Spring 2013

Enabling sustainable power distribution networks by using smart grid communications

Chun-Hao Lo
New Jersey Institute of Technology

Copyright Warning & Restrictions

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted material.

Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be "used for any purpose other than private study, scholarship, or research." If a, user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of "fair use" that user may be liable for copyright infringement,

This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve violation of copyright law.

Please Note: The author retains the copyright while the New Jersey Institute of Technology reserves the right to distribute this thesis or dissertation

Printing note: If you do not wish to print this page, then select "Pages from: first page # to: last page #" on the print dialog screen

ABSTRACT

ENABLING SUSTAINABLE POWER DISTRIBUTION NETWORKS BY USING SMART GRID COMMUNICATIONS

by
Chun-Hao Lo

Smart grid modernization enables integration of computing, information and communications capabilities into the legacy electric power grid system, especially the low voltage distribution networks where various consumers are located. The evolutionary paradigm has initiated worldwide deployment of an enormous number of smart meters as well as renewable energy sources at end-user levels. The future distribution networks as part of advanced metering infrastructure (AMI) will involve decentralized power control operations under associated smart grid communications networks. This dissertation addresses three potential problems anticipated in the future distribution networks of smart grid: 1) local power congestion due to power surpluses produced by PV solar units in a neighborhood that demands disconnection/reconnection mechanisms to alleviate power overflow, 2) power balance associated with renewable energy utilization as well as data traffic across a multi-layered distribution network that requires decentralized designs to facilitate power control as well as communications, and 3) a breach of data integrity attributed to a typical false data injection attack in a smart metering network that calls for a hybrid intrusion detection system to detect anomalous/malicious activities.

In the first problem, a model for the disconnection process via smart metering communications between smart meters and the utility control center is proposed. By modeling the power surplus congestion issue as a knapsack problem, greedy solutions for

solving such problem are proposed. Simulation results and analysis show that computation time and data traffic under a disconnection stage in the network can be reduced.

In the second problem, autonomous distribution networks are designed that take scalability into account by dividing the legacy distribution network into a set of subnetworks. A power-control method is proposed to tackle the power flow and power balance issues. Meanwhile, an overlay multi-tier communications infrastructure for the underlying power network is proposed to analyze the traffic of data information and control messages required for the associated power flow operations. Simulation results and analysis show that utilization of renewable energy production can be improved, and at the same time data traffic reduction under decentralized operations can be achieved as compared to legacy centralized management.

In the third problem, an attack model is proposed that aims to minimize the number of compromised meters subject to the equality of an aggregated power load in order to bypass detection under the conventionally radial tree-like distribution network. A hybrid anomaly detection framework is developed, which incorporates the proposed grid sensor placement algorithm with the observability attribute. Simulation results and analysis show that the network observability as well as detection accuracy can be improved by utilizing grid-placed sensors.

Conclusively, a number of future works have also been identified to furthering the associated problems and proposed solutions.

ENABLING SUSTAINABLE POWER DISTRIBUTION NETWORKS BY USING SMART GRID COMMUNICATIONS

by
Chun-Hao Lo

A Dissertation
Submitted to the Faculty of
New Jersey Institute of Technology
for the Degree of
Doctor of Philosophy in Electrical Engineering

Department of Electrical and Computer Engineering

May 2013

APPROVAL PAGE

ENABLING SUSTAINABLE POWER DISTRIBUTION NETWORKS BY USING SMART GRID COMMUNICATIONS

Chun-Hao Lo

Dr. Nirwan Ansari, Dissertation Advisor — Date
Professor of Electrical and Computer Engineering, NJIT

Dr. Ali Abdi, Committee Member — Date
Associate Professor of Electrical and Computer Engineering, NJIT

Dr. Sui-Hoi (Edwin) Hou, Committee Member — Date
Associate Professor of Electrical and Computer Engineering, NJIT

Dr. Ali Mili, Committee Member — Date
Professor of Computer Science, NJIT

Dr. Roberto Rojas-Cessa, Committee Member — Date
Associate Professor of Electrical and Computer Engineering, NJIT

BIOGRAPHICAL SKETCH

Author: Chun-Hao Lo

Degree: Doctor of Philosophy

Date: May 2013

Undergraduate and Graduate Education:

- Doctor of Philosophy in Electrical Engineering,
  New Jersey Institute of Technology, Newark, NJ, USA, 2013
- Master of Science in Telecommunications Engineering,
  New Jersey Institute of Technology, Newark, NJ, USA, 2007
- Master of Engineering in Electrical Engineering,
  University of Detroit Mercy, Detroit, MI, USA, 2005
- Bachelor of Science in Electrical and Computer Engineering,
  The Ohio State University, Columbus, OH, USA, 2003

Major: Electrical Engineering

Presentations and Publications:

Chun-Hao Lo and Nirwan Ansari, "CONSUMER: A Novel Hybrid Intrusion Detection System for Distribution Networks in Smart Grid," IEEE Transactions on Emerging Topics in Computing Special Issue on Cyber-Physical Systems, submitted.

Chun-Hao Lo and Nirwan Ansari, "Decentralized Controls and Communications for Autonomous Distribution Networks in Smart Grid," IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 66-77, March 2013.

Chun-Hao Lo and Nirwan Ansari, "Chapter 4: IEEE 802.15.4 Based Wireless Sensor Network Design for Smart Grid Communications," Handbook of Green Information and Communication Systems, M. S. Obaidat, A. Anpalagan and I. Woungang, eds., Academic Press, 2013.

Chun-Hao Lo and Nirwan Ansari, "Alleviating Solar Energy Congestion in the Distribution Grid via Smart Metering Communications," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1607-1620, September 2012.

Chun-Hao Lo and Nirwan Ansari, "The Progressive Smart Grid System from Both Power and Communications Aspects," IEEE Communications Surveys & Tutorials, vol. 14, no. 3, pp. 799-821, Third Quarter 2012.

To my Father, Mother, and my fiancee

"Blessed are those who have not seen and yet have believed." *–John 20:29*

ACKNOWLEDGMENT

This dissertation would not have been possible without the help and support of many people in God's plan. First of all, I would like to express my profound gratitude to my dissertation advisor, Professor Nirwan Ansari, for his professional guidance and endless patience throughout these years. Without his support, this dissertation would never be completed.

Second of all, it is an honor for me to have Professor Abdi, Professor Hou, Professor Mili, Professor Rojas-Cessa as my dissertation committee members. Their valuable time and comments have always been greatly appreciated.

Third, I am most grateful to my beloved family: to my father, mother, and sister for providing me encouragement, mental and spiritual support; to my fiancee (Catharine Yang) for entering my life, making sacrifices, and staying besides me at all times; and to my dogs (Henry and Max) for accompanying me and their unconditional love for many years. This dissertation is dedicated to them.

Last, but not least, I would also like to thank my colleagues and friends who have encouraged and supported me during this long journey including Jingjing Zhang, Nan Wang, Khondaker Salehin, Patchara Sutthiwan, Tao Han, Yan Zhang, Benjamin Huang, Dennis Huang, and many others.

CONTENTS

Contents
(Continued)

Contents
(Continued)

Chapter **Page**

LIST OF TABLES

Table **Page**

LIST OF FIGURES

Figure **Page**

List of Figures
(Continued)

Figure **Page**

CHAPTER 1

INTRODUCTION

Electric power grid is one of the national critical infrastructures provisioned with reliability and security assurance. After the Second Industrial Revolution, most parts of the grid structure and operation have remained unchanged for decades [1, 2, 3]; many electric facilities and equipment in the grid are based on old technologies except a few minor improvements such as upgrades on material types and construction designs used for transformers, transmission lines, electric poles, and insulators [4]. In addition to the fact that utilities have monopolized electricity supplies and markets, several crucial factors have seriously drawn attention to the necessity for consolidation of smart grid paradigms and concepts: the dramatic growth in population, end-user electronic devices, global greenhouse gas emissions, power consumption, and power outages.

The aging infrastructure has also brought up a dilemma for people in the power industry regarding whether or not they should invest on replacing the life-expired fossil fuel or nuclear power plants with renewable energy sources (RESs) such as neighborhood/household-based photovoltaic (PV) solar and wind power systems. The grid system is mostly proprietary and manipulated by a number of regional utility operators in the deregulated electricity market. There is barely (real-time) communications in distribution networks as compared to that in transmission networks that links the entire distribution networks between power supplies and customers' loads operated under a *passive* system [5]. Smart grid development is envisaged to tackle the aforementioned issues by integrating advanced computing, information and communications technologies

(CICTs), as well as distributed RESs into the existing grid, especially into its distribution networks.

1.1 Conventional Electric Power System

An electric power system is fundamentally composed of three operational sectors: Generation, Transmission, and Distribution. *Generation* is a process of producing power at various power plants by employing numerous types of energy resources, e.g., fossil fuels, nuclear, and renewables. *Transmission* involves power delivery by ramping up the power to high-voltage (HV, $>$ 300kV) through step-up transmission transformers for high energy delivery efficiency and ramping down the power to medium-voltage (MV, $>$ 100kV) through step-down transmission transformers before entering distribution networks. *Distribution* delivers the power by further ramping it down to low-voltage (LV, $<$ 100kV) through step-down distribution transformers to various customers at the end-use *consumption* sectors, i.e., residential, commercial, and industrial (RCI) users. Series of the actions are regulated by a set of standards (e.g., IEEE, IEC, DNP, ANSI, CIP) [6, 7, 8] as well as a batch of data collection and system automation [9]. Transmission lines and distribution feeders connecting diverse electrical components and end-use customers throughout the system construct the so-called *power grid*. The four major network components of the power grid are:

- **Power facilities and equipment** mainly comprise power generators, transformers, stations, substations, and control centers in which electrical components[1] are built from multiple vendors.

[1]Examples of electrical components include conductors, protective devices, capacitors, reactors, intelligent electronic devices, programmable logic controllers, and remote terminal units.

- **Control systems** installed in the power grid for wide-area monitoring and control as well as substation and distribution automation, are typically the conventional Supervisory Control And Data Acquisition and Energy Management Systems (SCADA/EMS) as well as the sophisticated synchrophasors Phasor Management Units and Phasor Data Concentrators (PMU/PDC). SCADA typically measures voltage, current, and frequency once every few seconds, whereas PMU/PDC delivers more and complex samples per second; they are medically analogous to the X-ray and MRI, respectively [10, 11].

- **Data flows** in the system carry various power factors and measurements for a number of applications, including substation and feeder monitoring, Volt-VAR (voltage-ampere reactive) control, FDIR (fault detection, isolation and restoration/recovery), transformer and motor temperatures, as well as the status of breakers, relays, and switchgear.

- **Communications protocols** used in data exchange and management among substations, are mostly proprietary and regulated by utilities, municipalities, or regulators. Communications in the HV/MV transmission grid systems currently have been administered under advanced and sophisticated control and monitoring as well as computing tools.

The legacy power grid infrastructure particularly in the United States has mostly been constructed in a *centralized* radial tree-like topology such that a single remote generator supplies power to multiple groups of end users through transmission and distribution lines. The infrastructure is greatly vulnerable to a single-point malfunction (whether due to intentional or unintentional reasons) that can affect multiple served regions through cascading failures, despite it is claimed reliable and controllable [12]. Moreover, the centralized method has limited the improvement of system performance in terms of network availability and operational flexibility [13]. The communications network topology is organized in a master-slaves architecture, and communications technologies used by utility companies vary from dedicated/private radio frequency (RF), fiber optics, twisted-pair telephone line, powerline, to satellite. However, most of utilities' operation systems are proprietary and operate under their own wide area networks (WANs). The

majority of communications are taken place in transmission networks among SCADA/EMS and PMU/PDC systems, whereas almost the entire distribution network is passive (that has little interaction between power system and loads) with limited communications and local controls, and provides no real-time monitoring of voltage and current [5]. Power distribution and management in distribution networks are mostly controlled by mechanical-electrical mechanisms and devices locally that are not optimized globally.

The current grid is considered energy inefficient from many aspects, and constrained by its centralized architecture as well as a lack of communications and controls in distribution and consumption sectors. According to the U.S. Energy Information Administration (EIA) Annual Energy Review 2009 [14], the efficiency of the current power grid is as low as approximately 30% because of the loss in energy conversion at power plants and the loss in transmission and distribution. The grid also suffers from sudden spikes in power demand that can cause power congestion and low power quality in consequence of brownouts or blackouts and equipment damages. The contemporary sophisticated methods using protection systems and demand prediction tools mostly relied on historical data are inefficient and expensive. Without penetrating distribution and consumption levels of the grid extensively, balancing power supply and demand will become more challenging in the near future.

1.2 Future Communications-Power Networked System: Smart Grid

Incorporating CICTs intelligence and distributed RESs into the distribution networks is envisioned to modernize the conventional power grid system. While there does not exist a perfect system in the world, smart grid development aims to moderate the effects of catastrophes (e.g., natural disasters, human errors, intentional attacks), and at the same time

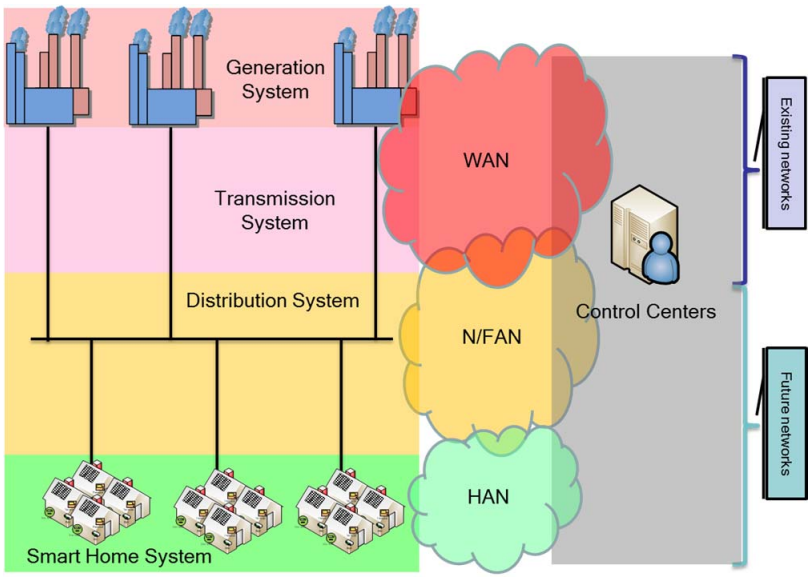


Figure 1.1 The next-generation distribution system: power grid towards smart grid.

to shorten the duration of recovery. *Smart grid* is designed to accommodate two-way data communications and power flows in real time and acquire attributes of self-coordination, -awareness, -healing, and -reconfiguration. Implementing smart control devices (sensors and actuators) throughout the distribution sector and smart meters in the consumption sector is foreseen to enhance operation efficiencies in *remote meter reading* for customer energy use, *bidirectional power delivery* for optimal power flow control, and *Volt-VAR regulation* for reliable power quality locally and globally. Figure 1.1 illustrates the layered power system network which is currently deployed or planned to be deployed in the near future. As mentioned earlier, most works have focused on the generation and transmission levels and only little effort has been made at the distribution and consumption levels. Future networks in smart grid comprise Field Area Networks (FANs), Neighborhood Area Networks (NANs), and Home Area Networks (HANs) that leave plenty of room for further investigation and exploration of the next generation electric power system. On top of the system, the smart grid communications infrastructure is layered into four essential

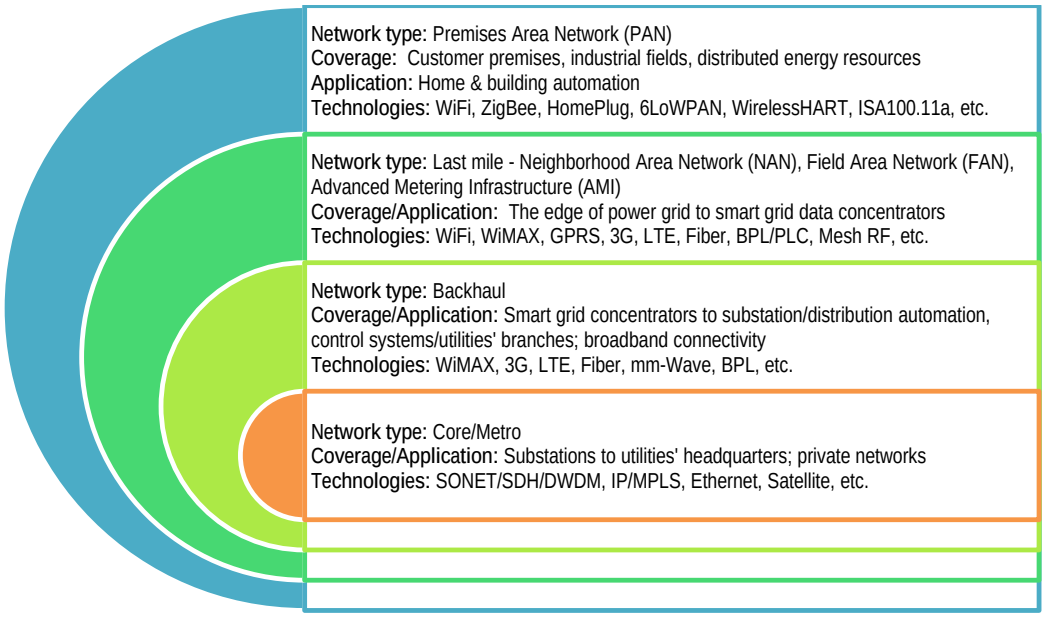


Figure 1.2 Smart grid communications networking layers.

networking sectors: *core* (or backbone, metro), *middle-mile* (or backhaul), *last-mile* (or access, distribution), and *premises*, as shown in Figure 1.2:

- The **core** sector operated under WAN supports the connection between numerous substations and utilities' headquarters. This layer requires high capacity and bandwidth availability to handle mountains of data transported from other sectors as well as multiple agents. The backbone network is usually built on fiber optics.

- The **middle-mile** sector operated under the head of Advanced Metering Infrastructure[2] (AMI) connects the data concentrators or aggregators with utility control centers. This layer not only needs to provide broadband media for substation and distribution automation, but the associated network installation needs to be as easy and cost-effective as possible. In addition, routes and links through which data flow in this portion ought to be flexible and uninterrupted. The overall performance should also be highly predictable for reliable data transport before entering the core.

- The **last-mile** sector mostly covers the areas of FAN and NAN in part of AMI. This layer is responsible for data transport and collection from smart meters to concentrators. There are a variety of wireline and wireless technologies available that

[2]AMI is a system between customers and utility operators in electricity and gas/water markets that enables real-time data measurement as well as frequent data collection and transmission to the utility operators and various parties.

can be implemented in this sector. Tailored technologies must provision broadband speed and security.

- The **premises** sector includes HANs, Building Area Networks (BANs), and Industrial Area Networks (IANs). Communications technologies supporting home and building automation in RCI sectors will be predominantly based on the IEEE 802.15.4, IEEE 802.11, and Power Line Communications (PLC) standards. Home energy management operated in HANs will regulate numerous components, such as thermostat, HVAC (heating, ventilation, and air conditioning), smart appliances, lighting control, electric vehicle (EV), and RESs. Data measurement, collection, and transport of this network have to be stabilized, accurate, secured, and privacy-cared.

The four networking sectors interconnected with one another fundamentally assemble the communications infrastructure for the overall smart grid. They are implemented with CICTs to facilitate power grid operation and management along with smart grid technologies and applications, ranging from *wide area monitoring* that manages the unprecedented number of distributed RESs and customer loads, *demand response* that enables customer participation in adjusting consumption as well as becoming prosumers[3], *RESs integration* that produces renewable energy and reverse power flows back to the grid, to *EVs plug-and-play* that charges and discharges power from and to the grid in systematic arrangements. Table 1.1 presents various technologies for the smart grid communications that will ultimately be adopted depending upon the associated network characteristics. For example, small utilities may take the advantages of using the existing cellular networks and collaborate with others to reduce capital and operating costs. On the contrary, large utilities would be more capable of building their own networks to avoid bandwidth sharing in order to earn more profits on the capital investment. Additionally, the geographical requirements, task objectives, as well as applications and services to consumers will also affect the choices of technologies deployment of the smart grid communications.

[3]Customers are not only the electricity buyers , but also the electricity sellers capable of contributing power surplus back to the grid if they have installed RESs on their premises.

Table 1.1 Potential Technologies Supporting the Smart Grid Communications

	Communications	Purposes & Description	Merits	Weaknesses & Challenges
Wireless Technologies	Cellular (GPRS/3G/4G) and LTE	Voice-initiated; Remote monitoring and control (e.g., SCADA) for substations and distributed energy sources; Simple text messaging support	Low implementation, operational, and maintenance costs using existing network infrastructures; Larger coverage; Better roaming and mobility support	Need for towers/base stations; Uneconomical call establishment on large scales; Unavailable coverage for some remote sites; Security-vulnerable
	WiFi (IEEE 802.11)	Data (and video)-initiated; Home energy interface; Connection among PCs, laptops, PDAs, and customer electronics, as well as smart metering solutions	Rapid installation; High flexibility; Solutions for aggregation points in urban areas	High interference-sensitivity; Small coverage; Power-hungry; Uneconomical on small scales; Security-vulnerable
	WiMAX (IEEE 802.16)	Last-mile wireless broadband access alternative to Cable and DSL; Smart metering network in AMI	Fast deployment when compared to wired solutions; Long-range; High speed for real-time applications and fast response	Need for towers/base stations; Low penetration while operating in very high frequency bands; High power consumption; Security-vulnerable
Wireline Technologies	SONET/SDH and E/GPON	Fiber optics-based; Broadband solutions for core, metro, and access networks	High bandwidth and large capacity support; Fast transmission; Negligible interference	Slow deployment and high cost installation if no existing infrastructure available especially in rural areas
	PLC (NB and BB) and BPL	Power-initiated; Particular communication channels in MV and LV fields; BPL broadband access alternative to Cable and DSL	Complementing cable and wireless solutions; Easy installation for indoors; Higher flexibility and mobility for end devices; Solutions for rural areas	Complex implementation for larger buildings; Phase switch challenge from indoor to outdoor and vice versa; Signal attenuation and high cost for repeaters deployment in localized areas; High interference over power lines
Network Types	WMN	Mesh network supported in communities and neighborhoods; Super mesh routers managing diverse applications	Easy and cost-effective installation; High reliability and flexibility; Self-configuration and healing	High complexity in data management; Low controllability in unlicensed spectrums; Lack of standards; Overheads
	WSN and WPAN (IEEE 802.15.4)	Small measures; Home, office, and smart appliance (energy) automation; Sensing, monitoring, control in fields of substations, industrial facilities, and distributed generation	Easy and rapid deployment; Low cost; High portability; Easy configuration	Power and memory constrained; Low data rate; Higher data loss; Very low coverage
Proprietary	Dedicated or Private	Pre-assigned and possession of mixed telecommunications technologies; Licensed spectrums	Less security-vulnerable; No sharing in bandwidth as well as profits on capitals; Higher independence	Lower flexibility and manageability; Very high installation cost

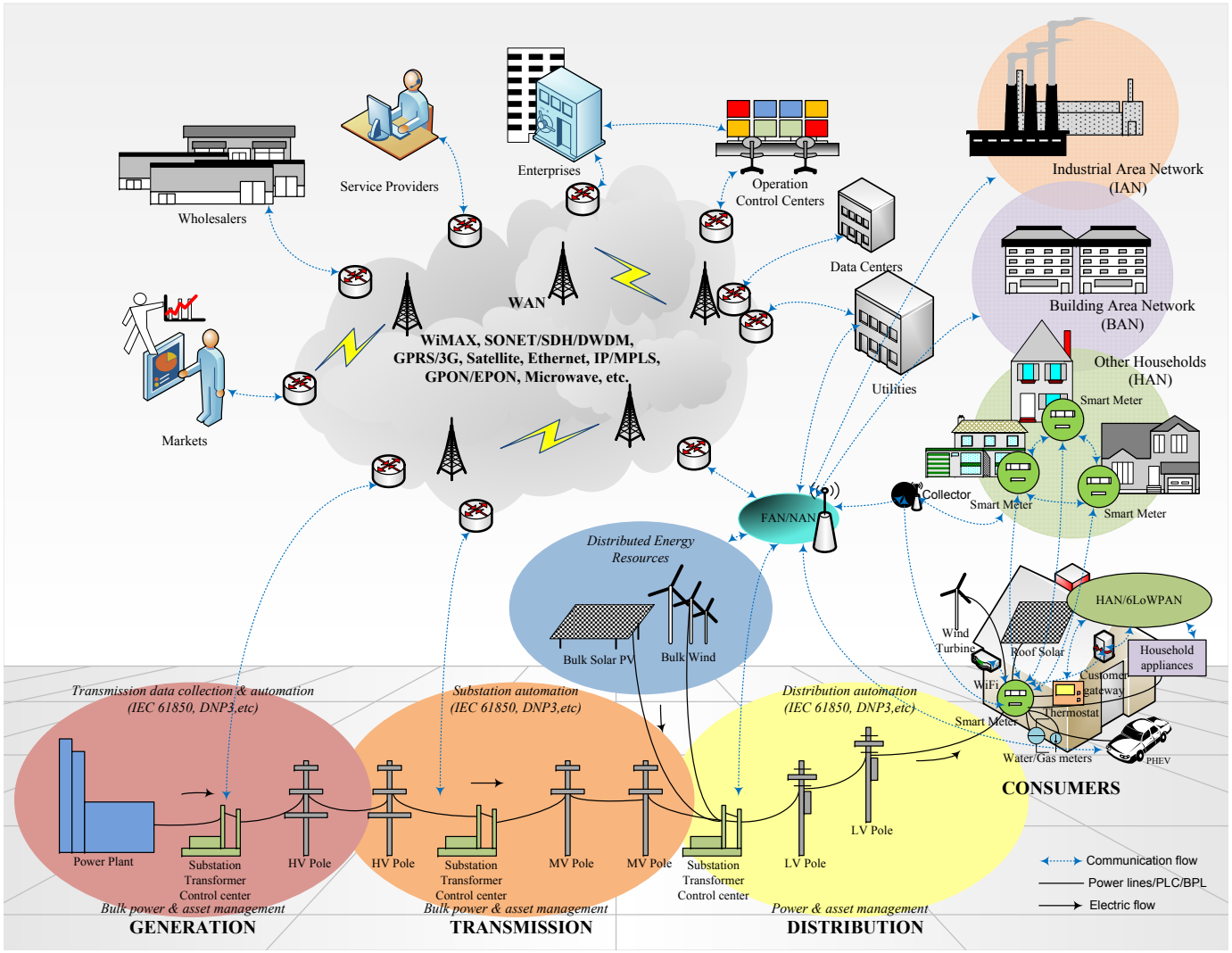


Figure 1.3 Smart grid ecosystem.

Figure 1.3 illustrates the entire smart grid overview in which a number of anticipated future networks deployed in the distribution and consumption sectors are going to evolve gradually from now. It is envisioned that enormous amounts of measurement data, control messages, and price signals will be required to run these emerging applications. Different applications may have different QoS (quality of service) and delay requirements. Notably, the sizes of mice data conveyed in smart grid are approximately tens of bytes for protection, control, monitoring applications and tens to hundreds of bytes for metering/billing, EV applications [15, 16]; the response time is in the order of a few seconds for the former applications and minutes or hours for the latter applications. For such reasons, efficient and effective communications and computation designs for associated power management are considerably desired.

1.3 Similarities between Power Network and Communications Network

Interestingly, the functionality of power systems has similar characteristics found in the Internet [17], in terms of network and operation designs. Essentially, both systems aim to deliver network resources from source to destination through optimized routes by using strategic algorithms while avoiding any congested and/or broken links. The similarities include

- **Network nodes**: power plants and energy storage, control centers, substations and transformers, circuit breakers and switches, and consumers ***versus*** content sources and data storage, service providers, terminals, edge/intermediate routers and switches, and subscribers.

- **Network links**: Power transmission cables and distribution feeders ***versus*** communications wireline cables and wireless links.

- **Network topologies**: Centralized infrastructure in power networks (designed to be *decentralized* in smart grid) ***versus*** hybrid infrastructures and ad-hoc mesh in communications networks.

- **Network electron resources**: Electricity ***versus*** analog and digital data.

- **Network transfer capabilities**: Power transmission capacity ***versus*** communications channel bandwidth.

- **Network operations**: Power ***versus*** data traffic load balancing via routing and switching across both networks.

Managing power delivery in the power network system is similar to organizing data packets transmission in communications network system, and yet they should be addressed and designed simultaneously because both real-time operations can be the cause and effect to one another. For example, implementing hundreds of thousands of smart meters in the consumption sector requires a scalable framework to instantly coordinate power circuitry control and data traffic. On the one hand, data packets delayed or dropped during transmission may incur increased electricity costs, energy inefficiency, or service interruption for the power system. On the other hand, if packet generation at smart meters is initiated by an event (e.g., a change in power flow direction) that is required to notify utility operators, the increasing traffic loads in communications networks may become more challenging to handle, and eventually deteriorate the network performance for both power and communications systems.

Data communications in smart grid plays a dominant role for the power system to function consistently while the efficiency of power transmission is also substantially dependent upon the advanced electric power facilities and technologies tailored for the grid system. Moreover, the performance of data transmission further relies upon how well the heterogeneous communications networks across smart grid are interconnected

and integrated. Conclusively, understanding power operations and features prior to the design of associated communications network operations is the key to build a completely integrated communications-power networked system for smart grid. This dissertation has been motivated to explore the frontiers of communications-power system integration, in which power surplus congestion, network scalability, and cyber-physical security are the three primarily foreseeable problems to be studied for the future power distribution system. For the first two problems, power control mechanisms and associated communications networking designs are developed to resolve the power issues, and at the same time to mitigate the corresponding heavy data traffic loads required for the resolution. For the third problem, a hybrid intrusion detection framework that incorporates grid sensor placement is proposed to effectively enhance fault detection of anomalous and malicious activities under a circumstance where some smart meters are compromised or smart metering communications is breached.

1.4 Outlines for the Remaining Chapters

The remaining chapters are outlined as follows:

Chapter 2 presents necessary *backgrounds* and *related works* for the three addressed problems as well as the existing proposed solutions, respectively.

Chapter 3 addresses the issue of *local power congestion* due to power surpluses produced by household-based PV solar units in a neighborhood. The problem is formulated as a knapsack problem to disconnect some PV solar units from the grid in order to alleviate congestion. Heuristic selection algorithms for candidate disconnection are proposed based on greedy methods. A framework of smart metering communications using wireless

technologies in NAN and a mechanism for exchanging measurement data and control messages are proposed to reduce traffic loads during the disconnection periods.

Chapter 4 further addresses the issue of *bidirectional power flow* where some households consume grid power while others supply power surpluses produced by household-based PV solar units in a distribution network. The problem is formulated as a power balance problem in which power balance may not be achieved within a micro grid itself, and therefore power sharing (or redispatching) from neighboring micro grids is initiated prior to requesting power from the macro grid, i.e., the HV transmission grid. The scalable Control Of Power flow dirEction (COPE) and Power Control and Communications (PCC) algorithms with Overlay multi-tier Communications Network Infrastructure (OCNI) are proposed to facilitate power flow management in the underlying Autonomous Distribution Networks (ADNs) as well as to reduce the amount of traffic loads throughout the OCNI.

Chapter 5 addresses the issue of *energy theft* initiated by one illegal customer launching a typical false data injection attack in a distribution network. The problem is formulated as a COmbiNation SUM of Energy pRofiles (CONSUMER) attack problem that compromises a number of smart meters in a coordinated manner such that lower power consumption is metered for the attacker and higher consumption for its neighbors. A hybrid intrusion detection framework which incorporates POwer Information and SEnsor placement (POISE) with the Grid-Placed Sensor (GPS) algorithm is proposed to provide network observability throughout the distribution network while being able to validate the correctness of customers energy usage by detecting anomalous and malicious activities at the consumption level.

Chapter 6 presents the conclusions and discusses the future work.

CHAPTER 2

BACKGROUNDS AND RELATED WORKS

The power grid system essentially entails Volt-VAR control, power flow management, and fault detection and isolation. In the past years, most of research works related to grid reliability have only focused on 1) *current carrying* from power generation, transmission, to distribution lines consisting of a number of transformers, buses, and circuit breakers, and 2) *protection system* interacting with the current carrying methods that can be affected by the performance of protective relays, reclosers, and the associated hardware [18]. As the smart grid vision has emerged recently, there have been limited research works on modeling telecommunications and distributed computing for the next generation grid operation. Imperatively, the cyber-physical system requires preliminary investigations into communications network modeling as well as system vulnerability analysis [19, 20, 21, 22] in order to cope with unprecedented design challenges in terms of future power network characteristics, communications network characteristics, and cyber-physical security threats, under the ongoing smart grid development.

2.1 Power Network Congestion

The centralized and radial tree-like power grid suffers from peak demands and corresponding power congestion. In order to alleviate *traditional power congestion* occurred in the MV and LV distribution networks, distributed energy resource (DER) units are anticipated to be located near customers' sites to provide local power supplies effectively to serve local loads. Such transformation results in the construction of multiple

micro grids (MGs) in the distribution system consisting of interconnected loads, RESs, and energy storage. The MG can be considered as a manageable generating-source or consuming-source region/entity depending on the status of power generation and consumption in its local area at certain time periods. The MG is operated in two modes: grid-connected mode and islanded mode [23, 24]. In the grid-connected mode, customers may be supplied by power from both the macro (main) grid and MG. When an incident (e.g., voltage drop, faults) is detected in the macro grid, MGs may automatically switch to the islanded mode until the incident is resolved. Most research works have devoted to the islanded operation and the transition between islanded and grid-connected modes [25].

The proliferation of distributed generation deployed in MG and neighborhoods will further increase the penetration of DER units and local generation capacity. Installing solar panels on rooftops of houses and buildings has dramatically increased recently in various countries. Customers may use solar energy they produce from the solar units to operate their household appliances and personal electronics. Any extra energy that is unused will flow back to the utility grid for credits on their bills, i.e., in the case of a grid-tie system. Note that *local power congestion* can potentially occur in the distribution grid once local distributed generation becomes more prevalent in the future [26]; too much solar power or surge in solar power may incur local congestion and deterioration in power grids during the low-consumption and high-production periods. Therefore, bidirectional power flow in grid distribution has to be managed and monitored via smart metering communications in the distribution network system.

Congestion management methods are required for deregulated electricity markets to resolve power congestion that occurs when there is not enough transmission capacity to support all demands for deliveries (transactions) that cannot be physically implemented

as requested [27, 28]. Congestion management employed in the power system has been developed based on a number of methods, including spot pricing theory, optimization model, and variants of optimal power flow techniques [29, 28, 30]. While utilities tackle the congestion problem using their own rules and bidding strategies, all of them aim to maximize their profits (minimize overall cost) by using tools such as *unit commitment* (UC) and *economic dispatch* (ED) in the competitive electric industry [31], where UC refers to scheduling generation units to match the forecast load and ED is adopted to meet the unexpected risen loads [32]. Essentially, *cost-free* methods[1] are firstly applied when congestion is revealed in the interconnected network. If congestion cannot be relieved, *not-cost-free* methods[2] are required to tackle the remaining unresolved issues [28, 29]. In either case, congestion management in power flow analysis is affected by both technical (security and stability) and economic (wholesale market price) aspects, which are usually contradictory.

Traditional congestion management and control is considered *passive* since most methods focus on redispatching/rescheduling generation from the supply side. Congestion management is claimed be more effective if demand control can be combined with supply management [33, 28, 30]. In an analogy between supply and demand in power and communications networks, congestion control usually managed at the transport layer of the OSI model (e.g., TCP) in communications networks is effectively employed to reduce senders' transmitting rates when the network is congested. Hence, instead of meeting user

[1]Cost-free methods include outing congested lines and utilizing the flexible AC transmission system (FACTS) to manage the power flow. They are called cost-free because their marginal costs are nominal.

[2]Not-cost-free methods include rescheduling and redispatching power generation in such a way that the power flow in transmission lines is more balanced throughout the network. This approach is more expensive because some generators may need to reduce their power generation while some are required to increase their output.

demands when a system can barely sustain, curtailing loads sometimes can dramatically improve system performance especially when a considerable amount of power or data are destined for the same destination. In fact, various demand response designs in smart grid projects are being deployed in the end-use sector including residential and commercial buildings [13, 21, 34].

An increasing number of research papers have focused on the implementation of energy management and scheduling techniques in houses and buildings [35, 36, 37, 38]. Shifting some major tasks of household appliances to off-peak periods and managing DER use efficiently during peak hours can achieve reduction in both energy cost and peak load. Erol-Kantarci and Mouftah [35] proposed a wireless sensor HAN based on IEEE 802.15.4 to manage the time use of household appliances depending on the availability of its local energy. A simple communications protocol with an energy management unit (EMU) deployed in houses was developed. Prior to energy use by consumers, communications between the EMU and appliances as well as between the EMU and energy storage are established. Energy is granted if energy in storage is available. Consumers have the option whether to consume the grid power or not when energy in storage is insufficient. Mohsenian-Rad *et al.* [36] proposed a strategy that enables communications among households as a group demand-side management to minimize both energy cost and demand peak-to-average ratio. Local optimization using game theory to curb aggressive consumers is achieved. Similarly, Ibars *et al.* [39] identified a congestion game in demand and generation management as one of potential games in game theory. A load balancing mechanism was proposed to avoid power overload and outage by minimizing the cost (which is a function of the congestion level) on the flow along the transmission lines between a single generation and multiple consumers. Molderink *et al.* [37] proposed

the three-step methodology (prediction, planning, and real-time control) to optimize the utilization of the grid power in a neighborhood by exchanging energy profiles among houses. Energy profiles are generated from local controllers installed in houses and aggregated for delivery to the global controller to make a global decision. Pedrasa *et al.* [38] proposed to maximize the profit of DER operation by scheduling DER in cooperation by using particle swarm theory. Notably, congestion is also foreseen in plug-in hybrid EV charging if the charging management is not handled properly in the distribution grid. One way to mitigate the problem is using queuing theory [40] to reduce the probability of overload by balancing the charging loads over time.

2.2 Power Two-way Directional Flow

Smart distribution introduces the concept of active/autonomous distribution networks (ADNs) in cooperation with distributed grid intelligence [41], multi-agent systems [42, 43, 44, 45], and active network management [46, 47]. ADNs are composed of multiple MGs, smart inverters, and intelligent distribution transformers that perform system (re)configuration management, power management, and fault detection management. Local controls for these key components can be achieved through fast control and communications, and need to be coordinated with the overall system controls. From the power network perspective, the primary issue for the power distribution operation with high penetration levels of DER units is Volt-VAR control as well as power flow management [48, 49, 44, 50, 51, 52, 53, 54]. In Volt-VAR control, for example, the variability of outputs of PV power generation subject to cloud transients would incur voltage harmonics and fluctuations, which could be detrimental to the distribution system. Smart inverters with PV and distributed storage systems can possibly control the voltage on the distribution

system by providing power when the voltage is low and by absorbing power when the voltage is high [55]. In power flow management, surpluses of power produced by DERs can be shared among the households as well as delivered to the neighboring distribution networks; this provision requires bidirectional power flows. Note that the reverse power flow from the distribution network back to the transmission network is prohibited in some countries, e.g., Japan [51].

While customers' houses and line feeders with electric poles will be implemented with smart meters and smart actuators/sensors, respectively, the distribution system can be seen as a large version of wireless sensor networks (WSNs) in which the nodes are strategically and statically deployed. Smart sensors can integrate communications with control functions in order to optimize system performance. From the communications network design standpoint, the centralized schemes (i.e., master-slaves relationship) applied in the legacy power system will become impractical once the size of distribution networks grows to a certain extent. Scalability has been extensively studied in wireless ad hoc and sensor networks [56] as well as addressed in the context of smart grid applications [57, 58]. Clustering is one primary technique that is adopted in WSN by breaking its network into multiple subnetworks to improve network performance and energy efficiency. Similar strategies such as partitioning [59, 60] and multilevel partitioning [61] tactics may also be applied to the distribution network and its overlay communications network in order to perform load balancing as well as to reduce power and communications costs in a decentralized and distributed manner. The costs for the power system may refer to power disturbance, power congestion, and power loss, whereas the costs for the communications system may indicate control overheads, signal interference, and data packet loss. In comparison with the conventional methods, several studies [62, 60, 63] have shown that

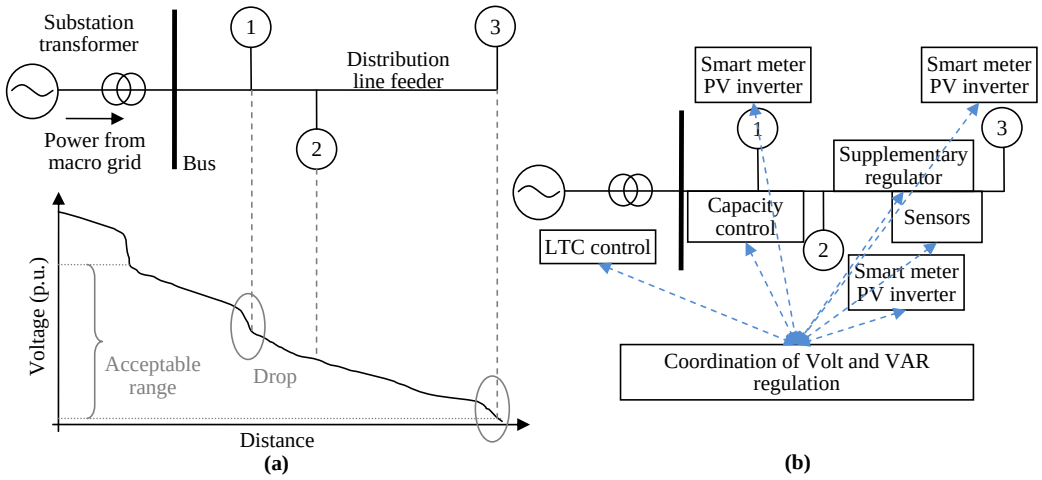


Figure 2.1 (a) Voltage profile for a typical distribution feeder, and (b) coordination via communications and control in the distribution network.

distributed control and management is a preferable approach to the designs of both power and communications networks for the future smart grid.

Electric power grid exhibits the characteristics of a small-world network [64]; however, Wang *et al.* [65] discovered that its grid topology is in fact very sparsely connected with a very low average nodal degree (2-5), and Hines *et al.* [66] indicated that electrical and physical distances can be influential factors which have not been extensively studied in the context of structural network analysis, e.g., voltage drop [50, 67]. As an example shown in Figure 2.1a, HV power is generated from the macro grid and ramped down to LV power to serve loads of customer 1, 2, and 3 in the distribution network. Voltage is decreased along the feeder as the distance increases. Voltage drop is discovered explicitly for customer 1 and 3 due to the increased current flow on the feeder while customers' power consumption (or loads) increase. The consequence causes decreased voltage for customers approaching the end of the feeder from the substation; nevertheless, voltage has to be maintained within an acceptable range (e.g., 120V$\pm$5%) along the feeder by utilizing capacitor banks. The control of voltage and active/reactive

power becomes more challenging for the operation of power distribution systems when the penetration level of DER units rises, with inclusion of plug-in EVs [54]. Volt-VAR control involves voltage regulating devices such as load tap changer (LTC) at the substation transformer, distribution sensors/supplementary regulators and capacitor banks along the feeder (on or close to electric poles), and smart meters with PV inverters at houses from which voltage information is collected in real time. Coordination by means of integrated control and communications along with the distribution equipment controllers can efficiently regulate voltage, reduce losses, conserve energy, and optimize utilization of system resources. Reference [67] introduces the smart distribution integrated Volt-VAR control and optimization as shown in Figure 2.1b.

The direction and amount of power flow in distribution networks require flexible and dynamic control operation [68]. The existing distribution networks were not designed to operate with bidirectional power flow; nonetheless, introducing appropriately specific loops techniques and developing a hybrid structure to enable meshed operation in the legacy radial system with intelligent circuit breakers and switches are potential approaches to provision the two-way power system in the future [69]. Nguyen *et al.* [45] proposed a distributed optimal routing algorithm with a power router interface to manage the power flow in the ADN. Moreover, the so-called contactless and bidirectional power transfer system compensated by an inductor-capacitor-inductor circuit has been proposed in [70, 71] and claimed to be a viable solution for smart grid applications, e.g., DERs, EVs.

Numerous literatures have been proposed to integrate CICTs into the current power systems [51, 47, 72, 73, 74, 44, 45, 48, 43, 53, 49, 75, 72, 76, 77, 78], including consideration of secure communications [79]. Particularly, Yang *et al.* [47] proposed communications infrastructures for MV and LV distribution networks. By using

microwave/T1 for MV network and satellite/T1 for LV network, the authors showed that these technologies can coexist and meet the delay requirement for data delivery. Majumder *et al.* [53] also designed communications systems using WSN to manage power flow within MGs and adopting wired network to support data exchange among MGs or communities. The low-cost and low-bandwidth WSN was proved to be sufficient to deliver local data measurements, and at the same time was able to improve the system reliability and operation accuracy. Furthermore, Erol-Kantarci *et al.* [73] considered multiple MGs throughout the distribution network where each MG can represent residential, commercial, and campus entities. Multiple MGs are grouped together as long as their outputs are balanced, i.e., power surplus is equal to consumption. In order to achieve survivability, the method is to form a ring topology (i.e., at least three MGs must be grouped) so that they can support each other. Because of varying power usage and production in geographical regions, group formation changes during different time periods. Meanwhile, partitioning MGs of distribution networks based on coalition game theory was introduced in [74]. Coalitions of MGs are formed according to the coalition formation algorithm incorporated with merge-split rules in which the tradeoff (i.e., power loss) value is determined for each MG whether to merge with other coalitions (or split from its coalition), until the network converges to a number of disjoint coalitions where there is no more incentive to further merge or split.

2.3 Energy Theft and False Data Injection Attack

During the evolutional movement in smart grid development, the conventional critical infrastructure is gradually exposed to the public such that part of the systems especially the distribution networks involving smart metering communications along with controls of

distributed generation and demand responses at consumption sites will potentially pose a number of security risks. Recently, several surveys and tutorials have elaborately addressed a number of security issues in terms of confidentiality, integrity, and availability (CIA), from passive attacks to active attacks [80, 81, 82, 83, 84, 85, 86, 87, 88, 89], such as eavesdropping, jamming, tampering, spoofing, altering, and other attacks against the protocol stacks of the OSI model; these attacks are foreseen inevitable and nontrivial within the context of the cyber-physical smart grid. Among which some literatures have emphasized the interrelationship between *cyber* and *physical* securities [90, 82, 80]. For example, there are two primary research directions in smart grid security. 1) *A breach of network availability*: a power system involves real-time models that perform state estimation to observe the current state conditions in the power network by obtaining real-time measurement data from network meters and devices. Without these data, state estimation cannot be effectively executed in real time, thus resulting in the incapability of decision making for network operators. If the network communications is intruded by denial of service (DoS) attacks or other schemes against data availability, the services will be interrupted in both communications and power systems. 2) *A breach of measurement data confidentiality and integrity*: due to the cause-effect attribute, if measurement data are further altered by intruders in a way that the attack is hard to be detected, not to mention customer privacy is invaded, but the undetectability will cause utilities to lose revenues and result in severe power outage and equipment damages. Countermeasures relied on cryptographic mechanisms, secure communications architecture and network designs, device security, and intrusion detection systems (IDS) are anticipated options for securing the future power system against malicious intrusions and attacks from all perspectives in a complementary manner, e.g., energy consumption analysis, communications security,

information theory, and data mining. The implementation of various strategic approaches will be based on different smart grid applications as well as communications requirements throughout the networks.

According to the Institute for Electric Efficiency (IEE) [91], one-third of households in the U.S. have had a smart meter (i.e., approximately 36 million smart meters) as of May 2012, and approximately 65 million smart meters will have been deployed by 2015. While the deployments continue to rise, a few energy theft incidents have been discovered that some illegal customers intended to lower their electricity bills via meter tampering, bypassing, or other unlawful schemes regardless of traditional or smart meters in places such as Ireland, Hong Kong, and Virginia U.S. [92]. Notably, energy theft is one dominant component of non-technical losses, which account for 10%–40% of energy distribution [93], e.g., \$1–6 billion losses due to energy theft yearly for utilities in the U.S. Moreover, the report [94] has revealed that the current installations of smart meter communications protocols and associated infrastructure do not have sufficient security controls to protect the electric power system against false data injection attacks, not to mention older meters which were not designed to adequately cope with such attacks. In addition to the physical attacks, network attacks by compromising meters can also introduce malicious measurement data and cause degradation of grid operation [95, 96]. While some protection schemes against malicious network traffic have been proposed for smart grid communications networks monitoring [97, 98, 99], detection mechanisms and analyses for identifying malicious measurement data and energy theft have been investigated explicitly in [100, 101, 102, 103, 96, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 93, 116].

Power grid is a feedback loop control system that relies on measurement data obtained from network measurement units such as meters and sensors. Based on the

available data, the control center executes a series of tasks such as topology processing, network observability analysis, state estimation, and bad measurement data processing in order to identify the current status of the power network [117]. Consequently, a number of decision making on controlling actuators, optimizing power flows, and analyzing possible contingencies are performed to ensure network stability and security, in accordance with what the system observes or estimates. In reality, the measurement data may not be always accurate because of errors in measurements, failures in telemetry and equipment, noises in communications channels, and possibly breached integrity by intentional intrusion or attacks. If the accuracy of measurement data is not as precise as it gets, the decision making can be mistaken in consequence of misguided state estimation.

For simplicity, the common formulation of the state estimation problem is to consider a DC (direct current) power flow model [117], that is, $\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}$, where $\mathbf{H}$ is the $m \times n$ Jacobian matrix representing m network equations related to network topology, $\mathbf{x}$ is the n-vector of the true states (unknown), $\mathbf{z}$ is the m-vector of measurements (known), and $\mathbf{e}$ is the m-vector of random errors. The state estimate $\hat{\mathbf{x}}$ can be obtained by calculating $\mathbf{G^{-1}H^{\mathsf{T}}Wz}$, where $\mathbf{G} = \mathbf{H^{\mathsf{T}}WH}$ is the state estimation gain matrix, $(.)^{\mathsf{T}}$ is the transpose of $(.)$, and $\mathbf{W}$ is a diagonal matrix whose entities are based on the reciprocals of the variance of measurement errors, which may represent meter accuracy. In order to detect bad measurement data affected by the noise vector $\mathbf{e}$ and meter accuracy $\mathbf{W}$ such that the residual $\mathbf{r} = ||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \delta$ (where $||.||$ is the L_2-norm and δ is a predetermined threshold), common techniques such as normalized residuals and hypothesis testing are sufficient to detect anomalies. Nevertheless, a recent study [96] observed that the traditional detection is not able to differentiate between natural anomalies and malicious intrusion attributed to *false data injection* (FDI) such that $\mathbf{z_b} = \mathbf{z} + \mathbf{a}$ and $\hat{\mathbf{x}}_\mathbf{b} = \hat{\mathbf{x}} + \mathbf{c}$, where $\mathbf{a} = \mathbf{Hc}$ is an

attack vector injected to the system that is designed to be a linear combination of the column vectors of $\mathbf{H}$ in order to bypass the detection, i.e., $||\mathbf{z_b} - \mathbf{H}\hat{\mathbf{x}}_\mathbf{b}|| = ||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$. The authors further showed that the attacker is required to compromise a number of meters (i.e., 30%–70% of meters in IEEE 9, 14, 30, 118, 300 bus test systems) in order to bypass detection and takes less than 10 seconds. This type of attacks is interchangeably called an *unobservable*, *undetectable*, or *stealth* attack that needs to be launched in a *coordinated* manner [103, 118, 80] with knowledge of the network configuration matrix $\mathbf{H}$ while not violating the physics of power flow. Having knowledge of $\mathbf{H}$ by the attacker has been assumed in most of the current studies. Although a full knowledge of the entire system gained by the attacker may be improbable, it is worth studying and developing a detection framework to identify the malicious attack in case of the attacker possibly having acquired partial knowledge and considerable capability and resource. In fact, the attacker being able to launch FDI without prior knowledge of $\mathbf{H}$ has been studied in [113], that is, if the network topology remains static and the independent loads vary insignificantly for a period of time, $\mathbf{H}$ can be inferred.

Several works have rigorously investigated the FDI attack by proposing various detectors or analyzing the damage effects on the power system. For examples, Kosut *et al.* [102] proposed a detection scheme based on generalized likelihood ratio test while comparing with other two detectors based on the residual error $\mathbf{r}$ derived from the state estimation that uses minimum mean square error technique. The authors studied the outcomes of maximizing the residual error and minimizing the detection rate for the attack. Yuan *et al.* [108] identified the attack launched in two different time periods (i.e., immediate and delayed attack) in which the former may lead the system to perform unnecessary load shedding whereas the latter may cause power overflows on some

transmission lines. However, the authors only modeled the immediate attack and showed that the attack leads to a high economic loss. Lin *et al.* [107] studied the effectiveness of the attack in terms of transmission cost and power outage rate by deceiving the amount of energy request and supply as well as the status of transmission lines by claiming a line is valid to deliver a certain amount of power while it is not and vice versa. Giani *et al.* [103] proposed countermeasures by utilizing known-secure PMUs (phasor measurement units) placement and illustrated that $p + 1$ PMUs are enough to detect p k-sparse attacks for $k \leq 5$ while assuming all lines are metered. Qin *et al.* [106] illustrated a case where the attack is detected but still *unidentifiable* in such a way that it is difficult for operators to know which set of meters are truly compromised. The authors proposed a three-step search process that firstly identifies the meter with the largest residual (which exceeds a predetermined threshold) after state estimation, secondly locate a feasible attack region associated with the meter, and finally check a set of suspicious meters located in the region by using a brute-force search.

2.4 Summary

Among existing literatures in the smart grid field, most of the works have been studied in an independent way; they can be categorized into five predominant areas: 1) **power-centric** [74, 43, 44, 45, 48, 49, 51, 73, 54], which focuses on analyzing power management and champions the addition of communications tools in coordinating various operations of the future power system in an efficient manner, such as Volt-VAR control, power flow, MG, and EV management; 2) **communications-centric** [75, 72, 47, 76, 53], which evaluates different technologies to support different capacities and data rates and determines how these technologies should be implemented in different domains in order to cope with

the required throughput and latency; 3) **power-communications-centric** [77, 78], which studies the energy cost affected by communications delay and data loss; 4) **energy use scheduling-centric** [36, 38, 35, 37], which develops various efficient algorithms to allocate households loads throughout the day by using optimization tools to minimize energy cost; and 5) **cyber-physical-security-centric** [79, 96, 100, 108, 119, 120, 98, 121, 103, 104, 101, 102, 105, 106, 107, 109, 110, 111, 112, 113, 114, 115, 93, 116], in which some designed appropriate cryptographic key management, authentication techniques, as well as security architecture for the smart grid communications, while others analyzed the state estimation of power systems associated with FDI attacks and proposed detection schemes.

CHAPTER 3

ALLEVIATION OF PHOTOVOLTAIC SOLAR POWER CONGESTION IN DISTRIBUTION NETWORKS VIA SMART METERING COMMUNICATIONS

3.1 Motivation

Power transmission congestion has been one of the major issues in the centralized power system network. According to the U.S. Department of Energy (DOE) 2009 National Electric Transmission Congestion Study [34], the two most critical congestion areas are 1) mid-state New York and southward along the Atlantic coastal plain to northern Virginia, and 2) the urban centers of southern California. Power flow in transmission lines often becomes congested when the network is overloaded due to rising power demand and power generation, insufficient transmission capacity and transfer capability, peak demands in urban regions, distant demands in rural regions, and a lack of power transmission lines. Although many works based on supply management on congestion relief have been proposed to solve traditional power congestion [29, 28, 30, 33], no works have determined and analyzed local power congestion attributed to power surplus produced by the local DERs. In fact, a recent study is reported in the Pacific Northwest [122] indicating that there is no sufficient transmission capacity to deliver a surplus of wind power from its region to the other, and thus the wind turbines may be shut down temporarily. Therefore, it can be foreseen that the prolific deployment of DERs close to end-use sectors may incur local congestion and deterioration in the distribution grid if power control and management is not properly engineered.

This chapter is structured as follows: Section 3.2 presents a power system model where congestion due to solar surplus may occur in a neighborhood. It further describes the operation of a PV solar system and discusses means of disconnecting solar units from the distribution grid. A framework of smart metering communications for the disconnection process is proposed. Section 3.3 formulates the congestion problem and analyzes both dynamic programming and greedy approaches for solving the defined knapsack problem. Heuristic algorithms are proposed for candidate unit (de)selection. Section 3.4 analyzes the simulation results of the proposed algorithms and discusses the findings. Finally, Section 3.5 summarizes the focal points and draws a conclusion.

3.2 System Models

3.2.1 Power System Model

In electric power systems, power flow analysis is essential to schedule and plan for the amount of power flows between two buses[1] of the interconnected system. Available Transfer Capability (ATC) of the transmission network is a measure of the transfer capability remaining in the physical transmission network for further commercial activity over and above already committed uses [123]. It has been a tool used for congestion management as well as for power marketers trading in the competitive electric market [124, 125]. ATC is computed as

$$ATC = TTC - TRM - ETC \tag{3.1}$$

[1] A bus is electrically equivalent to a single point on a circuit, and it marks the location of one of two things: a generator that injects power, or a load that consumes power; it provides a reference point for measurements of voltage, current, and power flows [32].

where TTC (total transfer capability) is the maximum amount of power that can be transferred over the network in a reliable manner while satisfying all security constraints, i.e., thermal, voltage, and stability limits; TRM (transmission reliability margin) is the amount of transmission transfer capability necessary to ensure the network is secure under a reasonable range of uncertainties[2] in system conditions; and ETC (existing transmission commitments) includes retail customer service and CBM (capacity benefit margin). CBM is the amount of transmission transfer capability reserved by load serving entities for generation reliability requirements [123]; it is reserved for emergency when power generation is insufficient in one area which needs to be supplied with purchased power from other regions [125]. ATC can be a very dynamic quantity for a specific time frame for a specific set of conditions. The key parameter ATC is used to assess and mitigate the solar power surplus congestion problem.

The ATC is presumably calculated and available at the UCC periodically[3]. It allows utilities to determine if the network at specific times is able to accommodate an aggregate of solar power surpluses. If not possible, a scheduling algorithm is required to disconnect some of solar units from the grid in order to maintain the system stability. Figure 3.1 illustrates an example of *five* households with rooftop solar panels connected to the distribution line. Each household has its *energy profile* available that contains data for solar power generation (G), household power demand (D), and unused power flowing back to the

[2]Uncertainties of transfer capability that may occur during a power transfer are always considered in determining the ATC [126]; they may involve equipment failures, inaccurate network parameters, imprecise transfer capability computation, varying loads due to environment and weather conditions, and power cost change in the electricity market.

[3]ATC of power transfers among subnetworks of the entire interconnected transmission network cannot be evaluated in isolation; regional or wide-area coordination is necessary from all entities to gather and post sufficient information. Therefore, it is reasonable to assume that ATC has to be calculated in real-time and available in order for network operators to be aware of the network congestion level.

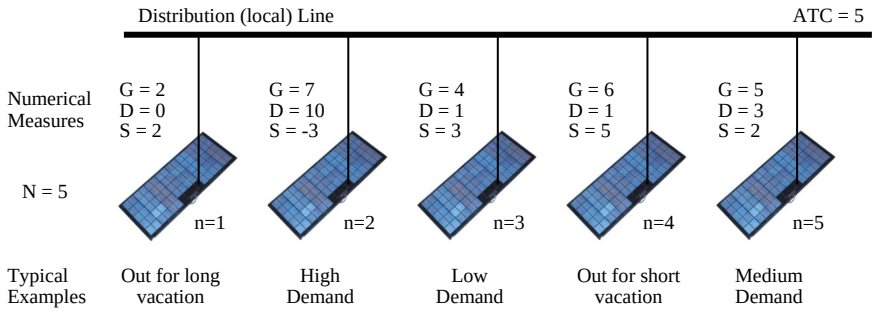


Figure 3.1 An example of the systematic model.

grid (*S*). In this example, each household has a solar surplus except for household *2*, which has a surplus value *-3* because it is consuming more energy than it can produce. Household *2*'s demand *10* may be compensated by the existing power (i.e., ETC including CBM in Equation 3.1), by an aggregate of solar surpluses *12* produced from others, or by partial existing power and solar surpluses. In either case, power is drawn from the distribution line and household *2* has to remain on the grid. From the utility perspective, the residual surplus can be used for commercial trading while satisfying the ATC limit. Since the line capacity cannot hold the residual surpluses, disconnecting some of the solar units is one approach to congestion avoidance. A set of feasible solutions of allowing the solar units to remain connected with the grid include $\{1,3,5\}$, $\{1,4\}$, $\{3,4\}$, and $\{4,5\}$, where $\{.\}$ represents a set of solar units. Despite the fact that choosing either of the combinations will not violate the ATC limit, the intention of maintaining as large number of units as possible in selection can minimize the number of disconnection as well as reconnection. Communications is required to perform the disconnection process. Efficient monitoring and congestion management can be provisioned via smart metering communications or SMC (to be discussed in Section 3.2.2).

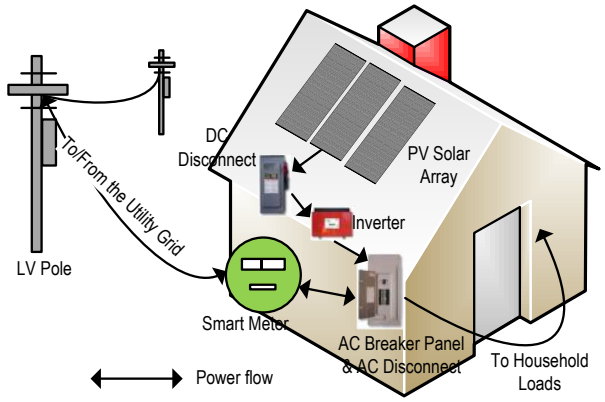


Figure 3.2 The grid-tie solar system mounted on rooftops.

A grid-tie system for the PV solar unit is analyzed rather than an off-grid (standalone) system. In fact, the grid-tie unit is preferred not only because it has higher energy efficiency, but also because the off-grid unit requires a bank of batteries or capacitors equipped for storing power to supply on its own, thus resulting in an extra cost for households [127].

The PV solar array system. A grid-tie solar system mounted on rooftops or on ground without batteries backup is composed of four major components: PV solar panels/array, DC Disconnect, inverter, and AC Disconnect/AC breaker panel (ACDBP) [128]. As illustrated in Figure 3.2, solar power is generated through the semiconductor cells of PV solar panels as a stream of direct current (DC). The maximum amount of power that can be produced depends on various factors, such as sun intensity, temperature condition, and techniques implemented in the inverter, e.g., maximum power point tracking (MPPT) [129]. The DC power generated from the solar panels flows to the DC Disconnect (switch/breaker box). The DC flow can be prevented from entering the DC Disconnect during emergency or maintenance on the utility grid system. In a normal situation, the grid-tie inverter transforms the DC power collected from the DC Disconnect into alternating current (AC) power for most of residential and commercial uses. It produces

power that meets the requirements of the utility grid so that the generated power is synchronized with the grid power before flowing into the grid. The ACDBP can also stop the current flow from entering the grid for emergency or maintenance purposes. Without the AC Disconnect, the consumer's load is also interrupted while the solar power is isolated from the grid [130].

There are essentially two ways to prevent the generated solar power from entering the grid: 1) Open the circuit between the solar panels and DC Disconnect, and 2) Open the circuit between the ACDBP and the grid. The former entirely isolates the generated power from the solar panels. The generated power may be grounded—this results in the lowest efficiency of energy use because households are unable to consume the energy. On the contrary, the latter allows households to consume their solar power from the AC breaker panel through another dedicated line[4]. Hence, this method is preferred despite the excess power is also sent into the ground while unused. Once energy consumption rises and approaches the amount the solar panels generate, the ACDBP is reconnected to the grid granted by the utility operator and the grid power can be provisioned; therefore, the second case is considered.

Congestion and overload–Causes and Remedies. Unexpected power demand and renewable energy production can potentially instigate congestion in both transmission and distribution grids. From a consumer perspective, variation and surge in loads are essentially attributed to consumers' needs and activities as well as environment and weather conditions. The former is usually unpredictable where historical data of consumption are required to estimate the prospective loads in advance. The latter is supervised with the

[4]The smart meter stops measuring the solar power generation because the line between the smart meter and the ACDBP is disconnected.

aid of weather forecast to match the correlated loads in specific regions and seasons. On the other hand, determination of transfer capability such as TTC and ATC (described in Section 3.2.1) in the interconnected grid is critical from a network perspective. Foreseeing the approximate amount of consumption without sufficient transfer capability calls for proper actions to avoid congestion. Therefore, demand response programs are applied to manipulate varying consumption such that consumers have a choice whether or not to consume energy based on the corresponding price signal received from utilities. The demand side management adopts peak shaving and valley filling strategies to reduce demand peak-to-average ratio, and at the same time to increase energy utilization.

Furthermore, solar power surpluses during renewable times can also overload the network when consumption is low and when the resources are limited, e.g., lack of energy storage, transfer capability, and transmission capacity. Several ways to tackle the issue may include

- *Sell excess power* to other regions in need or *maximize energy use* during renewables production. However, utilities may run out of capability to sell the surpluses when consumption is low or people not being home.

- *Shut down some power plants* such as fuel oil, natural gas, or even nuclear. Nevertheless, this may put the grid in danger due to the intermittency and variability of renewables generation. In addition, some generators cannot be turned back on within a short period of time.

- *Store surplus energy* in additional storage as much as possible for later use. Nonetheless, current energy storage is still expensive and inefficient.

- *Disconnect a number of solar units* from the grid.

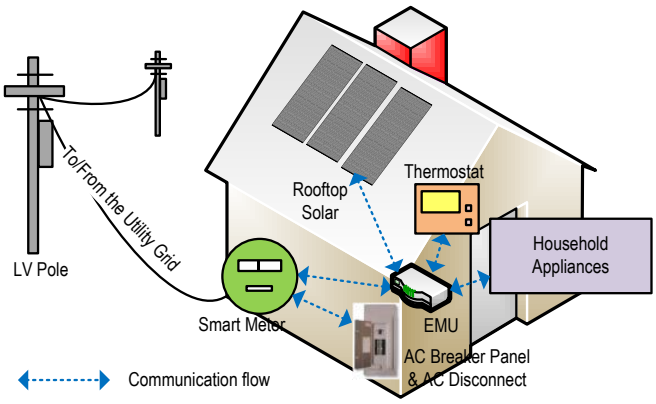


Figure 3.3 Communications in HAN between smart meter and EMU as well as between EMU and solar unit, appliances, and thermostat.

3.2.2 Communications System Model: SOlar UNit Disconnection (SOUND)

Communications in the legacy electric power system has been partially proprietary and based on simple protocols. In fact, no communications or simple communications is preferred in fault detection management [24]; shutdown is the quickest and safest way in the protection system. In order to enhance the network visibility for utility operators, integrating ICT and smart grid technologies is necessary to achieve effective distributed control and monitoring. There are various choices of communications technologies for NAN and HAN. Implementation of wireless technologies either based on IEEE 802.11 WiFi [131] or IEEE 802.15.4g for NAN and IEEE 802.15.4 ZigBee [132] for HAN as part of SMC in the AMI is proposed. IEEE 802.11 supports high data rate to relay an aggregate of data collected from smart meters to the UCC. IEEE 802.15.4 provides reasonable data rates for small-size data packets with low power transmission, whereas IEEE 802.15.4g (smart grid utility network) tailors sub-GHz frequency bands for better RF penetration and less interference. The HAN design referred in Reference [35] equips each house with an EMU. In the proposed scheme (as shown in Figure 3.3), the PV solar unit, household appliances, thermostat, and ACDBP, are physically connected with the smart meter. The

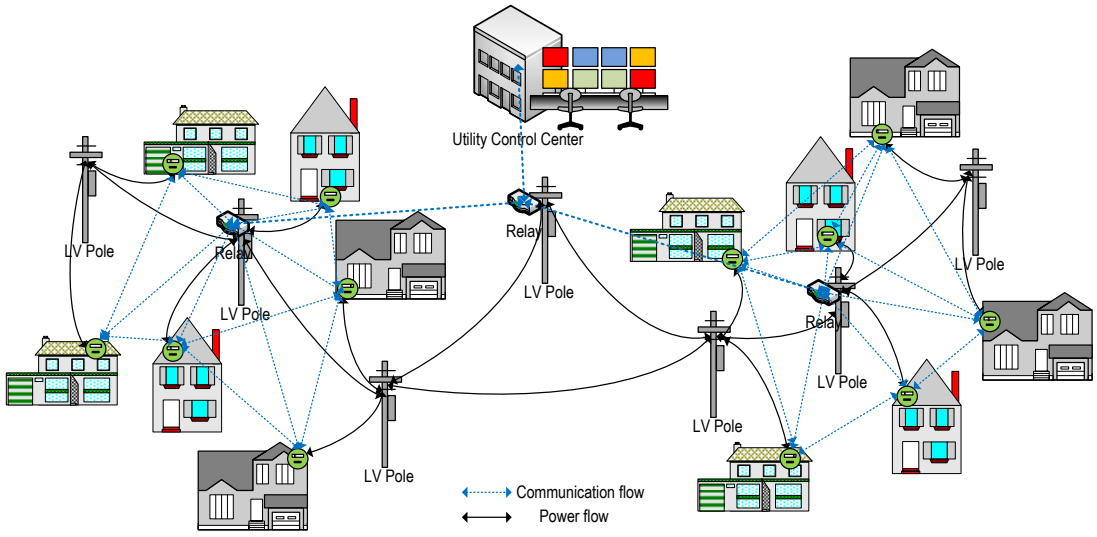


Figure 3.4 SMC infrastructure in NAN.

smart meter has multiple built-in functionalities supporting different wireline and wireless communications protocols of powerline communications (PLC) and RF technologies [133]. The EMU plays as an intermediate node (e.g., gateway) which coordinates households energy consumption and records solar generation. It also consults with the smart meter to determine if low energy cost can be obtained when grid power is needed. The smart meter also measures and records both solar power generation/surplus and households energy consumption. The measured data at the smart meter are transmitted to UCC via SMC. In Figure 3.4, SMC in NAN consists of smart meters, relay/aggregation nodes, and an UCC.

SMC is constructed as a wireless mesh network. Figure 3.4 illustrates the case where a neighborhood is composed of twelve households and three relay nodes. Data packets containing energy profiles are periodically transmitted in uplink from the smart meters, through relay nodes, and received at the UCC. Upon data reception, the UCC performs computation based on the proposed algorithms (to be discussed in Section 3.3) and sends

the notification packets back to the smart meters if their solar units need to be disconnected from the grid. For example, if the UCC determines that no power congestion is found in the network, no action is taken at the UCC. When unit disconnection is required, each smart meter associated with its corresponding solar unit to be disconnected receives notification from the UCC[5], and sends a signal to ACDBP to disconnect its solar unit from the grid. Consequently, the smart meter stops transmitting data to the UCC[6]. Since the disconnection would not affect household consumption from the solar generation (as discussed on p. 33) for a period of time, data transmission between the smart meter and UCC is not required[7].

Once consumption arises or generation decreases and EMU is aware that grid power is needed while communicating with appliances and solar units, EMU notifies the smart meter of the event. The smart meter starts transmitting a request packet to the UCC to see whether reconnection can be done. The UCC replies with a price signal. If the household agrees to consume the grid power based on the time-of-use (TOU) price, the reconnection is granted. Otherwise, disconnection remains until congestion is relieved. For households which remain connected, the corresponding smart meters periodically transmit data information to the UCC. The mechanism of the proposed system model is summarized in Algorithm 1.

---

[5]In the proposed mechanism, the number of disconnected units is minimized so that the number of notification packets in *downlink* is kept as small as possible.

[6]At the same time, the number of data packets in *uplink* is minimized while households are disconnected from the power grid.

[7]Disconnection makes the households equivalently operate in the islanded mode. Power is self-provisioned, and therefore no data transmission is necessary from the disconnected smart meters during the disconnection period.

3.3 Problem Definition and Formulation

N households which have PV solar units installed on rooftops or on ground in a neighborhood are considered. Each household is denoted by $n, n = 1, 2, ..., N \in \mathcal{N}$, and the corresponding PV solar unit is denoted as x_n.

Algorithm 1 SOlar UNit Disconnection (SOUND) Process via SMC

Require: All units are connected to the grid.

Ensure: Periodic data transmission from smart meters to UCC.

while power congestion is discovered **do**
    if a unit has no surplus **then**
        Remain on the grid.
    else[a surplus exits]
        Disconnection is considered (to be discussed in Sec. 3.3)
        UCC signals units to be disconnected.
        The disconnected units stop transmitting data to UCC and stay in islanded and standby modes.
        Reconnection is granted from UCC when grid power is needed or congestion is removed.
    end if
end while

Household n may (not) consume energy in Watt per hour (Wh) during solar power generation; the corresponding demand value is represented by a nonnegative integer and denoted by $P_{D,n} \in \mathbb{N}$. There is (not) power surplus from unit x_n when the generated power in Wh is more (less) than it is needed; the corresponding surplus value is an integer and denoted by $P_{S,n} \in \mathbb{Z}$. In the selection process, only $\widehat{\mathcal{N}} = \mathcal{N} \backslash \mathcal{M}$ households are

considered where $|\mathcal{M}| \leq |\mathcal{N}|$ and households denoted by $m, m = 1, 2, ..., M \in \mathcal{M}$, do not have surpluses (i.e., $P_{S,m\in\mathcal{M}} \leq 0$) and have to remain on the grid. Finally, the capacity of the distribution line is a nonnegative integer and denoted by $P_{ATC} \in \mathbb{N}$.

3.3.1 Assumptions

Without loss of generality, a list of primary assumptions are considered:

- Sunlight is available most of the time during PV solar power production.
- Variability of demands and surpluses is managed and controlled through EMU and smart meters in HAN.
- All solar units are grid-tie systems and no additional energy storage is available for households.
- Households may continue to consume solar energy while solar units are disconnected from the grid.
- The disconnection at the AC Disconnect can be done by the smart meter via communications.
- Power loss and system constraints (e.g., real and reactive power[8] in terms of voltage, frequency, and phase) are not considered.

3.3.2 Formulation of Knapsack Problem for Power Surplus Congestion

The solar power congestion issue in the distribution grid can be tackled as one type of knapsack problems. In the scenario, the solar units either remain *connected* on the grid or are *disconnected* from the grid; a 0/1 knapsack problem where $x_n = 0$ if unit n is scheduled

[8]Active power is the actual power consumed by customers in addition to power losses consumed in heating the wires and other electrical equipment; it is usually measured in kilowatts (kW). Reactive power is the power compensated by the generation source to energize certain portions of the AC power system when there is a time shift in voltage and current; it is measured in volt-ampere reactive (VAR).

to be *off* the grid and $x_n = 1$ to be *on* the grid is considered. Therefore, the total number of connected units is calculated as

$$U = \sum_{n \in \widehat{\mathcal{N}}} x_n, \quad x_n \in \{0, 1\} \tag{3.2}$$

It is a binary (decision) integer programming problem. The objective is to maximize the number of connected units (equivalently to minimize the number of disconnected units) subject to a limited capacity that the network can accommodate the surpluses of connected units:

$$\begin{aligned} &\max \quad U \\ &s.t. \quad \sum_{n \in \widehat{\mathcal{N}}} P_{S,n} \cdot x_n \leq P_{ATC}, \quad x_n \in \{0, 1\} \end{aligned} \tag{3.3}$$

From a power standpoint, maintaining a large number of connected units allows more households not only to use their solar power, but also to be able to sell the power surplus to the utility. From a communications perspective, data traffic congestion may be reduced owing to fewer packets sent out from the UCC for the disconnection process.

Meanwhile, maximizing the total power demand value is desired while satisfying the capacity requirement:

$$\begin{aligned} &\max \quad \textstyle\sum_{n \in \widehat{\mathcal{N}}} P_{D,n} \cdot x_n \\ &s.t. \quad \sum_{n \in \widehat{\mathcal{N}}} P_{S,n} \cdot x_n \leq P_{ATC}, \quad x_n \in \{0, 1\} \end{aligned} \tag{3.4}$$

The strategy is to protect households with high energy efficiency from being disconnected. The efficiency of energy use of household n, η_n, is a nonnegative real number, and defined as the ratio of power demand to power surplus. Similarly, the global energy efficiency (η)

is the ratio of cumulative power demands to cumulative power surpluses, i.e.,

$$\begin{aligned} \eta_n &= \frac{P_{D,n}}{P_{S,n}} \in \mathbb{R} | \eta_n \geq 0 \\ \eta &= \frac{\sum P_{D,n}}{\sum P_{S,n}} \in \mathbb{R} | \eta \geq 0, \quad n \in \widehat{\mathcal{N}} \end{aligned} \tag{3.5}$$

Taking energy efficiency into account will encourage the households with lower efficiency of energy use to utilize energy during solar power generation. Consequently, the ultimate goal of having less power surpluses flowed to the grid and more units connected to the grid can be achieved.

3.3.3 Solutions for the Typical Knapsack Problem

SMC involves enormous data transmission between the UCC and smart meters for various purposes, e.g., meter data collection, device control, and fault detection. The efficiency of computation at the UCC is critical to the system performance. When the UCC receives energy profiles from the smart meters, it has to quickly figure out which households in $\widehat{\mathcal{N}}$ should be disconnected from the grid once power congestion is detected. The number of households covered by a utility company can be as large as from thousands to hundreds of thousands. Using the brute-force approach to solving a knapsack problem would take $O\left(2^n\right)$ exponential time to obtain the result; the computation running time tends to escalate exponentially when the number of nodes increases. Since scalability is a main concern for both computation and communications, the network has to be divided into subnetworks to form a number of clusters; a decentralized scheme would allow the UCC to manage and control data computation and data traffic more effectively.

The knapsack problem has been proven a NP-complete problem [134]. Existing solutions to solve knapsack problems include dynamic programming, backtracking, branch

and bound, and greedy approaches. Greedy algorithms are proposed to obtain a suboptimal solution that is good enough to avoid power congestion.

Dynamic programming. Considering adopting the dynamic programming method for solving the formulated knapsack problem: dynamic programming decomposes a knapsack problem problem into a number of local subproblems and computes optimal solutions of the subproblems to obtain a global optimal solution. Instead of finding all 2^n possible solutions exhaustively, dynamic programming looks at smaller capacities $c \leq C$ (from 1 to C) and determines which unit n (from 1 to N) can be included subject to the subcapacity limit while achieving the maximum demand value at each iteration. Therefore, dynamic programming requires a table (where the approach trades space for time) to memoize the subsolutions. By looking up the table in a bottom-up manner, a global optimal solution can be obtained. The algorithm fills $(N+1)(C+1)$ entries in the table. Each entry requires 1 execution and N executions are needed to trace the solution. The overall complexity is asymptotically reduced to $O(NC)$ [134], which is solvable in a polynomial time. Unfortunately, DP becomes prohibitive when the capacity C is too large, e.g., $> 10^4$ in the power congestion problem. One way to reduce the size of the table is to find the greatest common divisor (GCD) among the surplus values and capacity, but the GCD usually equals 1 from a large set of values.

Greedy strategy. Typically, a greedy algorithm can solve the knapsack problem in approximately $O(n)$ running time [134]. One greedy approach to solve the knapsack problem is to construct permutations by ordering the energy profiles collected at the UCC. Selecting the candidates among households can be based on the following three methods: the highest power demand first, the greatest power efficiency first, and the lowest power surplus first. The three strategies are described as follows:

1. *Nonincreasing power demand (NID)*: NID tends to maximize the total value of power demand disregarding the associated power surplus by adding demand values in descending order:

$$P_{D,1} \geq P_{D,2} \geq \ldots \geq P_{D,n}, \quad n \in \widehat{\mathcal{N}}$$

   For this reason, NID is likely to reach the capacity limit quickly. It has the worst performance in cumulative demands and U as compared to other schemes.

2. *Nonincreasing power efficiency (NIE)*: NIE aims to improve the NID scheme by considering surplus values as a complementary factor to balance the output of the system performance. NIE executes Equation 3.5 and accumulates the demand values in descending order of energy efficiency:

$$\eta_1 \geq \eta_2 \ldots \geq \eta_n, \quad n \in \widehat{\mathcal{N}}$$

   Although a high power efficiency indicates efficient energy use, different combinations of demand and surplus values can have the same or similar ratios which are hard to differentiate; this is the key factor that prevents NIE from obtaining a large U. Overall, NIE achieves the highest total demand value among the three at the cost of a reduced U.

3. *Nondecreasing power surplus (NDS)*: NDS tends to pick as many units as possible while it accumulates surplus values in ascending order:

$$P_{S,1} \leq P_{S,2} \ldots \leq P_{S,n}, \quad n \in \widehat{\mathcal{N}}$$

Therefore, the method achieves the largest U as compared to others. However, NDS disregards the corresponding demand values as opposed to NID.

3.3.4 Heuristic Selection Algorithms for Disconnecting Candidate Units: MNDS and RVS

While introducing the ordering strategy for unit selection, two algorithms which adopt the NDS scheme to fulfill the first optimization problem are proposed, i.e., Equation 3.3. Note that it is reasonable to select a unit beginning with the smallest surplus because its energy efficiency is likely high; however, in the case where a unit with a small surplus is due to a small amount of generation, its energy efficiency can be low if the demand is small. Moreover, units which have small surpluses connected to the grid are kept in order to avoid frequent disconnection and reconnection. This is because the corresponding demands can fluctuate such that surpluses may no longer exist and yet the grid power is required. Therefore, for the first proposed scheme, NDS is combined with NIE to enhance the overall energy efficiency and demand, i.e., Equation 3.4. For the second proposed scheme, NDS is applied backwards with NIE to get rid of units (to be disconnected) which do not meet the design criteria. Meanwhile, the capacity constraint must hold.

Modified NDS (MNDS). *Methodology* – Data information about solar power demands and surpluses of N households are assumed to have been collected from the smart meters and available at the UCC. Only units in $\widehat{\mathcal{N}}$ are considered when other units in $\widehat{\mathcal{M}}$ do not have surpluses available. No units are disconnected while the network is not overloaded. The overload status of the network is discovered by subtracting the capacity

limit by the total surplus of units in $\widehat{\mathcal{N}}$.

$$P_O = \sum_{n \in \widehat{\mathcal{N}}} P_{S,n} - P_{ATC} \tag{3.6}$$

When overload is detected (i.e., $P_O > 0$), the NDS scheme is performed (see Line 4-6 in Algorithm 2). Units are selected based on their surpluses in ascending order. After some iterations, the algorithm will stop at iteration i when an overload of the capacity is found, i.e.,

$$\sum_{n=1}^{s-1} P_{S,n} \leq P_{ATC} \quad \text{and} \quad \sum_{n=1}^{s} P_{S,n} > P_{ATC}, \quad n \in \widehat{\mathcal{N}}$$

where $P_{S,s}$ is defined as the *split surplus value* and cannot be added because the capacity constraint will be violated. Unit s $(= i)$ is assigned as the *split unit*, which constitutes the solution vector $\widehat{\mathbf{x}}$ with $\widehat{x}_n = 1$ for $n = 1, 2, \ldots, s-1$ and $\widehat{x}_n = 0$ for $n = s, s+1, \ldots, \widehat{N}$, i.e.,

$$\begin{aligned} \widehat{\mathbf{x}} &= \begin{bmatrix} \widehat{x}_1 & \widehat{x}_2 & \ldots & \widehat{x}_{s-1} & \widehat{x}_s & \widehat{x}_{s+1} & \ldots & \widehat{x}_{\widehat{N}} \end{bmatrix} \\ &= [\underbrace{1 \quad 1 \quad \ldots \quad 1}_{\widehat{\mathbf{x}}_l} \quad \underbrace{0 \quad 0 \quad \ldots \quad 0}_{\widehat{\mathbf{x}}_r}] \end{aligned} \tag{3.7}$$

Unlike the original NDS scheme, MNDS tries to further improve the overall energy efficiency from what NDS can achieve while maintaining U, i.e., $s-1$ units. In order to do this, the overflowed power P_E is determined by adding the split surplus value:

$$P_E = \sum_{n=1}^{s} P_{S,n} - P_{ATC}, \quad n \in \widehat{\mathcal{N}} \tag{3.8}$$

With the knowledge of P_E, which is incorporated into the two conditions (Lines 9 and 12) specified in Algorithm 2, the number of candidate units in $\widehat{\mathbf{x}}_l$ and $\widehat{\mathbf{x}}_r$ (see Equation 3.7) is determined for an one-to-one substitution.

Algorithm 2 Modified NDS (MNDS)

if capacity is not overloaded $P_O \leq 0$ **then**
    No household/unit $\widehat{x}_n \in \widehat{\mathcal{N}}$ is disconnected
else
    for $\forall \widehat{x}_n \in \widehat{\mathcal{N}}$ **do**
        Perform NDS algorithm to keep the first $s-1$ units ON where $s \geq 2$
    end for
    Calculate P_E by adding the surplus of unit s, $P_{S,s}$
    for units in $\widehat{\mathbf{x}}_l$ **do**
        if $P_E \leq P_{S,j}$, $j = (1, 2, .., s-1)$ **then**
            Select unit $\widehat{x}_l$ with $min\{\eta_j, \eta_{j+1}, ..., \eta_{s-1}\}$, η_l, to be the candidate
            for units in $\widehat{\mathbf{x}}_r$ **do**
                if $P_{S,k} - P_{S,s} > P_{S,l} - P_E$, $k = (s, s+1, ..., \widehat{N})$ **then**
                    Select unit $\widehat{x}_r$ with $max\{\eta_s, \eta_{s+1}, ..., \eta_{k-1}\}$, η_r, to be the candidate
                    if $\eta_l < \eta_r$ **then**
                        Unit $\widehat{x}_l$ is substituted by unit $\widehat{x}_r$
                    end if ▷ Nothing changed otherwise
                    Break
                end if
            end for
            Break
        end if
    end for
end if

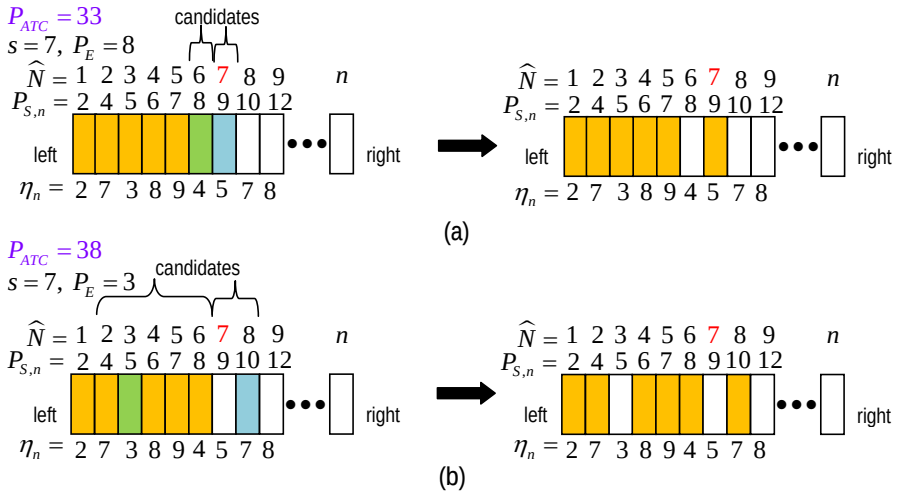


Figure 3.5 An illustration of the MNDS algorithm: Two situations during the substitution are shown, where (a) depicts only one candidate found in $\widehat{\mathbf{x}}_l$ and $\widehat{\mathbf{x}}_r$, respectively, and (b) demonstrates multiple candidates found in $\widehat{\mathbf{x}}_l$ and $\widehat{\mathbf{x}}_r$, respectively.

Figure 3.5 illustrates the surplus values of units in $\widehat{\mathcal{N}}$ sorted in ascending order from left to right, and the corresponding energy efficiency values for the comparison purpose. Considering $P_{ATC} = 33$ as shown in Figure 3.5(a), unit *7* is found as the split unit (whose surplus value is *9*) while the first six units have an aggregate of surplus values of *32*. Adding the split surplus value would make the total *41* and result in overload. While knowing $P_E = 8$ derived from Equation 3.8, unit *6* whose surplus value is *8* is determined to be the only one candidate in $\widehat{\mathbf{x}}_l$ (Line 10). Subsequently, the outcome of searching for candidates in $\widehat{\mathbf{x}}_r$ is unit *7* only (Line 13). As a result, unit *6* is removed from the list and unit *7* which has higher energy efficiency is added without exceeding the capacity limit, i.e., $\sum_{n=1}^{5} P_{S,n} + P_{S,7} = 33 \leq P_{ATC}$.

In another situation where more than one units found in $\widehat{\mathbf{x}}_l$ and $\widehat{\mathbf{x}}_r$, assuming $P_{ATC} = 38$ is shown in Figure 3.5(b). The split unit is unit *7* again and $P_E = 3$ is derived, implying that any surplus values larger than or equal to *3* in $\widehat{\mathbf{x}}_l$ are qualified for substitution, i.e., units *2-6* (line 9). While unit *3* whose surplus value is *5* happens to have the lowest efficiency

value among others, an intention to find the units in $\widehat{\mathbf{x}}_r$ that satisfy the requirement (line 12) takes place by subtracting P_E by $P_{S,3}$ (i.e., *5-3=2*) and by subtracting $P_{S,7}$ by $P_{S,9}$ (i.e., *12-9=3*). The outcome shows the candidates in $\widehat{\mathbf{x}}_r$ to be unit *7* and unit *8*.

As a result, unit *3* is substituted by unit *8* whose energy efficiency is higher than that of unit *7* and unit *3*, without exceeding the capacity limit, i.e., $\sum_{n=1}^{2} P_{S,n} + \sum_{n=4}^{6} P_{S,n} + P_{S,8} = 37 \leq P_{ATC}$. While the one-to-one substitution can preserve as many units as NDS can, MNDS outperforms NDS in greater energy efficiency once an available substitute is found.

Complexity – The MNDS scheme inherits the property of the sorting algorithm (Line 5) which approximately takes $n\log(n)$ executions in the average and worst cases. Accumulating surplus values and calculating P_E may take n executions. The main feature of MNDS is searching for candidates in both $\widehat{\mathbf{x}}_l$ and $\widehat{\mathbf{x}}_r$ that can take n executions, respectively. Comparing the final candidate in $\widehat{\mathbf{x}}_l$ with the final candidate in $\widehat{\mathbf{x}}_r$ requires 2 executions (Lines 14-15). Therefore, the overall complexity of MNDS is asymptotically reduced to $O(n\log(n))$.

ReVerse Selection (RVS). *Methodology* – A reverse method is further proposed to deselect units to be disconnected from the grid instead of selecting units to be connected in the previous methods. The RVS scheme is preferred when the number of disconnected units is less than $\widehat{N}/2$. In order to do this, the energy profiles are sorted in descending order of surplus values from left to right, as shown in Figure 3.6. The RVS scheme deselects units with lower energy efficiencies among others according to the requirements constituted in Algorithm 3, where two conditions are considered: iterations prior to the last iteration (Line 15), and the last iteration (Lines 7, 11, 13).

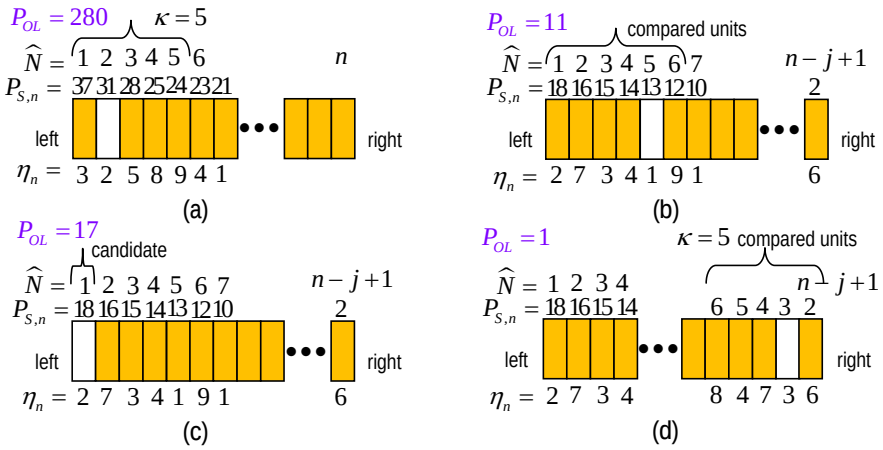


Figure 3.6 An illustration of the RVS algorithm: Four situations during the deselection process are shown, where (a) depicts the first five units being compared during the first $j - 1$ iterations, while (b), (c), and (d) demonstrate the last iteration j being performed, (b) depicts a comparison among the first six units, (c) depicts the first unit being deselected when it is the only one that satisfies the condition, and (d) depicts a comparison among the last five units.

Similarly, data information about demands and surpluses are assumed to have been received at the UCC. An overloaded network is identified by executing Equation 3.6. If overload is observed (i.e., $P_O > 0$), the deselection process begins. The permutation is constructed by sorting the surplus values of units in descending order that is contrary to NDS and MNDS. When multiple iterations are required to deselect units during the process (i.e., when the updated overload value is larger than the greatest surplus value), an arbitrary number κ of units are inspected from the first unit and the unit that has the lowest energy efficiency is selected (Line 15). The parameter κ ($\leq \widehat{N}$) is an adjustable number and is defined as the inspection range in the RVS scheme. Considering $P_O = 280$ shown in Figure 3.6(a), one iteration of deselecting a unit is not enough to fulfill the capacity constraint. In this situation, the first five surplus values of units are compared and unit *2* is deselected in order to maintain a high energy efficiency.

Algorithm 3 ReVerse Selection (RVS)

if capacity is not overloaded $P_O \leq 0$ **then**
    No household/unit $\widehat{x}_n \in \widehat{\mathcal{N}}$ is deselected from the list
else
    Sort $P_{S,n}, \forall n \in \widehat{\mathcal{N}}$ in *descending* order and pick κ
    for $\forall \widehat{x}_n \in \widehat{\mathcal{N}}$ **do**
        if $P_O < P_{S,n}$ where unit $\widehat{x}_n$ has the smallest surplus **then**
            Deselect unit $\widehat{x}_i$ with $min\{\eta_{n-\kappa+1}, \eta_{n-\kappa+2}, ..., \eta_n\}$, η_i, from the list (see Fig. 3.6(d)), and Break
        else
            if $P_O \leq P_{S,1}$ **then**
                if $P_O > P_{S,2}$ **then**
                    Deselect unit $\widehat{x}_1$ from the list (see Fig. 3.6(c)), and Break
                else[see Fig. 3.6(b)]
                    Deselect unit $\widehat{x}_p$ with $min\{\eta_1, \eta_2, ..., \eta_{i-1}\}$ such that $P_O > P_{S,i}$, η_p, from the list, and Break
                end if
            else[Next round is required; see Fig. 3.6(a)]
                Deselect unit $\widehat{x}_k$ with $min\{\eta_1, \eta_2, ..., \eta_\kappa\}$, η_k, from the list
            end if
        end if
    end for
end if

Notably, picking a large κ may increase the overall energy efficiency and demand at the cost of a smaller U as compared to NDS and MNDS; the outcome of RVS would approach that of NIE. Also note that when $\kappa = 0$, the outcome of RVS would be identical to that of NDS in reverse. The recursion continues until the residual overload at iteration j is found either larger than or smaller than the surplus value of the last unit, i.e., unit $\widehat{N} - j + 1$. Both cases indicate one more unit to be deselected.

In the former case (Lines 9-14), the overload value is compared with the surpluses starting from the first unit until it is found greater than the ith surplus. Since the first $i - 1$ surpluses are larger than the overload value, one of them with the least energy efficiency is chosen for disconnection. For examples, assuming $P_O = 11$ as shown in Figure 3.6(b), those before unit *7* (i.e., units *1-6*) will require a comparison of their energy efficiencies. As a result, unit *5* is deselected. Furthermore, Figure 3.6(c) shows a particular situation where $P_O = 17$; unit *1* with surplus value being larger than the overload value is directly deselected without a comparison. On the other hand, the latter case (Lines 6-7) applies the same method for the recursive iterations such that the last κ units are compared, and one of them with the minimum energy efficiency is chosen for disconnection. Figure 3.6(d) considers $P_O = 1$, where unit $n - j$ whose surplus value is *3* is deselected among the last five units.

Complexity – The RVS algorithm also involves the sorting process which takes $n \log(n)$ executions. Since the complexity of RVS is dominated by the first $j - 1$ iterations, the complexity of the last iteration j is neglected. In the worst case, the first $j - 1$ iterations can take approximately $n\kappa = n^2$ executions if $\kappa = n$. However, the purpose of RVS is to enhance the overall efficiency while preserving as large U as possible; κ is chosen small so that the overall complexity of RVS can still be asymptotically reduced to $O(n \log(n))$.

3.4 Simulations and Results

The simulations are twofold: the first set is undertaken to demonstrate the viability of the selection algorithms (NID, NIE, NDS, MNDS, and RVS), whereas the second set is conducted to examine the upstream data traffic in a SMC network.

3.4.1 Performance of the Selection Algorithms

The first simulation represents a special case assuming that power surplus exists from each household (i.e., all N units are considered in the selection process; $M = 0$), whereas the second simulation shows a general situation in which some households consuming more power than they produce must remain on the grid, i.e., only $\widehat{N}$ units are taken into account; $M > 0$. For both simulations, $P_{ATC} = 30,000$ and $\kappa = 5$ are chosen.

In the first simulation, $N = 50$ is set for scenarios (a)-(d), (e), (g), and (h), in Table 3.1. Note that both scenarios (e) and (f) are the same (i.e., sharing identical probability distributions and parameters); hence, scenario (e) with $N = 50$ and scenario (f) with $N = 500$ are set to observe the effect of N becoming large. The power demand value (P_D) and power surplus value (P_S) are generated according to uniform distribution (UD) denoted by $\mathcal{U}$(*min,max*) and folded-Gaussian distribution (FGD)[9] denoted by $\mathcal{FG}(\mu, \sigma^2)$. P_D and P_S are discrete random variables with probability mass functions (PMFs) $f_D\left(P_D; \mu_D, \sigma_D\right)$ and $f_S\left(P_S; \mu_S, \sigma_S\right)$, respectively. Different parameters are designed in *eight* scenarios to elicit how the variations can affect the selection schemes.

[9]FGD is derived from the Gaussian distribution $\mathcal{N}(\mu, \sigma^2)$ by taking the absolute values of all negative real numbers and rounding them to the nearest integers. In other words, if X is a discrete Gaussian random variable with mean μ and variance σ^2, $D = |X|$ is a discrete folded Gaussian random variable that has a folded Gaussian distribution.

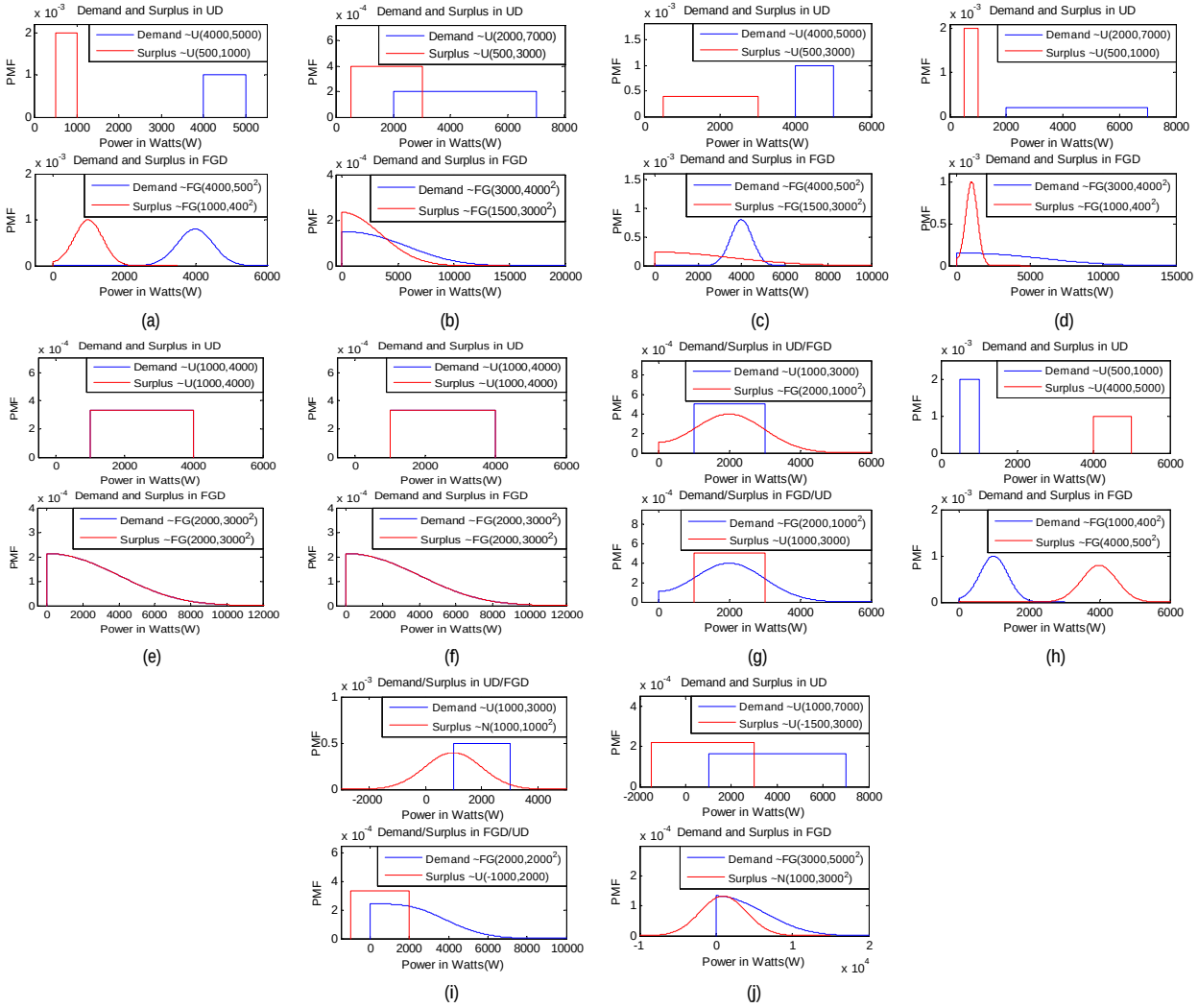


Figure 3.7 PMFs of demand and surplus corresponding to the scenarios in Table 3.1.

Table 3.1 The Outcomes of Algorithms Applied to Different Scenarios in Figure 3.7 Correspondingly

M	Small σ_D and σ_S $(D>S)$												Large σ_D and σ_S											
$=0$	N=50	UD						FGD						N=50	UD						FGD					
	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$
	NID	182892	29771	6.14	0.96	40	0.95	131245	29849	4.40	0.89	31	0.86	NID	106403	29760	3.58	0.86	18	0.72	105357	29898	3.52	0.84	14	0.56
	NIE	188472	29578	6.37	1	42	1	145415	29507	4.93	1	36	1	NIE	123358	29513	4.18	1	24	0.96	124362	29634	4.20	1	22	0.88
	NDS	187470	29539	6.35	0.99	42	1	143557	29393	4.88	0.99	36	1	NDS	114393	29097	3.93	0.94	25	1	103848	28779	3.61	0.86	25	1
	MNDS	188141	29580	6.36	0.99	42	1	144845	29517	4.91	0.99	36	1	MNDS	117908	29389	4.01	0.96	25	1	110361	29501	3.74	0.89	25	1
	RVS	188533	29770	6.33	0.99	42	1	145389	29608	4.91	0.99	36	1	RVS	120681	29623	4.07	0.97	25	1	115945	29374	3.95	0.94	25	1
	(a)													(b)												
	Small σ_D and large σ_S													Large σ_D and small σ_S											
	N=50	UD						FGD						N=50	UD						FGD					
	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$
	NID	84617	29767	2.84	0.72	18	0.72	63426	29887	2.12	0.60	14	0.56	NID	198752	29781	6.67	0.99	40	0.95	175315	29852	5.87	0.98	31	0.86
	NIE	114893	29226	3.93	1	25	1	102382	29006	3.53	1	25	1	NIE	200044	29724	6.73	1	41	0.98	177548	29775	5.96	1	33	0.92
	NDS	114405	29160	3.92	0.99	25	1	101384	28824	3.52	0.99	25	1	NDS	187629	29546	6.35	0.94	42	1	145835	29379	4.96	0.83	36	1
	MNDS	114874	29241	3.93	0.99	25	1	102292	29045	3.52	0.99	25	1	MNDS	191528	29640	6.46	0.96	42	1	153743	29690	5.18	0.87	36	1
	RVS	114951	29453	3.90	0.99	25	1	102395	29046	3.53	1	25	1	RVS	194631	29812	6.53	0.97	42	1	161544	29764	5.43	0.91	36	1
	(c)													(d)												
	Same PMFs and $\sigma_D = \sigma_S$																									
	N=50	UD						FGD						N=500	UD						FGD					
	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$
	NID	43658	29573	1.48	0.84	12	0.67	72087	29891	2.41	0.83	13	0.54	NID	48344	29616	1.63	0.56	12	0.44	123999	29991	4.1345	0.4337	16	0.20
	NIE	51774	29445	1.76	1	17	0.94	86010	29615	2.90	1	21	0.88	NIE	86110	29589	2.91	1	25	0.93	285445	29940	9.5339	1.0000	66	0.84
	NDS	46053	28925	1.59	0.91	18	1	70843	28752	2.46	0.85	24	1	NDS	67820	29389	2.31	0.79	27	1	229768	29625	7.7559	0.8135	79	1
	MNDS	48246	29272	1.65	0.94	18	1	75548	29467	2.56	0.88	24	1	MNDS	70473	29486	2.39	0.82	27	1	236359	29846	7.9193	0.8306	79	1
	RVS	49946	29581	1.69	0.96	18	1	79741	29323	2.72	0.94	24	1	RVS	73382	29617	2.48	0.85	27	1	245104	29831	8.2164	0.8618	79	1
	(e)													(f)												
	Different PMFs and $\sigma_D = \sigma_S$													Small σ_D and σ_S $(S>D)$											
	N=50	UD	FGD					FGD	UD					N=50	UD						FGD					
	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$
	NID	42545	29832	1.43	0.82	16	0.67	46723	29596	1.58	0.92	15	0.71	NID	5877	27342	0.21	0.98	6	0.86	11627	28769	0.4042	0.97	7	0.78
	NIE	51300	29428	1.74	1	23	0.96	50450	29545	1.71	1	18	0.86	NIE	6320	28749	0.22	1	7	1	12058	28893	0.4173	1	8	0.89
	NDS	47948	29026	1.65	0.95	24	1	41187	29088	1.42	0.83	21	1	NDS	5245	28553	0.18	0.84	7	1	8628	28343	0.3044	0.73	9	1
	MNDS	49360	29310	1.68	0.97	24	1	44015	29530	1.49	0.87	21	1	MNDS	5652	28741	0.20	0.89	7	1	9863	28799	0.3425	0.82	9	1
	RVS	50426	29494	1.71	0.98	24	1	46098	29671	1.55	0.91	20	0.95	RVS	6182	29295	0.21	0.96	7	1	11152	28855	0.3865	0.93	8	0.89
	(g)													(h)												
>0		Small σ_D and large σ_S						Large σ_D and small σ_S						Large σ_D and σ_S												
	N=100	UD	FGD					FGD	UD					N=100	UD						FGD					
	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	scheme	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$	demand	surplus	η	$\bar{\eta}$	U	$\bar{U}$
	NID	114609	29946	3.83	0.83	48	0.73	219744	29864	7.36	0.99	82	0.93	NID	332154	29896	11.11	0.95	72	0.88	428280	29753	14.39	0.98	77	0.89
	NIE	135852	29616	4.59	1	64	0.97	221650	29724	7.46	1	85	0.97	NIE	345234	29573	11.67	1	79	0.96	437144	29388	14.87	1	83	0.95
	NDS	131288	29276	4.48	0.98	66	1	205716	29129	7.06	0.95	88	1	NDS	328022	28875	11.36	0.97	82	1	409186	27736	14.75	0.99	87	1
	MNDS	132806	29468	4.51	0.98	66	1	209898	29534	7.11	0.95	88	1	MNDS	332617	29272	11.36	0.97	82	1	416713	29076	14.33	0.96	87	1
	RVS	134936	29648	4.55	0.99	65	0.98	215536	29640	7.27	0.98	88	1	RVS	338486	29516	11.47	0.98	82	1	425492	28986	14.68	0.99	87	1
	(i)													(j)												

Figure 3.7 explicitly illustrates various PMFs and Table 3.1 summarizes the outcomes correspondingly.[10] One thousand experiments are run to average the results for each scenario. In each scenario, different widths of PMFs (determined by σ_D and σ_S) and (non)overlap between the two PMFs (determined by μ_D and μ_S) are presented. An ideal situation in which the efficiency of energy use is high for each household ($\eta \gg 1$) is mostly found in Figure 3.7(a), (c), and (d), whereas the opposite ($\eta \ll 1$) in Figure 3.7(h). Figure 3.7(e) and (f) consider a full overlap between the two PMFs while others test on partial overlaps. It can be determined from Table 3.1 when the NDS, MNDS, and RVS schemes are able to outperform NIE with respect to U. The first observation shows that the NID scheme has the worst performance in all cases; this is because NID disregards surplus values in favor of high demand values while accumulating demand values in descending order. Secondly, the NIE scheme obtains the highest cumulative demand values most of the time and can achieve as large U as NDS can in some conditions (e.g., Table 3.1(a), (c), and (h)); however, NIE cannot always achieve a large U due to the nonincreasing accumulation of energy efficiency, which is directly proportional to demand values, similar to NID. Examples can be found in Table 3.1(b), (d), (e), (f), and (g); larger σ_D and σ_S likely yield more combinations having the same or similar energy efficiency values.

Furthermore, $N = 100$ is set in the second simulation where only units with surpluses are considered for selection. Two scenarios are shown in Figure 3.7(i) and (j) and Table 3.1(i) and (j), and similar outcomes are also achieved. From the set of these two simulations, it is observed that a number of conditional factors must be satisfied in order for the proposed schemes to outperform NIE with respect to U: 1) both σ_D and σ_S are large,

[10]Note that in Table 3.1, $\overline{\eta}$ is the ratio of the energy efficiency of schemes (NID, NDS, MNDS, RVS) to that of NIE, and $\overline{U}$ is the ratio of the total number of connected units achieved in schemes (NID, NIE, MNDS, RVS) to that in NDS.

2) $\sigma_D \geq \sigma_S$, 3) σ_S cannot be too small, 4) there is a partial overlap between $f_D\,(P_D)$ and $f_S\,(P_S)$, and 5) κ must be small enough.

3.4.2 Analysis of Uplink Data Traffic Loads in the SMC Network

The environment for simulating the SMC network is developed under OPNET Modeler. A SMC network consisting of one UCC and 50 smart meters randomly placed in a 500×500 square meters area are constructed (as shown in Figure 3.8(a)). The IEEE 802.15.4 standard protocol for its wireless communications infrastructure is adopted; a ZigBee coordinator (used for UCC) and ZigBee routers (used for smart meters) with full functionalities are selected in order to form a mesh topology. The frequency band of 2.4GHz is chosen to support a data rate of up to 250kb/s depending on the distance between the devices up to 100 meters, as described in [132]. In the SMC network (presented in Section 3.2.2), each smart meter periodically transmits a data packet with its energy profile information to the UCC. The UCC has no packets to send back to smart meters until notification packets for disconnection are required. Since most of the data packets are involved in the upstream of the SMC during the selection process, the many-to-one upstream data traffic is only considered.

Three scenarios are developed in the simulation: the first scenario represents a default situation where periodic data transmission from smart meters to UCC always takes place even if some smart meters are disconnected from the grid; the second scenario assumes 25 smart meters are called to disconnect from the grid (therefore, stop data transmission), and the disconnected smart meters are assumed dispersed or balanced throughout the topology (shown in Figure 3.8(b)); the third scenario follows the second scenario except that the disconnected smart meters are concentrated mostly in one area (shown in Figure 3.8(c)).

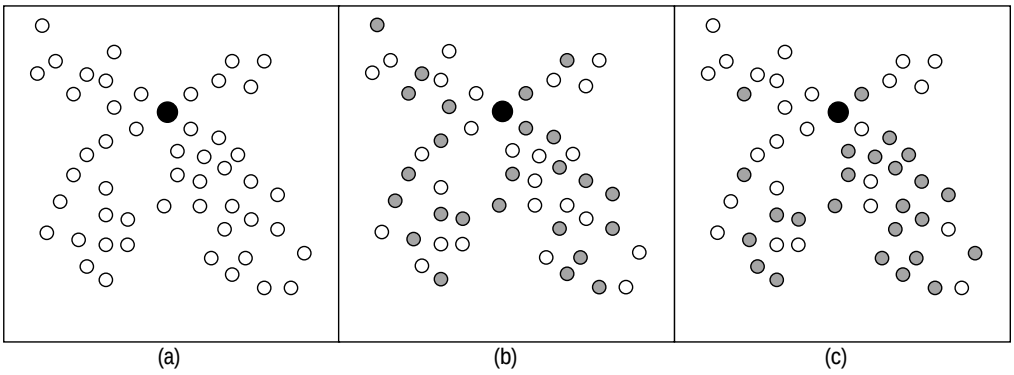


Figure 3.8 The simulated network topology in which the dark circle represents UCC whereas white/gray circles represent the connected/disconnected smart meters.

For each scenario, acknowledgement for data reception is activated and different sizes for data packets transmitted from smart meters to the UCC are tested: 500b, 1kb, and 2kb. Furthermore, each smart meter transmits a data packet to the UCC every 5 seconds and the simulation time lasts for an hour. A notification of disconnection is taken place at approximately $1,200$ second. From the simulation results as shown in Figure 3.9, the total data traffic is reduced by approximately 50% whereas E2E delay is reduced by $4\% - 8\%$; this is because the proposed algorithm halts the data transmission from the disconnected smart meters during the disconnection period. Note that the location of disconnected smart meters based on the selection process may affect the performance of data traffic and E2E delay. As observed from Figure 3.9, the topology of disconnected smart meters located in a concentrated region involves more data traffic (due to extra control bits) and larger E2E delay than that located in a dispersed manner.

3.5 Summary

In this chapter, power congestion in the electric power system is investigated. Congestion can occur in a traditional way due to variability of demands and intermittency of renewable

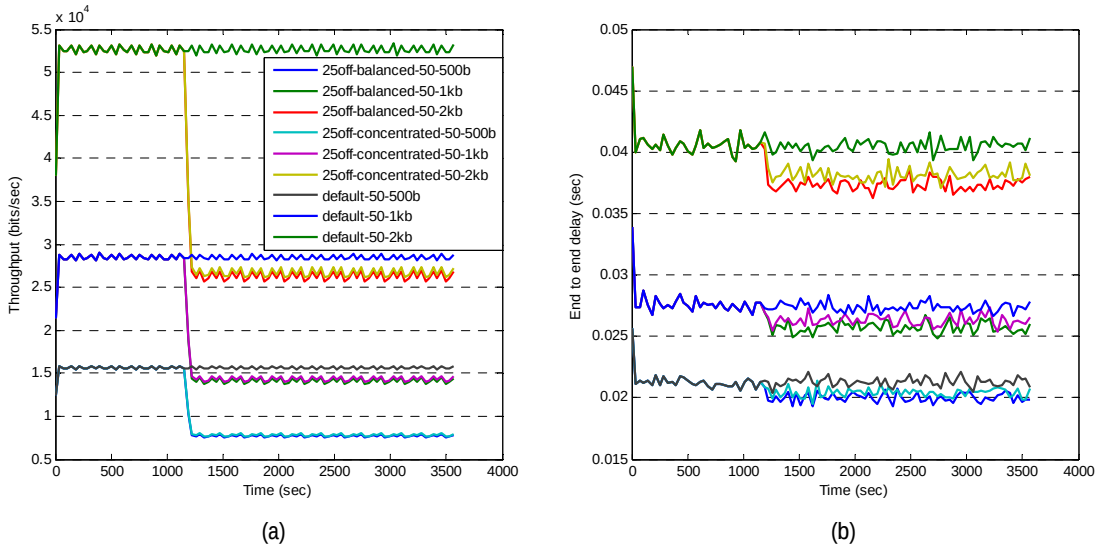


Figure 3.9 Involved data traffic (a) and global end-to-end delay (b) between the UCC and smart meters.

energy when network resources are limited. Similarly, local congestion is foreseen to exist in the distribution grid when the number of solar units in neighborhoods increases and when energy consumption is low. The solar surplus congestion in the distribution grid is formulated as one type of 0/1 knapsack problems and solved by greedy strategies. The objectives are achieved by maximizing the number of connected units on the grid as well as improving cumulative demand values subject to the power capacity constraint. Computation time of the selection algorithms as well as data traffic loads in the smart metering communications is taken into consideration. Extensive simulations have shown that the proposed algorithms for disconnecting solar units during the selection process have achieved the objectives. The proposed models for (dis/re)connection minimize computation time at the utility control center. The upstream data traffic via smart metering communications and corresponding end-to-end delay are also reduced based on the simulation results. The proposed schemes benefit utilities in both economic and technical terms.

CHAPTER 4

DECENTRALIZATION OF CONTROLS AND COMMUNICATIONS FOR DISTRIBUTION NETWORKS IN SMART GRID

4.1 Motivation

Traditional power congestion caused by rising energy generation and consumption (or loads) in the legacy electric power grid has encouraged utilities to implement DER units in the MV and LV distribution networks. The method of renewable-based distributed generation supporting local loads (e.g., households installed with PV solar systems) is foreseen to reduce power losses and improve reliability. Surpluses of power produced by DER units can be shared among households and delivered to the neighboring distribution networks [50, 49]. However, the power sharing incurs bidirectional flows in addition to the fact that the existing distribution networks were not designed to operate with bidirectional power flow. Several works to use loop techniques [69], power router interface [45], and inductive power transfer (IPT) technology [71] have been investigated to tackle flow of power, but none of them specified communications explicitly. The balance of power (i.e., power generation and loads to be balanced) which is one of the primary issues in the power system has been focused from centralized operations to decentralized coordination that emphasizes a desire for distribution automation in active control and management.

This chapter is structured as follows: Section 4.2 provides a typical power distribution system model for the investigation into the power network operation, and presents the development of an overlay communications network infrastructure for the active distribution network. Section 4.3 formulates the power balance problem and adopts

the graph theory tool[1] for solving the associated power flow issue in a residential network. Section 4.4 analyzes the simulation results of the proposed methodology and discusses the findings. Finally, Section 4.5 summarizes the focal points and draws a conclusion.

4.2 System Models

4.2.1 Autonomous Distribution Network (ADN)

A distribution network model (a modified model of [54]) is considered to investigate the operation of a power system, as shown in Figure 4.1. The model consists of *one* power source (which can be a group of conventional power plants) in the macro grid, *four* distribution networks, and *nine* buses (i.e., Bus 1-6, 8, 10, 14, depicted by the thick lines). Note that only the distribution network connected to Bus 4 is shown while other networks (which are connected to Bus 1-3) also possess the same structure properties for simplicity. The typical distribution network is composed of *eight* neighborhoods (i.e., Block 7, 9, 11-13 ,15-17), and each neighborhood which is constructed with *fifteen* households forms a MG.

Traditionally, power is generated by fuel-based power plants in remote locations, routed or switched through the HV transmission system, and delivered to the residential sites in the distribution network; power flow is unidirectional. With customers' capability to install DER units on their premises, contributing power back to the grid incurs bidirectional power flow in the power system. Each MG is a grid entity that sometimes can provide or absorb a range of real and reactive power to or from other MGs, before requesting

[1]Graph theory has been an useful tool applied in various fields such as computer science (task scheduling), sociology (social network), chemistry and physics (atoms topology), transportation (road network), power systems (grid operation), and communications (the Internet). In communications networks studies (including sensor networks), it is used to explicitly illustrate the relations among nodes in terms of communications connectivity. In this chapter, graph theory is used to analyze the distribution grid and associated power flow management.

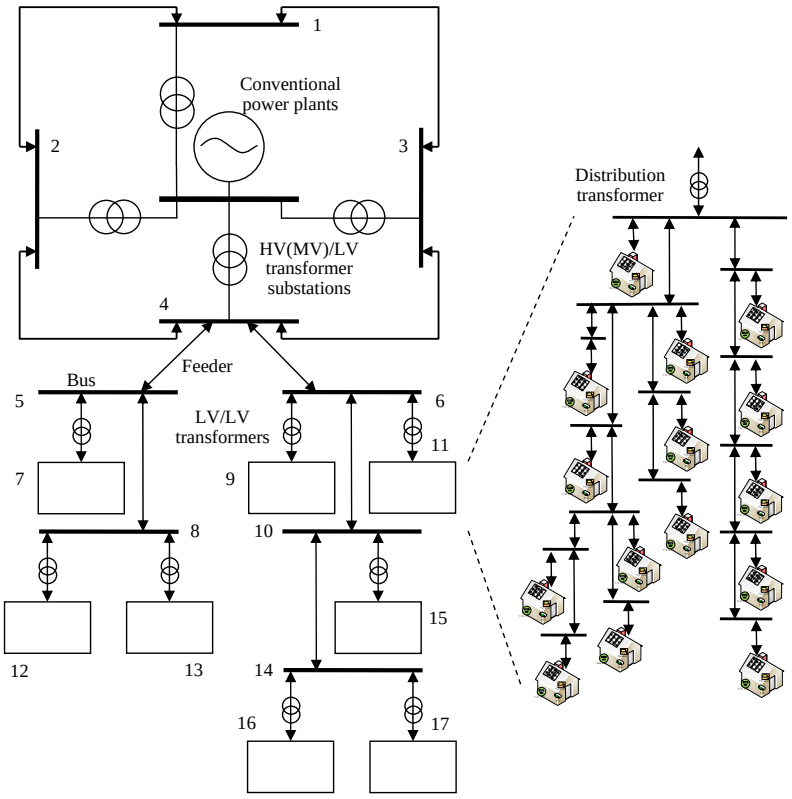


Figure 4.1 A systematic model for the power distribution system and associated residential network.

power from the macro grid. The overall distribution system can be interpreted by node representation from graph theory (shown in Figure 4.2a); each bus represents a node where power can be injected, extracted, or injected and extracted simultaneously by cumulative generation and loads during different time periods. Note that nodes 5, 6, 8, 10, 14 are not directly connected to households but to the associated residential networks.

Each distribution network is designed as a cluster, $\{c_1, c_2, \ldots, c_s\} \in C$, where $s = |C| = 4$ for the example shown in Figure 4.2. Cluster c_i, $i = 1, 2, .., s$, is partitioned into a number of groups, $\{g_1, g_2, \ldots, g_k\} \in c$, $\forall c \in C$, where $g_1 \cap g_2 \cap \ldots \cap g_k = \emptyset$ (i.e., groups are not overlapping), and all clusters are assumed to have the same group size k $(= 3)$. Each group, g_i, $i = 1, 2, .., k$, is composed of multiple MGs, $\{h_1, h_2, \ldots, h_j\} \in g$,

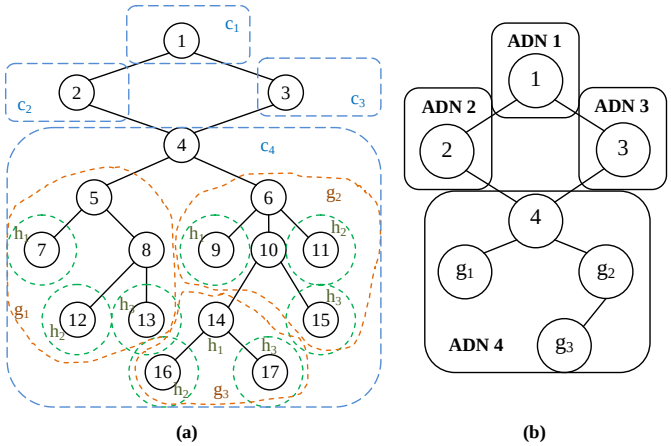


Figure 4.2 (a) A connected, undirected graph for the distribution system model in Figure 4.1, and (b) contraction of the graph and formation of ADNs.

$\forall g \in c$. All groups are assumed to have the same MG size j except the third group ($i = 3$) which has MG size $j - 1$; from the given example, MG 7, 12, 13 are merged into Group g_1; MG 9, 11, 15 are merged into Group g_2; and MG 16, 17 are merged into Group g_3. The grouping method assumes that each distribution transformer in residential networks is connected to the same number of households; meanwhile, for the network balancing purpose, the number of MGs in each group is kept the same as much as possible. The balance of power in the power system can be interpreted as follows:

$$P = \sum_{c \in C} P_c + P_{GEN} + P_{LOSS} \approx 0 \tag{4.1}$$

where $P_c \in \mathbb{Z}$, $\forall c \in C$, is the output power of cluster c, P_{GEN} is the total power generated in the macro grid and delivered to the clusters, and P_{LOSS} is the total power loss during power transmission. Since power sharing is possible among MGs [52, 49], it is also possible among groups as well as among clusters. In this way, renewable energy production can be utilized whenever it is available through power sharing among entities in order to minimize the amount of power requested from the macro grid, i.e., $P_{GEN} = 0$; this

can be done by effectively controlling the output power P_c as much as possible subject to P_{LOSS}, which is not considered in this dissertation. The output power of cluster c is the summation of the output power of groups, $P_c = \sum_{i=1}^{k} P_{g_i}$, $\forall c \in C$; the output power of each group g is the summation of the output power of MGs, $P_g = \sum_{i=1}^{j} P_{h_i}$, $\forall g \in c$, $P_g \in \mathbb{Z}$; the output power of each MG h is the summation of the output power of households, $P_h = \sum_{i=1}^{n} P_{v_i}$, $\forall h \in g$, $P_h, P_v \in \mathbb{Z}$, where $\{v_1, v_2, \ldots, v_n\} \in V_h$, $\forall h \in g$ denote the buses connected with associated households in the residential networks. Note that each MG is assumed to have the same household size n, as mentioned earlier. Consequently, Figure 4.2a can be coarsened to the graph shown in Figure 4.2b where each decentralized group governs its voltage control and power flow in its corresponding cluster. The non-overlapping groups constitute an ADN, which is able to perform power control management internally and interact with neighboring ADNs externally to sell or buy renewable power before requesting power from the conventional power pants.

4.2.2 Overlay Communications Network Infrastructure (OCNI)

It is assumed that *power nodes* with communications interfaces (e.g., smart meters with PV inverters, circuit breakers, line sensors, convertors, voltage regulators, capacitor banks) in MGs are strategically deployed in positions so that their connectivity is ensured; relay nodes are placed to mitigate constraints such as transceivers' transmit-power level, MAC (medium access control), and routing issues [56, 135]. The positions of nodes in the system are fixed, and therefore the OCNI model for the power system is developed practically based on its underlying power network to facilitate both power flow and communications traffic management.

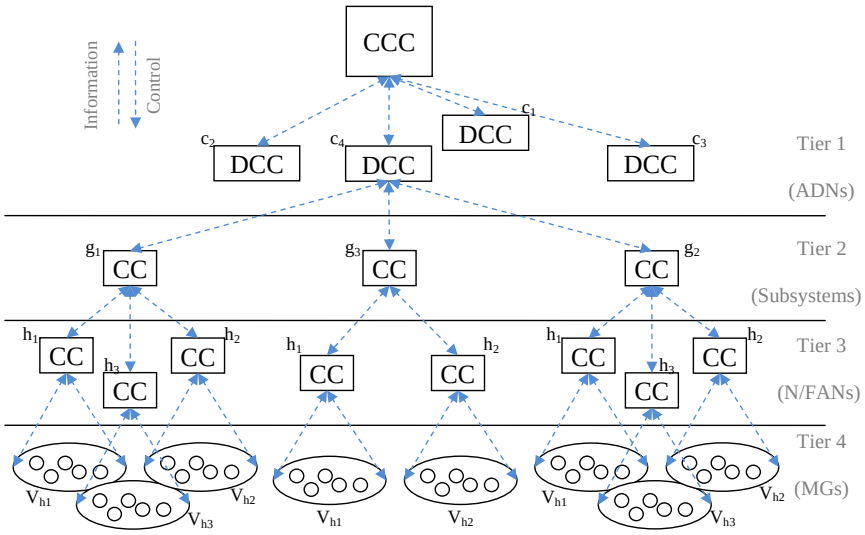


Figure 4.3 The four-tier communications infrastructure for the ADN.

The OCNI model, illustrated in Figure 4.3, is structured into *four* tiers (from the bottom to the top): 1) entire households grouped into a number of MGs at Tier 4, 2) sets of MGs forming neighborhood/field area networks (N/FANs) such that each MG belongs to a corresponding control center (CC) at Tier 3, 3) coupled or consolidated MGs managed by an associated subsystem CC at Tier 2, and 4) overall ADNs at Tier 1 such that each ADN consisting of a number of subsystems is under control of its distribution control center (DCC). The CCs at Tier 2 and 3 govern the corresponding networks below them. The DCCs owned by distribution system operators (DSOs) at Tier 1 monitor and control power flow for the corresponding ADNs. The central control center (CCC) owned by transmission system operators (TSOs) in the transmission network is in charge of delivering power to the distribution system upon ADNs' requests. Power nodes at Tier 4 are associated with the CCs at Tier 3 (using WSNs based on IEEE 802.15.4) via one-hop or multi-hop transmissions; the CCs at Tier 3 are associated with the CCs at Tier 2 using technologies such as 3G and WiFi; and the CCs at Tier 2 are associated with the DCCs at Tier 1 using

technologies such as 4G and fiber optics, as well as communications between the DCCs and CCC using broadband technologies.

The operation of each ADN is to collect voltage profile and associated data measurements from the power nodes at Tier 4, and deliver this data information through *uplink* transmission to the CCs at the upper tiers for the local power flow analysis. In the *downlink*, the associated CCs send control signals to the power nodes to adjust power output in order to optimize the network resources while maintaining the system reliability. Since the size of data packet generated by the power nodes is relatively small (e.g., tens to few hundreds of bytes), using aggregation technique can improve bandwidth utilization at upper tiers. In MGs at Tier 4, fast control of individual power units requires real-time and detailed information on DERs and loads. Fortunately, the study [12] has demonstrated that the control complexity can be greatly reduced when using coupled MGs: 1) a system consisting of many MGs does not need fast communication, and 2) redispatching power among MGs does not need detailed information on individual power units for the corresponding communications systems to deliver. Therefore, the hierarchical OCNI with the grouping technique for ADNs can potentially simplify control complexity and economize communications bandwidth at the upper tiers; this benefits both power control and communications management.

4.3 Problem Definition and Formulation

Bidirectional power flow due to renewable power generation contributed from the residential networks requires an effective mechanism to manage power flow in the distribution system, in which the system reliability is maintained, and at the same time instant renewable production is consumed in order to maximize energy utilization.

Balancing power generation and loads is the fundamental rule to stabilize the power system, i.e., the quantity of total generation matches that of total loads. Hence, the objective is to balance Equation 4.1, which is rewritten as $P = \sum_{c \in C} P_c \approx 0$; that is, only balancing the energy generated by households is focused in the problem while the power loss is assumed negligible as mentioned earlier. Energy from macro grid is ignored so that renewable power sharing within MGs, among MGs in a group, among groups, and among ADNs is prioritized in the bottom-up order, to balance the power distribution system whenever possible.

Determination of the cumulative output power of an ADN at Tier 1 (shown in Figure 4.3) is first to discover the cumulative output power of MGs at Tier 4, i.e., P_h, $\forall h \in g$. Given the residential network for every MG as depicted in Figure 4.1, the network topology can be interpreted by using node representation (shown in Figure 4.4): a connected, undirected tree graph $G = (V, E)$ with a set of vertices $v_1, v_2, \ldots, v_n \in V$ and a set of edges E. The vertices represent buses, and edges represent line feeders between two buses. Each household has a smart meter installed with a grid-tie PV system mounted on the rooftop. Each PV unit generates a certain amount of power (in kW) during a certain time period based on sun radiation[2]. When the amount of generated power is sufficient to support its household's load, there is either a surplus or no surplus to flow into the bus. On the other hand, when PV generation is insufficient to support its household's load, power is drawn from the bus. Hence, each vertex (bus) is injected or extracted with positive or negative power $P_{v_i} \in \mathbb{Z}$, respectively, by household v_i. During different time periods,

[2]The stochastic nature of renewable energy production may be tackled by means of historical data and smart inverters. Meanwhile, it can also be traced by periodic data collection and coordination via communications; the more frequent the data are collected, the more accurate the status is obtained, but the more the traffic is generated and conveyed in the network.

household v_i can be a generating or consuming unit; household v_i can also be an idle unit when its generation and load are balanced. Note that power is injected to the bus with PV generation that is unused by a household; the term *generation* refers to *surplus* power instead of purely total generation. For a connected, tree digraph G, each edge is an ordered pair (v, w) of vertices.

Definition 1. *A forward directed edge, edge* (w, v)*, refers to the forward flow from* w *to* v*. Furthermore, the directed edge, edge* (v, w)*, also refers to the reverse flow of edge* (w, v)*, e.g., edge* (v_1, v_2) *represents a forward flow whereas edge* (v_2, v_1) *represents a reverse flow of edge* (v_1, v_2) *as per Figure 4.4.*

Definition 2. *A graph contains a set of parent vertices* $w_1, w_2, \ldots, w_l \in W \subset V$*, e.g.,* $w(v_4) = w(v_5) = w(v_6) = v_2$ *as per Figure 4.4.*

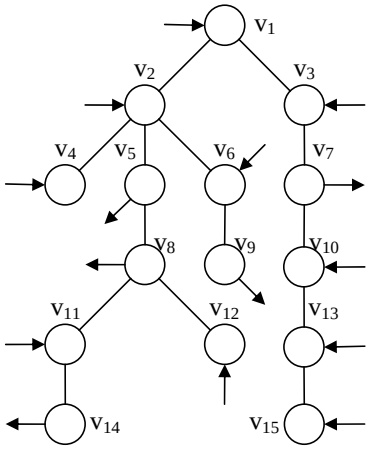
Definition 3. *The capacity of edge* (v, w)*,* $cap(v, w)$*, is a mapping,* $cap : E \to \mathbb{N} \backslash \{0\}$*, which represents the maximum amount of flows that can pass through edge* (v, w) *and is a positive integer.*

For a feasible flow $f : E \to \mathbb{N}$, the following three types of constraints must be obeyed [136]:

$$f(v, w) \leq cap(v, w), \quad \forall (v, w) \in E \tag{4.2}$$

$$\sum_{(w,v)\in E} f(w, v) = \sum_{(v,w)\in E} f(v, w), \quad \forall v \in V \tag{4.3}$$

$$f(v, w) \geq 0, \quad \forall (v, w) \in E \tag{4.4}$$



(a)

Input				Output	
V^T	D^T	W^T	P_V^T (kW)	E	$f(v,w)$ (kW)
v_1	1	v_0	6	(v_1,v_0)	24
v_2	2	v_1	2	(v_2,v_1)	7
v_3	2	v_1	1	(v_3,v_1)	11
v_4	3	v_2	3	(v_4,v_2)	3
v_5	3	v_2	-1	--	0
v_6	3	v_2	4	(v_6,v_2)	2
v_7	3	v_3	-3	(v_7,v_3)	10
v_8	4	v_5	-6	(v_8,v_5)	1
v_9	4	v_6	-2	(v_6,v_9)	2
v_{10}	4	v_7	6	(v_{10},v_7)	13
v_{11}	5	v_8	8	(v_{11},v_8)	4
v_{12}	5	v_8	3	(v_{12},v_8)	3
v_{13}	5	v_{10}	5	(v_{13},v_{10})	7
v_{14}	6	v_{11}	-4	(v_{11},v_{14})	4
v_{15}	6	v_{13}	2	(v_{15},v_{13})	2

(b)

Figure 4.4 (a) A connected, undirected graph for the residential network model in Figure 4.1 with a set of injection of power generation and extraction of power loads, and (b) the digraph information table.

Constraint 4.2 specifies the *capacity limit* of edge (v, w) where the amount of power delivered during a certain time period from vertex v to vertex w is subject to the capacity of distribution line feeders. When generated power to be delivered for the nodes in need is greater than the line can hold, some power may not be delivered. Constraint 4.3 introduces *conservation of flows* such that accumulated power flow into vertex v is equal to the amount of power flow out of vertex v. Finally, Constraint 4.4 is to satisfy the *nonnegativity* requirement such that the value of flow must be nonnegative regardless of the flow direction.

4.3.1 Assumptions

Without loss of generality, a list of primary assumptions are considered:

- Renewable energy is sufficient in the distribution network during daylight with high penetration of PV systems, especially in the summer season and when consumption is low in some regions.

- No large energy storage is available; when renewable energy is produced, it needs to be consumed immediately for high energy utilization.
- No reverse power flows back to the transmission grid.
- Voltage, current, frequency for active and reactive power are managed via coordination by means of control and communications.
- Distance among households is small enough such that power loss in transmission can be neglected or tolerated.
- Power flow delivered along the feeders is always under the transfer capacity; power congestion is not considered in this chapter.

4.3.2 Macro Grid Power and Micro Grid Renewable Power Flows throughout the ADN: Control Of Power flow dirEction (COPE)

In normal operation, power flows from a higher to a lower voltage level, as in the conventional passive power network from HV transmission to MV/LV distribution. Similar to the active distribution network, the variability of PV generation and loads will fluctuate the voltage profiles of MGs. As an example illustrated in Figure 4.4, some have positive power (available surplus) injected into the node while others have negative power (loads) extracted from the node. Note that v_0 (which is not shown in Figure 4.4) may refer to node $5, 6, 8, 10, 14$. In this example, the cumulative output power is 24 (without considering power loss) which is realized by collecting the measured data from the power nodes at the instant via communications; the surplus induced by the cumulative output power at v_1 should be exported to other MGs. However, power may flow in a direction which is not preferred due to power laws. For instance, one power unit injected into v_3 can compensate for the load at v_7 that results in a forward direction. Similar to v_2, output power 2 can compensate for the load at v_5 causing another forward direction. Without global

information on each node, the system resource cannot be efficiently utilized. Therefore, it is necessary to determine how power should flow so that the utilization of energy is enhanced and system reliability is ensured; meanwhile, some voltage control algorithms using reactive power regulation proposed in power engineering research can be used to support the proposed design, e.g., [49, 50, 52, 53].

In order to control the power flow given graph properties, a *bottom-up* approach is proposed to first determine the *depth* information (denoted by $D = (1, 2, \ldots, d)$) of the tree and begin with the nodes with the largest depth d, i.e., the leaf nodes. In the right branch of the given example, v_{15} has positive power of 2, which should be flowed in a reverse direction, i.e., from v_{15} to v_{13}. The cumulative output power of v_{13} is a summation of reverse power from v_{15} and power generation by the associated household. Similarly, in the left branch, v_{14} has negative power of 4 that requires its parent v_{11} to support its load in a forward direction, while v_{11} compensates its residual power of 4 for the load at v_8. The process is repeated until the cumulative output of v_1 is derived. Note that power is balanced at v_5, and v_3 has an aggregate of power 11 flowed in a reverse direction to v_1; these result in different outcomes than what was discussed above. The proposed scheme COPE is shown in Algorithm 4, which is operated in each MG in parallel at Tier 4 as well as applied to operations at the upper tiers.

Theorem 1. *Given a radial tree-like topology G, the proposed bottom-up approach for calculating the paths of power flow is the shortest path.*

Proof. The directed distance from a vertex u to a vertex v in a tree digraph is the length of the shortest directed walk from u to v. Since the digraph G contains no loops, the power

flow from each vertex passes through or flows into other vertices at most once. Therefore, the shortest path is obtained. □

Algorithm 4 Control Of Power flow dirEction (COPE)

1: *Initiation*: Perform breadth-first search or depth-first search to obtain the characteristics of an undirected graph G.
2: *Input*: A table containing $(V^{\mathsf{T}}, D^{\mathsf{T}}, W^{\mathsf{T}}, P_V^{\mathsf{T}})$ information is sorted in descending order of D^{T}, where $(.)^{\mathsf{T}}$ is the transpose of $(.)$.
3: *Output*: A digraph G presenting the direction and amount of power flow, i.e., E and $f(v, w)$.
4: $P_{W(V[n])} = 0$
5: **for** $\forall v \in V$ **do**
6: $\quad P_{W(V[i])} \leftarrow P_{V[i]} + P_{W(V[i])}$
7: $\quad$ **if** $P_{V[i]} > 0$ **then**
8: $\quad\quad f\left(V\left[i\right], W\left(V\left[i\right]\right)\right) = P_{V[i]}$ ▷ reverse flow
9: $\quad\quad E \leftarrow \left(V\left[i\right], W\left(V\left[i\right]\right)\right)$
10: $\quad$ **end if**
11: $\quad$ **if** $P_{V[i]} < 0$ **then**
12: $\quad\quad f\left(W\left(V\left[i\right]\right), V\left[i\right]\right) = P_{V[i]}$ ▷ forward flow
13: $\quad\quad E \leftarrow \left(W\left(V\left[i\right]\right), V\left[i\right]\right)$
14: $\quad$ **end if**
15: **end for**

The given example shows an unbalanced situation in a MG ($P_h > 0$); a reduction in power injection is required by increasing households' loads, e.g., using heat pump water

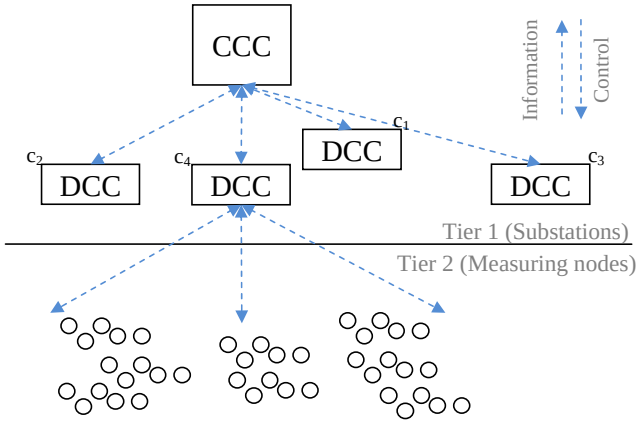


Figure 4.5 The two-tier communications infrastructure for the conventional distribution network in contrast to Figure 4.3.

heaters to store thermal energy [51]. Conversely, when a MG has greater consumption than generated solar power ($P_h < 0$), solutions such as demand response and conservation programs introduced in smart grid applications can be applied, e.g., raising energy costs and delaying appliances operations. For market business and utility operation reasons, importing or exporting renewable power from or to other regions can be done by using the proposed power sharing scheme in descending order of the tier number throughout the ADNs.

4.3.3 Uplink and Downlink Data Traffic across the OCNI: Power Control and Communications (PCC)

The Centralized Scheme. Traditionally, power systems are regulated under a two-tier hierarchical master-slave architecture, similar to the organization illustrated in Figure 4.5. System control devices such as remote terminal units (RTUs) located at Tier 2 act as slave data concentrators and periodically report their measurements (on relays, current, breakers) via a hard-wired connection to a master RTU along with associated DCC at Tier 1 [68]. According to Little's Theorem [137], if a total set of RTUs $\mathcal{M}$ generate average traffic at a

rate of $\overline{\lambda}_{\mathcal{M}}$ and an additional set of emerging smart meters $\mathcal{V}$ generate average traffic at a rate of $\overline{\lambda}_{\mathcal{V}}$, the overall system throughput is derived as $L = L_{\mathcal{M}} + L_{\mathcal{V}}$, where $L_{\mathcal{M}} = \overline{\lambda}_{\mathcal{M}}\mathcal{M}$ and $L_{\mathcal{V}} = \overline{\lambda}_{\mathcal{V}}\mathcal{V}$; the single DCC will be required to upgrade its processing capacity in order to accommodate the aggregate traffic of the measuring nodes (N=$\mathcal{M}$+$\mathcal{V}$). For example, if the execution time of an operation for power quantity analysis of the DCC takes t_{proc} seconds on average, the DCC cannot process more than $1/t_{proc}$ operations/sec in the long run, i.e., $L_a \leq 1/t_{proc}$; the maximum attainable throughput L_a is an upper bound determined by the processing capacity of the DCC that could queue up the unprocessed operations and cause the system to enter an unsteady state when $L > L_a$.

In addition to the processing time t_{proc}, considering other delay factors that compose the overall end-to-end delay T spent in a data communications network system is also critical: $T=(t_{trans}+t_{prop}+t_{proc}+t_{queu})\chi$, where t_{trans} is the transmission delay, t_{prop} is the propagation delay, t_{queu} is the queuing delay, and χ is the number of hops in a multi-hop network environment. Despite the fact that the centralization of legacy operation allows the DCC to obtain a global knowledge of its corresponding distribution network status at each certain time period, it can degrade the system performance due to the limitation of L_a and the requirement of T being directly proportional to N, as well as single-point failures. The centralized scheme is essentially delivering *fine-grained* information from each individual measuring node to the DCC due to the simplicity of legacy one-way power delivery architecture.

The Decentralized Approach. In order to relieve the computational complexity and bandwidth capacity at the DCC, decentralization of power-communications operations in OCNI is proposed to achieve a number of merits: 1) *local processing for quick decision making*: a set of sub-CCs are added in the middle tiers as multi-agent coordinators in

order to perform local power flow optimization at both LV (e.g., $240/120$V at Tier 3) and MV/LV (e.g., $26/13/4$kV at Tier 2) levels to obtain global optimization, 2) *end-to-end delay reduction*: the addition of sub-CCs decreases the distances between the power nodes and operation centers to operate power sharing by cooperatively compensating for power within and among MGs, 3) *traffic load deduction*: a) when power balance can be fulfilled at one tier, transmitting data to upper tiers is not necessary (unless the upper-tier CCs request it for other purposes), and b) the original amount of data containing detailed information on the power nodes is not required to be transmitted completely to the upper-tier CCs when power sharing among MGs and ADNs is activated, and 4) *scalable*: the network scalability does not have to depend upon the quantity of power nodes but upon the scale of added sub-CCs at Tier 3 and Tier 2 from the entire distribution network perspective. In contrast to the centralized scheme, the multi-tier OCNI for ADNs is designed to mitigate heavy traffic loads by means of *coarse-grained* information delivered in the uplink transmission:

$$\alpha_i = \frac{L_{i\_(i-1)}}{L_{(i+1)\_i}}, \quad i \in \{1, 2, 3\} \tag{4.5}$$

where α_i is the *abstraction* ratio which depends on the operation requirement of the CCs at Tier i (i.e., $0 < \alpha_i \leq 1$); $L_{(i+1)\_i}$ is the total amount of data received from Tier $(i+1)$, and $L_{i\_(i-1)}$ is the amount of data to be transmitted to the CC at Tier $(i-1)$. For example, in the process of power balancing, the CC at Tier 3 will need to acquire L_{4_3} amount of data from its associated power nodes in the MG in order to have a local knowledge of the network status while performing its operation. When the support of power sharing with neighboring MGs is required (either power import or export), the CC at Tier 3 will contact the associated CC at Tier 2 by sending correlated information regarding its lower-tier network condition with its L_{3_2} amount of data, which is usually smaller than what it received, i.e., $L_{3\_2} <$

L_{4_3}; this is because the Tier-2 CC does not need to know everything about the network condition of Tier-3 fully supervised by the Tier-3 CC, and interestingly, it may be possible for the Tier-3 CC to send only a notification message (even abstract data are not required) to the Tier-2 CC indicating how much power in total it has to export/import to/from the other MGs in order to support its power balance. The methodology of PCC is illustrated in Algorithm 5.

Data traffic loads in both uplink and downlink transmission involved at each tier of the distribution network are investigated. At a given time period, the uplink traffic loads performing information collection and downlink traffic loads administering control processes (which are often broadcasts in nature) are described in Table 4.1 and Table 4.2, respectively.

4.4 Simulations and Results

Performance of the proposed OCNI design in comparison with that of the traditional system operation by considering the four cases are investigated, as shown in Table 4.3. In reality, on the one hand the amount of data traffic in the network can be reduced by the intermediate aggregation or concentration nodes to improve payload efficiencies for the small packets generated by the measuring devices; on the other hand, the traffic can also be escalated by necessary retransmissions due to signal interference and packet collisions especially in unscalable and crowded network environments. The goals here are to discriminate the outcomes between the proposed OCNI and the legacy operation, as well as to demonstrate that the methodology aims to alleviate abundant data transmissions across the distribution network in the context of smart grid applications.

Algorithm 5 Power Control and Communications (PCC) in ADNs

Require: All units are connected to the grid (in both power and communications perspectives).

Ensure: Periodic uplink and downlink data transmission between Tier 4 and Tier 3.

while unbalanced power is discovered in a MG **do**
  if solutions provided in Sec. 4.3.2 mitigate the problem **then**
    Power control and data communications remain in Tier 4 and Tier 3.
  else[solutions do not effectively work]
    Power sharing with other MGs is necessary, and communications with CC at Tier 2 takes place.
    if unbalanced problem is still unsolved **then**
      Power sharing with other groups is necessary, and communications with DCC at Tier 1 takes place.
      if unbalanced problem still remains **then**
        Power sharing with other ADNs is necessary, and communications with CCC takes place.
        Power from macro grid is granted if needed; otherwise, disconnecting PV systems is required.
      end if
    end if
  end if
end while

Table 4.1 Description of Presumptive Traffic Loads via **Uplink Transmissions** between Adjacent Tiers in OCNI

Tier Index	Amount of Traffic Load	Description
4 to 3	$L_{4\_3} = \overline{\lambda}_{N_h} N_h,$ $\forall h \in g,$ $\forall g \in c, \forall c \in C$	This is where the fundamental power control and communications operations take place while each MG is governed by its associated Tier-3 CC simultaneously to monitor and control power flow individually. The number of households $\lvert V_h \rvert$ and other nodes M_h (e.g., sensors along the feeders) that make the total power nodes $N_h = \lvert V_h \rvert + M_h$ in the corresponding MG are considered; the expected traffic arrival rate of these nodes is $\overline{\lambda}_{N_h}$.
3 to 2	$L_{3\_2} = \alpha_3 \sum_{j=1}^{\lvert g \rvert} \left(\overline{\lambda}_{N_{h_j}} N_{h_j} \right) +$ $+ \overline{\lambda}_{M_g} M_g, \forall g \in c, \forall c \in C$	This is where an aggregate of data traffic is collected from Tier-3 CCs and other measuring nodes M_g in the corresponding group. The Tier-3 CCs will generate abstract data containing sufficient information on $\lvert g \rvert$ MGs status with α_3 and transmit to the corresponding CC at Tier 2.
2 to 1	$L_{2\_1} = \alpha_2 \sum_{k=1}^{\lvert c \rvert} L_{3\_2,k} +$ $+ \overline{\lambda}_{M_c} M_c, \forall c \in C$	Similar to the above, an aggregate of data traffic is collected from Tier-2 CCs and other measuring nodes M_c in the corresponding ADN. The Tier-2 CCs will generate abstract data containing sufficient information on $\lvert c \rvert$ groups status with α_2 and transmit to the corresponding DCC.
1	$L_{1\_ccc} = \alpha_1 \sum_{s=1}^{\lvert C \rvert} L_{2\_1,s}$	Similar to the above, an aggregate of data traffic is collected from Tier-1 DCCs. The Tier-1 DCCs will generate abstract data containing sufficient information on $\lvert C \rvert$ ADNs status with α_1 and transmit to the CCC.

Table 4.2 Description of Presumptive Traffic Loads via **Downlink Transmissions** between Adjacent Tiers in OCNI

Tier Index	Amount of Traffic Load	Description
3 to 4	$L_{3\_4} = \overline{\lambda}_{3\_4} N_h,$ $\forall h \in g, \forall g \in c, \forall c \in C$	The fundamental level requires the CCs of N/FANs to send control messages to all the power nodes in the corresponding MGs; the expected traffic arrival rate of the CCs is $\overline{\lambda}_{3\_4}$.
2 to 3	$L_{2\_3} = \overline{\lambda}_{2\_3} \left(\|g\| + M_g\right),$ $\forall g \in c, \forall c \in C$	Similar to the above, the CCs of subsystems send control messages to all the CCs and other measuring nodes M_g in the corresponding N/FANs with the expected traffic arrival rate $\overline{\lambda}_{2\_3}$.
1 to 2	$L_{1\_2} = \overline{\lambda}_{1\_2} \left(\|c\| + M_c\right),$ $\forall c \in C$	Similar to the above, the DCCs of ADNs send control messages to all the CCs and other measuring nodes M_c in the corresponding subsystems with the expected traffic arrival rate $\overline{\lambda}_{1\_2}$.
1	$L_{ccc\_1} = \overline{\lambda}_{ccc\_1} \|C\|$	Similar to the above, the CCC sends control messages to all the DCCs with the expected traffic arrival rate $\overline{\lambda}_{ccc\_1}$.

Table 4.3 Data Traffic for Power Balance Conveyed in the **Decentralized** (OCNI) and **Centralized** (Cen.) Operations

Scheme	Case	Total Amount of Traffic	Description
OCNI	1	$L_{4\_3} + L_{3\_4}$	Power balance (PB) is possible within MGs.
	2	$L_{3\_2} + L_{2\_3} + L_{3\_4} \|g\|$	PB is not possible within MGs, but possible among MGs in N/FANs.
	3	$L_{2\_1} + L_{1\_2} + (L_{2\_3} + + L_{3\_4} \|g\|) \|c\|$	PB is neither possible within MGs nor in N/FANs, but possible among groups in subsystems.
	4	$L_{1\_ccc} + L_{ccc\_1} + [L_{1\_2} + + (L_{2\_3} + L_{3\_4} \|g\|) \|c\|] \|C\|$	PB is not possible within MGs, N/FANs, subsystems, but possible among ADNs; if not possible among ADNs, either macro grid power or PV unit disconnection is required.
Cen.	–	$(\overline{\lambda}_{\mathcal{M}} \mathcal{M} + \overline{\lambda}_{\mathcal{V}} \mathcal{V}) + + \overline{\lambda}_{cen} (\mathcal{M} + \mathcal{V})$	PB is performed throughout the distribution networks with DCCs. $\mathcal{M} = \sum_{k=1}^{\|c\|} M_{g_k} + \sum_{s=1}^{\|C\|} M_{c_s}, \forall g \in c, \forall c \in C$ and $\mathcal{V} = \sum_{\forall h \in g, \forall g \in c, \forall c \in C} (V_h + M_h)$.

4.4.1 Traffic Loads Disseminated between Adjacent Tiers in Accordance with Power Dynamics

In the simulations, the average data traffic of each power node transmitted in uplink is set identical, i.e., $\overline{\lambda}_{N_h} = \overline{\lambda}_{M_g} = \overline{\lambda}_{M_c} = \overline{\lambda}_{\mathcal{V}} = \overline{\lambda}_{\mathcal{M}} = 160$bps; the average control traffic of each CC responded in downlink is also set identical, i.e., $\overline{\lambda}_{3_4} = \overline{\lambda}_{2_3} = \overline{\lambda}_{1_2} = \overline{\lambda}_{ccc_1} = \overline{\lambda}_{cen} = 80$bps; the number of the measuring nodes M_g and M_c in the corresponding N/FAN and subsystem are set to 50 and 100, respectively. All the CCs at the same tier are assumed to apply the same α. Three demonstrations are undertaken to quantitatively analyze the outcomes of adjusting the abstraction ratios and the number of power nodes in the MGs while determining the amount of traffic involved at each tier categorized into cases: 1) $N_h = 100$ and $\alpha = 0.2, 0.6, 1$ in which all of CCs in the network operate with the same abstraction ratio, e.g., $\alpha_3 = \alpha_2 = \alpha_1 = 0.2$ in Figure 4.6a; 2) $N_h = 500$ and CCs at different tiers have distinct α values for their operations (Figure 4.6b); and 3) $N_h = 500, 1000, 2000$ while $\alpha_3 = \alpha_2 = \alpha_1 = 0.6$ (Figure 4.6c).

It is discovered that balancing power flow via coordination within each MG in parallel shown in case 1 generates the least traffic loads, whereas case 4 conveys the most traffic throughout the network because power balance cannot be achieved at the lower tiers and requires involvement of CCs at the upper tiers to resolve the problem; meanwhile, the legacy centralized scheme demands all the data transmission and traffic in order to perform its power flow management. In Figure 4.6a, if the upper-tier CCs are able to manage the unbalanced network with much less information (interpreted by smaller α) received from the lower-tier CCs, much more data traffic can be reduced; conversely, if fine-grained information (interpreted by $\alpha = 1$) is desired for the upper-tier CCs to do the job, the

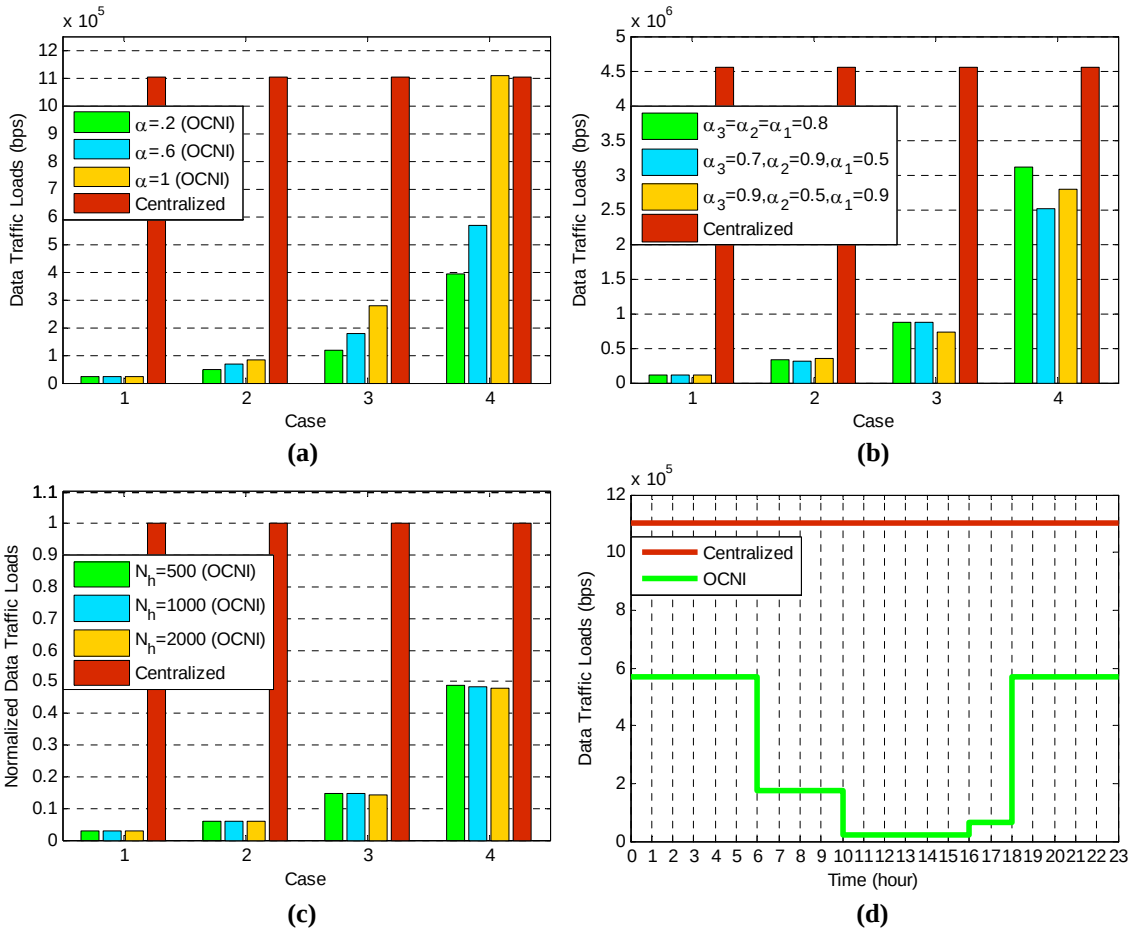


Figure 4.6 Analysis of data traffic under OCNI and legacy system when (a) coarse-grained information is applied, (b) abstraction values are varying, (c) quantity of power nodes in a MG is varying, and (d) both operations are tested throughout the day.

traffic loads considered in case 4 will reach approximately the same amount produced by the centralized scheme.

More interestingly, applying different α at CCs of different tiers has great impacts on the amount of traffic loads traversed at the upper tiers. Given the same amount of measuring nodes and traffic arrival rates in the network, Figure 4.6b shows that the mid-gray line is greater than the dark-gray line in case 3, but they become opposite in case 4; this is because the DCC requires most of information its lower-tier CCs have in hand while the CCC only needs information from the DCCs to a certain degree in the case of $\alpha_2 = 0.9, \alpha_1 = 0.5$,

whereas the dark-gray line depicts the opposite case. It is further noticed that an increase in the number of power nodes of MGs barely changes the normalized rates of data traffic loads among the four cases because the aggregate data rate is directly proportional to the number of nodes, given the fixed traffic arrival rates and abstraction ratios, as illustrated in Figure 4.6c. In summary, the demerits of the decentralized OCNI operation are twofold: 1) CCs at Tier 3 only have their own local network knowledge while other CCs at upper tiers may have limited knowledge of the lower-tier network, and 2) OCNI may generate more traffic than the centralized scheme owing to the negotiation messages exchange among CCs, when case 4 is taken place (i.e., contacting CCC is required) and the abstraction ratio is 1 (i.e., fine-grained information is required, see case 4 in Figure 4.6a). Nevertheless, OCNI is able to efficiently control the traffic of data loads based on its underlying power operation from LV to MV/LV levels in terms of network delay, and at the same time the amount of uplink data traffic will be essentially determined by 1) how often data are collected from the measuring nodes so that the granularity of content collection is satisfied in order to maintain the system reliability, 2) the volume of information of the lower-tier CCs required by the upper-tier operators who are then able to conduct power balancing operations at their level, and 3) the amount of renewable energy produced and consumed in regard to the pattern of customers' energy profiles, as well as the allocation of energy storage.

4.4.2 Overall Traffic Loads Disseminated during Different Time Intervals of the Day

Figure 4.6d demonstrates the amount of data traffic conveyed in the network throughout the day when $N_h = 100$ and $\alpha = 0.6$. While the legacy operation involves all the data transmission as expected, traffic in OCNI shows a pattern in accordance with energy profiles. The pattern can be categorized into four phases; for example, in phase 1 (0-6

hour), people are asleep and PV units are not generating power, and therefore macro grid power is needed; in phase 2 (6-10 hour), people get up and go to work at sunrise, and therefore power sharing among ADNs using solar power may be possible; in phase 3 (10-16 hour), solar power is generated at the maximum while most of people are not at home, and therefore power balance may be achieved within the MGs; in phase 4 (16-18 hour), more people are coming home from work at sunset and start using appliances (e.g., oven, TV, dishwasher) that require macro grid power again, i.e., back to phase 1. To further decrease the traffic loads towards the CCC, implementing energy storage and other RESs such as micro wind turbines to support power during the nights is also a feasible solution. Notably, balancing power generation and loads within the MG has great potentials to reduce traffic loads transmitted to the upper tiers; however, it may be an unlikely case due to a small quantity of participating power nodes. Increasing the node quantity in a MG may ease power balance, but at the same time increases both control and communications complexities. Both case 2 and case 3 show a more practical phenomenon that is likely to occur in the future distribution system when renewable power and customer loads can be balanced.

4.5 Summary

In this chapter, a typical power system model which reflects today's radial tree-like topology feature is investigated. A multi-tier communications infrastructure OCNI is developed to facilitate active operations of the underlying autonomous distribution networks. Power balance is one primary issue in the power system that can be more challenging with higher penetration of distributed energy resources in terms of control and communications complexities. A micro grid consisting of households with installed PV

systems in a residential network is considered. The objective is to enhance the utilization of renewable energy generated by PV systems without energy storage in the distribution system. Balancing PV solar generation and household loads within the micro grid is initially tackled by using the proposed algorithm COPE to derive the shortest paths for power sharing among households by means of voltage control and communications in coordination. The proposed autonomous distribution network with the multi-tier overlay communications infrastructure is constructed such that power sharing and associated communications are initially performed in each individual micro grid at the lower tier. The simulation results show that not only the methodology PCC has great potentials to save considerable bandwidth owing to the reduction of data traffic loads at the upper tiers, but also power balancing through power sharing at the upper tiers is a more practical condition due to higher chances of power compensation among micro girds at the cost of greater involvement of information exchange among subnetworks.

CHAPTER 5

A HYBRID INTRUSION DETECTION SYSTEM FOR DISTRIBUTION NETWORKS IN SMART GRID

5.1 Motivation

In order to launch false data injection (FDI) attacks, most of studies have assumed the attacker has partial knowledge of $\mathbf{H}$ and considerable capability and resource, and yet believed that a full knowledge of the entire system gained by the attacker should be improbable. More reasonably, $\mathbf{H}$ can be inferred by the attacker who has no prior knowledge of $\mathbf{H}$ if the network topology remains static and the independent loads vary insignificantly for a period of time [113]. The studies have rigorously investigated the FDI attack by proposing various detectors and analyzing the damage effects on the power system in terms of anomaly determination, power transmission costs, and power outage rates [102, 103, 107]. Among which it is worth noting that the authors in [103] discovered that the unobservable attack can be effectively detected by determining the phase parameters via known-secure PMUs placement in a power system environment. Nevertheless, most of the existing works have addressed the FDI attack problem at the HV or MV transmission/distribution level and almost none at the LV distribution/consumption level where smart meters are deployed. The end-use level has been realized to be the most vulnerable sector in which the utilities have the least control of and the greatest uncertainty about the future distribution grid development.

This chapter is structured as follows: Section 5.2 illustrates the system measurement model prior to the discussion of the attack problem and proposed detection designs. Section

5.3 presents the problem formulation, attack model, and countermeasures. Section 5.4 analyzes the simulation results of the proposed detection framework and discusses the findings. Finally, Section 5.5 summarizes the focal points and draws a conclusion.

5.2 System Measurement Model

AC (alternating current) and DC power flow models are essentially used for studying state estimation. Nevertheless, the DC power flow model is often assessed due to its inexpensive computation and simplicity [138]. Moreover, a DC power grid is a foreseeable approach for the future distribution network [139] because 1) many distributed generators (e.g., household/neighborhood-based solar power systems) supply DC power, 2) AC grid-connected inverters are not needed, and 3) overall costs and power losses can be reduced. The ability to perform state estimation relies on the sufficiency of measurement data available in a network. In other words, the observability of a network has to be analyzed before state estimation can be processed.

Definition 4. *A network is said to be* ***observable*** *[117] if all flows in the network can be observed by obtaining information in a set of sufficient measurement data such that no power flows in the network for which* $\mathbf{Hx} = \mathbf{0}$*,* $\forall P \in \mathbf{x}$*; otherwise, there is (are)* ***unobservable*** *state(s) where nonzero power flows exist in the network.*

Consider a DC network model that has three state variables as shown in Figure 5.1: to ensure that the power network is balanced, there is at least one state that acts as a generation or load node, i.e., $P_1 + P_2 + P_3 = 0$. Figure 5.1a shows an underdetermined and partially observable case where only state P_1 is observable, and one of the states P_2, P_3 is unobservable, and another dependent state is indeterminate. Figure 5.1b shows an

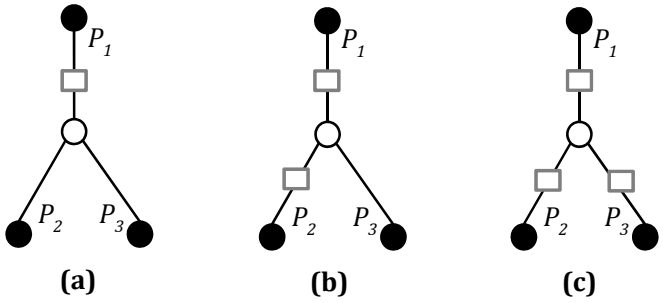


Figure 5.1 Observability of a network comprised of generation and load nodes (black circle), bus node (white circle), lines (representing connectivity), and meters/sensors (gray rectangle) in three cases: (a) underdetermined and partially observable, (b) observable and sufficient, and (c) observable but overdetermined.

observable and sufficient case where both states P_1 and P_2 are observable, and dependent state P_3 can be computed from the network model equation with the other two known state variables. Figure 5.1c shows that all states P_1, P_2, P_3 are observable and form an overdetermined system, but can be solved as a least-squares problem. This model is used to study the proposed CONSUMER attack model as well as grid sensor placement for the distribution network of smart grid in this chapter. Moreover, the characteristics of the emerging smart grid network are considered as follows:

- Nodes (e.g., smart meters, grid sensors) strategically deployed throughout distribution grids are *static*. In other words, grid operators have full knowledge of network topologies in terms of geographical locations and coordinates.

- Nodes are *wire-powered* while attached to power lines and taking various measurements such as voltage, current, frequency, and metering.

- The majority of data traffic generated at the nodes are *periodic* for real-time monitoring and control.

- Each measurement data generated at the nodes (representing individual customer energy consumption and grid line conditions for state estimation) *cannot be fused* at aggregation nodes as opposed to traditional sensor network scenarios where data of sensors tracking their surrounding environmental conditions (e.g., temperature) are

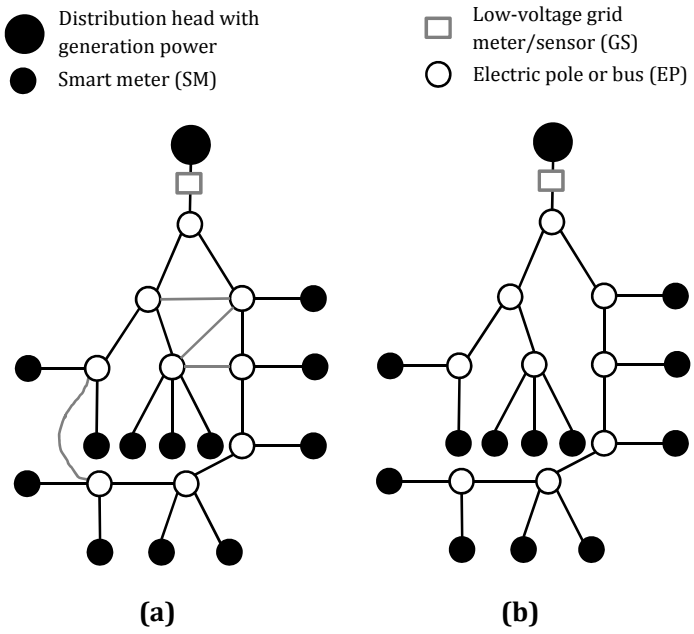


Figure 5.2 A neighborhood distribution network (a) with loops, and (b) without loops.

aggregated at cluster nodes to generalize the current network status by determining the correlation of the multiple obtained measurements.

5.3 Problem Definition and Formulation

Most parts of the current distribution networks are characterized by radial tree-like topologies, which may or may not contain loops or cycles, as shown in Figure 5.2. The distribution network consists of four components: 1) a root aggregation node (marked by a big black circle) at which power is generated or delivered from other sources, such as macro grid or neighboring distribution networks, 2) a grid sensor (GS) node (marked by a gray rectangle) that constantly measures aggregation power P_{agg}, corresponding to the quantity of multiple end loads, 3) a number of electric poles (EPs) or buses (marked by white circles), $l = 1, 2, ..., n_{EP} \in \mathcal{N}_{EP}$, with distribution lines/feeders, transformers and capacitors (not shown) that construct a distribution grid and supply power to customers,

and 4) a number of household smart meters (SMs; marked by small black circles), $n = 1, 2, ..., n_{SM} \in \mathcal{N}_{SM}$, that have two-way communications capability of reporting household energy consumption to the utility control center and receiving associate feedback messages in real time.

Notably, Figure 5.2a shows a distribution network that has loops found among some EP nodes, whereas Figure 5.2b depicts a network with no loops representing a spanning tree. Any spanning tree $G(V_T, E_T)$ from its originally connected graph $G(V, E)$ can be computed by using various algorithms, e.g., Prim's algorithm [140], where V is a collection of vertices, E is a collection of edges, and $V_T = V$. In other words, any connected distribution network $G(V, E)$ can have at least one spanning tree $G(V_T, E_T)$ with the fewest edges among EP nodes[1] while the four network properties must be obeyed: 1) the network connectivity is maintained, 2) the spanning tree starts with the distribution head node, 3) the EP node cannot be a leaf node, and 4) the SM node must be a leaf node. Under this condition, the spanning tree topology as illustrated in Figure 5.2b can be discovered, and therefore considered in the studied model in order for us to determine the minimum number of grid sensors to be placed on edges such that the network is sufficiently observable (to be discussed on p. 96).

Power flow is further assumed unidirectional (in a traditional way) such that power is delivered from the root of the tree to the end leaves. A practical scenario is considered where utility operators currently have limited knowledge about the real-time conditions of distribution networks (e.g., the difficulty of exactly knowing how and how much power is delivered across feeders/lines as well as discovering how and where faults are caused if

[1]How to find such a spanning tree of the cyclic distribution network is beyond the scope of this chapter.

erroneous activities are present) in a geographically and temporally fine-grained manner due to lack of grid sensors along with effective coordinated monitoring. As shown in Figure 5.2, for a power balance circumstance, the summation of individual loads (of all leaves) must be equal to the amount of measurement metered at the aggregation GS node. If the aggregated load value exceeds or lessens the GS measurement for a tolerable amount, an anomalous activity is detected and alarmed, but somehow may not be identified easily whether it is caused by natural errors or malicious attacks.

5.3.1 The CONSUMER Attack Model

In the CONSUMER attack model, the FDI model (introduced in [96]) is applied to construct the studied attack scenario at the smart meter level. The typical distribution network (shown in Figure 5.2) has its own network topology and configuration matrix $\mathbf{H}$ and a set of true states in $\mathbf{x} = [P_1, P_2, \ldots, P_{n_{SM}}]^\mathsf{T}$ indicating the energy consumption status of household smart meters. It can be assumed that the accuracy of smart meter (i.e., $\mathbf{W}$) is nearly precise and the noise vector $\mathbf{e} \sim \mathcal{N}(0, \sigma^2)$ is normally distributed so that the estimate $\hat{\mathbf{x}} = [\hat{P}_1, \hat{P}_2, \ldots, \hat{P}_{n_{SM}}]^\mathsf{T}$ where $\hat{P}_1 + \hat{P}_2 + \cdots + \hat{P}_{n_{SM}} = \hat{P}_{agg}$ is satisfied.

The attacker is assumed to have (partial) knowledge of $\mathbf{H}$ whether it is obtained illegally or deduced by its own observation. The goal of the attacker is to launch the CONSUMER attack by injecting attack vector $\mathbf{a}$ with $\mathbf{c}$ to produce a compromised vector $\bar{\mathbf{z}} = [P_{\bar{z}_1}, P_{\bar{z}_2}, \ldots, P_{\bar{z}_{n_{SM}}}]^\mathsf{T} \neq 0$ in which $\sum \mathbf{a} = 0$ particularly such that there exists load alterations and the altered linear combination cannot be easily detected by a traditional bad measurement data detector. The indicator χ_i is considered for which smart meter of household i is compromised if $\chi_i = 1$ and otherwise if $\chi_i = 0$, that leads to $\bar{\mathbf{z}} = [P_{\bar{z}_1}\chi_1, P_{\bar{z}_2}\chi_2, \ldots, P_{\bar{z}_{n_{SM}}}\chi_{n_{SM}}]^\mathsf{T}$. The objective of the attacker is to lower its own energy

consumption level by raising others'. Owing to constrained resources, the attacker tries to minimize the number of compromised smart meters while achieving its objective subject to the inviolability of an aggregated load value. The minimization problem for a CONSUMER attack is formulated as

$$\min \quad \sum_{i=1}^{n_{SM}} \chi_i$$

s.t.

$$\sum_{i=1}^{n_{SM}} P_{\bar{z}_i}\chi_i = P_{agg}, \quad \chi_i \in \{0,1\}, \quad \forall i \in \bar{\mathbf{z}}, \tag{5.1}$$

$$\tilde{P}_i^{\min} \leq P_{\bar{z}_i} < P_i, \quad \exists! i \in \bar{\mathbf{z}} : \text{is the attacker},$$

$$\chi_i = 1, \quad i \in \mathcal{A}, \tag{5.2}$$

$$P_{\bar{z}_i} \leq \tilde{P}_i^{\max}, \quad \forall i \in \bar{\mathbf{z}} \backslash \mathcal{A}, \tag{5.3}$$

$$P_i \geq 0, \tilde{P}_i^{\min} \geq 0, \tilde{P}_i^{\max} \geq 0, \quad \forall i. \tag{5.4}$$

This problem is analogous to the coin change problem, which is NP-hard [141]. Both problems aim to match a given integer value (equality Constraint 5.1) while minimizing the number of components (objective function) for the outcome. As opposed to the coin change problem, the CONSUMER problem considers multiple sets of power value ranges corresponding to multiple households' energy profiles with predicted ranges of energy consumption (inequality Constraints 5.2, 5.3, and 5.4), and that at most one value within the range belonging to one household is selected and each household is picked at most once.

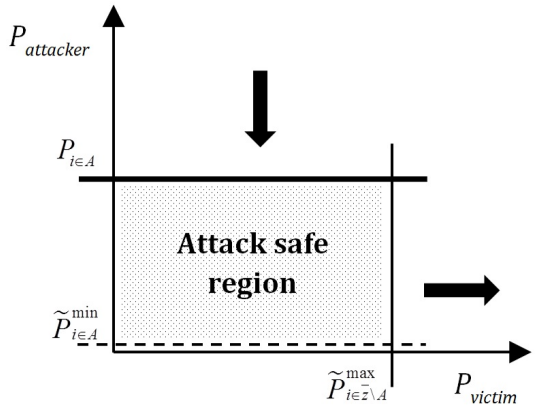


Figure 5.3 The attack region for a one-to-one pair between the attacker and the victim.

Theorem 2. *A CONSUMER attack can be launched successfully by compromising as few as **two** smart meters (one for the attacker and one for the victim) in any spanning tree which meets the four aforementioned network properties (p.89).*

The proof of the theorem is trivial. Since there is only one grid sensor measuring an aggregated energy consumption value of the entire distribution loads, a CONSUMER attack on any two of the households can easily become undetected and hence, unidentified. For example, Figure 5.3 depicts an attack safe region associated with one attacker and one victim that is bounded by three major values: $P_{i\in\mathcal{A}}$ which is the current energy consumption value of the attacker, $\tilde{P}^{\min}_{i\in\mathcal{A}}$ which is the minimum predicted consumption value of the attacker in the next time period, and $\tilde{P}^{\max}_{i\in\bar{\mathbf{z}}\setminus\mathcal{A}}$ which is the maximum predicted consumption value of the victim in the next time period. In a one-attacker-one-victim scenario, the attacker tries to decrease its consumption by increasing the victim's as much as to be in a horizontally narrow rectangular zone shown in Figure 5.3. Essentially, under an *unconstrained* case, the attacker can pick any arbitrary nonnegative value (Constraint 5.4) and performs subtraction on its consumption amount and addition on the victim's to avoid detection as long as Constraint 5.1 is held; the minimization problem will be

reduced to a simple linear programming problem. On the other hand, under a *constrained* case, the attacker cannot simply pick any number but needs to determine appropriate $\tilde{P}^{\min}_{i\in\mathcal{A}}$ and $\tilde{P}^{\max}_{i\in\bar{\mathbf{z}}\setminus\mathcal{A}}$ in order to avoid detection as anomalous activities. In fact, utilities might implement various kinds of prediction methods to predict and monitor households' energy consumption in the future time periods, and that would complicate the problem. Any anomaly activity that deviates from the correspondingly estimated regression lines beyond a predetermined threshold will trigger an alarm in the intrusion detection system. Unless the attacker has prior knowledge of what the thresholds are, $\tilde{P}^{\min}_{i\in\mathcal{A}}$ and $\tilde{P}^{\max}_{i\in\bar{\mathbf{z}}\setminus\mathcal{A}}$ cannot be chosen too aggressively. Therefore, for the attacker to launch a more sophisticated CONSUMER attack, Constraints 5.2 and 5.3 (which can be treated as part of countermeasures in the proposed hybrid detection solution) must be considered carefully. In addition to these constraints, the costs of compromising smart meters via coordinated communications on the spatial and temporal scales are also challenges from the attacker perspective.

5.3.2 Countermeasures for the Utility Defender: IDS with POISE and GPS

It is unlikely to have a one-size-fits-all solution for detecting anomalous or malicious activities in smart grid. A framework that integrates the characteristics of power network load consumption dynamics, communications network traffic dynamics, and network observability analysis via grid sensor placement is developed for an evolutionary intrusion detection system, as shown in Figure 5.4. The last item of the proposed framework is covered in this chapter, and the first two items are left for the future works. In a cyber-physical smart grid AMI network, the uplink transmission from smart meters to control centers as well as downlink transmission in an opposite way is vulnerable to a breach of confidentiality, integrity, and availability (CIA). While a general FDI attack can

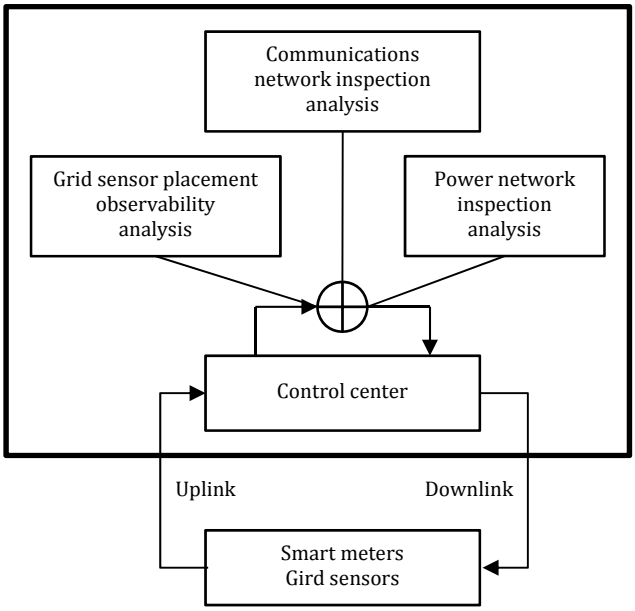


Figure 5.4 POISE: a hybrid intrusion detection system.

be launched on the two way links, the CONSUMER attack is specifically instigated in the uplink transmission causing utility operators to make wrong decisions in consequence of receiving falsified measurement data which are hardly distinguishable from the legitimate ones. There are two fundamentally challenging questions in the context of the smart grid intrusion detection system design:

1. What is an adequate threshold for defining an anomaly activity, e.g., in the application of characterizing customers energy consumption behavior while they may be elusive to some extent? Does it even exist?

2. How to effectively distinguish between (unintentionally) anomaly and (intentionally) malicious activities?

While these intriguing questions require further research in the next few years, some insights into the following first two detection methods based on both power and communications networks dynamics analyses are provided, followed by a grid sensor placement mechanism proposed to effectively enhance the intrusion detection process.

Power Network Inspection. A power grid system obeys a series of control theories based on laws of physics. Data measurement collection not only involves power load consumption measurement but also voltage, current, and power factor elements. Observations on phase differences on the transmission/distribution level studied in [103] can be further evaluated on the distribution/consumption level. Another useful metric for designing specification or rule-based anomaly detection systems is to deeply understand different classes of customer energy consumption patterns at different time scales, e.g., usage trends on weekdays, weekends, monthly, seasonal, and annual basis corresponding to individual activities and weather conditions. Many approaches for characterizing household electricity demands including Fourier series, Gaussian processes, neural networks, fuzzy logic, as well as regression and autoregression have been studied [142]. Meanwhile, the existing scheme of detecting illegal customers based on Support Vector Machine (SVM) learning and rule-based algorithms has also been investigated in [93]. These methods could be effectively incorporated in the intrusion detection system at the application level to improve detection accuracy. Furthermore, computational intelligence [143] can also be readily applied for intrusion detection.

Communications Network Inspection. In addition to the methods of power dynamics inspection, extensive studies on traditional low-power WSN attack scenarios [87] at the physical, MAC, and network layer levels are complementary intrusion detection tools to be integrated into the smart grid communications security environment, specifically against the jamming, replay, and DoS attacks. Several dominant metrics such as data sending rate, receiving rate, packet loss rate, and signal strength will be tailored to effectively facilitate the detection of anomaly activities in smart grid communications in response to compromising or breaching circumstances.

Intrusion Detection System with Power Information and Sensor Placement – IDS with POISE. Smart meter deployment has been initiated worldwide in the past few years. The rationale for replacing the traditional meters with smart meters is plentiful, but the fundamental one is to be able to monitor and control customer energy consumption more efficiently in real time through two-way communications by leveraging the state-of-the-art wire/wireless and power line communications technologies. By gaining knowledge of individual energy usage patterns, utilities can deal with primary issues easily such as peak demands alleviation, remote meter reading, and distributed renewable energy sources accommodation, in order to increase energy efficiency and reduce greenhouse gas emission. The entire smart grid AMI network consisting of a number of control centers and hundreds of thousands of smart meters is likely to operate using the IP Protocol with IPv6 addresses assignment connected to the Internet [144]. Smart meters support multiple communications protocols that facilitate smart energy management in HANs and mesh routing in NAN. Many have considered utilizing the existing networks such as WiFi and wireless mesh networks to communicate under unlicensed bands for economic reasons. This strategy creates network uncertainties by exposing security vulnerabilities of smart metering communications to the public.

In the meantime, grid sensor placement across the distribution network is proposed in which these grid sensors with simpler functionalities (than smart meters) are owned by utilities and construct grid sensor networks operating in dedicated or licensed bands specified in IEEE 802.15.4g Smart Utility Network (SUN), e.g., see [145, 144] for further studies. The grid sensor network is much less vulnerable to malicious attacks and is designed as surveillance guards in the distribution grid. Moreover, deploying grid sensors on lines/feeders (as low-voltage sensors) brings utilities a number of potential benefits:

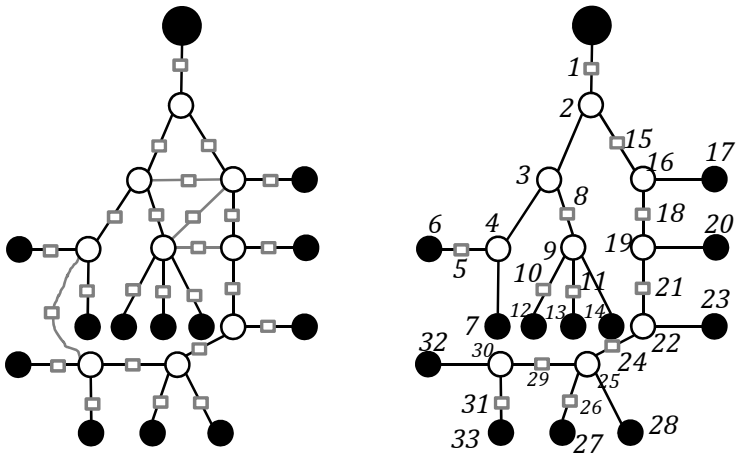


Figure 5.5 A neighborhood distribution network deployed with a number of grid sensors in (a) overdetermined case, and (b) sufficient case.

1) greater transparency and stability can be achieved owing to the substantial observability of power flow conditions on each segment and portion of the network, 2) voltage fluctuation due to varying input of renewable energy sources (e.g., household/neighborhood-based PV solar systems) can be effectively monitored, and 3) optimization in volt-var control and optimal power flow operations can be intelligently performed. Hence, utility operators will have a full knowledge of their supervised network topologies in terms of geographical locations with coordinates of grid sensors as well as smart meters while monitoring the network quality and ensuring cyber-physical security. At this stage, all deployed grid sensors are assumed intrusion resistant and their measurement data are trustworthy (i.e., false alarm rate is zero) so that the measurement data of smart meters can be compared with that of grid sensors to detect and identify any falsified data by compromised smart meters.

As discussed in Sec. 5.3, the existing distribution grid is not transparent to the utilities to a certain degree. The design of sensor grid placement can help provide topological

observability by deploying a sufficient number of grid sensors to guarantee state estimation solvability. In Figure 5.5a, every grid line is placed with a sensor that results in an overdetermined system. In order to reduce the redundancy to a sufficient number while observability is still satisfied, a grid-placed sensor (GPS) algorithm is proposed, as shown in Algorithm 6.

Algorithm 6 Grid-Placed Sensor (GPS) - loop free

Input: Given a connected, undirected spanning tree graph $G(V_T, E_T)$ with depth $D_T = 1, 2, \ldots, d$ information.

Output: An observability indicator matrix I_O that represents observability status of each edge.

Place a GS node at the root node's edge.

for $\forall d \in D_T$ **do**

    Determine the number of children u of $v(d), \forall v \in V_T$

    if $u = 1$ **then**

        No GS node is placed.

    else if $u > 1$ **then**

        A GS node is placed on any $(u - 1)$ of the u edges connected to the child, and mark *1* for the GS-placed edges in I_O.

    end if

    Repeat for other v if having the same d.

end for

For the considered spanning tree illustrated in Figure 5.5b, the network graph $G(V_T, E_T)$ with depth levels $1, 2, \ldots, d \in D_T$ is constructed by a set of EP and SM nodes $v_1, v_2, \ldots, v_n \in V_T$ and a set of edges E_T, where $\mathcal{N}_{SM} \subseteq V_T, \mathcal{N}_{EP} \subseteq V_T, |V_T| =$

$|\mathcal{N}_{SM}| + |\mathcal{N}_{EP}|$, and $|.|$ is the cardinality. In Figure 5.5b, the white circles are the EP nodes and black circles are the SM nodes. At the beginning, the GS node v_1 is directly placed on the edge between the generation source and distribution bus, i.e., v_2. In the next step, the algorithm starts with EP node v_2 and discovers that it has two children, which can be EP or SM nodes. Either $e(v_2, v_3)$ or $e(v_2, v_{16})$ placed with a GS node v_{15} in between will make both edges become observable, according to Def. 4 in Sec. 5.2. Note that $e(w, v)$ or $e(v, w)$ denotes the edge e that connects both node w and v. Both edges becoming observable are then marked with *1* in the $n \times n$ observability matrix I_O. Repeat the process for the right branch. The algorithm starts with EP node v_{16} and discovers that it also has two children. Consequently, either $e(v_{16}, v_{19})$ or $e(v_{16}, v_{17})$ placed with a GS node v_{18} will make both edges become observable; again, the two observable edges are marked with *1* in I_O. Notably, although SM node v_{17} has metering capability to make $e(v_{16}, v_{17})$ observable already, the GS node v_{18} is placed in order to later verify whether or not the measurement data of SM node v_{17} is legitimate. The process is repeated until it reaches the leaves with the largest d.

Theorem 3. *The entire spanning tree network is said to be (sufficiently) observable if* $G - I_O = 0$.

Proof. Both G and I_O are $n \times n$ matrices. Every edge connecting two nodes that exists in the network topology is marked with *1* in G, and *0* otherwise. Correspondingly, every existing edge in the network that becomes observable after running the GPS algorithm is marked with *1* in I_O, and *0* otherwise. Therefore, an observable network will make both G and I_O matrices identical. □

Theorem 4. *In a spanning tree topology scenario where the EP node cannot be a leaf and the SM node must be a leaf, the number of GS nodes placed on edges for the network to be observable is the same as the number of SM nodes.*

Proof. In the GPS algorithm, each process starting from the EP node of the root determines the number of children the EP node has. The algorithm starts adding $(u-1)$ GS nodes to u children of the associated EP node, until it reaches the leaf with the largest d. With the condition where there always exists a SM node as a leaf connected to its parent EP node, the total number of GS nodes will eventually sums up to $|\mathcal{N}_{SM}|-1$ in addition to the GS node at the root. □

5.4 Simulations and Results

Two types of simulations are conducted in this chapter in order to analyze the outcomes of the proposed CONSUMER attack model as well as grid sensor placement for detecting the attack, respectively.

5.4.1 Study of Successful CONSUMER Attacks in Different Constraint Scenarios

In the first simulation, a value of 5kWh is set for the actual amount of power the attacker consumes at a certain time period and it aims to lower the consumption for what it actually pays to four differently reduced values (4kWh, 3kWh, 2kWh, and 1kWh); this means that the rest of power has to be compensated by a number of chosen neighboring victims in order for the attack to be undetected, as shown in Figure 5.6. Three conditions are considered in terms of the constraint level while the attacker performs such action. In an unconstrained scenario, there is no upper bound value for the attacker to steal. Therefore, it only needs to compromise as low as one smart meter from the neighbors (in addition to its own meter to

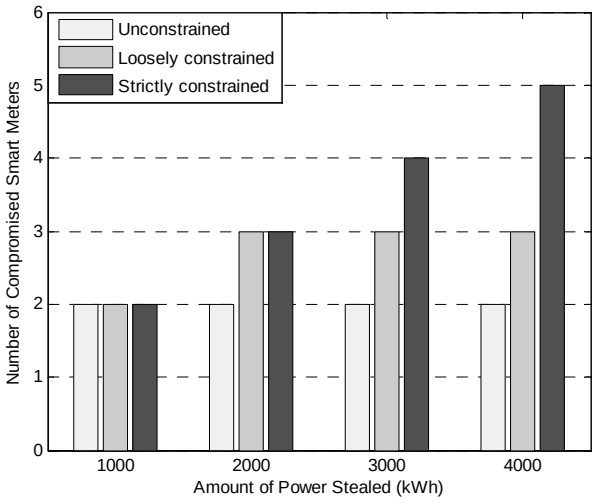


Figure 5.6 Requirements for a successful CONSUMER attack under different constraints.

make a total of two) for stealing the four different amounts of power. On the other hand in the more practical cases where there are upper bounds predetermined at the utility control centers that the attacker must be aware of for not being detected: an expected amount of 2kWh is set that can be tolerated in fluctuation of customers energy consumption for a loosely constrained case, and an expected amount of 1kWh for a strictly constrained case. From the results, it is discovered that more smart meters need to be compromised to achieve the stealing targets while bypassing detection.

Note that compromising a large number of smart meters is believed to be an improbable scenario because there are upper and lower bounds for the victims and attacker's energy consumption patterns upon which the utility control center constantly monitors. However, a probable case should be emphasized for which the attacker may change its strategy to launch p k–sparse attacks where p is the number of attacks and k is the number of compromised smart meters. In other words, the attacker can perform the CONSUMER attack by constructing p clustered attacks in which k smart meters are

compromised simultaneously throughout the network still without being detected. This interesting attack scenario will be investigated in the future works.

5.4.2 Analysis of Network Observability and Corresponding Detection Rates

In the second simulation, how detection rate varies with different levels of network observability in terms of the number of grid sensors placed in the network is investigated. From an attacker point of view, it can have $\binom{n_{SM}}{k_{SM}}$ of ways to compromise k_{SM} out of n_{SM} smart meters. Similarly, from a utility defender point of view, the operator has to determine $\binom{n_{GS}}{k_{GS}}$ of possible ways that k_{GS} out of n_{GS} grid sensors may become unavailable and cause partial unobservability of the network when n_{GS} is a sufficient number for the network to be observable. In the worst case, the detection rate can be as low as zero when compromised smart meters are next to each other (whether they are connected to the same parent node or connected to their parents whose edge is shared by each other) and where exactly the grid sensor becomes unavailable. Two examples may be depicted from Figure 5.5b: 1) *the worst undetectable and unidentifiable cases*: consider the case that SM nodes v_{27} and v_{28} are compromised and at the same time GS node v_{26} is unavailable, thus causing unobservability on $e(v_{25}, v_{27})$ and $e(v_{25}, v_{28})$ – the CONSUMER attack on these two smart meters is undetected; also consider the case that SM nodes v_{17} and v_{20} are compromised, in which case the unavailability of GS node v_{18} can cause $e(v_{16}, v_{17})$ and $e(v_{19}, v_{20})$ to be unobservable, and hence undetectable on SM nodes v_{17} and v_{20}; and 2) *the unidentifiable but detectable case*: consider the case that SM nodes v_{17} and v_{23} are compromised and GS node v_{18} becomes unavailable, in which case SM node v_{23} is detected as an attacked node by observing GS nodes v_{21} and v_{24} but SM nodes v_{17} and v_{20} cannot be identified whether

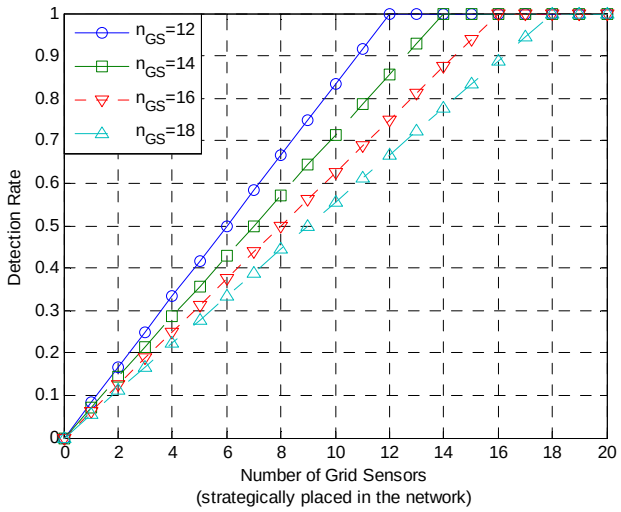


Figure 5.7 Network observability versus detection rate.

one or all of the smart meters are attacked. Hence, SM nodes v_{17} and v_{20} must be further inspected by the utility and therefore, considered as a detected case.

Figure 5.7 shows the average detection rate that considers all possible combinations of smart meter attacks and grid sensor availabilities. Since the number of smart meters and grid sensors are identical (proven in Thm. 4), and at the same time the number of times the smart meters to be attacked and the number of times the grid sensors to become unavailable are equally likely, the outcomes of the detection rate and grid sensor availability shown in Figure 5.7 exhibit a linear relationship. From the results, note that the slope of the detection rate is steeper when the number of grid sensors (as well as smart meters) is smaller. On the other hand, the slope of the detection rate declines when the number of grid sensors increases. This means that a smaller network with a lower number of sufficient n_{GS} deployed is more vulnerable to unobservability as compared to a larger network, given the same number of GS nodes becoming unavailable.

5.5 Summary

In this chapter, a breach of data integrity attributed to false data injection attacks for the future power grid environment is investigated. An attack model (CONSUMER) is formulated to illustrate that by compromising smart meters, illegal customer "can steal" electricity by lowering its energy consumption and raising others in a neighborhood distribution network. A novel hybrid intrusion detection system framework that incorporates power information and sensor placement has been developed to detect malicious activities such as CONSUMER attacks while the traditional bad measurement data detectors cannot. An algorithm for placing grid sensors on lines or feeders strategically throughout a spanning-tree distribution network is proposed to provide sufficient network observability for aiding detection performance. It has been shown that compromising a large number of smart meters may be improbable as well as indicated that the attack may turn into a multiple clustered attack with a few compromised smart meters. It has also been shown that the detection rate can be improved by the proposed grid sensor placement with sufficient observability; however, it can also be degraded by unavailability of grid sensors.

CHAPTER 6

CONCLUSIONS AND FUTURE WORKS

In this dissertation, extensive simulations have been conducted to substantiate the viability of the proposed solutions in tackling the three potential problems in the future power distribution network, namely, power surplus congestion, bidirectional power flows, as well as energy theft associated with false data injection attacks. Several intriguing questions raised from this investigation require further studies. For example, the essential attributes such as packet loss, varying power demands and solar surpluses, and fairness need to be taken into consideration for the selection of disconnecting solar units proposed in Chapter 3 when the decision is made at the utility control center. These attributes can potentially alter the network topology at different time periods in terms of selection outcomes, and thus affect the system performance. Similarly, communications designs for resource allocation and scheduling to tackle signal interference and traffic under the power-communications networked system developed in Chapter 4 should be explored further.

Moreover, intrusion detection for the smart grid system (deployed with millions of smart meters and grid sensors) studied in Chapter 5 will attract further investigation for the coming years. Below a few insights into some potential research topics associated with the proposed intrusion detection framework.

1. The complementary detection methods of utilizing power and communications networks inspection incorporated in the proposed framework can be developed further to improve detection performance.

2. Grid sensors in Chapter 5 were considered fully trustable. For practical scenarios, trustworthiness of meters and sensors can be explored to determine possible impacts

on the proposed intrusion detection framework by addressing uncertainties of network dynamics in the context of smart grid security, e.g., the attacker can launch an observability attack by compromising or disabling some of the grid sensors, thus making intrusion detection more challenging.

3. Further development of effective and efficient countermeasures are desired to cope with variants of the CONSUMER attack.

4. Grid sensor localization and associated observability studies can be further extended to grid isolation designs. For example, grid isolation may be employed to prevent catastrophic failures from cyber-physical attacks, but the grid in islanded mode must remain observable as well.

5. The proposed CONSUMER attack design, which is currently limited to a one-player attack, can be extended to a multi-player attack where more than one attacker try to steal electricity at the same time period. The design can be remodeled as a cooperative attack for searching a local or global maximum outcome, as well as a non-cooperative (selfish) game for finding the Nash equilibrium, without being detected by the detectors. The aforementioned p clustered CONSUMER attacks with k–sparse compromised smart meters can be further studied.

6. Since smart meters and grid sensors are mounted on power lines/feeders, power consumption is not a primary concern in the smart grid environment. Moreover, these devices are likely to have higher capabilities as compared to the traditional or dust sensors (that perform single detection application) in terms of computation and memory. In fact, delay is a primary constraint for different smart grid applications since there can be mission-critical events in addition to routine activities. Therefore, this critical metric has to be considered while designing bandwidth allocation and scheduling for different classes of traffic in smart grid communications. However, the crowded network environment may cause severe interference and measurement data collisions. A potential solution may be leveraging on the duty-cycle (on and off) scheduling technique via grid sensors selection in order to reduce or balance network traffic, while the observability of the power network as well as connectivity of the communications network is maintained. How to design smart metering networks and grid sensor networks is still an interesting topic.

7. As compared to traditional WSN studies, power consumption by smart meters and grid sensors in smart grid communications should be remodeled by incorporating on-site renewable energy utilization for energy efficiency in parallel with the ongoing research on green communications. Additionally, the concept of data aggregation in the smart grid context is also different from that in legacy WSN. Most of meters and sensors installed on lines/premises carry significant measurement data and cannot be fused in a traditional way because they effectively represent particular state

conditions and individual loads that are utilized for monitoring/billing purposes at the utility control center.

BIBLIOGRAPHY

[1] S. Collier, "Ten steps to a smarter grid," *IEEE Ind. Appl. Mag.*, vol. 16, no. 2, pp. 62–68, Mar.-Apr. 2010.

[2] L. Freris and D. Infield, *Renewable Energy In Power Systems*. Chippenham, United Kingdom: Wiley, 2008.

[3] T. L. Friedman, *Hot, Flat, and Crowded: Why We Need a Green Revolution and How It Can Renew America*. New York, New York: Farrar, Straus and Giroux, 2008.

[4] J. See, W. Carr, and S. Collier, "Real time distribution analysis for electric utilities," in *Proc. IEEE Rural Electric Power Conf.*, North Charleston, SC, USA, 26-29 Apr. 2008, pp. B5–B5–8.

[5] K. L. J. W. J. Ekanayake, N. Jenkins and A. Yokoyama, *Smart Grid: Technology and Applications*. New Delhi, India: Wiley, 2012.

[6] R. DeBlasio and C. Tom, "Standards for the smart grid," in *Proc. IEEE Energy 2030 Conf. (ENERGY)*, Atlanta, GA, USA, 17-18 Nov. 2008, pp. 1–7.

[7] IEEE smart grid standards. IEEE Smart Grid. [Online]. Available: http://smartgrid.ieee.org/standards

[8] E. W. Gunther. (2009, 21-24 Sept.) Standards: Help or hindrance in Smart Grid deployments. EnerNex. GridWeek Conference in Washington, DC. [Online]. Available: http://www.pointview.com/data/2009/09/31/pdf/Erich-Gunther-4476.pdf

[9] C. Strauss, *Practical Electrical Network Automation and Communication Systems*. Burlington, Massachusetts: Newnes, 2003.

[10] "The smart grid: An introduction," Book publication, U.S. Department of Energy (DOE), 2008. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf

[11] K. Narendra and T. Weekes, "Phasor measurement unit (PMU) communication experience in a utility environment," Easun Reyrolle Ltd (ERL) Phase Power Technologies Ltd., CIGRE Conference on Power System, Tech. Rep., 19-21 Oct. 2008. [Online]. Available: http://www.erlphase.com/downloads/papers/08_CIGRE_PMU_Communication_Experience.pdf

[12] R. Lasseter, "Smart distribution: Coupled microgrids," *Proc. IEEE*, vol. 99, no. 6, pp. 1074–1082, June 2011.

[13] A. Kwasinski, "Implication of smart-grids development for communication systems in normal operation and during disasters," in *32nd Int'l Telecom. Energy Conf. (INTELEC)*, Orlando, FL, USA, 6-10 June 2010, pp. 1–8.

[14] (2010, Aug.) Annual energy review 2009. U.S. Energy Information Administration. [Online]. Available: http://www.eia.gov/totalenergy/data/annual/pdf/aer.pdf

[15] R. H. Khan and J. Y. Khan, "A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network," *Comput. Netw.*, vol. 57, no. 3, pp. 825–845, 2013.

[16] D. Grifith, M. M. Souryal, and N. Golmie, "Chapter 10: Wireless networks for smart grid applications," in *Smart Grid Commun. and Netw.*, E. Hossain, Z. Han, and H. V. Poor, Eds. CRC Press, 2012.

[17] L. Tsoukalas and R. Gao, "From smart grids to an energy Internet: Assumptions, architectures and requirements," in *Proc. 3rd IEEE Int'l Conf. Electric Utility Deregulation and Restructuring and Power Technol. (DRPT)*, Nanjing, China, 6-9 Apr. 2008, pp. 94–98.

[18] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *IEEE Power Energy Soc. General Meeting*, Minneapolis, MN, USA, 25-29 July 2010, pp. 1–6.

[19] D. E. Bakken, R. E. Schantz, and R. D. Tucker, "Smart grid communications: QoS stovepipes or QoS interoperability," in *Proc. of Grid-Interop*, Denver, CO, USA, 17-19 Nov. 2009.

[20] M. Rosenfield, "The smart grid and key research technical challenges," in *Symp. VLSI Technol. (VLSIT)*, Honolulu, HI, USA, 15-17 June 2010, pp. 3–8.

[21] M. Sooriyabandara and J. Ekanayake, "Smart grid - technologies for its realisation," in *IEEE Int'l Conf. Sustain. Energy Technol. (ICSET)*, Kandy, Sri Lanka, 6-9 Dec. 2010, pp. 1–4.

[22] T. Overman and R. Sackman, "High assurance smart grid: Smart grid control systems communications architecture," in *1st IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 19–24.

[23] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids," *IEEE Power and Energy Mag.*, vol. 5, no. 4, pp. 78–94, July-Aug. 2007.

[24] R. Lasseter, "CERTS microgrid," in *IEEE Int'l Conf. Syst. of Syst. Eng. (SoSE)*, San Antonio, TX, USA, 16-18 Apr. 2007, pp. 1–5.

[25] A. Dobakhshari, S. Azizi, and A. Ranjbar, "Control of microgrids: Aspects and prospects," in *IEEE Int'l Conf. Netw., Sens. and Control (ICNSC)*, Delft, Netherlands, 11-13 Apr. 2011, pp. 38–43.

[26] A. Ipakchi and F. Albuyeh, "Grid of the future," *IEEE Power and Energy Mag.*, vol. 7, no. 2, pp. 52–62, Mar.-Apr. 2009.

[27] S. Güner and B. Bilir, "Analysis of transmission congestion using power-flow solutions," in *Proc. 5th IASME/WSEAS Int'l Conf. Energy & Environment (EE)*, Cambridge, UK, 23-25 Feb. 2010, pp. 330–333.

[28] S. Dehghan, M. Moradi, and A. Mirzaei, "Improving congestion relief management as ancillary service in operation planning phase with demand side's presence," *Canadian J. Electr. Electron. Eng.*, vol. 2, no. 5, pp. 145–152, May 2011.

[29] A. Saini and A. Saxena, "Optimal power flow based congestion management methods for competitive electricity markets," *Int'l J. Comput. Electr. Eng.*, vol. 2, no. 1, pp. 73–80, Feb. 2010.

[30] B. Liu, J. Kang, N. Jiang, and Y. Jing, "Cost control of the transmission congestion management in electricity systems based on ant colony algorithm," *Energy Power Eng.*, vol. 3, no. 1, pp. 17–23, Feb. 2011.

[31] L. L. Grigsby, *Power Systems*, 2nd ed., ser. The Electrical Engineering Handbook, R. C. Dorf, Ed. New York, New York: CRC Press, 2006.

[32] A. von Meier, *Electric Power Systems: A Conceptual Introduction*, 1st ed. Hoboken, New Jersey: Wiley-IEEE Press, 2006.

[33] J. Liu, M. Salama, and R. Mansour, "Identify the impact of distributed resources on congestion management," *IEEE Trans. Power Del.*, vol. 20, no. 3, pp. 1998–2005, July 2005.

[34] (2009, Dec.) National electric transmission congestion study. U.S. Department of Energy. [Online]. Available: http://congestion09.anl.gov/documents/docs/Congestion_Study_2009.pdf

[35] M. Erol-Kantarci and H. Mouftah, "Wireless sensor networks for cost-efficient residential energy management in the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 314–325, June 2011.

[36] A. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.

[37] A. Molderink, V. Bakker, M. Bosman, J. Hurink, and G. Smit, "Management and control of domestic smart grid technology," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 109–119, Sept. 2010.

[38] M. Pedrasa, T. Spooner, and I. MacGill, "Coordinated scheduling of residential distributed energy resources to optimize smart home energy services," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 134–143, Sept. 2010.

[39] C. Ibars, M. Navarro, and L. Giupponi, "Distributed demand management in Smart Grid with a congestion game," in *1st IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 495–500.

[40] K. Turitsyn, N. Sinitsyn, S. Backhaus, and M. Chertkov, "Robust broadcast-communication control of electric vehicle charging," in *1st IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 203–207.

[41] B. McMillin, R. Akella, D. Ditch, G. Heydt, Z. Zhang, and M.-Y. Chow, "Architecture of a smart microgrid distributed operating system," in *IEEE/PES Power Syst. Conf. Expo. (PSCE)*, Phoenix, AZ, USA, 20-23 Mar. 2011, pp. 1–5.

[42] R. Roche, B. Blunier, A. Miraoui, V. Hilaire, and A. Koukam, "Multi-agent systems for grid energy management: A short review," in *IEEE 36th Annual Conf. Ind. Electron. Soc. (IECON)*, Glendale, AZ, USA, 7-10 Nov. 2010, pp. 3341–3346.

[43] C. Colson and M. Nehrir, "Agent-based power management of microgrids including renewable energy power generation," in *IEEE Power Energy Soc. General Meeting*, Detroit, MI, USA, 24-28 July 2011, pp. 1–3.

[44] H. E. Z. Farag, E. F. El-Saadany, and R. Seethapathy, "A two ways communication-based distributed control for voltage regulation in smart distribution feeders," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 271–281, Mar. 2012.

[45] P. Nguyen, W. Kling, G. Georgiadis, M. Papatriantafilou, L. A. Tuan, and L. Bertling, "Distributed routing algorithms to manage power flow in agent-based active distribution network," in *IEEE PES Innovative Smart Grid Tech. Conf. Europe (ISGT Europe)*, Gothenburg, Sweden, 11-13 Oct. 2010, pp. 1–7.

[46] L. Ochoa, C. Dent, and G. Harrison, "Distribution network capacity assessment: Variable DG and active networks," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 87–95, Feb. 2010.

[47] Q. Yang, J. Barria, and T. Green, "Communication infrastructures for distributed control of power distribution networks," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 316–327, May 2011.

[48] K. Nara, S. Ishizu, and Y. Mishima, "Voltage control availability of distributed generators in power distribution system," in *IEEE Russia Power Tech.*, St. Petersburg, Russia, 27-30 June 2005, pp. 1–6.

[49] H. Kobayashi and H. Hatta, "Reactive power control method between DG using ICT for proper voltage control of utility distribution system," in *IEEE Power Energy Soc. General Meeting*, Detroit, MI, USA, 24-28 July 2011, pp. 1–6.

[50] M. Mahmud, M. Hossain, H. Pota, and A. Nasiruzzaman, "Voltage control of distribution networks with distributed generation using reactive power compensation," in *37th Annual Conf. IEEE Ind. Electron. Soc. (IECON)*, Melbourne, Australia, 7-10 Nov. 2011, pp. 985–990.

[51] H. Hatta, S. Uemura, and H. Kobayashi, "Cooperative control of distribution system with customer equipments to reduce reverse power flow from distributed generation," in *IEEE Power Energy Soc. General Meeting*, Minneapolis, MN, USA, 25-29 July 2010, pp. 1–6.

[52] A. Ghosh, R. Majumder, G. Ledwich, and F. Zare, "Power quality enhanced operation and control of a microgrid based custom power park," in *IEEE Int'l Conf. Control and Autom. (ICCA)*, Christchurch, New Zealand, 9-11 Dec. 2009, pp. 1669–1674.

[53] R. Majumder, G. Bag, and K.-H. Kim, "Power sharing and control in distributed generation with wireless sensor networks," *IEEE Trans. Smart Grid*, vol. 3, no. 2, pp. 618–634, June 2012.

[54] M. Masoum, P. Moses, and K. Smedley, "Distribution transformer losses and performance in smart grids with residential plug-in electric vehicles," in *IEEE PES Innovative Smart Grid Technol. (ISGT)*, Anaheim, CA, USA, 17-19 Jan. 2011, pp. 1–7.

[55] R. Dugan and M. McGranaghan, "Sim city," *IEEE Power Energy Mag.*, vol. 9, no. 5, pp. 74–81, Sept.-Oct. 2011.

[56] S. Zhao and D. Raychaudhuri, "Scalability and performance evaluation of hierarchical hybrid wireless networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 5, pp. 1536–1549, Oct. 2009.

[57] J. Bergmann, C. Glomb, J. Götz, J. Heuer, R. Kuntschke, and M. Winter, "Scalability of smart grid protocols: Protocols and their simulative evaluation for massively distributed DERs," in *1st IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 131–136.

[58] J. Zhou, R. Hu, and Y. Qian, "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1632–1642, 2012.

[59] A. Sen, P. Ghosh, V. Vittal, and B. Yang, "A new min-cut problem with application to electric power network partitioning," *European Trans. Electr. Power*, vol. 19, no. 6, pp. 778–797, Sept. 2009.

[60] G. Ezhilarasi and K. Swarup, "Distributed load flow using partitioning and equivalencing of power networks," in *Proc. 16th National Power Syst. Conf.*, Hyderabad, India, 15-17 Dec. 2010, pp. 335–340.

[61] G. Karypis and V. Kumar, "A fast and high quality multilevel scheme for partitioning irregular graphs," *SIAM J. Sci. Comput.*, vol. 20, pp. 359–392, Dec. 1998.

[62] M. Shahraeini, M. Javidi, and M. Ghazizadeh, "Comparison between communication infrastructures of centralized and decentralized wide area measurement systems," *IEEE Trans. Smart Grid*, vol. 2, no. 1, pp. 206–211, Mar. 2011.

[63] M. Li, P. Luh, E. Litvinov, and P. Zhang, "Analysis of a partially decentralized framework for operating future power systems," in *IEEE Power Energy Soc. General Meeting*, Detroit, MI, USA, 24-28 July 2011, pp. 1–6.

[64] L. Kocarev and V. In, "Network science: A new paradigm shift," *IEEE Netw.*, vol. 24, no. 6, pp. 6–9, Nov.-Dec. 2010.

[65] Z. Wang, A. Scaglione, and R. Thomas, "Generating statistically correct random topologies for testing smart grid communication and control networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 28–39, June 2010.

[66] P. Hines, S. Blumsack, E. Cotilla Sanchez, and C. Barrows, "The topological and electrical structure of power grids," in *Proc. 43rd Hawaii Int'l Conf. Syst. Sci. (HICSS)*, Koloa, HI, USA, 5-8 Jan. 2010, pp. 1–10.

[67] (2011, Mar.) Volt and var control and optimisation. Smart Distribution Wiki. [Online]. Available: http://wiki.powerdistributionresearch.com/index.php?title=Volt_and_Var_Control_and_Optimisation

[68] F. Bouhafs, M. Mackay, and M. Merabti, "Links to the future: Communication requirements and challenges in the smart grid," *IEEE Power Energy Mag.*, vol. 10, no. 1, pp. 24–32, Jan.-Feb. 2012.

[69] M.-C. Alvarez-Hérault, D. Picault, R. Caire, B. Raison, N. HadjSaid, and W. Bienia, "A novel hybrid network architecture to increase DG insertion in electrical distribution systems," *IEEE Trans. Power Syst.*, vol. 26, no. 2, pp. 905–914, May 2011.

[70] U. Madawala and D. Thrimawithana, "A two-way inductive power interface for single loads," in *IEEE Int'l Conf. Ind. Technol. (ICIT)*, Valparaiso, Chile, 14-17 Mar. 2010, pp. 673–678.

[71] U. Madawala, M. Neath, and D. Thrimawithana, "A power-frequency controller for bi-directional inductive power transfer systems," *IEEE Trans. Ind. Electron.*, vol. 60, no. 1, pp. 310–317, Jan. 2013.

[72] Z. Fadlullah, M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 60–65, Apr. 2011.

[73] M. Erol-Kantarci, B. Kantarci, and H. Mouftah, "Reliable overlay topology design for the smart microgrid network," *IEEE Netw.*, vol. 25, no. 5, pp. 38–43, Sept.-Oct. 2011.

[74] W. Saad, Z. Han, and H. Poor, "Coalitional game theory for cooperative micro-grid distribution networks," in *IEEE Int'l Conf. Commun. Workshops (ICC)*, Kyoto, Japan, 5-9 June 2011, pp. 1–5.

[75] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: visions and potentials for the smart grid," *IEEE Netw.*, vol. 26, no. 3, pp. 6–13, May-June 2012.

[76] R. Deng, S. Maharjan, X. Cao, J. Chen, Y. Zhang, and S. Gjessing, "Sensing-delay tradeoff for communication in cognitive radio enabled smart grid," in *2nd IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, 17-20 Oct. 2011, pp. 155–160.

[77] H. Li and W. Zhang, "QoS routing in smart grid," in *IEEE Global Telecommun. Conf. (GLOBECOM)*, Miami, FL, USA, 6-10 Dec. 2010, pp. 1–6.

[78] D. Niyato, P. Wang, Z. Han, and E. Hossain, "Impact of packet loss on power demand estimation and power supply cost in smart grid," in *IEEE Wireless Commun. Netw. Conf. (WCNC)*, Quintana-Roo, Mexico, 28-31 Mar. 2011, pp. 2024–2029.

[79] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[80] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[81] M. Kim, "A survey on guaranteeing availability in smart grid communications," in *14th Int'l Conf. Advanced Commun. Technol. (ICACT)*, PyeongChang, South Korea, 19-22 Feb. 2012, pp. 314–317.

[82] Y. Mo, T.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[83] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[84] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," in *10th Int'l Conf. Envir. Electr. Eng. (EEEIC)*, Rome, Italy, 8-11 May 2011, pp. 1–4.

[85] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of cyber-security issues on smart grid," in *2nd IEEE PES Int'l Conf. Exhibition Innovative Smart Grid Technol. (ISGT Europe)*, Manchester, UK, 5-7 Dec. 2011, pp. 1–7.

[86] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[87] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[88] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, Aug. 2012.

[89] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *1st IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 350–355.

[90] C. Neuman and K. Tan, "Mediating cyber and physical threat propagation in secure smart grid architectures," in *2nd IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, 17-20 Oct. 2011, pp. 238–243.

[91] (2012, May) Utility-scale smart meter deployments, plans, and proposals. Institute for Electric Efficiency. [Online]. Available: http://www.edisonfoundation.net/iee/Documents/IEE_SmartMeterRollouts_0512.pdf

[92] L. Enbysk. (2013, Jan.) Energy theft: From bad to worse (and what some utilities are doing about it). Smart Grid News. [Online]. Available: http://www.smartgridnews.com/

[93] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and R. C. Green, "High performance computing for detection of electricity theft," *Int'l J. Elect. Power Energy Syst.*, vol. 47, pp. 21–30, 2013.

[94] (2012) nCircle 2012 smart grid cyber security survey. nCircle Information Risk & Security Performance Management. [Online]. Available: http://www.ncircle.com/index.php?s=resources_surveys_Survey-SmartGrid-2012

[95] M. Costache, V. Tudor, M. Almgren, M. Papatriantafilou, and C. Saunders, "Remote control of smart meters: Friend or foe?" in *7th European Conf. Comput. Netw. Defense (EC2ND)*, Gothenburg, Sweden, 6-7 Sept. 2011, pp. 49–56.

[96] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Sec. (CCS)*, Chicago, IL, USA, 9-13 Nov. 2009, pp. 21–32.

[97] Z. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," *IEEE Netw.*, vol. 25, no. 5, pp. 50–55, Sept.-Oct. 2011.

[98] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 809–818, Dec. 2011.

[99] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[100] J. Valenzuela, J. Wang, and N. Bissinger, "Real-time intrusion detection in power system operations," *IEEE Trans. Power Syst.*, press.

[101] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye, "Detecting false data injection attacks on dc state estimation," in *Proc. 1st Workshop Secure Control Syst. (SCS)*, Stockholm, Sweden, 12 Apr. 2010, pp. 232–237.

[102] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[103] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures," in *2nd IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Brussels, Belgium, 17-20 Oct. 2011, pp. 232–237.

[104] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, Dec. 2011.

[105] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Trans. Power Syst.*, press.

[106] Z. Qin, Q. Li, and M. Chuah, "Defending against unidentifiable attacks in electric power grids," *IEEE Trans Parallel Distrib. Syst.*, press.

[107] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *3rd IEEE/ACM Int'l Conf. Cyber-Physical Syst. (ICCPS)*, Beijing, China, 17-19 Apr. 2012, pp. 183–192.

[108] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, June 2011.

[109] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in *IEEE GLOBECOM Workshops*, Houston, Texas, USA, 5 Dec. 2011, pp. 1162–1167.

[110] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, 2012.

[111] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *1st IEEE Int'l Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 226–231.

[112] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[113] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 27–33, Jan. 2013.

[114] Y. Zhang, W. Chen, and J. Black, "Anomaly detection in premise energy consumption data," in *IEEE Power Energy Soc. General Meeting*, Detroit, Michigan, USA, 24-28 July 2011, pp. 1–8.

[115] S. Salinas, M. Li, and P. Li, "Privacy-preserving energy theft detection in smart grids," in *9th Annual IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw. (SECON)*, Seoul, Korea, 18-21 June 2012, pp. 605–613.

[116] Z. Xiao, Y. Xiao, and D.-C. Du, "Exploring malicious meter inspection in neighborhood area smart grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 214–226, Mar. 2013.

[117] A. Monticelli, *State Stimation in Electric Power Systems: A Generalized Approach*, ser. Int'l Series in Eng. Comput. Sci. Norwell, Massachusetts: Kluwer Academic, 1999.

[118] S. Cui, Z. Han, S. Kar, T. Kim, H. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sept. 2012.

[119] N. Saputro and K. Akkaya, "Performance evaluation of smart grid data aggregation via homomorphic encryption," in *IEEE Wireless Commun. Netw. Conf. (WCNC)*, Paris, France, 1-4 Apr. 2012, pp. 2945–2950.

[120] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, press.

[121] Y. Wang, W. Lin, and T. Zhang, "Study on security of wireless sensor networks in smart grid," in *Int'l Conf. Power Syst. Technol. (POWERCON)*, Zhejiang, China, 24-28 Oct. 2010, pp. 1–7.

[122] C. de Morsella. (2011, 14 May) Wind turbines may be shut down in pacific northwest. Green Economy Post. [Online]. Available: http://greeneconomypost.com/wind-turbines-shut-pacific-northwest-15566.htm

[123] (1996, June) Available transfer capability definitions and determination. North American Electric Reliability Council. [Online]. Available: http://www.westgov.org/wieb/wind/06-96NERCatc.pdf

[124] C. Barbulescu, S. Kilyeni, D. Cristian, and D. Jigoria-Oprea, "Congestion management using open power market environment electricity trading," in *45th Int'l Univ. Power Eng. Conf. (UPEC)*, Cardiff, Wales, UK, 31 Aug.-3 Sept. 2010, pp. 1–6.

[125] M. Ramezani, M.-R. Haghifam, C. Singh, H. Seifi, and M. Moghaddam, "Determination of capacity benefit margin in multiarea power systems using particle swarm optimization," *IEEE Trans. Power Syst.*, vol. 24, no. 2, pp. 631–641, May 2009.

[126] M. M. bin Othman, A. Mohamed, and A. Hussain, "Determination of transmission reliability margin using parametric bootstrap technique," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1689–1700, Nov. 2008.

[127] F. Jiang, "Investigation of solar energy for photovoltaic application in singapore," in *Int'l Power Eng. Conf. (IPEC)*, Singapore, 3-6 Dec. 2007, pp. 86–89.

[128] Solar electricity basics. Homepower. [Online]. Available: http://homepower.com/basics/solar/#SolarElectricPanels

[129] A. Pandey, N. Dasgupta, and A. Mukerjee, "High-performance algorithms for drift avoidance and fast tracking in solar MPPT system," *IEEE Trans. Energy Convers.*, vol. 23, no. 2, pp. 681–689, June 2008.

[130] AC disconnect switches for inverter-based generation. Pacific Gas and Electric Company. [Online]. Available: http://www.pge.com/b2b/newgenerator/acdisconnectswitches/

[131] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11™, 2007.

[132] *Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)*, IEEE Std. 802.15.4, 2006.

[133] Smart e-meter: AMR/AMI. Texas Instruments. [Online]. Available: http://focus.ti.com/docs/solution/folders/print/407.html

[134] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems*, 1st ed. Berlin, Germany: Springer, 2004.

[135] E. Lloyd and G. Xue, "Relay node placement in wireless sensor networks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 134–138, Jan. 2007.

[136] J. L. Gross and J. Yellen, *Handbook of Graph Theory*. Boca Raton, Florida: CRC Press, 2003.

[137] D. P. Bertsekas and R. Gallager, *Data Networks*, 2nd ed. Englewood Cliffs, New Jersey: Prentice Hall, 1992.

[138] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling, "Usefulness of DC power flow for active power flow analysis with flow controlling devices," in *8th IEEE Int'l Conf. AC DC Power Transm. (ACDC)*, Savoy Place, London, UK, 28-31 Mar. 2006, pp. 58–62.

[139] K. Kurohane, T. Senjyu, A. Yona, N. Urasaki, T. Goya, and T. Funabashi, "A hybrid smart AC/DC power system," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 199–204, Sept. 2010.

[140] R. Sedgewick and K. Wayne, *Algorithms*. Westford, Massachusetts: Pearson Education, 2011.

[141] D. Pearson, "A polynomial-time algorithm for the change-making problem," Department of Computer Science, Cornell University, Tech. Rep., 1994.

[142] F. McLoughlin, A. Duffy, and M. Conlon, "Evaluation of time series techniques to characterise domestic electricity demand," *Energy*, vol. 50, pp. 120–130, 2013.

[143] N. Ansari and E. Hou, *Computational intelligence for optimization*. Boston, Massachusetts: Kluwer Academic, 1997.

[144] C.-H. Lo and N. Ansari, "The progressive smart grid system from both power and communications aspects," *IEEE Commun. Surveys Tutorials*, vol. 14, no. 3, pp. 799–821, 2012.

[145] ——, "Chapter 4: IEEE 802.15.4-based wireless sensor network design for smart grid communications," in *Handbook on Green Inf. and Commun. Syst.*, M. S. Obaidat, A. Anpalagan, and I. Woungang, Eds. Academic Press, 2013.