2011 American Control Conference
on O'Farrell Street, San Francisco, CA, USA
June 29 - July 01, 2011

Reconfigurable Interdependent Infrastructure Systems: Advances in Distributed Sensing, Modeling, and Control

Anthony M. Giacomoni, *Graduate Student Member, IEEE*, S. Massoud Amin, *Senior Member, IEEE*, and Bruce F. Wollenberg, *Life Fellow, IEEE*

***Abstract*--Secure and reliable operation of complex interactive power networks poses significant theoretical and practical challenges in analysis, modeling, simulation, prediction, control, and optimization. In addition, mathematical models of such interactive systems are typically vague (or may not even exist); moreover, existing and classical methods of solution are either unavailable, or are not sufficiently powerful. In this paper, we briefly address this problem, and discuss recent advances in distributed sensing, modeling, and control, particularly at the consumer level. Such advances contribute toward the development of an effective, intelligent, distributed control of power system networks to achieve the overall objectives of efficiency, robustness, security, and reliability.**

I. Introduction

MANY national and international critical infrastructures are complex interdependent/networked dynamical systems; these include the following overlaid and coupled systems:

- Electric power grids
- Oil and gas pipelines
- Telecommunication and satellite systems
- Cyber infrastructure
- Transportation networks
- Banking and finance systems
- State and local water supply, emergency, and other services.

Management of disturbances in all such complex interdependent networks, and prevention of undesirable cascading effects throughout and between networks, requires a basic understanding of true system dynamics, rather than mere sequences of steady-state operations. Effective, intelligent, distributed control is required so that, after a disturbance, parts of the networks will remain operational and even automatically re-configure themselves.

For the most part, no present methodologies are suitable for understanding the behavior of such systems. For example, in many complex networks involving human-machine interfaces, the most important element in successful recovery after a failure is the adaptability of human participants. Adaptability's criticality is unquestioned, but automating it is beyond current capabilities.

Manuscript received September 25, 2011. This work was supported by the National Science Foundation under grant number 0831059.

The authors are with the Electrical and Computer Engineering Department, University of Minnesota, Minneapolis, MN 55455 USA (email: giaco013@umn.edu; amin@umn.edu; wollenbe@umn.edu).

Modeling these networks, especially in the case of economic and financial market simulations, requires modeling the systemic risk emanating from the bounded rationality of actual human thinking, unlike that of a hypothetical "expert" human as in most applications of artificial intelligence. Furthermore, a pertinent question is at what resolution should automated sensing, modeling, and control be started to achieve the overall objectives of efficiency, robustness, security, and reliability?

In this paper, the challenges associated with the secure and reliable operation of interconnected electric power networks and recent advances in distributed sensing, modeling, and control at the consumer level are discussed. Section II describes the challenges facing electric power grids, Section III describes smart grids and advanced metering infrastructure, Section IV presents a tool for demand side energy management, and Section V provides an analysis of demand response at the distribution level. Finally, Section VI states some conclusions.

II. Electric Power Grids

A. Operating States

The various operating states of a power system are depicted in Fig. 1.

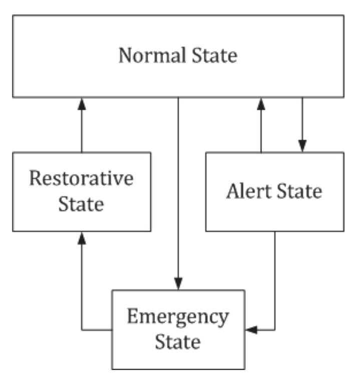

Fig. 1. Power system operating states.

The system is characterized as having multiple states, or "modes," during which specific operational and control actions/reactions are taking place:

- ***Normal mode:*** economic dispatch, load frequency control, maintenance, forecasting, etc.
- ***Alert mode:*** red flags, precursor detection, reconfiguration and response
- ***Emergency/Disturbance mode:*** stability, viability, and integrity -- instability, load shedding, etc.

978-1-4577-0079-8/11/$26.00 ©2011 AACC

- ***Restorative mode:*** rescheduling, resynchronization, load restoration, etc.

Each of the above-noted states provides guidance on how to measure and adapt to disturbances. For example, the emergency state is subdivided into three crises (stability, viability, and integrity), which include dynamics and time frame characteristics. Stability emergencies include transient and oscillatory instability, which occur in periods of a few to tens of seconds. Viability emergencies are longer-term operation contingencies, such as voltage instability, which may last for several minutes up to hours. An example is the precursor signatures present in the reactive power measurements during the August 2003 northeastern United States and Canada blackout.

In addition, the above system is multi-scale in time, operational space, and its dynamics. The time-scale of actions and operations within the power grid (often continental in scale) range from: microseconds to milliseconds for wave effects and fast dynamics (such as lightning), milliseconds for switching overvoltages, 100 milliseconds or a few cycles for fault protection, 1 to 10 seconds for tie-line load frequency control, 10 seconds to 1 hour for economic load dispatch, 1 hour to a day or longer for load management, load forecasting, and generation scheduling, and several years to a decade for new transmission or generation planning and integration.

B. Challenges

Electrical infrastructure is becoming increasingly interconnected and complex, thus, posing new challenges for its secure, reliable, and efficient operation. The infrastructure is a complex dynamic network, geographically dispersed, non-linear, and interacting both among itself with communication systems, fuel supplies, and markets, and with its human owners, operators, and users. No single entity has complete control over its operation, nor does any such entity have the ability to evaluate, monitor, and manage it in real time. In fact, the conventional mathematical methodologies that underpin today's modeling, simulation, and control paradigms are unable to handle the complexity in its dynamics, and its increasing interconnectedness [1].

As an example, widespread outages and huge price spikes during the last two decades have raised public concern about grid reliability at the national level. The potential for larger-scale and more frequent power disruptions is considered higher now than at any time since the great Northeast blackout of 1965. Furthermore, the potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energize and control their operations. Such circumstances have highlighted the need to strengthen the nation’s electric power grid, to make it smarter, more secure, and more reliable.

Due to its size, complexity, and cost, the transformation of the existing electrical grid will need to occur in several stages over time with equipment being gradually replaced as it reaches the end of its operating life. Estimates by the U.S. Department of Energy (DOE) assess the value of the nation’s electricity infrastructure to exceed $800 billion. Power plants comprise approximately 60% of this value, distribution facilities 30%, and transmission facilities 10%. Thus, the grid represents a total investment of approximately $320 billion [2].

III. Smart Grids and Advanced Metering Infrastructure

A. Smart Grids

The term “smart grid” refers to the use of computer, communication, sensing, and control technology, which operate in parallel, with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, and facilitating the interconnection of new generating sources to the grid.

Recent policies in the U.S., China, India, EU, and other nations, combined with the potential for technological innovations and business opportunities, have attracted a high level of interest in smart grids. Smart grids are seen as a fundamentally transformative, global imperative for helping the planet deal with its energy and environmental challenges. The ultimate goal is for an end-to-end electric power system (from fuel source, to generation, transmission, distribution, and end use) that will:

- Allow secure and real-time two-way power and information flows
- Enable integration of intermittent renewable energy sources and help to decarbonize power systems
- Enable energy efficiency, effective demand management, and customer choice
- Enable the secure collection and communication of detailed data regarding energy usage to help reduce demand and increase efficiency.

In 2007, the United States Congress passed the Energy Independence and Security Act outlining specific goals for the development of the nation’s smart grid. Section 1301 of this Act states that, “It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
2) Dynamic optimization of grid operations and resources, with full cyber-security…” [3].

Pertinent R&D programs aimed at developing smart and self-healing grids, and the associated terminology, date back to the 1990s, although the concept was first envisioned in 1978 [4]. Of particular interest is a largescale research program conducted jointly by the Electric Power Research Institute (EPRI) and the U.S. Department of Defense (DOD) during 1998-2002, titled Complex Interactive Networks/Systems Initiative (CIN/SI). This work provided the mathematical foundations and simulations for the smart self-healing grid and showed that the grid can be operated close to the limit of stability given adequate situational awareness combined with better secure communication and controls [5].

B. *Advanced Metering Infrastructure (AMI)*

1) *Description and Capabilities*

Presently, many utilities and other stakeholders are increasingly involved in deployment of smart grid technologies including Advanced Metering Infrastructure (AMI). AMI provides two-way communication between customers and utilities. The implementation of AMI represents the first step in the digitalization of the electric grid. Several countries including Italy, the Netherlands, Denmark, Sweden, and the United States have already taken initial steps toward the deployment of AMI by installing automated meter reading (AMR) systems, which can read measurement registers remotely. Sweden, for example, had nearly 100% utilization of AMR systems as of July 1, 2009 in order to meet legislation requiring that all electricity consumers with a main fuse of 63*A* or smaller have monthly energy meter readings [6].

Such devices will allow for numerous advanced capabilities, including the ability to:

- Track customer usage such as total energy consumption
- Remotely connect and disconnect customers
- Send out alarms in case of problems
- Provide real-time pricing
- Remotely read measurement registers
- Send power quality data
- Dim customer usage for non-paying customers
- Remotely receive firmware upgrades in order to update software and incorporate new functionality.

The input and output signals for a typical AMI system is shown in Fig. 2.

In addition, AMI provides grid operators with increased control over gird operations with improved ability to manage demand. For example, several customers could be simultaneously turned off on short notice in an emergency in order to balance the grid. For demand side management, AMI could be integrated into home automation systems or Home Area Networks (HANs) for automatic responses to varying real-time prices [7]. Consumer surveys indicate that many consumers are interested in real-time pricing, and results from Ameren's Energy Smart Pricing Plan (ESPP) pilot in Illinois and its ensuing Power Smart Pricing program have provided proof that consumers can and will respond to price signals [8].

2) *Vulnerabilities*

Despite the increased interest in the utilization of AMI, there has been very little assessment or R&D effort to identify the security needs for such devices. Smart meters, however, are extremely attractive targets for exploitation since vulnerabilities can be easily monetized through manipulated energy costs and measurement readings. Currently, in the U.S. alone, it is estimated that $6 billion is lost by electricity providers to consumer fraud in the electric grid [9].

Possible threats to the electrical grid introduced by the use of AMI include:

- Fabricating generated energy meter readings
- Manipulating energy costs
- Disrupting the load balance of local systems by suddenly increasing or decreasing the demand for power
- Gaining control of possibly millions of meters and simultaneously shutting them down
- Sending false control signals
- Disabling grid control center computer systems and monitors
- Disabling protective relays.

As more utilities move toward using Internet protocol (IP)-based systems for wide area communications and the trend of using standardized protocols continues throughout the industry [10], maintaining the security of such devices will be critical. AMI introduces earnest privacy concerns, as a data "tsunami" of immense amounts of energy use information will be stored at the meter. Breaches into this data could expose customer habits and behaviors [9], [11]. Such arguments have led to the recent moratoriums on AMI installation in numerous Northern California communities and other areas throughout the country [12]. As a result, several key privacy concerns need to be addressed [3], [13], which include:

- Personal Profiling – using personal energy data to determine consumer energy behavioral patterns for commercial purposes
- Real-time Remote Surveillance – using live energy data to determine whether people are in a specific facility or residence and what they are doing

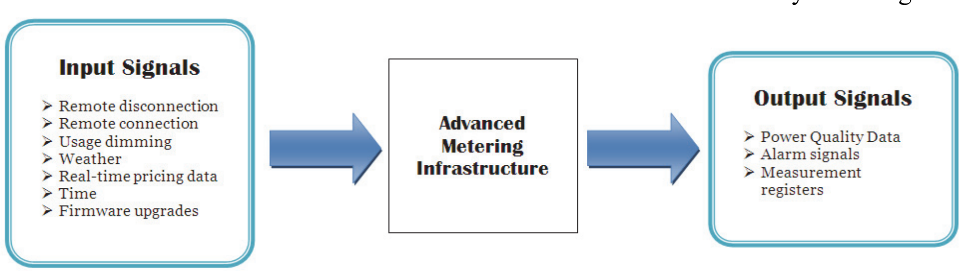

Fig. 2. Typical AMI input and output signals.

- Identity Theft and Home Invasions – protecting personal energy data from criminals who could use them to harm consumers
- Activity Censorship – preventing the use of energy for certain activities or taxing those activities at a higher rate
- Decisions Based on Inaccurate Data – shutting off power to life-sustaining electrical devices or providing inaccurate information to government and credit-reporting agencies.

In addition, AMI systems will need to be defended against more traditional cyber threats such as mobile/malicious code and denial-of-service attacks, misuse and malicious insider threats, accidental faults introduced by human error, and the problems associated with software and hardware aging [14].

IV. Demand Side Energy Management

An example of a recent advance in demand side energy management is the development and deployment of "smart" power cables produced by Packet Power [15]. The smart power cables allow users to digitally record electrical energy consumption and other desired energy use information wirelessly to an Internet database. Online software then utilizes the data to generate energy management reports for the user according to his or her specifications.

Sample results are shown in Fig. 3 and Fig. 4. Fig. 3 depicts the electrical energy consumption for several rooms of a small two-bedroom apartment over a 24-hour period. The energy consumption for each of the rooms along with the cumulative consumption of the entire apartment is shown. Fig. 4 provides the corresponding average temperature at each of the measurement cables used to record the data, which were located throughout the apartment.

V. Demand Response Analysis

To investigate the effects of advanced demand response capabilities, a simulation was performed in MATLAB using the IEEE 123 node test feeder.

A. Test Case

A one-line diagram of the IEEE 123 node test feeder is shown in Fig. 5. The feeder is of modest complexity with 4 substations and 12 switches. Key system characteristics are listed in Table I. Data for the IEEE 123 node test feeder and other test feeder cases are available from [16]. It was assumed that all elements were balanced in both impedances and loadings, which has traditionally been chosen as the best compromise between available resources and required results for such an analysis [17].

B. Customer Load Model

Each customer was modeled to have the load demand curve shown in Fig. 6, which is divided into three levels. The lowest level represents load that a customer absolutely requires in order to maintain basic living functions such as running water, a working septic system, and minimal lighting. It is assumed that this type of load comprises one-tenth of a customer's total electricity demand, and it is served regardless of electricity price.

The next level represents nondiscretionary load. It includes load that is necessary for a customer to maintain his or her basic quality of life, but it can be done without for short periods or in the event of an emergency. Examples of this type of load include water heaters, refrigerators, and basic electronics such as a TV, radio, or computer. It is assumed that this type of load comprises four-tenths of a customer's electricity demand, and it is served as long as the electricity price is below some upper price limit, which is the same for all customers.

The last level represents discretionary or supplemental types of load that can be scheduled in advance or are unnecessary to maintain one's basic quality of life. Examples of this type of load include washers, dryers, dishwashers, and air conditioning. This type of load is assumed to comprise one-half of a customer's electricity demand and it is only served if the electricity price is below one's willingness to pay (WTP). The WTP for each customer was randomly generated

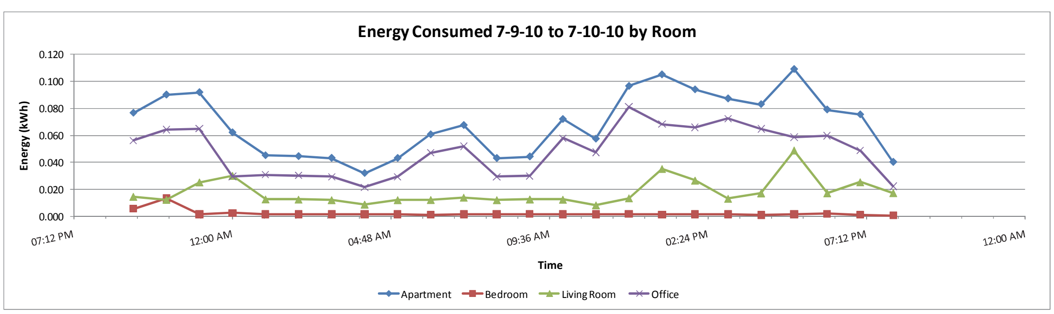

Fig. 3. Energy consumption over a 24-hour period.

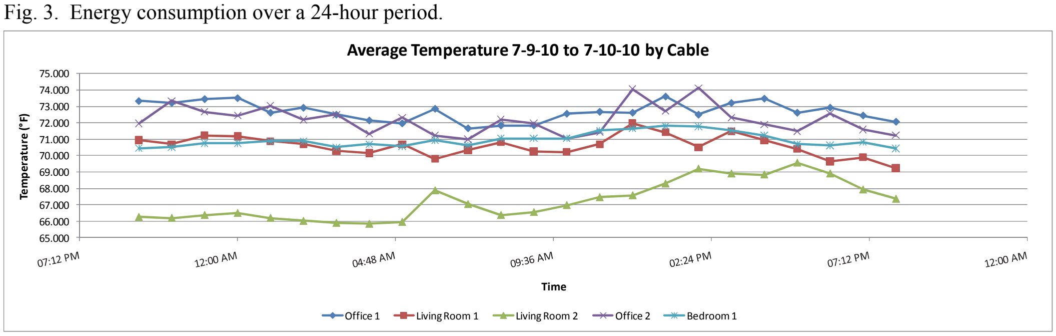

Fig. 4. Average temperature for each cable over a 24-hour period.

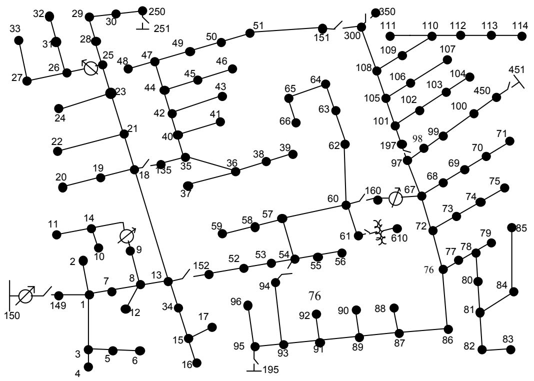

Fig. 5. IEEE 123 node test feeder one-line diagram [16].

TABLE I
IEEE 123 NODE TEST FEEDER KEY SYSTEM CHARACTERISTICS

	Value
Substations	4
Switches	12
Lines	118
Load (kW)	761.25
Base Voltage (kV)	4.16
Base Complex Power (MVA)	10

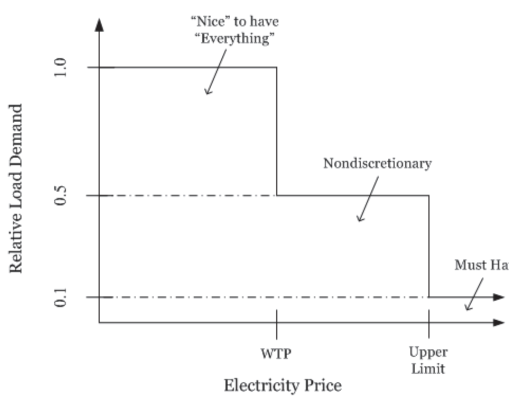

Fig. 6. Customer load demand curve.

from a uniform probability distribution in the range [0,100] $/MWh.

C. Smart Meter Capabilities

Each smart meter is designed with demand response capabilities to shift discretionary and supplemental load from periods when the electricity price is above its owner's WTP or is unavailable to periods when the electricity price is below its owner's WTP and service is available. During each period, the amount of discretionary load not served due to disturbances or price is calculated and then shifted to the next available period that meets its WTP.

Furthermore, several protective measures are built into each smart meter to combat key threats to the power grid as described in [18]. To prevent abnormal loads from overburdening the system, each smart meter caps its owner's load demand during each hour to three times its average peak load based on past data. If an owner's initial load demand for one hour is below this limit, then additional load may be shifted to that hour until the limit is reached, as long as the electricity price is below his or her WTP.

To prevent brownouts from occurring, each smart meter is programmed to serve only necessary or "Must Have" load as shown in Fig. 6 when the price of electricity rises above some predefined upper limit set by the local electric utility. These functions help prevent adversaries from compromising the system and ultimately undermining consumer confidence.

D. Simulations

A simulation was performed for a length of 1,368 hours. The electricity price and load demand curve data were obtained from the Midwest Independent Transmission System Operator (MISO) [19]. The electricity prices used were the real-time market clearing prices (MCPs) for each hour during the period from July 6, 2009 - August 31, 2009, and ranged from 1.79 $/MWh to 78.85 $/MWh. An electricity price of 100 $/MWh was set as the upper price limit as shown in Fig. 6. The load demand curve for each customer was generated using the MISO actual load curve from July 6, 2009 - August 31, 2009 scaled to the value of each customer's peak load. The smart meters were enabled to shift discretionary or supplemental load as described above, and also to serve all discretionary load in the first available period regardless of price, as is the case in conventional distribution system operations.

E. Results

A plot of the load served with advanced demand response capabilities enabled, without demand response capabilities enabled, the initial load demand curve, and the real-time MCPs is shown in Fig. 7. Furthermore, Table II shows a comparison of the average cost of the discretionary load served with and without demand response capabilities enabled.

TABLE II
DISCRETIONARY LOAD COST COMPARISON
(W/DR-WITH DEMAND RESPONSE, W/O DR-WITHOUT DEMAND RESPONSE)

	w/DR	$w/o\ DR$
Average Discretionary Load Cost ($\$/MWh$)	10.56	11.40

F. Discussion

The use of demand response was found to appreciably decrease the cost of discretionary load served, but it also introduced significant oscillations into the load demand curve. Moreover, demand response does not flatten the load demand curve as one might expect, since the peaks in the real-time MCPs do not correspond precisely to the peaks in the demand curve. Therefore, the electricity supply for the system must be able to endure these additional oscillations in load when demand response capabilities are enabled.

It must be noted, however, that the real-time electricity prices will be affected if all consumers have demand response capabilities enabled and are able to see real-time prices in order to make decisions about their electricity consumption. Nevertheless, such market restructuring faces numerous technological and regulatory barriers that are not likely to be overcome in the near future. As a result, several utilities are allowing customers to enroll voluntarily in demand response programs, such as Con Edison [20], and

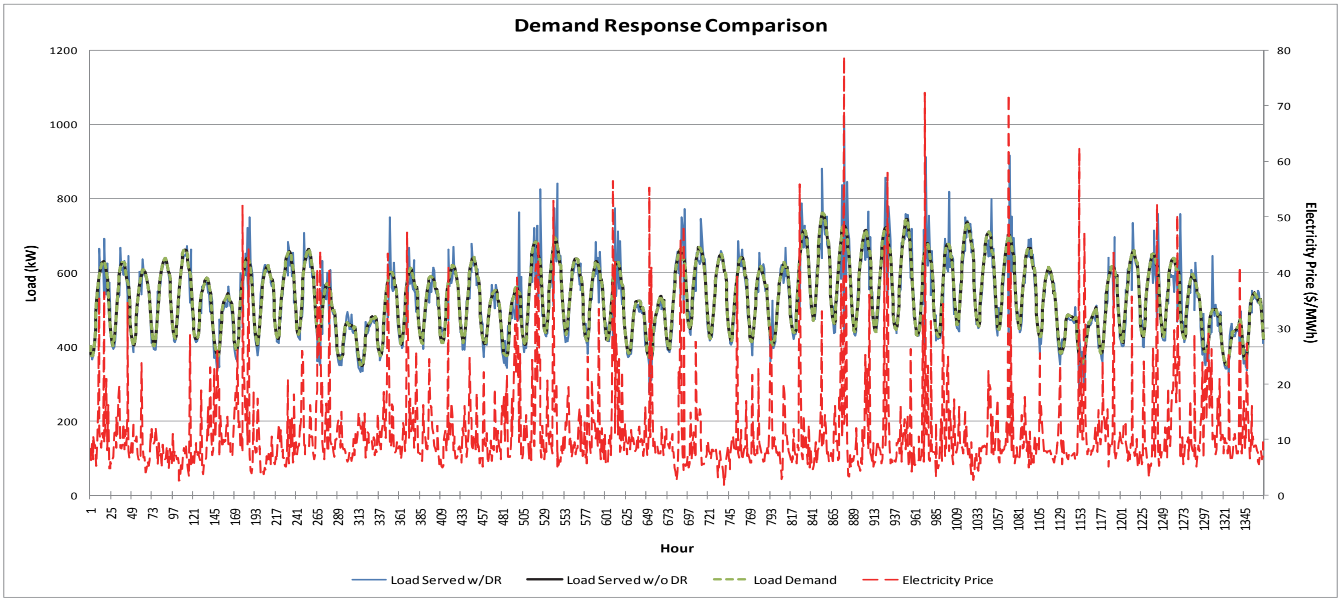

Fig. 7. Demand response comparison (w/DR-with Demand Response, w/o DR-without Demand Response).

Southern California Edison [21], while the vast majority of customers still receive fixed prices.

VI. Conclusion

This paper provides a brief tutorial on power networks from the macro level of interdependent complex infrastructure systems, down to the micro level of smart energy distribution systems. Several challenges associated with the secure and reliable operation of interconnected power, sensing, and communication networks are highlighted. Advances in distributed sensing, modeling, and control at the consumer level, along with a tool for demand side energy management, are also presented. Furthermore, simulation results show the effects of demand response capabilities on power system operations at the distribution level. Much work remains to be done in these highly nonlinear, uncertain, and coupled dynamical systems and related areas.

VII. Acknowledgment

The authors gratefully acknowledge Packet Power for the resources that contributed to Section IV of this work.

References

[1] M. Amin, "Self-healing, resilient, robust and smart infrastructure systems," in *Handbook of Science and Technology for Homeland Security*. New York: Wiley and Sons, Forthcoming in 2010.

[2] A. Phillips, "Staying in shape," *IEEE Power & Energy Magazine*, vol. 8, no. 2, pp. 27-33, March/April 2010.

[3] NIST, "Smart Grid Cyber Security Strategy and Requirements," The Smart Grid Interoperability Panel–Cyber Security Working Group, DRAFT NISTIR 7628, February 2010.

[4] F. C. Schweppe, "Power systems '2000': hierarchical control strategies," *IEEE Spectrum*, pp. 42-47, July 1978.

[5] Electric Power Research Institute, "Complex Interactive Networks/Systems Initiative: Final Summary Report: Overview and Summary Report for Joint EPRI and U.S. Department of Defense University Research Initiative," Washington, DC, 2002.

[6] A. Mannikoff and H. Nilsson, "Sweden-reaching 100 percent 'smart meters' July 1, 2009," in *IEEE Power and Energy Society General Meeting*, Calgary, 2009.

[7] G. Deconinck, "An evaluation of two-way communication means for advanced metering in Flanders (Belgium)," in *IEEE Instrumentation and Measurement Technology Conference Proceedings*, Victoria, 2008, pp. 900-905.

[8] Energy Insights, "2008 National Residential Online Panel Real-Time Pricing (RTP) Survey," IDC, Framingham, 2008.

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

[10] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836-1846, November 2008.

[11] F. Cleveland, "Cyber Security Issues for Advanced Metering Infrastructure," in *IEEE T&D Conference*, April 2008, pp. 1-5.

[12] F. Barringer, "New electricity meters stir fears," *The New York Times*, p. A12, January 30, 2011.

[13] J. Cline, "Opinion: will the smart grid protect consumer privacy?," *Computerworld*, November 2009.

[14] F. T. Sheldon, S. G. Batsell, S. J. Prowell, and M. A. Langston, "Position Statement: Methodology to Support Dependable Survivable Cyber-Secure Infrastructures," in *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 2005, p. 310a.

[15] Packet Power. (2010, September) [Online]. http://www.packetpower.com/index.php

[16] W. H. Kersting, "Radial distribution test feeders," in *IEEE Power Engineering Society Winter Meeting*, Columbus, 2001, pp. 908-912 vol. 2.

[17] H. L. Willis, *Power Distribution Planning Reference Book*. New York: Marcel Dekker, Inc., 1997.

[18] I. Winkler, "Opinion: The hackability of the smart grid," *Computerworld*, December 2009.

[19] Midwest ISO. (2010, May) Midwest ISO - Documents. [Online]. http://www.midwestiso.org/publish

[20] Con Edison. (2010, September) Demand Response/Day-Ahead Hourly Pricing Program. [Online]. http://www.coned.com/energyefficiency/vol_time_pricing.asp

[21] Southern California Edison. (2010, September) Demand Response Program. [Online]. http://www.sce.com/b-rs/demand-response-programs/demand-response-programs.htm