determination of the cause of the problem at hand.

2.2. Market manipulation: physical power system and its energy marketplace

The production and distribution of electric power is very different from other types of energy sources, such as natural gas. Electricity cannot be transported and stored at the discretion of the utilities or their customers. Once energy is generated, the ability to direct its flow is limited. The primary means to control the flow of electricity is by controlling generation, which determines how power will flow through the transmission system. California, for example, is a net consumer of electric power generated by net suppliers in the Pacific Northwest through the California-Oregon Inter-tie transmission line [30]. To get net power to flow south over this transmission system, generation is allowed to increase above usage loads in Oregon/Washington and decreased below loads in California. This involves the coordination of independent power utilities and transmission line owners, all with differing capacity parameters, and is far more complex than simply transporting a physical product to the location of its demand. California utilities coordinate these operations through the California Independent System Operator (Cal-ISO) Corporation. Cal-ISO plans electrical power flow by pre-scheduling generation plant operations in advance, taking into account the constraints of the physical transmission line model of the California grid. This proceeds in a series of stages. In the first stage, Cal-ISO calculates the week-ahead schedule during which all participating utilities submit wholesale pricing bids on the amount of power they anticipate as excess supply or as net demand. As the delivery date approaches, the schedule is updated daily, then hourly,

until reaching the final 5-minute spot market to adjust for realtime operating conditions. This differs from a complex, realtime control problem in that updates to the original schedule must include financial inducements for operators to change generation plans upon which they originally placed monetary bids. This is done through a system of structured payments and surcharges designed to provide economic incentives and fairness in support of robust business operations. The result is that the scheduled generation control plan for the physical system, designed by power engineers, becomes tightly coupled with the business economics of the utilities and the designed market structure.

Cal-ISO has automated both the financial bidding procedure and the planned generation schedule as much as possible. Initial power demand and supply is found using an automated price clearing program that matches bids submitted to the system by remote utilities. The generation schedule is subsequently calculated by an automated procedure using simulated state-estimation under the constraints of the power grid physical topology and inter-tie capacities. A suitable physical generation schedule that matches the capacity of the grid and balances power demand price bids with supply bids is accepted as the relevant advance schedule.

Manipulations of energy markets can cause loss of power service without attacking the physical infrastructure itself. The basic scheme used by Enron was market arbitrage of energy prices on major California inter-ties leading to widespread rolling blackouts. Enron traders probed the automated energy market (a "cyber information exchange) in 2000 to discover its trading algorithms. Exploiting this information, as well as using their assets for power supply in Nevada and Oregon, Enron traders issued artificial energy contracts to drive the price of energy up, defrauding Californians of almost $50B by shedding load (they never could utilize) [23].

The effects of Enrons energy market attacks were felt in the physical power delivery system as well. Due to apparent congestion on critical long distance inter-ties, Cal-ISO implemented rolling blackouts as an emergency measure to alleviate the imaginary congestion. The overall physical power delivery infrastructure, designed to be robust against a variety of equipment failure and natural faults, proved vulnerable to attacks in the associated market based coordination mechanism. Furthermore, the attacker obtained knowledge of the topology and its capacity by probing the control software. The topology was designed according to sound power engineering principles, but vulnerable to market manipulation.

Monitoring the scheduling and trading software with standard cyber-security techniques would not show any compromise of vulnerable software components. Even though the grid power delivery system tolerates random physical disruption, automated market-based control resulted in blackouts from financial manipulation. Many aspects of this particular misuse instance of the power grid software could have been protected and prevented. A simple specification that checked inter-tie bid values with the capacities of assets they serve could have detected the activity in its probing stage. (related ideas of vulnerability, detection and the detection of vulnerability probes, in cyber security) In hour-ahead scheduling with associated payments and surcharges, one might discover vulnerable inter-tie links serving primarily hard load demand as ripe for overscheduling misbehavior. Finally, a global analysis of aggregate idle generation capacity and realtime load could alert operators to unnecessary emergency blackout procedures that could be lifted.

An exploit, described as Enron-like, has been recently reported, *e.g.*, [19], indicating that such problems persist to this day.

3. The Smart Grid and its new security challenges

For improved efficiency, our current power grid is being upgraded with a control system that uses the full power of modern sensor and computing technology, *i.e.*, an integrated modern IT control plane. The Smart Grid features:

- Distributed control: The current grid operates on a hierarchical control model. Control decisions made at the top level are enforced down to the individual small operator level. Inefficiencies in power generation and distribution can be reduced using a more decentralized control model. Wind power, say, that suddenly becomes available, can be utilized by a neighboring system operator in a distributed Smart Grid control architecture without updating a global power grid generation schedule for all performers [27].

- Customer/Grid Integration to more carefully match supply to demand: In the current power grid, demand from customers is represented as an abstracted aggregated power load external to the system. The power grid is designed with a threshold capacity that matches aggregated customer peak load. In a Smart Grid, integrating customer's sites into the grid control system, load can be partially modulated to reduce the

burden on the grid during peak hours. Scheduling of certain interruptible tasks (PHEV charging, appliance usage, *etc.*) using control signals from the Smart Grid can avoid the need for over-provisioning of generation, transmission and distribution systems, *e.g.*, [5, 26].

- Market-based Control: A challenging aspect of Smart Grid design is the use of pricing as a means for control. The incentive for customers to shift load is typically based upon tier-based or even real-time retail price information delivered to the customers SmartMeter. In California the overall grid generation schedule, coordinating all power generation, transmission and distribution in the state, is wholesale market based using an automated software bidding system [2, 1]. This system has proven to be vulnerable to manipulation and instability that extends even into the physical grid itself.

To attain a Smart Grid that considers features points (1)(3) above, augmented with enhancements to achieve security in power and market delivery, will entail a study of economic market models with stability as one objective but also include consideration of new sources of power and usage, both on the producer and the consumer sides. We emphasize that security enhancements need to take place at both the market level and the system level, requiring independent and reliable state-estimation models. It is desirable to integrate the two control models, so that operators can detect and respond to activity, malicious or caused by natural disturbances, that threaten either level; the unification of the models permits the investigation of attacks at one level that are handled at the other or of attacks at both levels that must be handled at both levels.

Regarding security of the Smart Grid marketplace, distributed control schemes are realized using market mechanisms. Payments and surcharges in the wholesale power market are used as inducement for independent suppliers/operators to increase or curtail power generation. Markets mechanisms are also seen as means to shed power load at Smart Grid retail customer endpoints (*e.g.*, higher energy prices during peak load periods). it is critical to augment standard cyber-security and power system design to include analysis of economic stability and behavior when determining the robustness and security of future Smart Grid design and components. Possible general suggestions include:

- Disclosure of economic conflicts-of-interest of energy market partici-

pants, and decision-making by the ISO considers those conflicts-of-interest.

- Consider the activity of former ISO employees in power suppliers and demand-aggregators, and the associated potential for exploitation of inside information.

- Require out-of-band acknowledgements, with CAPTCHA, of interactions with energy market participants, especially during periods of relatively-high demand or failure response.

- Improve attribution and accounting to track insider attacks.

The Smart Grid framework may actually heighten the threat of manipulation and cascading failures, because:

- new vulnerabilities may be added, *e.g.*, due to additional data interfaces;

- the system may over-react more quickly than before to similar vulnerabilities; or

- a distributed, hierarchical framework (*e.g.*, involving demand aggregators) to may be required process the increased volume of smart-metering telemetry, *i.e.*, a "big data" problem.

Other important Smart Grid cyber-security problems have received considerable attention, including securing digital energy signaling and pricing communications, attacks from malicious compromise and control of grid hardware (sensors, SCADA controlled assets, control room interfaces), protecting the privacy of individuals using dynamic energy usage control, and attack resistant SmartMeter hardware [4, 21, 20].

4. Future overnight, automated scheduling of electrical vehicle demand

Smart Grid components will be deployed to customer sites to allow for controlled load balancing. Fixed schedule, tiered retail pricing schemes are already used by PG&E customers with SmartMeters in California, as well as many other locations. Eventually dynamic scheduled tiered pricing will be deployed with actual on-site electrical consumption controlled by automated

Home Area Network (HAN) energy gateways [15]. The HAN energy manager runs a configurable, automated procedure to adjust usage in response to changes in retail energy pricing level received from the utility. Obviously it is critical to build security into these systems just as in the Smart Grid management systems themselves. Widespread deployment of HAN energy gateways may also be a monoculture vulnerability; an exploit crafted for a single device could potentially affect all devices in a large region. New and novel stealthy economic attacks against customers might be feasible. Guarantees on the security and reliability of these devices are obviously critical.

On the side or residential or industrial consumption of power, privacy is an issue that has been raised. Consider a personal residence with 128 devices/appliances each transmitting a 16bit measurement of power consumption every second. The total transmission rate is only 2 kbits/s, much less than a single telephone/voice call. So, strong public and/or symmetric key encryption is feasible, and so a "side channel" threat is likely negligible even if a broadcast (*e.g.*, wireless) LAN is used to network SmartMeters and signal near-term demand (the latter for scheduling purposes). This said, the utility or other third-party concentrators of energy-usage data (*e.g.*, Google through its PowerMeter service) should perhaps not be entirely trusted to maintain privacy [24].

Regarding the scheduling of residential demand, in one decentralized scenario, the grid controls demand through signaled spot pricing typically based on a combination of currently (real-time) assessed demand (through SmartMeters), and the demand of the recent past (*e.g.*, "day ahead" pricing). In another centralized scenario, the consumers plug their high-energy appliances (*e.g.*, HVAC) into a circuit controlled by the grid (demand aggregator), allowing the grid to periodically cycle power from those circuits so as to peak-shave aggregate demand. We assume in the following that consumers are incentivized to use such circuits by price discounts.

Consider the case of automated scheduling of Plug-in Electric or Hybrid-Electric Vehicles (PHEV/PEV) overnight, a growing segment of electricity demand [8]. This type of demand is flexible in that it can be deferred and paused, and thus ideally suited to exploit renewable wind energy supply [9], however there is the deadline ahead of the morning commute (*i.e.*, a finite time-horizon for scheduling). Also, certain popular car battery types, such as LI-ion [29], require non-constant power profiles [28, 13] which complicates scheduling [22].

In the decentralized context, the aim of consumers would be to desyn-

chronize demand, *e.g.*, [5, 26]. They could employ randomization as in packet networking contexts, *e.g.*, ALOHA transmits packet at random time after a collision, and Random Early Discard (RED) was used to try to desynchronize TCP sessions at the onset of congestion avoidance. These packet-networking systems have experienced their own problems in the past, including those of end-user cooperation, so the Smart Grid could police compliance with mechanisms to desynchronize demand.

For a centralized scheduling context (*e.g.*, [22]), consider the reliability of the attestation of the true required power by the consumers. Such attestations may be subject to "natural" measurement noise, *e.g.*, [18]. On the other hand, the consumer's computer may be infected by malicious software that deliberately misrepresents demand[2], or the consumers themselves may be deliberately misrepresenting demand[3] (at the presumed discounted rate for the circuit controlled by the grid), leading to grid-state estimation error [21, 20, 18] with respect to consumer demand/load. For the latter case, suppose the consumer knows that the objective of the grid is to maximize the *number* of satisfied customers. Such a goal may result in scheduling bias against customers with larger demand, thus incentivizing them to request the mimimal amount of charge they require to make their morning commute, but that is also clipped on the right[4].

In some states, consumers can sell their locally stored energy, typically generated from solar and wind sources, and possibly even from PHEV/PEV batteries themselves, back to the grid during overage periods or to deal with stability issues [14]. So, one can also envision a scenario involving a a coalition of consumers[5] that overstate/feign demand in an attempt to drive up the price of energy (say at the end of the charging interval close to the start-time of the morning commute), while being prepared to shed this feigned demand for profit, or being in a position to profit by *providing* energy back to the

[2]Perhaps simultaneously for many infected consumers, recall HAN monoculture vulnerabilities.

[3]Much nuisance and more significant types of malicious attack activity online is facilitated by the ease with which hackers can act anonymously. It is not clear the degree to which such anonymity will be possible for the residential consumers of a future Smart Grid.

[4]Obviously, it may be desireable that consumers are charging only what they need particularly in periods of high demand.

[5]Possibly, an coalition orchestrated by infection by a common virus.

grid.

Recall that this consumer-side perspective is part of a broader problem of reliable state estimation of the whole grid in the presence of false data. Recently, deliberately caused state-estimation errors have been considered for the real-time (not dynamic) setting, *e.g.*, [21, 20, 18], where:

- complete grid-state information is estimated from a limited number of observable states (here including instantaneous consumer demand owing to SmartMeters),
- sensitivity to the observed (and assumed manipulatable) states of the solution of a constrained linear program model for the grid markeplace including [10]:
  - power stations with different prices and capacities of supply,
  - transmission lines with power constraints,
  - linear power flow equations for the grid, often simplified via "DC" approximation.

Since PEV/PHEV demand is characterizable, a demand aggregator can consider historical charging profile (even if just day-ahead), in addition to same-day attestations of demand, and instantaneous (real time) demand measurements. In so doing, the demand aggregator can police individual consumer demand. Given discrepencies between historical and current demand, the demand aggregator can try to decide among the following hypotheses:

- natural measurement noise,
- limited capacity due to aging [12] (causing a clipping of the power-demand profile on the right),
- unexpected additional load, *e.g.*, another simultaneous PEV/PHEV charging task or appliance operation, other types of
- none of the above, *i.e.*, deliberate misrepresentation of demand.

Given deliberate misrepresentation of demand, the demand aggregator may attempt to correct the requested demand of individual consumers based on their historical demand data. Continuing along these lines, we can formulate leader-follower (grid-consumers)games with deception; *e.g.*, [11], and Sec. 3.4 of the JASON report [17] on the role of game theory to reason about the cost-benefit trade-offs of both attacker and defender.

5. Conclusion: Summary Challenges for the Smart Grid

In summary, the fundamental challenges for a Smart Grid architecture will e to provide stability, robustness and security in both electrical power delivery and market delivery infrastructures, more specifically:

- Robust integrative models of future Smart Grid topologies (generation, transmission, distribution) and the wholesale power markets used to affect control (financial and regulatory).
- Vulnerabilities in Smart Grid control models that might lead to manipulation and exploitation of power delivery systems and markets.
- Methods for protecting distributed power delivery systems using monitoring, diagnosis and security aware feedback control.
- Market structures that promote stability in an integrated Smart Grid power delivery system.

[1] Z. Alaywan. Facilitating the congestion management market in california. *California Independent System Operator*, April 1999.

[2] Z. Alaywan. Imbalance energy at the california iso. *California Independent System Operator*, June 2003.

[3] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Trans. Power Systems*, 20(4), Nov. 2005.

[4] R. Berthier, W.H. Sanders, and H. Khurana. Intrusion detection for advanced metering infrastructures: Requirements and architectural directions. In *Proc. IEEE Int'l Conf. on Smart Grid Communications (SmartGridComm)*, Oct. 2010.

[5] S. Caron and G. Kesidis. Incentive-based energy consumption scheduling algorithms for the smart grid. In *Proc. IEEE SmartGridComm*, Gaithersburg, MD, Oct. 2010, Extended version http://www.cse.psu.edu/∼kesidis/papers/smartgridcomm10-extended.pdf.

[6] S. Corsi and C. Sabelli. General blackout in Italy sunday september 28, 2003, h. 03:28:00. In *Proc. IEEE Power Engineering Society (PES) General Meeting*, June 2004.

[7] The smart grid: An introduction. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages 2009.

[8] EPRI. Impact of plug-in electric vehicle technology diffusion on electricity infrastructure: Preliminary analysis of capacity and economic impacts. product id # 1016853. http://mydocs.epri.com/docs/Portfolio/PDF/2010_P018.pdf, 2010.

[9] European Wind Energy Association. Wind energy: The facts. part 2, chapter 2 - Understanding variable output characteristics of wind power. 2009.

[10] J.J. Grainger and W.D. Stevenson. *Power System Analysis*. McGraw-Hill, 1994.

[11] J.P. Hesanha. Application and value of deception. In A. Kott and W.M. McEneaney, editors, *Adversarial Reasoning*. Chapman and Hall / CRC Computer Info. & Sci. Series, 2006.

[12] How to prolong lithium-based batteries. Available at http://batteryuniversity.com/learn/article/how_to_prolong_lithium_based_batteries.

[13] IBT Power. Lithiumion technical data, 2012, Available at http://www.ibt-power.com/Battery_packs/Li_Ion/Lithium_ion_tech.html.

[14] IEA. The role of energy storage for mini-grid stabilization. Technical Report IEA-PVPS T11-02:2011, International Energy Agency, 2011.

[15] Intel home energy management platform. http://www.intel.com/p/en_US/embedded/applications/energy/energy-management.

[16] A. Ipakchi and F. Albuyeh. Grid of the future. *IEEE Power and Energy Magazine*, Mar. 2009.

[17] JASON. Science of cyber-security. Technical Report JSR-10-102, JASON, The MITRE Corp., Nov. 2010, http://www.fas.org/irp/agency/dod/jason/cyber.pdf.

[18] L. Jia, R.J. Thomas, and L. Tong. Malicious data attack on real-time electricity market. In *Proc. IEEE Int'l Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, May 2011.

[19] D. Kasler. Electricity trading probed. http://www.sacbee.com/2012/07/30/4672960/electricity-trading-probed.html#storylink=cpy, Jul. 30, 2012, last modified Sep. 20, 2012.

[20] O. Kosut, L. Jia, R.J. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: attack strategies and countermeasures. In *Proc. IEEE SmartGridComm*, Gaithersburg, MD, Oct. 2010.

[21] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and Systems Security (TISSEC)*, 14(1), May 2011.

[22] H. Lu, G. Pang, and G. Kesidis. Automated scheduling of deferrable PEV/PHEV load in the smartgrid. Technical Report CSE-12-004, Pennsylvania State University, CSE Dept, Nov. 2012, http://www.cse.psu.edu/research/publications/tech-reports/2012/CSE-12-004.pdf.

[23] R. McCullough. Congestion manipulation DeathStar. Technical report, McCullough Research, June 5, 2002.

[24] P. McDaniel and S.W. Smith. Security and privacy challenges in the smart grid. *IEEE Security and Privacy Magazine*, May/June 2009.

[25] K. Mets, T. Verschueren, W. Haerick, C. Develder, and F. De Turck. Optimizing smart energy control strategies for plug-in hybrid electric vehicle charging. In *Proc. IEEE/IFIP Network Operations and Management Symposium (NOMS) Workshops*, April 2010.

[26] G. Pang, G. Kesidis, and T. Konstantopoulos. Avoiding overages by deferred aggregate demand for PEV charging on the

smart grid. In *Proc. IEEE ICC Selected Areas in Communications Symposium: Smart Grids*, June 2012, Extended version http://www.cse.psu.edu/research/publications/tech-reports/2011/CSE-11-009.pdf.

[27] M. Pipattanasomporn, H. Feroze, and S. Rahman. Multi-agent systems in a distributed smart grid: Design and implementation. In *Proc. IEEE/PES Power Systems Conference and Exposition*, Mar. 2009.

[28] C. Simpson. Battery charging. *National Semiconductor*, 2011, Available at http://cegt201.bradley.edu/projects/proj2008/lcc/pdf /national_battery_charging.pdf.

[29] Tesla Motors Company. Roadster innovations/battery: Increasing energy density means increasing range. http://www.teslamotors.com/roadster/technology/battery.

[30] S. Wiggerhaus. California-Oregon Intertie (Path 66) and Pacific DC Intertie (Path 65). Technical report, Bonneville Power Administration, March 2004.